OPERAZIONE SAFETY-NET

MIGLIORI PRATICHE PER COMBATTERE LE MINACCE ONLINE, MOBILI E TELEFONICHE

MESSAGING, MALWARE AND MOBILE ANTI-ABUSE WORKING GROUP

&

LONDON ACTION PLAN

1011101011100EVALUATE0100100110RESPOND1010010 JUNE 1, 2015 1010010DEVELOP1001100DETECT0100COLLABORATE

CAUCE

LONDON ACTION PLAN
INTERNATIONAL CYBERSECURITY ENFORCEMENT NETWORK

M3AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP

This report refers to some commercial products as possible solutions to various electronic threats. Inclusion of these products does not constitute an endorsement by organizations that have endorsed or contributed to this report.

PREAMBOLO

Nel mese di ottobre del 2011, i membri del "London Action Plan" (LAP) e del "Messaging, Malware and Mobile Anti-Abuse Working Group" (M^3AAWG) hanno fatto una presentazione al Comitato OCSE sulla politica dei consumatori (CCP) a proposito della prospettiva corrente sulle raccomandazioni anti-spam dell'OCSE su come affrontare le future minacce online.

Nel corso della riunione, un delegato canadese del LAP ha osservato che, mentre l'attuale serie di raccomandazioni anti-spam dell'OCSE sono state di grande successo nel mobilitare il settore e i governi ad agire per affrontare lo spam, potrebbe essere utile una maggiore comprensione della nuova e più sofisticata generazione di minacce online. Sulla base di un follow-up iniziale con il delegato canadese del CCP e il presidente del CCP, Il Coordinamento Nazionale Anti-Spam ha preparato ad "Industry Canada" uno schema per una relazione da redigere da parte di membri volontari del M^3AAWG e del LAP. Lo schema è stato condiviso e concordato dai membri del M^3AAWG e del LAP ed è stato valutato dal Segretariato CPP.

Il 6 giugno 2012, i membri di LAP e del M^3AAWG si sono incontrati a Berlino per iniziare il processo di sviluppo del rapporto che è stato pubblicato nel mese di ottobre dello stesso anno. Tre anni dopo, questo rapporto è stato aggiornato per riflettere lo scenario in evoluzione e le nuove forme tramite le quali i criminali informatici sono in grado di trarre profitto ed evitare il rilevamento.

Il rapporto originale è stato diviso in quattro sezioni principali:

i) Malware and Botnets,
ii) ISP and DNS,
iii) Phishing e Ingegneria Sociale, e
iv) Minacce nel Mobile.

Questa seconda versione del rapporto include gli aggiornamenti delle quattro sezioni originali e copre nuove aree tra cui il Voice over Internet Protocol (VoIP), la frode nella telefonia vocale, la falsificazione del Caller ID, i problemi di abuso dei i servizi di Hosting e Cloud e le molestie on-line.

Il processo di aggiornamento di queste migliori pratiche ha comportato un invito inviato al M^3AAWG e ai membri del LAP per la ricerca di collaboratori per il report. Gli esperti del settore sono stati scelti come capi di sezione e questi capi hanno anche raccolto input e contributi di esperti esterni al M^3AAWG e ai membri del LAP. Un elenco di contributori si trova alla fine di questo rapporto.

Il M^3AAWG, il LAP e il CAUCE (Coalition Against Unsolicited Commercial Email) hanno ufficialmente approvato questo rapporto. Inoltre, i contributori apprezzerebbero un feedback sulla relazione dal CCP OCSE, dal "Working Party on Information Security and Privacy" (WPISP) dalla "Committee on Information, Communications and Computer Policy" (ICCP). Se appropriato, i contributori avrebbero anche piacere ad accogliere un'ulteriore collaborazione su questa iniziativa in altre sedi.

CONTENUTI

SINTESI

Questo rapporto fornisce ai lettori una descrizione in linguaggio semplice delle minacce che affrontano le imprese, i fornitori di rete ed i consumatori nel contesto delle minacce online e mobili. Come molti di noi sono consapevoli, Internet e le tecnologie mobili sono stati fattori chiave dell'economia globale nel corso degli ultimi venti anni. Queste tecnologie impattano, giorno per giorno, quasi ogni aspetto delle nostre vite e sono anche stati incorporate in quasi ogni modello di business e nelle catene di fornitura. Nel momento in cui i nostri computer portatili, gli smartphone e i tablet sono diventati integrati nella nostra vita personale e lavorativa, la nostra dipendenza da questi dispositivi è cresciuta. Usiamo i dispositivi per contattare parenti e amici, negozi e banche on-line, per entrare in contatto con le agenzie civiche e i funzionari preposti, per interagire con i colleghi di lavoro e i partner, per razionalizzare le catene di fornitura e fornire prodotti just-in-time dagli impianti di produzione ai punti vendita al dettaglio.

Con la crescente dipendenza dei consumatori e degli affari e la rapida migrazione delle transazioni commerciali verso le piattaforme online e mobili arrivano le minacce da criminali informatici. I criminali informatici traggono profitto dall'invio di spam, dal phishing, dall'inserimento di malware sui siti web, dalla diffusione botnet, dal reindirizzamento del traffico Internet verso siti web malevoli, dal dirottamento di servizi cloud e hosting e dall'inserimento di spyware sui computer e sui dispositivi mobili.

L'impatto economico di questi attacchi senza fine non è facilmente misurabile, sia per paese o su scala globale, così come le perdite derivanti dalla criminalità informatica sono spesso dichiarate poco o per nulla dalle vittime, dalle istituzioni finanziarie che coprono le spese della perdita, o da parte delle imprese che sostengono tutto, dai costi di difesa e di ripristino del servizio ai tempi di inattività a causa di attacchi.

L'obiettivo principale di questa relazione non è solo di studiare la minaccia per gli ambienti on-line, mobili e VoIP che minacciano i consumatori, imprese e governi ogni giorno ma, ancora più importante, di suggerire le migliori pratiche per il settore e per i governi su come affrontare queste minacce. Il punto centrale della relazione si divide su cinque aree principali:

MALWARE E BOTNET

Malware e botnet sono tra le minacce più gravi per l'economia di Internet. Il software dannoso o "malware" è stato creato o utilizzato dai criminali per compromettere le attività dei computer, raccogliere informazioni sensibili o accedere ai sistemi informatici privati. Le botnet sono gruppi di macchine infettate da malware che comunicano (spesso attraverso una complessa rete di computer infetti) per coordinare la loro attività e per raccogliere le informazioni prodotte dalle singole infezioni malware. Le botnet sfruttano le impressionanti capacità di potenza di calcolo e larghezza di banda che arrivano dall'essere in grado di controllare più di un milione di computer.

I criminali continuano a cambiare o "mutare" il loro di malware al fine di evitare il rilevamento e la bonifica. Di conseguenza, la maggior parte di software Anti-Virus (A/V) ha difficoltà ad identificare le minacce emergenti e recenti. Una quota crescente di malware può rilevare quando viene "monitorato" mentre è in esecuzione, magari da un ricercatore anti-virus, e altera le caratteristiche per rendere impossibile agli esperti di malware rilevare o analizzare le sue funzioni. Alcuni malware possono addirittura rispondere ai tentativi di monitoraggio e analisi contro-attaccando con un attacco di tipo “Denial of Service” distribuito (DDoS).

Per questo motivo sta diventando sempre più difficile per la comunità della sicurezza online stare al passo con l’ambiente delle minacce malaware.

Phishing e Ingegneria Sociale

Il termine Phishing si riferisce alle tecniche che vengono utilizzate da malintenzionati per ingannare la vittima a rivelare informazioni sensibili personali, aziendali o finanziarie.

Il Phishing è in costante aumento per quanto riguarda la frequenza, la raffinatezza e i danni, da quando è emerso come una minaccia a metà degli anni 1990, e non sta mostrando segni di cedimento. In effetti, il phishing è in aumento dal 2011, quasi un quarto dei destinatari aprono e-mail di phishing e oltre il dieci per cento cliccano su allegati dannosi. Inoltre, il tipo di dati richiesti attraverso il phishing è diventato sempre più prezioso, evolvendo da semplice accesso alle e-mail e ai singoli conti bancari dei consumatori che sostengono le perdite di migliaia di dollari, verso obiettivi considerati, al giorno d’oggi, di alto valore.

Gli obiettivi di alto valore, vale a dire gli account aziendali contenenti segreti commerciali o quelli che consentono privilegi speciali a conti bancari e finanziari, sono stati ripetutamente e frequentemente sfruttati, producendo, con un singolo evento, catastrofiche violazioni di proprietà intellettuale e perdite finanziarie di centinaia di milioni di dollari, con un numero imprecisato di tali eventi che si verificano ogni anno.

Anche se il phishing non è nuovo, l’intensificazione nel numero, negli obiettivi e nella sofisticazione degli attacchi negli ultimi anni rappresenta una minaccia sempre crescente per aziende, governi e consumatori ed erode anche la fiducia generale nell'economia digitale. Le difese devono essere coordinate per sfruttare soluzioni condivise, aperte e trasparenti per massimizzare l'efficacia, ridurre al minimo i costi e aumentare la fiducia del pubblico.

Sfruttamento delle Vulnerabilità dell’ Internet Protocol e del Domain Name System

Una varietà di attività illegali sfruttano le vulnerabilità associate agli indirizzi Internet Protocol (IP) e al Domain Name System (DNS). Gli exploit più gravi del DNS sono rappresentati dai “resolver exploit” o “cache poisoning”, dove i malintenzionati introducono dati alterati per reindirizzare il traffico Internet verso versioni falsificate dei siti web popolari.

Ogni computer su Internet ha un indirizzo IP, che viene utilizzato per identificare quel computer nello stesso modo in cui i telefoni sono identificati da numeri telefonici. Gli indirizzi IP tradizionali, conosciuti come indirizzi IPv4 (Internet Protocol versione 4), sono numeri binari a 32 bit, scritti come quattro numeri decimali, come ad esempio 64.57.183.103. La prima parte dell'indirizzo, in questo caso 64.57.183, spesso identifica la rete e il resto dell'indirizzo, in questo caso 103, il computer specifico ("host") sulla rete. La divisione tra la rete e l'host varia a seconda delle dimensioni della rete, quindi l'esempio di cui sopra è esclusivamente rappresentativo. Dal momento che gli indirizzi IP sono difficili per gli esseri umani da ricordare e sono legati a reti fisiche, il DNS è un database distribuito di nomi che consente alle persone di utilizzare nomi come www.google.com, piuttosto che l'indirizzo IP corrispondente 173.194.73.105.

Nonostante le sue enormi dimensioni, il DNS ottiene ottime prestazioni utilizzando un sistema di delega e le cache. Ossia diverse organizzazioni sono responsabili, ognuna per la loro parte, del sistema dei nomi di dominio e i siti finali ricordano i recenti risultati DNS che hanno ricevuto. Dal momento che non sarebbe pratico memorizzare tutti i nomi del DNS in un unico database, lo si è diviso in zone che sono memorizzate su server diversi, ma logicamente collegati tra loro in un immenso database distribuito e interoperabile.

Gli exploit degli IP e dei DNS causano un rischio elevato perché in molti casi i consumatori sono completamente ignari che sono stati reindirizzati su un sito fasullo invece di quello che effettivamente volevano visitare.

Minacce per Cellulari, VoIP, e Telefonia

Con l'avvento degli smartphone e dei mercati di applicazioni per dispositivi Android, Apple, Windows e Blackberry, l'ambiente e-commerce è cresciuto fino a includere i dispositivi mobili. Mentre i consumatori migrano le loro attività di e-commerce verso piattaforme mobili, i malintenzionati che cercano di trarre profitto e truffare sono stati pronti a seguire. Inoltre, l'ambiente mobile crea opportunità uniche per nuovi tipi di attacchi e minacce rivolte sia ai consumatori che alle imprese.

I dispositivi mobili offrono una maggiore funzionalità e facilità d'uso per i consumatori. Essi sono spesso portati dai singoli utenti, sono tipicamente mantenuti attivi, hanno spesso il GPS abilitato e in grado di rilevare la posizione. A causa di questo, i dispositivi mobili sono intrinsecamente più attraenti per gli attacchi dannosi.

Negli ultimi anni l'ambiente mobile ha visto un maggiore sviluppo di malware, le prime botnet mobili, un aumento di truffe con messaggi (SMS) a tariffa maggiorata ed exploit sofisticati che sono stati associati con il Jailbreaking (slegare un dispositivo da una fonte designata e affidabile di applicazioni software) dei dispositivi mobili.

Con la crescita degli abbonamenti mobili a banda larga, le minacce al Voice over Internet Protocol (VoIP) e alla telefonia sono in aumento. La frequenza e la gravità delle truffe di tipo “robocall” è in crescita e la nuova tecnologia che permette ai malintenzionati di nascondere o cambiare i loro numeri di telefono in uscita per ingannare gli incauti obiettivi rende queste frodi più efficaci. Dal momento in cui sempre più servizi di telefonia vanno in rete, gli attacchi di Denial of Service telefonico (TDOS) sono allo stesso modo in crescita in termini di dimensioni e frequenza. Questi tipi di attacchi possono essere devastanti quando prendono di mira i servizi essenziali in modo da rendere inutilizzabili i sistemi telefonici e far sì che le chiamate di individui legittimi che cercano di raggiungere, ad esempio, i vigili del fuoco o un'ambulanza non sono in grado di arrivare a destinazione.

I criminali informatici hanno una forte preferenza per operare in un ambiente transnazionale, complicando ulteriormente gli sforzi di applicazione. Ad esempio, un venditore illegale di pillole on-line che vive negli Stati Uniti potrebbe inviare spam pubblicizzando quei farmaci da un computer compromesso in Brasile, indirizzando i potenziali acquirenti verso un sito web con un nome di dominio russo, mentre fisicamente il sito è situato in Francia. I pagamenti con carta di credito degli ordini possono essere elaborati attraverso una banca in Azerbaijan, con gli ordini che vengono spediti da un sito situato in India, e i ricavi incanalati verso una banca di Cipro. I criminali sanno che, operando in questo modo, molti fattori complicano ogni indagine ufficiale sui loro crimini on-line e riducono la loro probabilità di essere scoperti. Questi fattori includono la mancanza di cooperazione, le differenze tra una giurisdizione all'altra e il costo delle indagini internazionali.

HOSTING & CLOUD

Hosting si riferisce ai fornitori di servizi che forniscono alle aziende accesso a siti web, ai file, alle reti interne (intranet), e forniscono l'accesso a Internet tramite diversi server interconnessi invece che con un server singolo o virtuale. “Host” sono le aziende che forniscono spazio su un server di proprietà o in locazione per l'utilizzo da parte dei clienti; essi possono anche fornire lo spazio dei data center e la connettività ad Internet. La maggior parte servizi di hosting di base sono servizi di hosting per i file di piccole dimensioni dei siti web. Molti fornitori di servizi Internet (ISP) offrono questo servizio gratuito agli abbonati. Questi host gestiscono gli ingranaggi che fanno funzionare Internet e, in termini di dimensioni, vanno dalle imprese individuali alle aziende di livello mondiale. Cloud Computing è la memorizzazione e l'utilizzo di dati e programmi su Internet invece di utilizzare il disco rigido del computer. La nuvola è solo una metafora per Internet. Risale ai tempi dei diagrammi di flusso e delle presentazioni che rappresenterebbero la gigantesca infrastruttura server-farm di Internet come nient'altro che una gonfia nuvola bianca.

Le minacce online e mobili che sfruttano risorse hosting e cloud sono in aumento e includono lo spam, il pubblicizzare siti web tramite spam (spamadvertising), il phishing, i siti web violati, il DDoS (Distributed Denial of Service), la scansione delle porte per le vulnerabilità sfruttabili, le pagine web deturpate, le violazioni dei copyright o dei marchi e il malware. Questo documento categorizza i tipi di hosting e delinea le aree di preoccupazione. Esso fornisce uno sguardo al corrente panorama delle minacce per quanto riguarda l’hosting e il cloud ed un breve sguardo ai metodi di risanamento utilizzati per affrontare tali criticità.

CONCLUSIONE

Al fine di salvaguardare Internet, e garantire la sua promessa ai cittadini del mondo, è essenziale che noi identifichiamo risposte efficienti ed efficaci per questa moltitudine di minacce. Questa relazione, presentata da un gruppo internazionale di esperti del settore e del governo, riassume le raccomandazioni circa le migliori pratiche per affrontare queste nuove e più sofisticate minacce online, mobili e di telefonia. La nostra speranza è che questo rapporto possa agevolare una effettiva e continuativa collaborazione tra questo gruppo e la comunità internazionale per affrontare queste minacce.

INTRODUZIONE: L'EVOLUZIONE DELLE MINACCE ONLINE

Dal 2006 la totalità di Internet e dell'economia mobile ha visto l'evoluzione delle minacce online e l'emergere di nuovi attacchi. Gli strumenti utilizzati per frodare e rubare le informazioni nell'ambiente online e in quello mobile oggi sono sempre più sofisticati, fornendo ai malintenzionati e ai truffatori una cassetta degli attrezzi estesa.

In questo contesto, come i tuoi genitori probabilmente hanno detto più di una volta, "un'oncia di prevenzione vale una libbra di cura". Questo rapporto non solo descrive l'ambiente delle minacce online, mobili e di telefonia in un modo che chiunque può capire, fornisce anche un elenco di strumenti da adottare, da parte dei governi e del settore, come migliori pratiche per prevenire che questi tipi di minacce si trasformino attacchi di successo.

Mentre gran parte di questa attività online illegale è neutralizzata prima che raggiunga gli utenti tipici finali per merito dei sistemi di filtraggio e delle tecniche di blocco attuali, lo spam rimane un veicolo importante, trasportando spesso carichi dannosi così come e-mail indesiderate e spesso dannose. Lo spam non è solo un fenomeno relativo all'e-mail. Si continua ad espandere in varie forme di nuovi mezzi di comunicazione. Ad esempio, lo spam attraverso la messaggistica mobile e il Voice over Internet Protocol (VoIP) è ormai comune, come lo sono i commenti di spam sui social media, blog e siti web, e tutto lo spam atto ad inquinare e degradare la qualità dei risultati di ricerca nei motori di ricerca on-line.

Nel settore dei domini (costituito principalmente dalla "Internet Corporation for Assigned Names e Numbers" (ICANN)), Registranti e Registri possono svolgere un ruolo determinante nell'ambito anti-abuso, in particolare, da quando nuovi protocolli Internet (ad esempio, IPv6) sono diventati prevalenti e un massiccio numero di nuovi domini di primo livello (TLD) è stato rilasciato. Tradizionalmente ci sono stati circa 24 domini di primo livello, come .com, .org, .net, .gov, più i domini di due lettere nazionali, come .ca per il Canada o .jp per il Giappone. Recentemente, l'ICANN ha introdotto oltre 500 nuovi domini di primo livello generici, tra cui .bike, .city e .clothing e ne ha centinaia di più in processo di attivazione.

Il nostro suggerimento è che siano i partecipanti dell'OCSE e delle altre organizzazioni internazionali a rafforzare la loro partecipazione nell'entità di coordinamento principale dello spazio dei domini, il Consiglio consultivo governativo dell'ICANN, lavorando per incoraggiare l'ICANN a raddoppiare gli sforzi nell'area della conformità contrattuale e nella supervisione dei registri e registranti.

Molto sforzo è stato profuso per abbattere le barriere e facilitare iniziative di cooperazione tra le aziende, le ONG, i governi, le autorità di regolamentazione e le forze dell'ordine. L'OCSE, il LAP, il M3AAWG e altre organizzazioni internazionali sono stati efficaci per lo sviluppo dell'esistente coordinamento pubblico-privato e la collaborazione tra più organizzazione. Ad esempio, il DNS Changer Working Group[i], e il Conficker Working Group[ii] sono combinazioni di esperti in materia, forze dell'ordine e rappresentanti del settore, che hanno avuto un notevole successo basato su un

modello di reciproca fiducia, mettendo da parte problemi di concorrenza. Questa collaborazione è stata un grande successo, e rimane vitale per i continui sforzi anti-abuso.

Tuttavia, continua ad esserci la necessità di una legislazione anti-spam e anti-abusi più forte, più comprensiva, tecnologicamente neutrale e di regimi normativi che facilitino la cooperazione transfrontaliera. Parte della soluzione potrebbe risiedere nel campo diplomatico, in particolare quando si tratta di consentire una più efficace attività di applicazione della legge transfrontaliera. Una educazione dell'utente finale sostanzialmente migliorata e la consapevolezza sono altri aspetti importanti di efficaci misure anti-abuso.

MALWARE E BOTNET

Il software dannoso o "malware" è stato creato e utilizzato dai criminali per compromettere le operazioni dei computer, raccogliere informazioni sensibili, o accedere ai sistemi informatici privati. Può apparire sotto diverse forme, dai programmi compilati agli script, o pezzi di codice inseriti in software altrimenti legittimi. "Malware" è un termine generico usato per riferirsi ad una varietà di forme di software ostile, invadenti o fastidiose. Il malware comprende generalmente virus informatici, worm, cavalli di Troia, dropper, spyware, adware, rootkit, spamware e altri programmi dannosi. Il malware è generalmente progettato per soddisfare una o più funzioni, che vanno dal facilitare l'introduzione di altri malware (ad esempio, dropper / downloader) alla raccolta di informazioni (per esempio, spyware). Altri tipi di malware possono specializzarsi nella compromissione dei computer, degli utenti e delle reti.

Le botnet sono gruppi di macchine infettate da malware simili che comunicano (spesso attraverso una complessa rete intermedia di computer infetti) per coordinare la loro attività e raccogliere le informazioni che le singole infezioni malware contengono. Le botnet sono più spesso chiamate con il nome del malware specifico che implementa e coordina la comunicazione, per esempio, Zeus e SpyEye. Tuttavia, ogni macchina in una botnet può contenere una varietà di componenti malware. Ad esempio, un nodo botnet Zeus può contenere il malware Zeus stesso (che gestisce la comunicazione delle botnet, il furto di informazioni e il download di altri malware), così come altre minacce, come spamware (come Cutwail) o componenti "di attacco" (come il malware Pushdo DDoS).

Le botnet possono essere grandi. Sono state rilevate botnet composte da più di un milione di macchine sotto il controllo di un singolo botmaster. Tuttavia, una botnet non deve essere necessariamente così grande per essere estremamente dannosa. Anche una botnet composta da 1.000 o 2.000 nodi (computer) può causare un enorme caos.

Agli inizi, il malware veniva spesso sviluppato da "hobbisti", persone abili nell'uso dei computer alla ricerca di una sfida o di divertimento. Da allora i criminali e la criminalità sempre più organizzata, hanno capito che si possono fare molti soldi con il malware. Un esempio di questo è il caso WinFixer, dove i criminali hanno cercato di spaventare le vittime portandole a fare pagamenti per la registrazione del software[iii]. Oggi, praticamente tutto il malware viene creato e utilizzato per scopi criminali. In misura minore, il malware può anche essere promosso dallo Stato e utilizzato dalle agenzie di intelligence per condurre azioni segrete contro i sistemi informatici di altri Stati, per spiare attivisti, giornalisti e dissidenti o può essere utilizzato da hacktivisti ed estremisti per scopi ideologicamente, politicamente o socialmente motivati.

Il malware è uno delle principali minacce per l'economia di Internet e viene utilizzato per condurre le seguenti attività:

- L'acquisizione di informazioni personali e aziendali tramite:
    - La cattura delle battiture dei tasti

    - La raccolta di login e password
    - La copia delle rubriche
    - Il furto di informazioni sensibili aziendali, di documentazione e/o di segreti commerciali o anche la cattura di informazioni sensibili governative o militari
    - La raccolta di informazioni bancarie e transazioni
- La facilitazione di devastanti attacchi DDoS per scopi nazionali, attivismo politico, o come preludio alla estorsione, tra molti altri scopi
- L'invio di spam via e-mail, SMS e altri metodi

I criminali stanno cambiando continuamente il malware per evitare il rilevamento e la cura. La maggior parte del software Anti-Virus (A/V) ha una storia poco felice quando si tratta di individuare le minacce attuali e recenti. Una quota crescente di malware può rilevare di essere "osservata" (forse da un ricercatore anti-virus) e modificare il suo comportamento per rendere più difficile ai ricercatori e agli analisti capirne il funzionamento. Alcuni malware cercheranno anche di scoraggiare il monitoraggio contrattaccando i ricercatori e gli analisti con un DDoS. A causa di questo, sta diventando sempre più difficile per la comunità della sicurezza online tenere il ritmo con cui l'ambiente delle minacce malware si sta evolvendo.

Lo Scenario Attuale della Minaccia del Malaware e delle botnet

Lo scenario non è cambiato ed è improbabile che lo faccia. La generale riluttanza dei governi, banche e aziende nel condividere dati privati o sensibili, ostacolata da barriere giuridiche e normative, reali o percepite, o da un timore di responsabilità, ha fatto sì che i produttori di malware continuino a mantenere il sopravvento quando si tratta di essere in grado di consegnare accuratamente il loro prodotto. Misurare in maniera precisa la portata del problema non è possibile dato che non ci sono parametri di misura universalmente accettati per le infezioni di malware, bot o botnet.

Per quanto riguarda il malaware veicolato dalle email, le email scritte male e poco plausibili sono state sostituite da nuove tecniche di phishing, discusse più avanti in questo rapporto. Anche se il volume di spam globale è diminuito negli ultimi anni, il social media è ormai sempre più utilizzato con tecniche come "clickjacking" o "likejacking", in cui un utente fa clic su un link al sito per guardare un video allettante e l'attaccante utilizza tale clic per pubblicare un commento a tutti gli amici di Facebook dell'utente, invitandoli a cliccare sullo stesso collegamento dannoso. Facebook ha in gran parte contrastato questo attacco, chiedendo all'utente di confermare un "like" prima di completare l'operazione se l'utente sta facendo un like di un dominio inaffidabile.

Per quanto riguarda il malware veicolato dai siti web, Symantec ha rilevato che nel 2013 gli attacchi basati sul Web sono aumentati del 23 per cento rispetto al 2012 e che 1 sito web su 8 aveva una vulnerabilità critica.[iv] Ciò indica che gli aggressori cercano di aggirare le contromisure di sicurezza utilizzando il Web per fornire il malware anziché allegarlo alle e-mail.

Le minacce contro i sistemi operativi Apple OSX e iOS, anche se relativamente poco numerose, rappresentano la propagazione di malware sul piattaforme che erano, fino ad oggi, relativamente prive di malware. I mezzi di attacco sono simili a quelli osservati per le piattaforme Windows e Android. Il fatto che molti strumenti di attacco sono diventati multi-piattaforma, facendo uso di exploit Java, per esempio, è di per sé un nuovo metodo di propagazione malware.

Lo Scenario Futuro della Minaccia del Malaware e delle botnet

Secondo il rapporto di McAfee "Previsioni della minacce[v]" il malware mobile sarà il motore della crescita sia in innovazione tecnologica che nel volume degli attacchi nel "mercato" complessivo del malware nel 2015. Sempre più spesso, si stanno anche verificando attacchi "ransomware" dannosi, alimentati dalla crescita della moneta virtuale. E' previsto che il rilascio di un numero crescente di applicazioni aziendali basate sul cloud possa creare nuove superfici d'attacco che saranno sfruttate da criminali informatici.

Infine, è difficile concepire nei prossimi anni molte altre minacce più significative rispetto a quelle poste dall' Internet of Things. Nel momento in cui miliardi di dispositivi saranno collegati a Internet ci sarà una crescente minaccia per l'infrastruttura di base costituita dai dispositivi senza patch o intrinsecamente insicuri. E' probabile che molti dispositivi collegati non riceveranno patch di sicurezza regolari; alcuni fornitori non considereranno la sicurezza come parte della loro responsabilità in quanto daranno priorità al rilascio del prodotto successivo e si concentreranno maggiormente sulle caratteristiche estetiche e pratiche.

I consumatori non potranno fare pressioni sui fornitori delle apparecchiature per le patch di sicurezza. Se, per esempio, un dispositivo funziona in modo soddisfacente come un frigorifero, lampadina o termostato, ma ha un problema di sicurezza con la sua cyber-funzionalità, i consumatori possono non essere motivati a sostituirlo unicamente per motivi di sicurezza. Di conseguenza, la lunga coda di dispositivi non sicuri continuerà a crescere.

Migliori Pratiche per Affrontare il Malaware

Mentre gran parte di ciò che è contenuto in questa sezione si concentra sull'educare gli individui e gli ISP va riconosciuto che affrontare il malware è un problema a livello di ecosistema che richiederà un approccio multi-sfaccettato e azioni da parte di una varietà di soggetti, non limitato agli ISP o all'educare gli utenti finali.

Per i governi e gli educatori, questa sezione si concentra sulla prevenzione, l'individuazione e la cura dei malware. Per i fornitori di servizi Internet, questa sezione si concentra sulla fornitura di consulenza per quanto riguarda ciò che un ISP può fare per aiutare le persone a rilevare il malware. La sezione si conclude con una discussione legale sul malware nelle aree legali e normative dei governi, così come nelle pratiche del settore.

MIGLIORI PRATICHE PER EDUCATORI E UTENTI

A) Migliori Pratiche: Prevenzione

Queste raccomandazioni si focalizzano su come gli individui possono evitare di venir infettati dal malaware.

1. **Scegli un Sistema Operativo Sicuro e Aggiornato**: Quando scegliete un sistema operativo (OS), cercatene uno che abbia la capacità comprovata di ridurre la vostra esposizione al malaware. Indipendentemente dal sistema che sceglierete siate sicuri di usare la più recente versione in produzione. I sistemi operativi moderni hanno sistemi di mitigazione integrati che possono aiutare a proteggere contro le falle usate dai malaware per compromettere un sistema.
2. **Installa le "patch" e Rimani Aggiornato**: Assicurati che i sistemi operativi e tutte le applicazioni, comprese le applicazioni helper (come Acrobat Reader, Flash Player, Java e QuickTime) siano totalmente "patchati" (cioè che tutti gli aggiornamenti siano stati scaricati appena disponibili) e aggiornati. La maggior parte dei problemi sfruttati dal malware hanno avuto patch disponibili da più di un anno. Per i sistemi che usano Microsoft Windows, Microsoft ha diversi download raccomandati disponibili[vi]. Secunia PSI[vii] è inoltre uno strumento noto che può aiutare a mantenere le applicazioni di terze parti aggiornate.
3. **Usa Solo Quello Che Ti Serve:** In generale è meglio scaricare o usare solo i programmi che sono necessari per completare il lavoro. Non scaricare programmi o file che non aggiungono funzionalità nuove o aggiuntive e cancella tutti i programmi che non sono utilizzati.
4. **Chiedi l'Aiuto degli Esperti**: Chiedi agli esperti qual è la migliore scelta per quello che ti serve (Gli "esperti" possono rispondere in diverse maniere, ma se sono le persone alle quali fai riferimento per avere supporto fre quello che ti dicono sarà quasi sempre la soluzione migliore nelle tue circostanze).
5. **Esegui un Programma Antivirus**: Anche se i prodotti antivirus non sono perfetti possono comunque aiutare. Per questo motivo scegline uno, usalo e mantienilo aggiornato scaricando gli aggiornamenti quando ti viene notificato di farlo. Pianifica una scansione completa del tuo sistema almeno una volta a settimana. Assicurati di scegliere un vero prodotto antivirus e cerca di non essere tratto in inganno nell'installare un prodotto falso che in realtà è esso stesso un malware! (E se il tuo programma antivirus non protegge anche contro lo spyware utilizza in aggiunta un programma anti-spyware).
6. **Usa un Firewall**: Anche se I firewall non sono infallibili un firewall hardware o software aggiungerà almeno un ulteriore livello di protezione.
7. **Utilizza Password Robuste**: Le password dovrebbero essere sufficientemente complesse da non essere indovinate o "crackate". Alcune persone fanno affidamento a password che sono lunghe almeno otto caratteri e includono un insieme di lettere maiuscole e minuscole, numeri e simboli speciali. Altri preferiscono un insieme da tre a cinque parole non correlate che sono facili da ricordare ma difficili da essere indovinate dai programmi per i computer. In entrambi i casi non usare sempre la stessa password su siti diversi. Per agevolare questo processo ci sono applicazioni per la gestione delle password.[viii]

8. **Fai Backup Regolari**: Se il tuo sistema viene infettato avere un backup pulito può essere tremendamente utile quando c'è bisogno di pulire e tornare online.
9. **Pulisci Tutti I File Temporanei Non Necessari**: Qualche malware può nascondere copie di se stesso tra i file temporanei e, anche se non ci sono file temporanei infetti, rimuovere questi file velocizzerà le scansioni del sistema e ridurrà la dimensione dei backup. Un programma comunemente usato per pulire i file temporanei in ambiente Windows è CCleaner.
10. **Non Eseguire Abitualmente Programmi Come Amministratore**: "Administrator," "root" e altri account che hanno permessi speciali devono essere usati solo quando stai facendo qualcosa che richiede tali privilegi (per esempio installazione intenzionale di nuovi programmi). Quando stai eseguendo attività ordinarie eseguili come un utente normale.
11. **Disabilita JavaScript (O usa NoScript)**: JavaScript (un linguaggio di scripting che non è associato a Java, nonostante il suo nome), può abilitare molte eccitanti applicazioni interattive; tuttavia è anche ampiamente abusato e utilizzato per far arrivare malware sui sistemi vulnerabili. Se non hai bisogno di JavaScript non abilitarlo nel tuo browser web.
12. **Blocca Nomi di Dominio Malevoli nel DNS**: Qualche malware si basa sull'abilità di tradurre correttamente nomi di dominio simbolici in numeri. Se tu blocchi la traduzione di tali nomi attraverso il tuo "domain name server" quel malware potrebbe non essere in grado di funzionare correttamente. OpenDNS è un esempio di società che offre questo tipo di record DNS filtrati dal malware
13. **Filtra/Disattiva l'E-mail Potenzialmente Pericolosa**: Il tuo amministratore della posta elettronica dovrebbe analizzare le email per allegati potenzialmente dannosi, link o altri contenuti che ti potrebbero essere inviati tramite e-mail. Un esempio di questi programmi è MIMEDefang.
14. **I File Scaricati Tramite Applicazioni P2P Sono Spesso Infettati**: Stai attento che molti dei file condivisi sulle reti peer-to-peer (P2P) possono essere intenzionalmente o accidentalmente infettati con malware.
15. **Considera che Ogni Chiavetta USB Possa Essere un "Tranello":** Se ti viene data una chiavetta USB o ne trovi una "persa" non collegarla mai al tuo computer. Potrebbe essere stata intenzionalmente infettata con malware e poi lasciata lì in modo che tu possa trovarla e possa installare malware sul tuo sistema.
16. **Non Usare Punti di Accesso Wi-Fi Non Conosciuti**: Qualche punto di accesso Wi-Fi aperto a tutti potrebbe intercettare tutto il traffico non criptato e, così facendo, può potenzialmente violare la tua privacy. L'utilizzo di Reti Private Virtuali (VPN) potrebbe offrire un certo grado di protezione. Assicurati che qualsiasi punto di accesso wireless che gestisci sia protetto con WPA2 (un protocollo e un certificato di sicurezza sviluppato dalla Wi-Fi Alliance per rendere sicure le reti di computer senza fili) per limitare l'accesso.

B) Migliori Pratiche: Identificazione
Queste raccomandazioni si focalizzano su come il malware viene riconosciuto quando i tentativi di prevenzione falliscono.

1. **Fai attenzione quando una scansione locale identifica qualcosa**: Una delle vie più comuni per identificare il malware è tramite una scansione antivirus. Un'altra opzione simile potrebbe essere quella di effettuare una scansione utilizzando, una tantum, uno strumento anti-malaware specifico come "cleanup only"[ix].
2. **Prendi nota quando il tuo sistema incomincia a comportarsi in maniera strana:** Un altro indicatore principale che c'è qualcosa di sbagliato è quando il sistema inizia a comportarsi in maniera "strana". Comportamenti strani possono includere un rallentamento o una interruzione improvvisa, la comparsa di finestre pop-up non desiderate (es.: false notifiche antivirus), il fatto che per accedere ad una pagina web sia richiesto prima di passare da un'altra oppure che ci siano alcuni siti non raggiungibili del tutto (in particolare se questi siti sono siti di aggiornamento o di materiale relativo alla sicurezza) e così via...
3. **Agisci quando il tuo ISP ti dice che il tuo sistema sta facendo attività non buone**: Per esempio il tuo ISP potrebbe farti sapere che il tuo sistema ha inviato dello spam oppure è stato coinvolto in un attacco verso un altro sistema su internet.

C) Migliori Pratiche: Rimedio
Queste raccomandazioni si focalizzano su come i sistemi infettati dal malware possono essere gestiti.

1. **Pulizia**: Questo approccio si basa sul fatto che l'utente (o qualcuno che agisce per suo conto) stia eseguendo uno o più prodotti antivirus sul sistema infetto nel tentativo di pulirlo (gli esperti potrebbero anche cancellare manualmente i file infetti in qualche caso). Questo processo potrebbe portare via tempo e, in definitiva, potrebbe o meno andare a buon fine. Anche dopo aver investito sforzi non indifferenti nel pulire un sistema infetto, l'infezione potrebbe rimanere o il sistema potrebbe essere instabile o inutilizzabile.
2. **Ripristino**: Se l'utente ha a disposizione un backup pulito, un'altra opzione potrebbe essere quella di ripristinare tale backup precedente. Questa opzione potrebbe comportare la perdita del lavoro effettuato dall'ultimo backup pulito a meno che tali file non siano stati preservati separatamente e possano essere ripristinati (si noti che, se tale operazione viene effettuata, occorre prestare molta attenzione nell'assicurarsi che ripristinare tali file non comporti una re-infezione). In generale, una strategia di ripristino funziona al meglio quando i backup sono frequenti ed è possibile scegliere tra più copie di backup.
3. **Reinstallazione Completa**: Con questa opzione il sistema viene riformattato, il sistema operativo e le applicazioni vengono re-installate da zero. Questo processo può richiedere molto tempo e spesso potrà essere vanificato dalla mancanza dei supporti originali (molti

produttori non offrono più una copia del sistema operativo su supporti fisici quando vendono nuovo hardware).

4. **Sostituire il Sistema:** Come ultima scelta, almeno una parte degli utenti potrebbe decidere semplicemente di rimpiazzare il loro sistema infetto piuttosto che pulirlo. Potrebbe anche essere l'unico modo per disinfestare in sicurezza una macchina compromessa. Questa opzione potrebbe essere interessante, per esempio, se il sistema infetto è vecchio, non è molto potente, se l'utente vuole cambiare sistema operativo o passare da un sistema desktop ad uno laptop. Nel gergo del settore questo tipo di azione si chiama "nuke & pave".

MIGLIORI PRATICHE PER L'INDUSTRIA E IL GOVERNO

A) Migliori Pratiche per Identificazione e Notifica (dagli ISP verso Utenti)

Molti ISP al giorno d'oggi avvisano i clienti se quest'ultimi sono stati infettati con il malware. Gli ISP possono usare una varietà di tecniche per notificare le infezioni individuali. Questa sezione offre una lista di attività che i diversi ISP dovrebbero intraprendere per informare gli utenti finali, tuttavia, questo non implica necessariamente che una specifica tecnica sia stata identificata come pratica migliore. Ci sono vantaggi e svantaggi associati ad ognuna di queste modalità di notifica. Alcuni esempi sono i seguenti:

1. **E-mail**: Quando un sistema infetto viene identificato l'ISP può informare l'utente per e-mail. Sfortunatamente spesso gli utenti non controllano mai l'email che l'ISP mette a loro disposizione e gli utenti potrebbero non fornire mai all'ISP l'indirizzo email che usano abitualmente. Gli utenti potrebbero inoltre essere diventati diffidenti delle e-mail di notifica come risultato dei diffusi attacchi di phishing e delle false richieste di assistenza tecnica che fanno credere erroneamente ai consumatori che il loro PC sia infettato con malware.
2. **Telefono**: L'ISP può anche avvisare l'utente tramite il telefono. Nel momento in cui si contattano i clienti è importante considerare che, mentre le chiamate automatizzate potrebbero essere considerate efficienti, gli utenti potrebbero essere sospettosi riguardo alle notifiche telefoniche come conseguenza degli attacchi di phishing telefonici. D'altro canto appropriate notifiche telefoniche potrebbero essere noiose e richiedere molto tempo se un grande numero di utenti infetti necessita di essere contattato.
3. **Messaggi di Testo**: Nei casi in cui l'ISP conosca il numero di telefono cellulare del cliente un'altra opzione potrebbe essere quella di inviare una notifica tramite SMS direttamente agli utenti.
4. **Posta Tradizionale (Cartacea)**: Un ISP può considerare di avvisare gli utenti attraverso la posta tradizionale, ad esempio tramite una inserzione nella bolletta mensile. Se l'ISP non manda già regolarmente posta al cliente il fatto di inviare notifiche postali *ad hoc* potrebbe essere costoso e di efficacia limitata, in particolare se l'utente è abituato a ignorare le comunicazioni postali convinto che siano solo messaggi promozionali.
5. **Tecnico a domicilio (Truck Roll)**: Nel caso in cui l'utente abbia sottoscritto un contratto di supporto a domicilio, un possibile approccio potrebbe essere quello di inviare un tecnico direttamente a casa del cliente (truck roll). Ovviamente il tecnico dovrà essere un grado di

fornire al cliente le opportune credenziali ed è opportuno constatare che questa potrebbe essere una opzione di notifica molto costosa.

6. **Notifiche Dirette (Web)**: Con questo approccio un ISP avvisa l'utente interponendo un messaggio di tipo "Interstizial" (sovrapposti alla pagina) quando l'utente cerca di visitare un normale sito web. Questo approccio può essere in qualche modo sconcertante per gli utenti ma è meno dirompente rispetto a qualche altro approccio, come quello denominato "giardino recintato" (si veda il punto seguente)
7. **Giardino Recintato (Walled-Garden)**: Se un ISP deve limitare immediatamente il danno che un utente infetto può causare, una opzione è quella di metterlo in quello che viene detto "giardino recintato" (walled-garden). Quando viene fatto, all'utente è permesso di accedere esclusivamente a siti selezionati allo scopo di curare l'infezione e mettere in sicurezza il suo sistema, e gli potrebbe essere consentito di continuare ad avere accesso VoIP esclusivamente per servizi di emergenza, ma tipicamente non potrà utilizzare la maggior parte delle risorse Internet. Deve essere sottolineato che questa strategia non vuole essere punitiva. I Giardini Recintati sono stati molto efficaci nel diminuire il numero di infezioni tra gli ISP più popolari e, di fatto, accelerare lo spostamento del malware e delle botnet verso i servizi di hosting.

Per informazioni aggiuntive si veda la Internet Engineering Task Force RFC6561 "Recommendations for the Remediation of Bots in ISP Networks".[x]

La notifica agli utenti finali non è limitata agli ISP. Altri soggetti rilevanti dell'ecosistema Internet che hanno un rapporto con gli utenti finali possono, e devono, effettuare le notifiche. Per esempio è stato ampiamente pubblicizzato che sia Google che Facebook hanno cercato di allertare gli utenti finali in merito a potenziali infezioni associate con il malware "DNS Changer"

B) Migliori Pratiche per la Sensibilizzazione

1. **Momento di insegnamento tramite confronto diretto**: Nello spiacevole evento quando il sistema di un cliente viene infettato, questo potrebbe essere un fondamentale momento di insegnamento quando le tecniche selezionate per scongiurare successive infezioni possono essere considerate particolarmente degne di nota.
2. **Sito web per la Sicurezza dei Clienti**: Il più semplice esempio per educare e sensibilizzare il cliente è probabilmente la creazione di un sito web per la sicurezza dei clienti che possa fornire consigli e l'accesso agli strumenti.
3. **Inserimenti nelle Bollette**: Se un ISP invia regolarmente informazioni ai clienti tramite posta tradizionale, questa potrebbe essere un'ulteriore opportunità per condividere raccomandazioni su come mettere in sicurezza i sistemi di quest'ultimi ed è qualcosa che può essere distribuito a tutti i clienti, anche a quello che non hanno ancora manifestato segni di infezione in quella data.
4. **Annunci tramite Servizi Pubblici (PSA)**: Un'altra opportunità per educare gli utenti sul malware potrebbe essere attraverso annunci tramite servizi pubblici tramite emittenti

televisive e radiofoniche. Per esempio, negli Stati Uniti la Campagna di Sensibilizzazione Nazionale sulla Sicurezza Informatica *STOP THINK CONNECT ("Fermati, Pensa, Connettiti")*, ha prodotto numerosi annunci pubblici messi in circolazione annualmente dal 2010.

5. **Materiali Promozionali**: Ci sono anche una moltitudine di materiali promozionali come tappetini mouse personalizzati, tazze, magliette, apribottiglie, penne o matite, o altri omaggi che possono aiutare a sensibilizzare sul malware e sulle minacce delle botnet.
6. **Concorsi**: Un'altra opportunità per condividere messaggi di sicurezza informatica potrebbe essere associate a concorsi, in particolare concorsi letterari per utenti in età scolare.
7. **Educazione Formale**: Un'altra componente vitale dell'educazione e della consapevolezza è quella di includere nelle scuole corsi di sicurezza informatica o di cittadinanza digitale. Affrontare la sicurezza informatica in generale, e in particolare malware e botnet, è un tema di sicurezza pubblica a lungo termine e, come altri temi di sicurezza pubblica, può essere affrontato al meglio definendo norme sociali che in molti casi potrebbero essere trasmesse meglio come parte della istruzione formale di una persona.

Data la rapida evoluzione del panorama delle minacce e della complessità dei malware e delle botnet, l'educazione e la consapevolezza possono essere solo parzialmente efficaci nel proteggere gli utenti finali. Gli sforzi legali, normativi, tecnici e del settore rimarranno la prima linea per affrontare il problema del malware e delle botnet. Tuttavia, una educazione di base e la consapevolezza delle minacce presenti su internet rimangono ingredienti necessari per proteggere gli utenti finali.

Il settore, le associazioni e i governi devono sviluppare e promuovere programmi di comunicazione finalizzati ad offrire agli utenti finali una conoscenza di base delle minacce e delle tecniche facilmente comprensibili su come proteggere se stessi.

Molte iniziative come queste esistono già e possono essere usate come modelli o semplicemente come una fonte per materiali informativi (si veda sotto). Diverse di queste risorse sono di ampio respiro piuttosto che strettamente focalizzate sulle problematiche collegate al malware e alle botnet.
Tuttavia, è meglio di solito fornire agli utenti finali un messaggio combinato sulla sicurezza su Internet piuttosto che numerosi consigli non coordinati. In altre parole, l'informazione dovrebbe essere concisa e coerente quando possibile

- National Cybersecurity Alliance - Keep A Clean Machine - http://www.stopthinkconnect.org/campaigns/keep-a-clean-machine (estratto della Campagna Nazionale Americana di Sensibilizzazione sulla Sicurezza Informatica "*STOP THINK CONNECT* " che è focalizzata su botnet e malware)
- Federal Bureau of Investigation (FBI): http://www.fbi.gov/scams-safetyhttp://www.fraud.org/tips/internet/general.htm
- Royal Canadian Mounted Police (RCMP): http://www.rcmp-grc.gc.ca/is-si/index-eng.htmhttp://www.rcmp-grc.gc.ca/is-si/index-eng.htm
- US National Initiative for Cybersecurity Education: http://csrc.nist.gov/nice/

- Federal Trade Commission (FTC): https://www.onguardonline.gov and http://www.consumer.ftc.gov/media/video-0103-hijacked-computer-what-do http://csrc.nist.gov/nice/

C) Migliori Pratiche Legali e Normative

Nel contesto forense applicato al malware, il testo "*Malware Forensics: Investigating and Analyzing Malicious Code*[xi]*"* suggerisce alcune migliori pratiche per le indagini di malware, tra cui:

- Definire e ridefinire obiettivi e traguardi investigativi fin da subito e frequentemente.
- Comprendere fin dall'inizio l'importanza di individuare prove a carico, a discarico, e mancanti.
- Progettare una metodologia per garantire che i passi investigativi non alterino, eliminino o creino prove, oppure possano mettere in allerta un sospettato compromettano le indagini in alcun modo.
- Creare e mantenere meticolosa documentazione passo-passo sulla analisi e sulla catena di custodia della documentazione.
- Non perdere mail il controllo delle prove.
- Definire, ridefinire e adattare questi principi guida nel corso di un'indagine, al fine di aiutare a chiarire e rendere più raggiungibili i traguardi e gli obiettivi di indagine.
- Pensare ai seguenti temi importanti fin dalle fasi iniziali:
    - La giurisdizione di una indagine richiede una certificazione o una licenza speciale per condurre una analisi digitale forense?
    - Quale autorità è preposta per indagare e quali sono i limiti di tale autorità?
    - Qual è la portata delle indagini autorizzate?
    - Come può essere evitata l'interferenza con i diritti della privacy dei relativi depositari di dati?

D) Migliori Pratiche per la Collaborazione guidata dal Settore e dal Governo

Le pratiche di sviluppo software sicuro rappresentano una delle migliori pratiche per limitare la diffusione di malware. La "Software Assurance Forum for Excellence in Code"[xii] (SAFECode) è una iniziativa globale guidata dal settore per individuare e promuovere le migliori pratiche per lo sviluppo e la distribuzione di software, hardware e servizi più sicuri e affidabili.

Il gruppo di lavoro numero 7 "Communications Security, Reliability and Interoperability Council (CSRIC)" della "US Federal Communications Commission" (FCC) ha rilasciato un codice di condotta volontario Anti-Bot per gli ISP e gli operatori di rete in data 22 marzo 2012, nell'ambito di una iniziativa di cooperazione tra industria e governo[xiii]. Il Codice si concentra sugli utenti Internet residenziali e comprende cinque aree di interesse per gli ISP: l'educazione, il rilevamento, la notifica, il rimedio, e la collaborazione. Per partecipare a questo codice, un ISP è tenuto ad

impegnarsi in almeno un'attività (vale a dire, agire in maniera significativa) in ciascuna delle seguenti aree generali:

- Educazione – aiutare ad aumentare l'educazione e la conoscenza degli utenti finali sulle problematiche legate alle botnet e come aiutare a prevenire le infezioni dei bot;
- Rilevamento – Identificare l'attività di botnet nella rete del provider, ottenere informazioni sull'attività della botnet nella rete del provider o mettere in condizione gli utenti finali di auto-determinare potenziali infezioni da bot sui propri dispositivi finali;
- Notifica – informare i clienti delle sospette infezioni da bot oppure metterli in condizione di determinare se loro possono essere stati infettati da un bot;
- Rimedio – fornire agli utenti finali informazioni su come possono rimediare alle infezioni dei bot o assisterli nel farlo;
- Collaborazione – condividere con gli altri ISP i suggerimenti e l'esperienza acquisita dalle attività SAFECode dei provider partecipanti.

Sistemi operativi e applicazioni correttamente configurate (rese sicure) possono anche ridurre il tasso di infezione da malware. L'agenzia della sicurezza degli Stati Uniti (NSA) fornisce una guida per la mesa in sicurezza dei computer da tutte le minacce, tra cui malware[xiv]. Nello stesso luogo sono disponibili ulteriori informazioni per router, sistemi wireless, switch, VoIP, server di database e applicazioni. Inoltre, ulteriori risorse per rendere più sicuro il sistema operativo e le applicazioni contro il software dannoso (compresi i dispositivi Android) possono essere trovate nella check list fornita dal "National Institute of Standards and Technology's (NIST)"[xv].

L'agenzia Koreana "Internet & Security" (KISA) fornisce gratis un servizio di protezione dagli attacchi DDoS ("DDoS Shelter") alle piccole imprese che non dispongono di strumenti adeguati per la protezione contro tale tipo di attacchi. Il DDoS Shelter filtra il traffico dannoso dell'attacco DDoS e lascia passare il traffico normale. Inoltre, KISA rileva IP potenzialmente zombie in un spamtrap e fa in modo che gli ISP nazionali posano agire in maniera appropriata contro questi IP sulle loro reti.

Ulteriori sforzi delle rispettive nazioni possono essere trovati ai seguenti siti web:

- International: https://code.google.com/p/evidenceontology
- Botfrei: https://www.botfrei.de/
- Switzerland Melani: http://www.melani.admin.ch
- Finland Ficora: http://www.ficora.fi/en
- EU AC/DC Project: http://www.acdc-project.eu/
- Canada: http://fightspam.gc.ca
- Australia: http://www.acma.gov.au/Citizen/Stay-protected/My-mobile-world/Dealing-with-mobile-spam/dealing-with-spam-i-acma

E) Migliori Pratiche per gli ISP

La minaccia del malware può essere minimizzata riducendo o eliminando i vettori di infezione. L' e-mail rappresenta ancora un metodo molto efficace con cui il malware si propaga. Per mitigare questo vettore, la maggior parte degli ISP, alberghi e punti di accesso liberi seguono la best practice di settore di bloccare la posta in uscita (porta 25) da qualsiasi computer sulla rete oltre ai loro server di posta. Questo impedisce ai computer infetti di propagare il malware tramite posta.

In Europa, alcuni ISP hanno fatto un ulteriore passo avanti. Gli utenti di queste reti di default hanno solo accesso al Web. Tutto il traffico per tutte le altre porte è negato. Per consentire agli utenti più esperti una maggiore flessibilità, questi fornitori di servizi Internet forniscono strumenti per consentire a specifici utenti autorizzati di utilizzare altre porte / protocolli e servizi.

In entrambi i casi, il monitoraggio del traffico bloccato può essere utilizzato come un primo indicatore della presenza di macchine infette da malware, nonché ostacolare la propagazione di malware e di comunicazioni di tipo "controllo e comando".

F) Migliori Pratiche per I Server e i Provider di Hosting

Attualmente, uno dei serbatoi più prevalenti di malware sono i server Web compromessi. Questi server diventano compromessi quando le patch di sicurezza aggiornate non vengono applicate sia per il sistema operativo che per le applicazioni di supporto e i framework Web, oppure a causa di password degli utenti non sicure. Queste compromissioni sono aggravate nelle piccole e medie imprese e in molti fornitori di hosting a causa del sottodimensionamento nel personale dedicato alla gestione degli abusi. L'automazione è utilizzata da alcuni per migliorare questi problemi e dovrebbe diventare una migliore pratica in tutto il mondo.

1. **Requisiti nei Termini di Servizio ai Clienti per Tempestivi Aggiornamenti di Sicurezza**: Tutti i clienti devono accettare di mantenere le attuali patch di sicurezza o consentire al fornitore di hosting di aggiornare i framework nelle loro directory.
2. **Mantenere le Patch di Sicurezza Aggiornate**: Tutte le patch di sicurezza dovrebbero essere aggiornate. Questo processo può essere manuale per ambienti molto ridotti oppure automatizzato attraverso script per i provider di hosting più grandi.
3. **Utilizzare Strumenti di Audit per Identificare gli Host**: Gli strumenti per eseguire il controllo a livello di server per identificare versioni non sicure del software devono essere eseguiti con frequenza almeno bi-settimanale e il software identificato dovrebbe essere aggiornato.
4. **Utilizzare Software di Sicurezza IT:** Strumenti (come Tripwire) dovrebbero essere utilizzati per monitorare l'integrità di ogni server.
5. **Eseguire Antivirus**: Eseguire il software antivirus frequentemente (se possibile due pacchetti diversi) per monitorare il contagio dei file di sistema modificabili.
6. **Considerare l'Utilizzo di Server nel Cloud:** Dal momento che i server nel cloud sono mantenuti in maniera professionale e utilizzati da molti clienti, essi tendono ad essere protetti meglio; d'altro canto, possono essere bersagli più ricchi per attacchi (ad es DDoS). Tuttavia, i server nel cloud devono essere considerati come una possibile alternativa per una maggiore sicurezza, tenendo in considerazione la reputazione del fornitore di cloud, le misure di

sicurezza messe in atto, e se i server sono stati oggetto di attacchi in passato. Maggiori informazioni sulle minacce per l'Hosting e per il Cloud e sulle migliori pratiche si possono trovare più avanti in questo rapporto.

PHISHING E INGEGNERIA SOCIALE

Il termine "Phishing" si riferisce alle tecniche che vengono utilizzate da malintenzionati per ingannare la vittima ad effettuare un'azione che non avrebbe altrimenti effettuato online, spesso per rivelare informazioni riservate quali i dati personali o finanziari. I truffatori si pongono come entità conosciute (amici o imprese), sfruttando le relazioni di fiducia esistenti per compromettere le loro vittime.

Il Phishing è in costante aumento in frequenza, sofisticatezza, ed entità dei danni da quando è emerso come una grave minaccia a metà degli anni 1990, e non mostra segni di cedimento. Il tipo di dati richiesti attraverso il phishing è diventato sempre più prezioso, evolvendo dal semplice accesso agli account di posta elettronica e ai conti bancari dei consumatori che hanno subito perdite individuali nell'ordine delle migliaia, agli obiettivi attuali di conti aziendali con privilegi speciali ("super-user") e le informazioni bancarie aziendali.

Questi attacchi possono portare a massicce violazioni dei dati dove le informazioni personali dei clienti vengono rubate in massa, la proprietà intellettuale di una società viene prelevata, oppure i dati e anche i sistemi fisici vengono distrutti. Ogni singolo evento può riguardare la proprietà intellettuale aziendale e causare perdite finanziarie fino a decine o addirittura centinaia di milioni di dollari, con un numero imprecisato di eventi che si verificano ogni anno.

Perché "Ph"?
Il termine phishing è derivato dal termine inglese "fishing" (pesca), in quanto i truffatori utilizzano "esche" per "pescare" le informazioni finanziare degli utenti e le password. Gli hacker hanno la tendenza di cambiare la lettera f in "ph", e il termine "phishing" è solo uno di questi esempi.
La trasformazione "da f a ph" non è nuova tra gli hacker e questo fenomeno apparì per la prima volta verso la fine degli anni 60 tra gli hacker dei sistemi telefonici che si definivano "phone phreaks."

I phisher ora falsificano messaggi e pagine Web in modo da renderle indistinguibili da quelle autentiche, utilizzando eserciti di macchine legittime compromesse (botnet) e software che può infettare (malware) per le stesse finalità che in precedenza richiedevano una interazione con l'utente finale più evidente. I phisher ha anche sviluppato un malware per cellulari che può rendere alcune misure di protezione inefficaci.

IL DANNO AI CONSUMATORI E AL SETTORE

Misurare l'impatto del phishing per i consumatori e per l'economia è un lavoro difficile, con risultati molto diversi. Un punto su cui viene raggiunto un accordo generale è che gli attacchi di phishing sono in aumento. Il rapporto annuale di Verizon sulle indagini riguardanti le violazioni dei sistemi mostra che, dopo un breve calo nel 2010, il phishing è aumentato per diversi anni di fila. Nel 2014 il phishing è stato riconosciuto come la numero 3 tra le cause delle violazioni dei dati[xvi] e nel 2013 sono aumentate del 23 per cento, da 253 a 312. Sempre nel 2014, gli aggressori hanno continuato a violare le reti con attacchi altamente mirati di "spear-phishing", che è sono arrivati all' 8 per cento degli attacchi complessivi. Questi attacchi sono diventati più sofisticati e mirati; con il 14 per cento in meno di e-mail inviate verso il 20 per cento in meno degli obiettivi. [xvii]

L' Anti-Phishing Working Group (APWG) produce rapporti trimestrali sulle tendenze del phishing; Il loro rapporto del 2014 ha rilevato il maggior numero di attacchi di phishing visto dal 2009. Lo stesso rapporto ha documentato l'aumento dei marchi come obiettivo, con 756 istituzioni interessate nella prima metà del 2014.[xviii,xix] Il rapporto mensile frodi della RSA di dicembre 2014 ha ipotizzato le perdite solo di un mese per causa del phishing pari a 453 milioni di dollari americani a livello globale o le perdite su base annua pari a circa 5 miliardi di dollari americani, con il 75 per cento degli attacchi che colpiscono gli Stati Uniti e il Canada[xx]. Anche se il phishing rappresenta una piccola parte delle perdite globali stimate per il crimine informatico, che sono stimate in 445 miliardi di dollari[xxi], 5 miliardi sono comunque una perdita significativa e prevenibile.

La prevenzione è anche diventata un lavoro considerevole, con il tempo medio dal click attestato ad un minuto e ventidue secondi e con i dati della APWG che suggeriscono che l'infrastruttura utilizzata per condurre queste campagne è molto vasta, con oltre 9.000 domini e quasi 50.000 URL di phishing monitorati ogni mese dai membri del gruppo.

IL PANORAMA DEL PHISHING

Il Phishing si distingue per il tipo di informazioni richieste, i tipi di bersagli attaccati, e i canali attraverso i quali vengono condotti gli attacchi. Il Phishing è normalmente identificato da un messaggio e-mail, SMS, o di altro tipo che contiene un link che reindirizza il destinatario ad una pagina web fasulla la quale richiede le informazioni sul conto, ad esempio username e password, numero di carta di credito o altre informazioni personali.

OBIETTIVI DEGLI ATTACCHI DI PHISHING – COSA CERCANO

Le informazioni ottenute dal phishing vengono generalmente utilizzate per un certo tipo di furto finanziario, sia direttamente contro la vittima, o su un altro bersaglio come ad esempio il datore di lavoro della vittima.

Come monetizzare i dati della carta di credito e numeri di previdenza sociale diventa sempre più difficile, "gli hacker perseguiteranno chiunque abbia informazioni di assistenza sanitaria", ha detto John Pescatore, direttore delle tendenze di sicurezza emergenti presso l'Istituto SANS, aggiungendo che negli ultimi anni gli hacker hanno sempre messo gli occhi sulle EHR (cartelle cliniche elettroniche), che possono essere facilmente trasformate in denaro contante.[xxii] Inoltre, il phishing è stato impiegato come la prima tappa nel processo di violazione di reti aziendali e governative permettendo di ottenere le credenziali per consentire l'accesso di sistemi.

Il Phishing, in sé, è di solito solo un primo passo e non prevede necessariamente fin da subito un furto finanziario diretto. La tendenza in crescita nel rubare record di assistenza sanitaria tipicamente inizia con attacchi di phishing per ottenere l'accesso ai sistemi. Una volta che l'accesso è ottenuto, i ladri utilizzano altri strumenti, come il malware e spyware, per rubare informazioni sensibili - nel primo trimestre del 2015 più di 120 milioni di pazienti statunitensi hanno avuto i loro dati rubati.[xxiii] Inoltre, lo spear phishing per ottenere credenziali di dipendenti aziendali è spesso uno dei primi passi di una violazione dei dati su larga scala ed è quindi il primo passo di una parte significativa delle perdite impressionanti attribuite alla violazioni dei dati.

Truffe 419 – Le prime e poco sofisticate forme di phishing, così chiamate in riferimento al capitolo 38 sezione 419 del codice penale nigeriano che criminalizza questo tipo di frode. ***"Qualsiasi persona che con qualsiasi falsa pretesa e con l'intento di frodare, ottiene da un'altra persona qualsiasi cosa in grado di essere rubata o induce qualsiasi altra persona a fornire a chiunque qualsiasi cosa che possa essere rubata, è colpevole di un crimine, ed è responsabile alla reclusione per tre anni."***

Queste sono le famose e-mail del principe della Nigeria o altri schemi di pagamento anticipato dove la vittima è ingannata nello spendere denaro in cambio di ricchezze indicibili alla fine del processo.

- Le tecniche, sia online che offline, che possono indurre le persone a divulgare informazioni sono spesso chiamate di "ingegneria sociale" e sono molto diffuse su Internet. Quando le prime e-mail di phishing sono emerse, gli aggressori non erano molto raffinati. Loro inviavano e-mail generiche a quante più persone possibile nella speranza che una certa percentuale venisse tratta in inganno. Quando le difese contro questo tipo di attacchi si irrobustirono, gli aggressori affinarono le loro strategie. Ci sono quattro forme comunemente note di phishing

i) un ***reindirizzamento*** *attraverso un link contenuto in un messaggio verso un indirizzo internet che può contenere un sito bancario, di e-commerce, o e-mail falso,*

ii) e-mail con un ***allegato html*** *che contiene il form di phishing,*

iii) un ***link/elenco*** *di un numero di telefono che la vittima deve cliccare o chiamare oppure*

*iv) un semplice phish del tipo **rispondi-a**, dove il messaggio contiene una richiesta di credenziali e all'utente viene chiesto di rispondere con le informazioni.*

Nelle prime due forme, il destinatario del messaggio fornisce informazioni personali, il più delle volte, inviando al criminale una e-mail contenente le credenziali rubate. Il phishing basato sul numero di telefono può prevedere sia un sistema telefonico automatico di risposta che richiede alle vittime le loro credenziali oppure una persona dal vivo che tenterà tecniche di ingegneria sociale su di loro. Le truffe 419, con promesse di ricchezze incalcolabili, e altre truffe di "pagamento anticipato" erano le prime forme di ingegneria sociale via e-mail. Nonostante i progressi del phishing, queste truffe esistono ancora al giorno d'oggi.

- **Spear Phishing / Phishing Mirato** - Mentre i tradizionali tentativi di phishing vengono spesso inviati indiscriminatamente a quasi tutti, gli attacchi di phishing mirati sono condotti contro individui o organizzazioni specifiche. Questo tipo di phishing di solito comporta, da parte dei truffatori, approfondite ricerche per imparare a conoscere i loro hobby, gli enti di beneficenza, i datori di lavoro del passato e le reti sociali, nel tentativo di rendere il loro attacco molto più plausibile e credibile. Può essere personalizzato per ingannare le vittime che sono tradizionalmente più preziose (e sospette) rispetto all'utente medio. Questi potrebbero essere i dipendenti di una società mirata che un attaccante sta cercando di penetrare. Una variante di spear phishing che è particolarmente efficace comporta un falso messaggio che sembra provenire da un fornitore, creditore o organizzazione conosciuta alla vittima contenente delle istruzioni fraudolente di pagamento per transazioni comunemente attese o normali.

- **VoIP / Vishing** – Nello stesso modo in cui la telefonia e le altre funzionalità vocali migrano verso meccanismi basati su Internet, noti collettivamente come "Voice over IP" o VoIP, allo stesso modo lo fanno le frodi. Questa integrazione di computer con sistemi telefonici rende possibile ingannare le vittime a cliccare link fraudolenti che effettuano automaticamente una chiamata telefonica, oppure che portano ad un sito web. La chiamata stessa può generare direttamente entrate per l'attaccante, o può indirizzare la vittima verso un ingegnere sociale che convince la vittima a rivelare informazioni. Gli smartphone aggravano la minaccia rendendo semplice per gli utenti questa integrazione Internet / Telefonia. Per ulteriori informazioni, consultare la sezione "Mobile e Voice" di questa relazione.

- **Fax** – Il Fax è stato uno dei primi metodi di phishing elettronico ed è stato in gran parte sostituito da altri metodi di attacco descritti qui. Tuttavia, l'avvento di fax inviati tramite Internet ha ridotto i costi e sta vivendo una rinascita. Dato che il suo uso è raro, non è sempre rilevato.

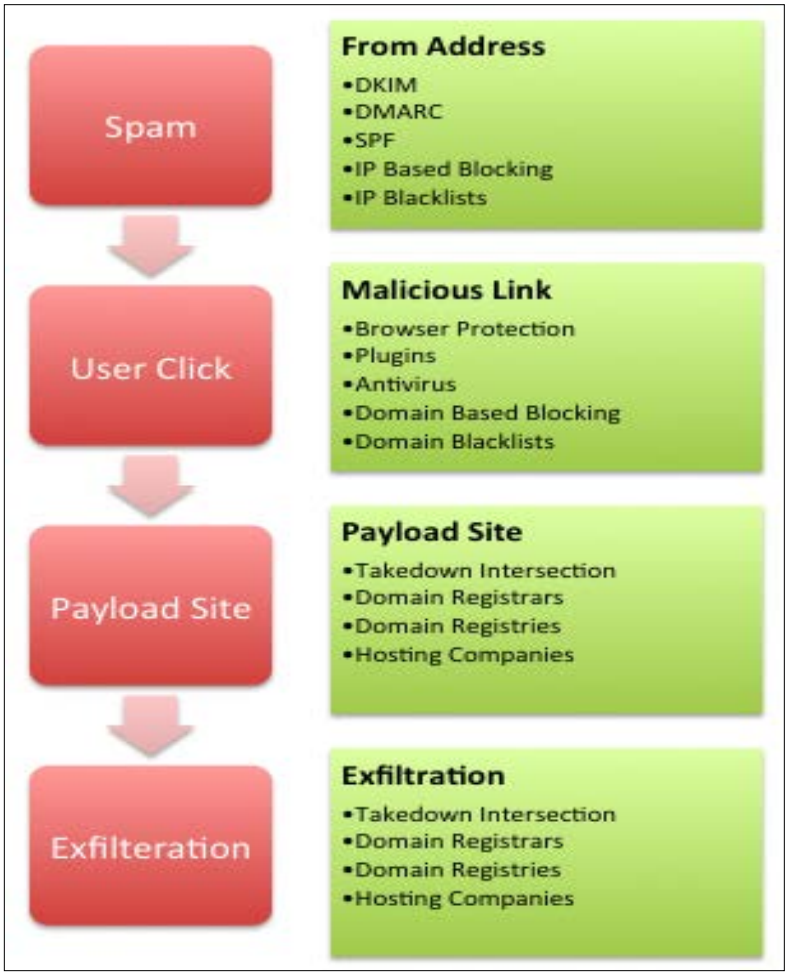
- **Social Networks** – Queste creano una esperienza di gruppo che contribuisce a dare un senso di fiducia, a sua volta utile per l'ingegneria sociale che sfrutta le relazioni online della vittima. Questo può funzionare molto bene quando l'attaccante imita un messaggio inviato da un amico online di fiducia o ha compromesso l'account dell'amico stesso.

CRONOLOGIA DI UNA TIPICA CAMPAGNA DI PHISHING

Una comune campagna di phishing per la raccolta delle credenziali d'accesso ha quatto elementi:

1. **Messaggio Iniziale (Spam)** – Un messaggio viene inviato e visto dall'utente finale. Sembra vero e perciò ha un alto grado di credibilità, contenendo tipicamente elementi falsificati di un messaggio legittimo e apparentemente proveniente da una fonte legittima, come la propria banca.
2. **Richiesta di Intervento (Click dell'Utente)** – La vittima è invitata a cliccare su un link o rispondere al messaggio con informazioni riservate. Le richieste di intervento più efficaci giocano sulla paura e l'avidità, che siano personali, oppure nei confronti dell'organizzazione per la quale lavora il destinatario. Un messaggio basato sulla paura può indicare che la vittima è già stata compromessa o può perdere l'accesso a una risorsa se non interviene, o che la società per cui lavora è soggetta ad una causa o ad una sanzione pecuniaria. Un messaggio basato sull'avidità può promettere uno sconto o una ricompensa finanziaria per la compilazione di un sondaggio o per fornire informazioni
3. **Payload** – Questo contenuto fa sì che la vittima possa divulgare le informazioni di interesse. Può essere nel messaggio iniziale oppure su un sito di destinazione, chiamato "pagina di destinazione". Il sito può essere compromesso, o può avere un nome di dominio simile per confondere l'utente finale. Il "Payload" di solito ha un form che richiede alla vittima di inserire informazioni riservate. Alcuni siti di phishing contengono anche un meccanismo di "drive-by download" in cui la visita del destinatario alla pagina web fa scattare un processo automatico di inventario del sistema e di sfruttamento con il risultato di caricare clandestinamente il malware sul computer della vittima, consentendo ai criminali di recuperare i dati riservati, dopo di che la vittima viene reindirizzata ad un sito legittimo.
4. **Sfruttamento / Fuoriuscita / Ottenimento di informazioni** – La fine del gioco di qualsiasi campagna di phishing è quello di convertire le credenziali raccolte in valore per i criminali. Una vasta gamma di schemi sono stati osservati, il più semplice è quello di accedere al conto e utilizzarlo per trasferire fondi o fare acquisti, mentre altri attacchi molto più sofisticati iniziano utilizzando il phishing per ottenere l'accesso ad un account di posta elettronica e quindi utilizzarlo come base per ingegneria sociale supplementare e / o distribuzione di malware con il potenziale di infiltrarsi profondamente dentro l'organizzazione del destinatario. Sono stati osservati anche tentativi di estorsione.

Ci sono un certo numero di punti nei quali il flusso di una campagna di phishing può essere prevenuto o interrotto, come indicato nello schema:



METODI DI SFRUTTAMENTO IN EVOLUZIONE

La forma più nota e originale del phishing ha visto i criminali accedere direttamente ad un istituto finanziario e tentare di trasferire fondi dal conto della vittima verso un altro conto sotto il controllo dei criminali. Quando le istituzioni finanziarie hanno iniziato a rilevare e bloccare più facilmente i trasferimenti internazionali di denaro fraudolenti, i criminali si sono adattati. Spostando il denaro su un conto interno o dello stesso istituto la frode spesso non viene rilevata così facilmente. A volte questo è stato realizzato attraverso il pagamento delle bollette online o semplici giroconti. In queste situazioni, il criminale, che era spesso all'estero, ha dovuto comprare i servizi di criminali nazionali per farli agire come “muli” di trasporto del denaro.

In altri casi, l'invito all'azione contenuto nella e-mail di phishing è destinato a suscitare la divulgazione dei dati della carta di credito. Con il numero di carta di credito, data di scadenza e il codice CVV, la carta può essere sia venduta sul mercato nero o utilizzata per tutte le tipologie di frodi del tipo “carta non presente”. Con il numero di carta di credito, scadenza e CVV, il phisher è libero di visitare quasi ogni rivenditore online e fare acquisti. Per eludere il rilevamento, vengono utilizzati i mercati criminali secondari per rispedizione e servizi di terminale remoto. Al fine di sconfiggere i sistemi di rilevamento delle frodi di vendita al dettaglio, il phisher acquisterà l'uso di

un indirizzo IP tramite servizi terminali remoti in un'area geografica corrispondente a quella della carta di credito della vittima. Allo stesso modo, se le spedizioni devono essere inviate, verrà utilizzato un luogo per ricevere i pacchetti che corrisponde con l'area geografica della vittima.

Gli attacchi di riutilizzo delle password sono ancora un'altra minaccia per i consumatori on-line che può derivare da un attacco di phishing. Poiché le persone spesso usano la stessa password su molti sistemi, i criminali sono in grado di utilizzare queste stesse user-ID e password in molteplici luoghi, comprese le banche, i rivenditori online e anche i sistemi di VPN aziendali (si veda la sezione Malware e botnet per ulteriori informazioni sulla creazione e la memorizzazione di password complesse).

Le violazioni dei dati su larga scala che hanno fatto notizia in questi ultimi anni iniziano spesso con qualche forma di phishing mirato o spear phishing di dirigenti o individui con accesso al controllo della rete aziendale. Tali attacchi hanno portato a reati finanziari diretti come il furto di credenziali e le informazioni personali dell'utente e la rivendita di queste negli ambienti criminali. Un grande e crescente numero di campagne di spear phishing sono anche a sostegno dello spionaggio industriale, di schemi di estorsione criminale, di infiltrazione sponsorizzata dallo stato e di altri crimini non finanziari.

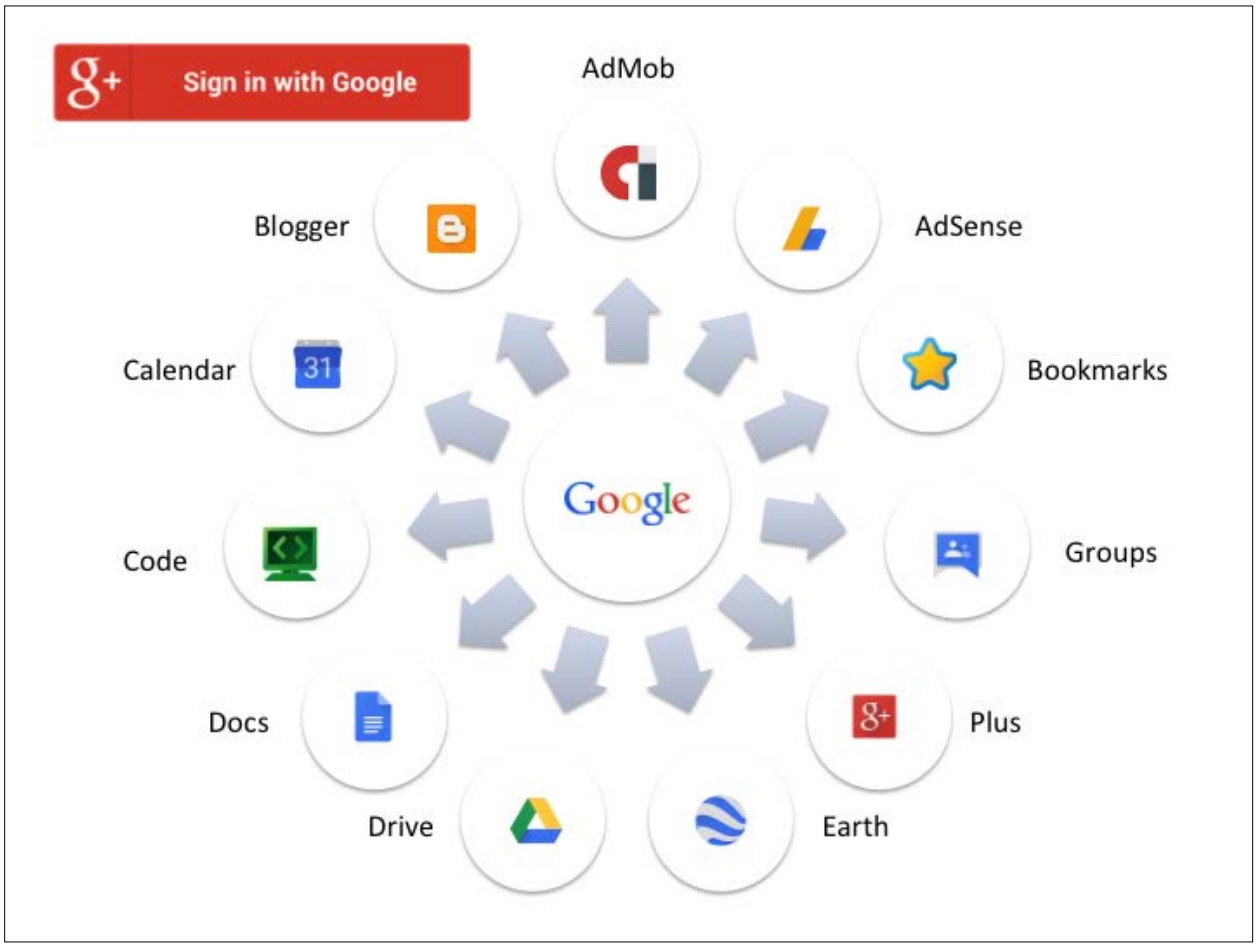
AUMENTO DELLA LEVA DEGLI ATTACCHI DI PHISHING

Mentre sempre più organizzazioni hanno migrato i loro sistemi di posta elettronica sul web, gli attacchi di phishing sono diventati sempre più frequenti per due motivi principali. In primo luogo, purtroppo, molte organizzazioni utilizzano ambienti di "Single Sign-on" con la stessa password per entrambi gli account di posta elettronica e le attività delle risorse umane, come il conto corrente bancario dove il denaro dovrebbe essere trasferito il giorno di paga. In secondo luogo, ogni volta che sia accede ad un account di posta elettronica aziendale, il criminale ha una piattaforma dalla quale può studiare l'organizzazione, imparare chi può avere accesso alle risorse digitali più preziose della società, compresi i conti bancari e la proprietà intellettuale, e indirizzare verso quei dipendenti. Tali attacchi possono essere lanciati sia da un account di posta elettronica di un dipendente che conoscono e del quale hanno fiducia, sia attraverso l'ingegneria sociale o la consegna di malware tramite allegati di posta elettronica simili a documenti aziendali comuni che si trovano nell'account compromesso.

Anche per quanto riguarda le e-mail non aziendali, gli attacchi di phishing contro provider di posta elettronica come Gmail, Yahoo, Outlook, e AOL sono sempre più comuni per molte delle stesse ragioni. Questi account possono sembrare "obiettivi di basso valore" e non sono sorvegliati diligentemente come gli altri ma offrono la possibilità di re-impostare le password o l'accesso diretto ad altri conti per una vasta gamma di attacchi. Questi account di posta elettronica compromessi hanno portato a volumi significativi di reati finanziari (ad esempio, controllo degli account, frodi tramite bonifici bancari) che sono ben documentati dalle istituzioni finanziarie.

Altri servizi, come i social network forniscono "single sign-on" ai consumatori per una vasta gamma di servizi. Ciò rende tali account obiettivi maturi per i phisher, in quanto possono monetizzare

direttamente tali servizi, reindirizzare le spedizioni di prodotti o in generale prendere controllo su molti aspetti della identità on-line di una persona. Il seguente diagramma mostra che se gli hacker possono infiltrarsi in un account Google, spesso hanno accesso a un gran numero di altre informazioni. Lo stesso si può dire per gli account di Apple e iTunes.



La maggiore sofisticazione dei criminali ha portato alla presa di mira di elementi infrastrutturali che permettono di fornire loro ancora maggiore leva potenziale. Ad esempio, i phisher ora possono accedere a Fornitori di servizi Email terzi (Email Service Provider - ESP), che inviano campagne email massive per conto dei marchi più grandi al mondo. I criminali accedono all'infrastruttura di un ESP tramite account compromesso, rubano liste di clienti, inviano messaggi non desiderati di phishing o malware ai destinatari inconsapevoli che credono che il messaggio provenga dalla mailing list di una società legittima.

Un'altra tendenza recente è la maggiore presa di mira di elementi portanti della infrastruttura Internet come gli account di hosting o le credenziali di registrazione domini. Una volta che il phisher ottiene l'accesso al controllo di infrastrutture fondamentali come queste, possono creare siti web, lanciare nuovi attacchi, e creare nuovi elementi infrastrutturali come i nomi di dominio

tramite i quali mistificare i loro schemi (vedere la sezione Hosting e Cloud Services). Una tattica particolarmente dannosa è quella di aggiungere sottodomini ad un nome di dominio che gode di una buona e consolidata reputazione, lasciando il dominio originale intatto. Questo consente ai criminali di sfruttare la buona reputazione di un dominio nelle loro campagne per aggirare i filtri ed evitare di essere bloccati o oscurati (si veda la sezione "I nomi di dominio e indirizzi IP").

MIGLIORI PRATICHE PER CONTRASTARE IL PHISHING E IL SOCIAL ENGINEERING

Ci sono una vasta gamma di migliori pratiche anti-phishing a disposizione delle organizzazioni per proteggere il loro marchio e i loro clienti. Detto questo, non c'è nessuna "formula magica" per le sfide che il phishing porta e deve essere affrontato durante l'intero ciclo di vita del processo - ogni passo che può essere contrastato nel flusso può proteggere decine di milioni di vittime a seconda della dimensione dell'attacco in questione e la portata delle varie soluzioni. Le imprese dovrebbero trattare questo problema con un approccio del tipo "difesa in profondità" - assumendo che alcune misure saranno efficaci per prevenire l'arrivo delle prime e-mail, ma alcune potranno passare rendendo necessarie ulteriori difese. Questa sezione metterà in evidenza alcune delle principali tecniche e le migliori pratiche, ma molti più dettagli e una consulenza specifica possono essere ottenuti da varie organizzazioni di settore, pubblicazioni governative, e soluzioni commerciali anti-phishing.

1. Prevenire il successo degli attacchi di phishing

La prima cosa da fare per affrontare gli attacchi di phishing è di impedire loro di raggiungere le vittime e / o in primo luogo di impedire a quest'ultime di visitare siti di phishing. Ci sono tre punti di contatto principali per realizzare ciò: fermare il flusso di e-mail per l'adescamento, impedendo che le esche raggiungano gli utenti e bloccando l'accesso a siti web di phishing e ad altre attività.

a. Prevenzione in uscita della consegna di esche

I relativamente recenti meccanismi di autenticazione delle email facilitano alcune facili protezioni contro alcune forme di phishing e di spoofing. Queste tecniche si basano sulla creazione di una infrastruttura di posta elettronica autenticata. I meccanismi di autenticazione più comuni per le e-mail sono SPF (Sender Policy Framework) [xxiv] e DKIM (DomainKeys Identified Mail) [xxv], che utilizzano i nomi di dominio[xxvi] come identificatori convalidati. Questi permettono al proprietario di un nome di dominio di controllare l'utilizzo di quel dominio nelle e-mail e ridurre lo spoofing.

Al fine di affrontare i problemi di phishing e spoofing del dominio con successo, i proprietari dei marchi e gli ISP hanno bisogno di condividere le informazioni tra di loro riguardo le proprie attività relative alla posta elettronica, come ad esempio le politiche per l'autenticazione e le segnalazioni sui problemi. Storicamente, questi accordi sono stati bilaterali e privati tra i proprietari dei marchi e i singoli ISP. Tuttavia, un consorzio di settore *ad hoc* ha sviluppato una specifica tecnica chiamata DMARC (Domain-based Message Authentication, Reporting & Conformance) [xxvii].

DMARC, introdotto all'inizio del 2012, sfrutta SPF e DKIM per fornire ai proprietari dei marchi un mezzo per comunicare facilmente agli ISP il modo in cui preferirebbero trattare eventuali messaggi impropriamente autenticati. DMARC fornisce anche agli ISP e agli altri destinatari di posta elettronica un meccanismo per restituire a proprietari dei marchi un feedback aggregato per quanto riguarda lo stato di salute delle loro pratiche di autenticazione e-mail così come informazioni di livello forense.

Per le attività di invio di posta elettronica, l'approccio consigliato è:

- *Verifica* – tramite un inventario di tutte le macchine e dei sistemi che inviano e-mail per conto dell'organizzazione, inclusi i sistemi esterni, quali E-mail Service Provider (ESP) o altri terzi
- *Pubblica* – il record di autenticazione e di sistema nel DNS
- *Modifica* – il software che si occupa dell'invio di e-mail in modo che utilizzi l'autenticazione e sia conforme alle regole
- *Stabilisci* – le relazioni di segnalazione per le attività che utilizzano il nome di dominio
- *Controlla* – tutte le segnalazioni disponibili per individuare schemi che richiedano attenzione
- *Mantieni* – le operazioni per conformità continua

Per le operazioni di ricezione posta, il supportare questi nuovi meccanismi implica innanzitutto l'aggiunta di moduli ai sistemi di filtraggio-posta esistenti.

b. Filtraggio dello spam in entrata

Uno dei metodi più importanti per fermare il danno da un attacco di phishing è l'adozione di un efficace filtro anti-spam. Attivare il filtraggio dello spam è importante, ma il filtraggio efficace richiede di più che avere solamente un prodotto commerciale installato sul gateway di posta elettronica. Le aziende e le agenzie governative dovrebbero anche migliorare il loro filtro anti-spam con l'aggiunta di informazioni sulle minacce che contribuiscono a rendere il filtro anti-spam più efficace.

Queste informazioni possono essere ottenute da "liste nere" (blacklist) create da organizzazioni specializzate come Spamhaus, SURBL, e altri (vedi riferimenti alla fine di questa sezione). Il filtraggio dello spam è strettamente legato alla segnalazione, in quanto le e-mail di phishing che penetrano con successo un filtro anti-spam sono le più urgenti da segnalare. Molti servizi di posta elettronica offrono un pulsante "Segnala Phish" o "Segnala Spam", che gli utenti dovrebbero essere incoraggiati ad usare.

Le tecniche per il filtraggio dello spam includono:

- *Autenticazione* – Chi invia le e-mail ha la possibilità di utilizzare metodi di autenticazione, tra cui DomainKeys Identified E-mail (DKIM), Sender Policy Framework (SPF), “Domain-based Message Authentication, Reporting and Conformance” (DMARC). Quando viene ricevuta una e-mail, viene controllata la presenza di un token di autenticazione. Nel caso del DMARC, il dominio di invio viene controllato per vedere se richiede l'autenticazione. Se il token non è valido o mancante l'e-mail può essere fraudolenta.

- *Reputazione IP* - L'indirizzo IP che invia l'e-mail potrebbe essere già noto per essere associato all'invio di spam. Rifiutando le e-mail provenienti da indirizzi IP con cattiva reputazione una grande quantità di spam può essere bloccata.

- *Filtraggio del Contenuto* – Il filtraggio basato su regole, controllando la posta elettronica per la presenza di parole o frasi proibite, o l’analisi statistica della posta elettronica (sistema di filtraggio spam di tipo Bayesiano) sono in grado di identificare le e-mail che hanno buone probabilità di essere spam. Aggiornare i filtri di contenuto con i dati provenienti da servizi di reputazione per gli host e / o gli URL (ad esempio sistemi DNSBL come Spamhaus / SURBL) migliora notevolmente questa tecnica.

- *Spam trap* – Attraverso la raccolta di e-mail inviate a indirizzi che non dovrebbero ricevere nessuna e-mail (utenti inesistenti) gli schemi possono essere identificati e applicati per bloccare le e-mail inviate a indirizzi legittimi.

c. Browser e altri tipo di blocco

La protezione contro gli attacchi di phishing è incorporata in molti prodotti e servizi dei quali consumatori, le imprese e le altre organizzazioni possono trarre vantaggio. Con la segnalazione diffusa di attacchi di phishing dai marchi e dal pubblico in generale, questi dati vengono alimentati nei prodotti che sono esposti al phishing, come i browser web, i server e i client di posta elettronica, i dispositivi di sicurezza (firewall, sistemi IDS / IPS, web proxy, firewall DNS), e i fornitori di servizi online di e-mail. Questi strumenti / dispositivi sono in grado di fornire una protezione ancora migliore se sono potenziati con i dati di intelligence relativi alle minacce. Esempi di questi sono i dati di reputazione per gli indirizzi IP, nomi di host / dominio, URL, indirizzi e-mail, e altri "indicatori" di un comportamento ingannevole.

Questi possono essere forniti in varie forme, tra cui tramite liste di blocco basate su DNS (DNSBL), liste di blocco aggiornate in tempo reale (RBL), liste di blocco URL e una tecnologia relativamente nuova chiamata “DNS Response Policy Zones” (RPZ). Tali tecnologie e dati possono essere utilizzati per tagliare tutte le comunicazioni verso indirizzi Internet bloccati. Le aziende hanno bisogno di creare criteri e norme operative per essere sicure di abilitare tali servizi nei loro ambienti. Ciò è particolarmente importante per i prodotti che fungono da gateway di posta elettronica e per gli strumenti globali di sicurezza di rete in modo da creare una difesa "a strati". Questa attitudine alla sicurezza deve essere ben pianificata e aggiornata su base regolare.

I singoli utenti possono anche proteggersi da molti attacchi semplicemente abilitando tali servizi nei loro browser (ad esempio, Google Safe Browsing, Microsoft Phishing Filter), aggiungendo una "barra degli strumenti" per il proprio browser, abilitando le impostazioni anti-phishing o anti-spam per i loro account web di posta elettronica, e attivando le protezioni anti-phishing nel loro software anti-virus.

2. Rilevamento

Il rilevamento degli attacchi di phishing impedisce sia l'attacco specifico, ma aiuta anche a rilevare attacchi futuri. Inoltre, senza rilevazione, i siti non possono essere recuperati per l'analisi forense, bloccati nei browser e nei filtri anti-spam, chiusi o indagati. Il rilevamento può assumere forme diverse, a seconda del punto di osservazione dal quale sta avvenendo rilevamento stesso. Quando si parla di rilevazione l'obiettivo finale è quello di rilevare il sito di phishing o la campagna e-mail appena creata, ma spesso i mezzi per il rilevamento trovano spazio nell'analisi del flusso di messaggi tra i criminali e le vittime potenziali.

- Utente/Impiegato: Poiché i consumatori sono il più probabile destinatario del messaggio, è importante che i marchi potenzialmente a rischio comunichino in modo efficace con i propri clienti cosa fare se vedono un e-mail sospetta. Gli attacchi di spear phishing vengono indirizzati ai dipendenti. La rilevazione sarà spesso nella forma di una e-mail vista da un cliente o dipendente del marchio oggetto dell'attacco, in questo senso fornire servizi di reporting e di educazione degli utenti costituisce un passo importante per la rilevazione di attacchi (vedi sotto)
- E-mail rifiutata: Per molti anni uno dei metodi più efficaci per convincere una potenziale vittima che un messaggio di phishing è legittimo è stato quello di utilizzare il dominio di invio del marchio imitato. E-mail da "@ paypal.com" o "@ bankofamerica.com" sono prese per oro colato da potenziali vittime che non sono a conoscenza di come facilmente gli indirizzi "Da:" possono essere contraffatti. Fortunatamente, quando tali messaggi non riescono a essere consegnati, spesso succede perché lo spammer li invia ad un account che è disattivato, chiuso, o non ha più abilitata la ricezione di messaggi, il server di posta sul lato ricevente "rimbalzerà" questi messaggi. Come descritto in precedenza nel caso dell'autenticazione e-mail, DMARC fornisce un protocollo per dirigere dove tali messaggi rifiutati devono essere inviati. L'analisi di questi messaggi rifiutati può spesso portare alla individuazione di nuove fonti di phishing e siti web.
- URL di riferimento: quando un kit di phishing utilizza della grafica, dei file JavaScript, dei fogli di stile, o un'altra proprietà del marchio imitato, i file di log del marchio imitato mostreranno che il file è stato referenziato da un sito di terzi. Se "sitocompromesso.com/tuabanca/verifica.php" è una pagina di phishing e utilizza la grafica da "tuabanca.com/graphics/logo.gif", il registro mostrerà che "logo.gif" è referenziato a da "sitocompromesso.com". L'analisi di questi URL di riferimento è un ottimo modo per individuare nuovi siti web di phishing. Questo può essere realizzato in casa con uno staff ben addestrato o in outsourcing ad uno dei molti fornitori.

- Spam in uscita: Dal punto di vista di una impresa, di un provider di hosting o di un ISP, ci sono diversi modi per rilevare le e-mail di phishing in uscita che vengono generate dalla rete. A seconda delle condizioni generali di servizio per il servizio fornito, la rete può essere in grado di osservare nelle e-mail in uscita la presenza di caratteristiche sospette, come i picchi inusuali di volume, disallineamenti del dominio del mittente, i tentativi di utilizzare le porte di posta elettronica da una rete non autorizzata, o l'inserimento di indirizzi IP della propria rete in varie liste di reputazione.
- Riutilizzo di credenziali: una tecnica recente per il rilevamento dei siti di phishing è stata quello di richiedere ai consumatori di utilizzare una coppia ID utente e password per accedere al sito di un marchio. Un plug-in nel browser del consumatore rileva qualsiasi tentativo di utilizzare lo stesso ID utente e password su qualsiasi altro sito, e riporta l'URL al marchio destinazione come URL sospetto da indagare.
- Prodotti per la sicurezza e software open-source ottimizzato contro il phishing: I server di posta elettronica, i moderni dispositivi di sicurezza e i servizi cloud utilizzano i feed di siti di phishing, di indirizzi IP, di nomi di dominio e di schemi noti per attacchi di phishing. Sulla base sia di confronti diretti che di analisi euristiche di URL inclusi nelle e-mail o in transito nella rete aziendale, le esche per il phishing e i "click" possono essere rilevati per il blocco, l'allarme, e l'azione

3. Segnalazioni

La segnalazione di attacchi di phishing serve a due scopi. Può aiutare i marchi che vengono falsificati a rispondere alla minaccia e fornire un percorso che può essere utile alle forze dell'ordine. Una volta che viene rilevato un attacco di phishing, ci sono diverse strade per la segnalazione per aiutare a proteggere tutta la comunità dal ricevere esche o dal visitare siti di phishing. I marchi e le organizzazioni che vengono contraffatti nelle esche di phishing e nei siti web possono avvisare i propri clienti, i dipendenti e i loro componenti - le vittime più probabili. Gli individui che incontrano i siti di phishing possono anche segnalarli e i marchi vittima possono aiutare, fornendo e promuovendo una metodologia semplice ai loro clienti e agli altri per segnalare loro il phishing.

Una volta che l'organizzazione ha capito che è il bersaglio di una campagna di phishing, è importante avvisare l'ecosistema anti-phishing composto da organizzazioni del settore, fornitori e chi si occupa di rispondere agli incidenti. Questo può essere fatto, per l'attacco phishing occasionale, riportando l'attacco attraverso uno dei siti elencati alla fine di questa sezione.

Per rendere la segnalazione più semplice possibile, molti marchi hanno creato indirizzi e-mail facili da ricordare, ad esempio "reportphishing@brand.tld". Per incoraggiare la segnalazione, i marchi dovrebbero rendere le informazioni su come segnalare un Phish facilmente accessibili sui loro siti web e sono incoraggiati a rendere queste informazioni disponibili nelle interazioni con i clienti.

La maggior parte dei bersagli principali di phishing utilizzano servizi di terze parti specializzati che hanno come competenza base la lotta contro i contenuti illegali / indesiderati on-line, in quanto hanno rapporti consolidati e processi con i principali fornitori, capacità di traduzione, e hanno personale specializzato in grado di investigare sulle minacce. Indipendentemente dal metodo di segnalazione utilizzato, riconoscere e segnalare gli attacchi di phishing in fretta può portare all'identificazione del criminale.

4. Indagini Aziendali e delle Forze dell'Ordine

La maggior parte delle indagini di phishing sono condotte dalla società il cui marchio viene imitato, o da venditori di informazioni sulle minacce o delle forze dell'ordine che agiscono per loro conto[xxviii]. Utilizzando molte delle tecniche descritte in "Analisi e Intelligence" di cui sopra, gli investigatori possono identificare e contare le vittime e le loro perdite, ma anche collegare tra loro i molti siti di phishing creati da o a beneficio finanziario dello stesso criminale.

Piuttosto che tentare di risolvere ogni caso in modo indipendente, le aziende sono incoraggiate a sviluppare rapporti con le agenzie investigative per comprendere i metodi migliori per lo scambio di tali informazioni. Negli Stati Uniti, il programma InfraGard dell'FBI le "US Secret Service's Electronic Crimes Task Forces" (Task force dei servizi segreti degli Stati Uniti sui crimini elettronici) sono programmi che aiutano a sviluppare tali relazioni. I centri nazionali come la "National Cyber Forensics & Training Alliance" (NCFTA) forniscono anche opportunità di approcci associativi pubblico-privato per le indagini di criminalità informatica. Lavorare con queste organizzazioni può aiutare i marchi ad essere sostenitori attivi nel processo di applicazione della legge. Spesso avere più marchi vittima rappresentati in un singolo caso conduce ad una risposta delle forze dell'ordine più attiva, fornendo allo stesso tempo la "sicurezza dei numeri" per i marchi vittima, che possono sentirsi a disagio ad essere nominati come vittime.

5. Educazione utenti/vittime

McAfee Labs ha registrato alla fine del 2014 che il phishing continua ad essere una tattica efficace per infiltrarsi nelle reti aziendali. Il loro studio ha trovato che l'80 per cento degli utenti aziendali non sono in grado di rilevare le truffe, con la Finanza e gli impiegati nelle risorse umane che ottengono risultati peggiori rispetto alla media. I dipendenti possono fare il test sulla conoscenza del phishing a questo indirizzo: https://phishingquiz.mcafee.com.[xxix] Numeri come questi mostrano quanto sia importante che le società e i programmi di governo continuino a fornire una formazione regolare e obbligatoria per i loro dipendenti. Questa è stata una delle raccomandazioni del "Federal Financial Institutions Examination Council" (FFIEC). SANS (www.sans.org) ha anche informazioni su come condurre un programma di phishing sul loro sito web SecuringTheHuman.[xxx]

Mentre è più difficile fornire una formazione per i consumatori, le aziende che sperimentano alti tassi di phishing sono invitate ad educare quando hanno l'opportunità di interagire con i loro clienti, sia essa sotto forma di un inserto nella bolletta, un avviso speciale quando il cliente accede al sistema on-line, o attraverso un messaggio registrato durante l'interazione telefonica con i consumatori. Le aziende che sono preoccupate di associare il loro marchio con il crimine informatico possono invece adottare un approccio pro-attivo, come ad la campagna "Stop. Think.

Connect.", o affermare che stanno supportando le attività di consapevolezza informatica incoraggiate dal governo, come ad esempio le annuali settimane e mesi di sensibilizzazione sulla sicurezza informatica offerti dalle nazioni più sviluppate.[xxxi, xxxii] Molte sono le risorse disponibili come parte di queste campagne di sensibilizzazione pubblica che possono essere adottate dalle società.

L'APWG incoraggia le imprese ad assistere con la formazione just-in-time adottando la "APWG Phishing Education Landing Page" come loro home page. I webmaster che vogliono chiudere un sito di phishing dopo essere stato compromesso sono anche incoraggiati a sostituire la pagina con la pagina dell'APWG.[xxxiii] Diverse organizzazioni hanno sviluppato le proprie eccellenti pagine di formazione per aiutare ad educare gli utenti. Questi includono Visa e "Stay Safe Online":

http://www.visasecuritysense.com/en_US/phishing-attack.jsphttp://www.visasecuritysense.com/en_US/phishing-attack.jsp
https://www.staysafeonline.org/

La Federal Trade Commission degli Stati Uniti usa un po' di spensieratezza per avvisare i consumatori dei rischi associati con il phishing raffigurando stratagemmi di phishing standard per allertare i consumatori su questo problema tramite i giochi online e i video di YouTube.

- Giochi Online: http://www.onguardonline.gov/media/game-0011-phishing-scams, and
- Video YouTube: https://www.consumer.ftc.gov/media/video-0006-phishy-home.

6. Coinvolgimento del settore

Le organizzazioni per la condivisione delle informazioni nel settore, come la FS-ISAC (Financial Services Information Sharing Analysis Center) e il "Canadian Financial Institutions' Computer Incident Response Team" (CFI-CIRT) sono anche le organizzazioni molto importanti per aiutare ad affrontare i crimini di phishing "multi-marchio".

Il coinvolgimento nei gruppi di difesa del settore, come l'Anti-Phishing Working Group (APWG)[xxxiv], il Messaging, Malware, and Mobile Anti-Abuse Working Group (M^3AAWG)[xxxv], l' Online Trust Association (OTA)[xxxvi], il Merchant Risk Council (MRC)[xxxvii], e il Forum of Incident Response and Security Teams (FIRST)[xxxviii] sono alcune delle molte organizzazioni associative che affrontano le frodi online e la criminalità informatica. I loro incontri, le pubblicazioni, e gruppi di interesse speciale offrono molti vantaggi ai marchi che sono affetti da phishing. L' APWG, per esempio, offre funzionalità di condivisione di informazioni complete e di reporting su larga scala di siti di phishing alle organizzazioni membre rendendola una risorsa primaria per i soggetti colpiti da attacchi di phishing.

RIFERIMENTI

STATISTICHE

- Anti-Phishing Working Group Phishing Activity Trends Report / Domain Use Report
  http://www.antiphishing.org/resources/apwg-reports/
  N.B.: L'APWG può fornire fogli di calcolo dei dati alla base dei report a partire dal 2006 dietro una richiesta scritta. Contattare:
  secretarygeneral@apwg.org]http://www.apwg.org/reports/APWG_CrimewareReport.pdf
- Anti-Phishing Working Group Global Phishing Survey:
  http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf
- The Anti-Phishing Working Group Web Vulnerabilities Survey
  http://www.apwg.org/reports/apwg_web_vulberabilities_survey_june_2011.pdfhttp://www.apwg.org/reports/apwg_web_vulberabilities_survey_june_2011.pdf
- Phishing: How many take the bait? Government of Canada
  http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspxhttp://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx

PROGRAMMI RIVOLTI AGLI UTENTI

- The Anti-Bot Code of Conduct for Internet Service Providers:
  http://www.m3aawg.org/abcs-for-ISP-code
- iCode.org - Internet Industry Association:
  https://icode.orghttps://www.ccc.go.jp/en_activity/index.html
- Anti-Botnet Advisory Center - ECO (Germany):
  https://www.botfrei.de/en/https://www.botfrei.de/en/
- STOP. THINK. CONNECT.: http://www.stopthinkconnect.org
- APWG Consumer Advice: http://www.antiphishing.org/resources/overview/
- APWG Educating Consumers: http://www.antiphishing.org/resources/Educate-Your-Customers/ http://www.stopthinkconnect.org

SEGNALARE IL PHISHING:

Anti-Phishing Working Group:
http://www.antiphishing.org/report-phishing/
e-mail: reportphishing@apwg.org

Principali provider / browser:
Google:
https://www.google.com/safebrowsing/report_phish/https://www.google.com/safebrowsing/report_phish/

Microsoft:
www.microsoft.com/security/online-privacy/phishing-scams.aspx#Reporthttp://www.microsoft.com/security/online-privacy/phishing-scams.aspx - Report
Yahoo:
https://safety.yahoo.com/Security/IVE-BEEN-PHISHED.htmlhttps://safety.yahoo.com/Security/IVE-BEEN-PHISHED.html
https://safety.yahoo.com/Security/IVE-BEEN-PHISHED.html
Risorse online dei produttori di software per la sicurezza:
http://www.phishtank.orghttp://www.phishtank.org
https://submit.symantec.com/antifraud/phish.cgihttps://submit.symantec.com/antifraud/phish.cgi
http://phishing.eset.com/reporthttp://phishing.eset.com/report
http://toolbar.netcraft.com/report_urlhttp://toolbar.netcraft.com/report_url
http://toolbar.netcraft.com/report_url
Stati Uniti:
L' Internet Crime and Complaint Center offer un sistema di segnalazione centralizzato per i crimini informatici che hanno causato perdite:
www.ic3.gov/default.aspxhttp://www.ic3.gov/default.aspx
US-CERT inoltre ha un posto dove tutte le segnalazioni di phishing possono essere inviate:
https://www.us-cert.gov/report-phishinghttps://www.us-cert.gov/report-phishing
e-mail: phishing-report@us-cert.gov
Il sistema di segnalazione spam della Federal Trade Commission fornisce dati alla "Consumer Sentinel Data Base", un sistema per le forze dell'ordine per tracce investigative: UCE@ftc.gov

Canada:
Centro Segnalazioni Spam:
fightspam.gc.ca
e-mail: spam@fightspam.gc.ca
Canadian Anti-Fraud Centre:
www.antifraudcentre.ca/english/reportit-howtoreportfraud.htmlhttp://www.antifraudcentre.ca/english/reportit-howtoreportfraud.html
www.antifraudcentre.ca/francais/reportit-howtoreportfraud.htmlhttp://www.antifraudcentre.ca/francais/reportit-howtoreportfraud.html
La Canadian Bankers Association elenca le pagine per "Segnalare il Phishing" per la maggior parte di banche canadesi: www.cba.ca/en/consumer-information/42-safeguarding-your-money/91-email-fraud-phishing

Regno Unito:
Il National Fraud & Cyber Crime Reporting Centre permette la segnalazione delle frodi, tentate frodi, le truffe e i virus online. I consumatori possono utilizzare il link qua sotto per segnalare le frodi.
www.actionfraud.police.uk/report_fraudhttp://www.actionfraud.police.uk/report_fraud
Il Action Fraud Business Reporting Tool è uno strumento per esperti professionisti nella sicurezza che possono aver bisogno di segnalare molti casi di frode al giorno:

https://app03.actionfraud.police.uk/report/Accounthttps://app03.actionfraud.police.uk/report/Account
https://app03.actionfraud.police.uk/report/Account
Irlanda:
https://www.botfrei.de/ie/ueber.html

Australia:
http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spam/reporting-spam-i-acmahttp://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spam/reporting-spam-i-acma
https://www.scamwatch.gov.au/content/index.phtml/tag/reportascamhttps://www.scamwatch.gov.au/content/index.phtml/tag/reportascam
https://report.acorn.gov.au/https://report.acorn.gov.au/
e-mail: report@submit.spam.acma.gov.au

Nuova Zelanda:
http://complaints.antispam.govt.nz/

Francia:
https://www.signal-spam.frhttps://www.signal-spam.fr
Il CERT-LEXSI francese, l'Europol, e il governi di Olanda e Lussemburgo offrono anche loro un sito per segnalare il phishing:
https://phishing-initiative.euhttps://phishing-initiative.eu
https://phishing-initiative.eu

MILGIORI PRATICHE COMUNI

- Cosa fare se il tuo sito è stato compromesso:
  http://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdfhttp://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdf

- Subdomain Registries Advisory
  http://www.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

- Raccomandazioni e Migliori Pratiche Anti-Phishing per i Registrars
  http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf

- Misure per Proteggere I Servizi di Registrazione Domini da Pratiche Abusive o dal Cattivo Utilizzo
  http://www.icann.org/committees/security/sac040.pdf

- M^{3}AAWG Migliori Pratiche Comuni per chi invia:
  https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf http://www.m3aawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2a-updated.pdf

- La Fiducia nelle Email Inizia con L'autenticazione (White Paper del M³AAWG sulla autenticazione E-mail) https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Email_Authentication_Update-2015.pdfhttp://www.m3aawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_2008-07.pdf

- M³AAWG /APWG Migliori Pratiche Anti-Phishing per ISP e Mailbox Provider: http://www.m3aawg.org/sites/maawg/files/news/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdfhttp://www.m3aawg.org/sites/maawg/files/news/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdf http://www.m3aawg.org/sites/maawg/files/news/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdf

NOMI DI DOMINIO E INDIRIZZI IP

Una varietà di attività dannose e illegali sfruttano le vulnerabilità del Domain Name System (DNS) come conseguenza di cattive pratiche commerciali e di sicurezza tra gli operatori di Internet che si occupano delle infrastrutture e dei registri dei nomi di dominio, registrar, rivenditori e fornitori di servizi per la privacy e di proxy. Una migliore gestione da parte degli operatori di rete e pratiche migliori da parte delle organizzazioni che gestiscono gli indirizzi IP e i nomi di dominio, o le organizzazioni che forniscono servizi di registrazione del nome di dominio, può consentire l'attenuazione di queste minacce.

PANORAMICA DELLA TECONOLOGIA

INDIRIZZI INTERNET PROTOCOL (IP)

Ogni computer su Internet ha un indirizzo IP, che viene utilizzato per instradare il traffico da e verso il computer. Gli indirizzi IP tradizionali, noti come IPv4, sono numeri binari a 32-bit, invariabilmente scritti come quattro numeri decimali, come ad esempio 64.57.183.103. La prima parte dell'indirizzo, che in questo esempio potrebbe essere 64.57.183, identifica la rete, e il resto dell'indirizzo, 103 in questo esempio, il computer particolare ("host") sulla rete. La divisione tra la rete e l'host varia a seconda delle dimensioni della rete, quindi l'esempio di cui sopra è semplicemente uno dei possibili. Una versione più recente chiamata IPv6 utilizza i numeri molto più grandi a 128 bit, scritti come blocchi di cifre separati da due punti, come ad esempio 2001: 500: 2f :: f. Quasi tutti gli indirizzi IPv4 sono stati assegnati, perciò da ora siamo nel bel mezzo di una transizione graduale verso IPv6.

Perché il traffico di rete fluisca da un computer ad un altro, per esempio, dal PC di un utente al web server di Google o viceversa, il traffico dal computer di partenza passa attraverso i computer intermedi, chiamati router, fino a raggiungere la destinazione.

Ci sono circa 500.000 percorsi di rete visibili ai router più grandi di Internet, conosciuti come i router backbone (Il numero totale di reti è considerevolmente maggiore, poiché un'unica rotta backbone comprende tipicamente decine di migliaia di reti di clienti). Per mantenere le tabelle di 500.000 rotte, i router backbone utilizzano un sistema chiamato Border Gateway Protocol (BGP) per lo scambio di informazioni, in modo che i router possono regolare automaticamente tali tabelle quando nuove reti vengono messe in linea o un collegamento tra le reti non riesce o è in fase di riparazione.

Un po' come i numeri di telefono, ogni indirizzo IP visibile in tutto il mondo deve essere univoco. Gli Internet provider e le grandi aziende ottengono blocchi di indirizzi direttamente dai registri Internet regionali come ARIN, che assegna lo spazio IP per gli Stati Uniti, in Canada, e parti dei Caraibi, mentre le imprese più piccole e gli individui utilizzano parti di blocchi assegnati ai loro fornitori di servizi Internet. Alcuni indirizzi IP non sono visibili all'esterno, per esempio 192.168.1.1 o 10.0.0.51; questi sono come le estensioni Private Branch Exchange (PBX) in un sistema telefonico aziendale, raggiungibili solo dall'interno propria rete dell'organizzazione.

Il Sistema a Nomi di Dominio

Dal momento che gli indirizzi IP sono difficili da ricordare per gli esseri umani e sono legati a reti fisiche, il Sistema a Nomi di Dominio - Domain Name System (DNS) è un database distribuito di nomi che consente alle persone di utilizzare nomi come www.google.com, piuttosto che l'indirizzo IP corrispondente 173.194.73.105 (per IPv4) o 2607: f8b0: 4000: 807 :: 1012 (per IPv6). Nonostante le sue enormi dimensioni, il DNS raggiunge ottime prestazioni utilizzando la delega e le cache. Dal momento che non sarebbe pratico memorizzare tutti i nomi del DNS in un unico database, è diviso in zone che sono memorizzati su server diversi, ma logicamente collegati tra loro.

In linea di principio, per trovare l'indirizzo di Google (www.google.com), il software di ricerca DNS sul computer di un utente, conosciuto come risolutore, prima contatta uno dei server DNS "root", che risponde che per tutti i domini .com è necessario chiedere un elenco di server DNS che hanno informazioni autorevoli per .com (in questo caso, gestito da Verisign). E poi contatta uno dei server .com, che a sua volta risponde che per tutti i nomi di google.com, è necessario chiedere un elenco di server DNS che hanno informazioni per i nomi a google.com (gestiti, ovviamente, da parte di Google). E poi contatta uno di questi server DNS, che fornisce gli indirizzi IP per www.google.com. http://www.google.com./

Dal momento che gli utenti di Internet tendono a cercare gli stessi nomi più volte, ogni rete e molti singoli computer hanno una cache che memorizza le query DNS recenti e le risposte. Quindi se qualcuno che usa la cache ha recentemente chiesto www.google.com, le query successive possono essere evase dalla cache piuttosto che andare di nuovo a chiedere ai server master. O se qualcuno chiede mail.google.com o www.yahoo.com, la cache fornisce i server per google.com (per mail.google.com) o i server per .com (per www.yahoo.com), riducendo notevolmente il numero di query al server master e velocizzando le risposte agli utenti.

Dato che ci sono una varietà di modi con cui i malintenzionati possono iniettare dati DNS fittizi in cache e nei singoli computer (alcuni discussi di seguito), il DNS Security Extensions (DNSSEC) aggiunge firme crittografiche sicure ai dati restituiti dal server DNS, in modo che i computer degli utenti possono verificare le firme per la validità e garantire che i dati DNS che usano sono validi, e arrivano dalla fonte corretta. DNSSEC è stato in sviluppo per 17 anni, ma ha avuto un utilizzo significativo solo negli ultimi anni. La gestione delle chiavi per DNSSEC è complessa, e può presentare una sfida per i gestori dei server DNS.

SFRUTTAMENTO DELLE VULNERABILITÀ DEI DNS

Il più grave sfruttamento delle vulnerabilità del DNS (Domain Name System) è rappresentato dai "Resolver exploit", tramite i quali i criminali informatici introducono dati falsi per reindirizzare il web e altro traffico verso versioni contraffatte dei siti web più popolari.

AVVELENAMENTO DELLA CACHE (CACHE POISONING)

Una categoria di tali sfruttamenti è l'avvelenamento di cache, che si tratta dell'utilizzo di falle di sicurezza per introdurre i dati falsi nella cache DNS che viene poi fornita ai computer delle vittime. Pochi utenti avranno la capacità necessaria per rilevare che il proprio computer sta utilizzando informazioni DNS false. Mescolando più exploit insieme, un malintenzionato può presentare una replica perfetta di qualsiasi sito web, ogni sigillo di fiducia, qualsiasi logo, e mostrare il nome di dominio corretto nella barra degli indirizzi del browser. Il risultato può essere il furto di credenziali, l'accesso alle risorse finanziarie, la compromissione delle informazioni aziendali o nazionali o il reindirizzamento degli introiti promozionali.

I "Resolver exploit" avvengono completamente all'interno del NSP (Name Service Provider, ad esempio un server dei nomi aziendali, o di un servizio DNS pubblico come OpenDNS o Google DNS) e dei sistemi degli operatori di rete, non necessitano di alcuna compromissione di computer di utenti.

Il DNSSEC se correttamente implementato da tutte le parti coinvolte nella ricerca di un nome, tra cui il registrante, il registro e NSP, impedirà il cache poisoning e altri abusi DNS. In questo momento, DNSSEC è scarsamente distribuito e non è ancora considerato una difesa affidabile contro l'avvelenamento della cache. La difesa attualmente utilizzata contro l'avvelenamento della cache si chiama "UDP Source Port Randomization", ma questa difesa ha richiesto, nel 2008, l'aggiornamento di tutti i software DNS.

Il software DNS, come tutti i software per infrastrutture Internet, deve essere aggiornato periodicamente per correggere i difetti noti quando vengono scoperti e riparati dal fornitore del software. Si raccomanda sempre un attento monitoraggio per rilevare condizioni anomale nelle infrastrutture online, ma tale controllo è di fondamentale importanza dopo ogni aggiornamento del software, dal momento che un aggiornamento potrebbe risolvere alcuni difetti e introdurne altri.

Anche la sicurezza contestuale deve essere menzionata. Se i software DNS fossero completamente privi di bug, sarebbe comunque necessario rendere sicuro, aggiornare e monitorare il sistema operativo compresi eventuali sistemi di virtualizzazione così come router, switch, firewall e sistemi di rilevamento / prevenzione delle intrusioni. La RFC 2196, il Site Security Handbook, fornisce una panoramica di questi problemi.

MIGLIORI PRATICHE:

1. Sostenere la diffusione mondiale di DNSSEC, per mettere in sicurezza la distribuzione dei dati DNS. Questo include la firma di tutte le zone di autorità con DNSSEC, e consentire la convalida DNSSEC in tutti i server DNS ricorsivi.
2. Utilizzare TSIG per tutti gli aggiornamenti DNS on-line e per le operazioni server-to-server di "trasferimento di zona", per garantire l'autenticità e l'autorizzazione.
3. Mantenere il software DNS aggiornato alla versione più recente raccomandata dal fornitore e monitorare l'infrastruttura DNS per anomalie sempre, ma soprattutto dopo l'installazione di una patch del fornitore.
4. Fornire un documento di Migliori Pratiche riguardante la politica di sicurezza dei risolutori DNS, per educare i gestori di rete e di sistema.

MINACCE MALAWARE VERSO IL DNS

Il metodo "DNS Changer" è un altro modo per falsificare le risposte DNS. Questo malware modifica il computer di ogni vittima in modo da cambiare i risolutori DNS utilizzati, sostituendo quelli controllati dal malfattore a quelli dell'utente per i principali ISP. Il malfattore fornisce quindi selettivamente risposte falsificate ogniqualvolta questo porterà entrate supplementari.

Il malware DNS Changer non funziona solo sui computer degli utenti, ma anche sui router casalinghi o delle piccole imprese. Il vantaggio del truffatore nel modificare le impostazioni del router è che il cambiamento sarà probabilmente più longevo e riguarderà tutti i computer, telefoni, iPad e altri dispositivi in casa o in ufficio – includendo potenzialmente i dispositivi di controllo della casa raggiungibili tramite web, come termostati, macchine fotografiche, cornici di fotografie, reti wireless e cablate, ecc. Il router può essere compreso nel servizio a banda larga fornito oppure può essere un dispositivo aggiuntivo acquistato e installato dall'utente.

L'FBI ha lavorato con il settore privato al fine di privare i criminali informatici “DNS Changer” delle loro risorse (e la loro libertà). [xxxix] Gli indirizzi IP utilizzati dai risolutori compromessi sono stati re-indirizzati a quello corretto, che ha funzionato per un paio di mesi, mentre gruppi di volontari hanno notificato gli ISP e gli utenti che sono stati colpiti. Nota: la strategia di base usata dai criminali DNS Changer funzionerebbe altrettanto bene se venisse riprovata – tutte le necessarie vulnerabilità sottostanti sono ancora presenti nelle apparecchiature talmente diffuse che non possono essere aggiornate dal fornitore.

Il rilevamento del traffico DNS indirizzato in maniera malevola può essere condotto a livello di provider attraverso il monitoraggio del traffico DNS in uscita del cliente che va verso un sistema di risoluzione diverso da quello che essi forniscono. Si noti che è molto comune per gli utenti tecnicamente avanzati - o quelli che intenzionalmente utilizzano un servizio di DNS diverso - inviare il loro traffico DNS altrove. Un'attenta progettazione dei sistemi di rilevamento è necessaria per evitare falsi positivi.

In futuro, gli utenti potrebbero essere indotti a passare a risolutori DNS di un malfattore tramite ingegneria sociale o qualche adescamento. Ad esempio, se i risolutori dei provider sono tenuti a negare l'accesso ad alcuni nomi DNS (come ad esempio quelli che forniscono contenuti pirata o in qualche modo illegali), gli utenti potrebbero rispondere alle offerte che promettono accesso DNS senza censure. Ci sono molte ragioni legittime per consentire agli utenti di scegliere il loro servizio risolutore DNS senza censura o interferenze.

MIGLIORI PRATICHE:

1. Educare il pubblico sui pericoli insiti nei cambiamenti dei risolutori DNS, per limitare gli attacchi di ingegneria sociale.
2. Incoraggiare gli operatori di rete a condividere i feed anonimi delle maggiori cache DNS non locali interrogate dalle loro reti, per identificare possibili risolutori DNS malevoli.
3. Fornire il feed a tutti i ricercatori anti-abusi verificati per aiutare il rilevamento di servizi che hanno ingannato gli utenti o stanno falsificando le risposte DNS e distinguerli dai servizi DNS legittimi
4. Sviluppare metriche basate su questi dati aggregati per contribuire ad identificare i criminali informatici e consentire azioni legali, per aggiornare una lista nera di risolutori malevoli, e per mettere in atto operazioni di mitigazione coordinate come avvenuto con DNS Changer.
5. Stabilire le migliori pratiche per l'anonimizzazione sufficienti ad evitare il collegamento tra utenti originali, i loro fornitori di servizi Internet e le attività sui DNS, per evitare ritorsioni contro gli utenti che aggirano la censura in quanto questo porterebbe gli utenti ad usare risolutori DNS più difficili da rilevare ma potenzialmente compromessi.

ATTACCHI TRAMITE ABUSO DI SERVIZI DNS

La facilità con cui i criminali informatici possono registrare e utilizzare nuovi domini li aiuta a condurre le loro frodi. Fornire informazioni false sull'identità e spesso utilizzando credenziali finanziarie rubate rende difficile rintracciare i veri proprietari dei domini che vengono utilizzati per commettere frodi. L'onere di rilevare un uso malizioso dei nomi di dominio è a carico dei ricercatori anti-abusi, spesso molto tempo dopo che l'attività dannosa è iniziata, o talvolta conclusa. L'onere di mitigare domini malevoli spetta ad ogni azienda che fornisce l'accesso ad Internet agli utenti – sia attraverso le richieste per arrestare attività dannose, o attraverso la spesso lenta propagazione di elenchi dei blocchi di dominio. Gli elenchi dei blocchi sono necessari perché le richieste per

reindirizzare, sospendere o cancellare i nomi di dominio sono spesso ignorate.

I criminali informatici abusano dei servizi di registrazione domini, utilizzando carte di credito rubate per registrare domini, registrando molti domini con grande velocità utilizzando l'automazione, registrando i domini tramite rivenditori o fornitori di privacy / proxy che non sono veloci nelle risposte o che sembrano permettere attività dannose, e passando attraverso molteplici domini, alcuni dei quali possono essere usati pochi minuti o addirittura secondi dopo la registrazione. I ricercatori degli abusi sono in genere in grado di monitorare solo i dati riguardanti le nuove registrazioni DNS tramite istantanee ogni 24 ore. Gli operatori delle block list hanno bisogno di tempo per riconoscere i domini malevoli e quindi per propagare le informazioni di reputazione dopo che il malfattore ha effettuato l'atto doloso.

I cybercriminali possono creare qualsiasi sottodominio basato su domini di loro proprietà, come ad esempio nomebanca.ssl-cgi.nomecriminale.com. Non vi è alcun limite al numero domini di questo tipo che possono creare - e senza alcun costo. Ingannare gli utenti non richiede un marchio, solo qualcosa che sembri plausibile. Nomi come ordine-sicuro.verificato.example.com sono accettati dalla maggior parte degli utenti, dato che sembrano le altre simili a quelli che hanno sempre visto.

Alcune entità effettivamente aiutano a commettere abusi sugli IP con la creazione di nomi di dominio che possono indurre in errore i consumatori. Questi servizi creano nomi di dominio che volutamente sembrano quelli dei marchi utilizzando errori di battitura, come SEARZ con la lettera 'Z' al posto della lettera 'S', o PAYPA1 con la cifra '1' al posto della lettera 'L'. Anche se questi domini non venissero mai utilizzati in una campagna di phishing, ce ne sono talmente tanti (milioni) che rendono difficile per i ricercatori distinguere i “typosquatter” relativamente innocui dalla prossima attività pericolosa prima che accada.

In aggiunta, gli aggressori possono falsificare i nomi di dominio attraverso altre tecniche, tra cui:

- Compromettendo le credenziali di accesso del registrante al pannello di controllo del registro (rubando la password che i clienti utilizzano per accedere al loro sito gestione del dominio),
- Compromettendo i sistemi del registrar al fine di rubare tutte o alcune delle password (note come codici EPP o auth-codes) necessarie per trasferire i nomi di dominio da un registrar ad un altro, e
- Compromettendo i name server o il database DNS del registrante al fine di alterare i dati nel domino della vittima in situ, senza reindirizzamento a monte.

MIGLIORI PRATICHE:

1. I registri dei nomi di dominio che operano nello spazio dei nomi sia dei domini di primo livello generici (gTLD) che nazionali, nonché i registrar con i quali fanno affari, dovrebbero realizzare e strettamente supervisionare programmi del tipo 'Know Your Customer'

(Conosci il tuo Cliente) per prevenire gli abusi di assegnazione del dominio. Ciò consentirà loro di determinare se e quando dovrebbero evitare di essere in affari con un registro, un registrar, un rivenditore o un fornitore di servizi di privacy / proxy.

2. Tutti i registri dei nomi di dominio, registrar, rivenditori e fornitori di servizi di privacy / proxy dovrebbero implementare obbligatoriamente HTTPS ed una autenticazione a più fattori per ridurre il rischio di furto di credenziali di account dei clienti e per proteggere meglio le sessioni di transazione dei loro clienti.
3. I registri dei nomi di dominio e i registrar dovrebbero prendere in considerazione accordi di cooperazione o protocolli d'intesa con le organizzazioni che aiutano a proteggere i consumatori, come LegitScript e l'Anti-Phishing Working Group (APWG). Attraverso la creazione di livelli predefiniti di fiducia, le segnalazioni di abuso ricevute da queste organizzazioni possono essere considerate dai registri o registrar in un modo molto più veloce e più efficace, come il programma di sospensione dei domini malevoli (Malicious Domain Suspension Program) dell'APWG.
4. I registri dei nomi di dominio e i registrar dovrebbero controllare rigorosamente le carte di credito rubate utilizzate per le registrazioni, per evitare che i domini malevoli vengano registrati.
5. Imporre obblighi di legge (nelle loro giurisdizioni nazionali) e contrattuali che i fornitori di servizi di registrazione domini, tra cui tutti i registri, i registrar, i rivenditori e fornitori di servizi di privacy / proxy devono rispettare, per quanto riguarda l'agire alle segnalazioni di abuso.
6. Per i servizi privacy / proxy, vi è un urgente bisogno di programmi di accreditamento da attuare e far rispettare. In questo modo si chiarirebbero le norme e i processi per la gestione delle richieste di *trasmettere*, passando le comunicazioni al cliente sottostante, e *rivelare*, divulgando l'identità del cliente. Questo vale per tutti i servizi di privacy e proxy, indipendentemente dal fatto che operino nello spazio gTLD o ccTLD e indipendentemente dal fatto che siano di proprietà, gestite o fatte funzionare da un registro o un registrar.
7. I registri e registrar di entrambi gli spazi gTLD e ccTLD dovrebbero evitare di fare affari con i fornitori di servizi sulla privacy / proxy non coperti da un programma di accreditamento.
8. Prima di elaborare le richieste per registrare nuovi nomi di dominio o accettare trasferimenti in entrata di domini, registrar e operatori ccTLD che offrono servizi di registrazione direttamente al pubblico dovrebbero verificare la reputazione di alcuni elementi nei dati di registrazione, come ad esempio:
    a. gli indirizzi e-mail utilizzati dal dichiarante, titolare del conto o uno qualsiasi degli altri contatti Whois,
    b. l'indirizzo IP da cui vengono richieste le transazioni,
    c. i nameserver che i clienti vogliono impostare per i loro nomi di dominio,
    d. gli indirizzi postali del dichiarante, e

e. un campione statisticamente valido di nomi di dominio già registrato dallo stesso cliente.

   A titolo di esempio, un servizio di convalida reputazione è fornito senza costi da "The Secure Domain Foundation" che consente ai registrar e registri interessati di decidere di rifiutare di creare nuovi nomi di dominio, o accettare trasferimenti in entrata, se uno degli elementi ha una cattiva reputazione, che indica una significativa recente attività malevola.

9. Migliorare algoritmi di reputazione in modo da includere l'età del dominio: i domini vecchi più di un anno, hanno meno probabilità di essere domini "usa e getta", alcuni responsabili dell'accreditamento della posta elettronica impediscono ai clienti di utilizzare domini creati da meno di un mese, ed esaminare i domini con meno di un giorno di vita è attualmente un modo efficace per identificare attività malevole.
10. Dal momento che i falsificatori di domini utilizzano indirizzi IP che sono di solito diversi da quelli utilizzati dai registranti, i registrar e i rivenditori dovrebbero abilitare il tracciamento degli indirizzi IP utilizzati per le attività degli account. Se per l'account di un cliente viene effettuato un accesso da un nuovo indirizzo IP, il registrar o il rivenditore devono informare sia il registrante che il contatto amministrativo del nome di dominio in questione.
11. Estendere il miglioramento del browser e le attività di educazione degli utenti a riconoscere i segnali del browser per la convalida estesa dei certificati ("barra verde") per evitare confusione con i siti che utilizzano termini come "sicuro" o "SSL".
12. Educare le imprese ad inviare agli utenti notifiche difficili da imitare per scoraggiare il phishing e il social engineering.
13. Per i siti e i software che utilizzano gli elenchi dei blocchi di dominio, incoraggiare un approccio multi-strato con una varietà nei tipi di elenchi di blocchi, compresi i metodi di blocco di preventivi, nonché gli elenchi dei blocchi più vecchi, ma reattivi, per migliorare l'efficacia del blocco.
14. Sostenere i progetti di DNS passivi come il "Security Information Exchange" (SIE) di Farsight Security Inc (FSI) che forniscono un allarme preventivo sia ai ricercatori accademici che commerciali circa sottodomini malevoli attivamente in uso.
15. Considerare tecnologie di firewall DNS come la "Response Policy Zones" (RPZ), un mercato aperto multi-fornitore multi-consumatore che fornisce raccomandazioni sulle politiche risoluzione DNS agli operatori DNS ricorsivi. (Vedere http://dnsrpz.info/).

ATTACCHI DNS VERSO SERVER WEB E DI ALTRE TIPOLOGIE

I criminali informatici sfruttano la reputazione dei domini legittimi entrando nei loro server web e depositando i file malevoli che infettano il dominio legittimo presente nell'URL. (Questa tecnica è immune agli elenchi dei blocchi di dominio a meno che tali elenchi non siano disposti ad elencare i domini legittimi che servono contenuti dannosi, bloccando così alcuni contenuti legittimi insieme a quelli dannosi.)

I criminali informatici utilizzano re-indirizzamenti web per presentare prima un dominio con una buona reputazione, quindi reindirizzare l'utente al sito di destinazione malevolo. Questi individui utilizzano più livelli di reindirizzamento e di recente anche reindirizzamento verso URL con indirizzi IP numerici, invece che nomi di dominio.

Il successo di tali tecniche dipende metodi di rilevamento inadeguati che sono solo in grado di riconoscere tali attacchi se gli utenti non "agiscono come una vittima farebbe" seguendo i re-indirizzamenti. Purtroppo alcuni addetti al marketing complicano ulteriormente il problema utilizzando più livelli di reindirizzamento per monitorare la risposta dei clienti alle e-mail marketing. I servizi di URL shortener sono spesso abusati e utilizzati per reindirizzare da un dominio noto come bit.ly al sito web malevolo del criminale informatico. E' difficile per un utente differenziare tra i milioni di URL bit.ly legittimi utilizzati per accorciare un indirizzo web lungo per post di Twitter, quelli che porteranno a malware o, per esempio, ad un annuncio per la vendita prodotti farmaceutici illegali.

Recentemente, l'ICANN stesso è stato vittima di un gruppo di hacker che ha ottenuto l'accesso dell'account ICANN a Register.com. In questo caso, gli aggressori hanno alterato le configurazioni DNS di diversi domini (icann.net iana-servers.com, icann.com, e iana.com) e hanno reindirizzato il traffico dei visitatori verso un sito web deturpato.

MIGLIORI PRATICHE:

1. Realizzare e mantenere un sistema che blocca i domini legittimi compromessi che servono contenuti dannosi, che dia una rapida notifica, ripeta il test e provveda al delisting, e fornisca assistenza per migliorare la sicurezza su tutti i server web relativi al sito compromesso.
2. Incoraggiare i servizi URL Shortener affinché controllino e ricontrollino tutti i redirect nella catena per ogni reindirizzamento che effettuano, e che lavorarino con più fornitori di servizi di protezione dagli abusi al fine di individuare nuovi abusatori.
3. Sviluppare l'educazione e le risorse per gli utenti sia del settore che finali su come identificare ed evitare servizi di URL Shortener che non mettono in pratica misure adeguate per prevenire gli abusi
4. Migliorare l'efficacia dei test di reputazione degli URL, tra le altre cose, includendo i reindirizzamenti, usando dei test che simulino un utente reale e sviluppando politiche riguardanti la profondità massima di reindirizzamento, il tutto per limitare l'abuso dei servizi di URL shortener e altri servizi di reindirizzamento URL vulnerabili.

ATTACCHI DI INDIRIZZI IP

Gli attacchi di indirizzi IP si dividono in due categorie generali, le e-mail che mentono sui loro indirizzi IP (spoofing), e le reti che utilizzano intervalli di indirizzi IP che non sono autorizzati ad utilizzare (annuncio non autorizzato).

FALSIFICAZIONE DELL'INDIRIZZO IP (IP SPOOFING)

Ogni pacchetto di dati inviati via Internet include gli indirizzi IP "sorgenti" del computer da cui è stato inviato e l'indirizzo del computer a cui è destinato. E' possibile per un computer ostile di mettere un falso (spoofed) indirizzo di origine del traffico in uscita. Per le operazioni nelle quali la destinazione invia pacchetti di ritorno verso l'indirizzo di origine, come ad esempio il DNS, questo può creare traffico indesiderato al vero indirizzo che è stato falsificato. E' facile inviare piccole richieste DNS che portano ad un gran numero di risposte, causando denial-of-service all'indirizzo falsificato.

MIGLIORI PRATICHE:

1. Gli ISP e le reti di transito dovrebbero filtrare la posta in arrivo, tenendo traccia della gamma di indirizzi assegnati ad ogni rete del cliente, e scartando il traffico proveniente da indirizzi sorgente al di fuori della gamma assegnata, per evitare che i loro clienti inviino traffico con indirizzi contraffatti. Questo è generalmente noto come BCP 38[xl], a seguito un documento IETF sulle migliori pratiche correnti. La BCP 84, un'altra migliore pratica corrente IETF, raccomanda che i fornitori a monte di connettività IP filtrino i pacchetti in entrata verso le loro reti da parte dei clienti a valle, e scartino tutti i pacchetti che hanno un indirizzo di origine che non è assegnato a quel cliente. [xli]

2. Incoraggiare una pratica universale di filtraggio in ingresso per tutte le reti dei clienti o nodi connessi.

ANNUNCI NON AUTORIZZATI (ROUGE)

Ogni rete può annunciare tramite BGP i propri intervalli di indirizzi IP. Le reti ostili possono annunciare intervalli di rete che non sono autorizzati ad utilizzare. Ciò può portare a reinstradamento e deviazione del traffico destinato alla rete vera e propria, oppure può consentire il traffico nascosto ("stealth"), annunciando una serie di indirizzi, effettuando un attacco, e poi ritirando l'annuncio. A meno che le vittime siano a conoscenza dell'annuncio non autorizzato, essi incolperanno il legittimo proprietario degli indirizzi.

MIGLIORI PRATICHE:

1. Gli operatori di rete dovrebbero implementare il filtraggio in ingresso definito nella BCP 84 [xlii] (come indicato sopra), per il quale gli annunci BCP in entrata da parte dei clienti e colleghi sono limitati ad un elenco esplicito di reti conosciute da assegnare a quel cliente o nodo.
2. Gli ISP dovrebbero cercare di, per quanto possibile, implementare BGPSEC (sicurezza BGP) per proteggere crittograficamente gli annunci di rotta e impedire la pubblicazione dei dati non autorizzati.

RUBARE INTERVALLI DI INDIRIZZI

Agli albori di Internet, l'assegnazione degli indirizzi è stata spesso fatta in modo abbastanza informale, con i dati incompleti. Di conseguenza, risulta assegnato un notevole spazio di indirizzamento ereditato (*legacy*) che può essere obsoleto, sia perché le organizzazioni hanno dimenticato l'indirizzo che hanno usato, oppure perché tali entità non esistono più. I criminali informatici hanno approfittato di questi indirizzi abbandonati falsificando i documenti o ri-registrando domini abbandonati utilizzati nelle e-mail, per ottenere il controllo dello spazio di indirizzamento legacy.

MIGLIORI PRATICHE:

1. I Registri Internet regionali dovrebbero realizzare e seguire le procedure per verificare l'identità dei proprietari presunti dello spazio legacy, per impedire ai criminali informatici di ottenere il controllo dello spazio di indirizzamento. ARIN, il RIR per il Nord America, ha procedure dettagliate per questo. [xliii]

RIFERIMENTI

- Wikipedia, Discussione su DNSSEC: http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensionshttp://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- RFC 2196, *Site Security Handbook*, B. Fraser, Ed., September 1997, http://www.rfc-editor.org/info/rfc2196
- RFC 4034 *Resource Records for the DNS Security Extensions*. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005, http://www.rfc-editor.org/info/rfc4034
- RFC 4035 Protocol Modifications for the DNS Security Extensions. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005, http://www.rfc-editor.org/info/rfc4035
- US CERT Vulnerability Note VU#800113, "Multiple DNS implementations vulnerable to cache poisoning", http://www.kb.cert.org/vuls/id/800113/http://www.kb.cert.org/vuls/id/800113/
- DNS Changer Working Group, http://www.dcwg.org/http://www.dcwg.org/
- Brian Krebs, "A Case of Network Identity Theft", http://voices.washingtonpost.com/securityfix/2008/04/a_case_of_network_identity_the_1.htmlhttp://voices.washingtonpost.com/securityfix/2008/04/a_case_of_network_identity_the_1.html
- Open Resolver Project, http://openresolverproject.org/http://openresolverproject.org/
- M[3]AAWG Senders Best Practices, https://m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

FCC

- FCC CSRIC III Working Group 4 reports on BGP Security Best Practices: http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

MINACCE PER I DISPOSITIVI MOBILI E LA VOCE

LO SCENARIO DEI DISPOSITIVI MOBILI

Con l'avvento degli smartphone e dei mercati delle applicazioni per i dispositivi Android, Apple, Windows e BlackBerry, i consumatori utilizzano sempre di più i loro dispositivi mobili per accedere ai conti on-line, fare acquisti ed effettuare altre operazioni finanziarie. Gli smartphone rappresentano il 70 per cento dei circa 1,85 miliardi di telefoni cellulari venduti nel mondo nel 2014[xliv], con Android e iPhone che sono i dispositivi predominanti attualmente in uso. Anche i tablet, che rendono la linea di demarcazione tra il telefono e il computer tradizionale più sfocata, sono diventati una realtà significativa in questo campo. Le vendite al dettaglio per i dispositivi mobili, tra cui i tablet, sono aumentate dall' 11 per cento del mercato globale e-commerce nel 2011[xlv] al 13 per cento nel 2014[xlvi]

A livello globale, ci sono circa 3,7 miliardi di utenti attivi di telefoni cellulari[xlvii], che superano il 50 per cento della popolazione mondiale di 7,3 miliardi[xlviii], e i telefoni cellulari rappresentano l'accesso a Internet primario per gran parte del mondo. Nel quarto trimestre del 2014 i venditori hanno spedito oltre 500 milioni di unità mobili in tutto il mondo[xlix].

MERCATI DI APP

A differenza del mercato software per i PC, dove le principali applicazioni sono sviluppate da un certo numero di fornitori ben noti e di fiducia e gli utenti sono meno propensi a installare applicazioni provenienti da fonti meno attendibili, l'ecosistema delle applicazioni mobili incoraggia gli utenti finali a caricare un gran numero di applicazioni a basso costo da fornitori più piccoli e spesso meno affidabili, tra cui una imprese unipersonali. In molti paesi, la maggior parte delle applicazioni sono ottenute da mercati di app con sicurezza inadeguata, che dispongono di applicazioni cariche di malware. In altri paesi, gli utenti possono essere inizialmente limitati a installare applicazioni solo sviluppate da chi ha sviluppato il sistema operativo del telefono o da mercati app approvati dal gestore; tuttavia, gli utenti possono sovrascrivere le impostazioni, consentendo l'accesso a qualsiasi mercato di app. I principali fornitori di sistemi operativi dei telefoni, tra cui, Google, Apple, Microsoft e RIM gestiscono mercati applicativi ad alto volume con maggiore sicurezza. Apple, per esempio, ha 1,4 milioni di applicazioni nel suo App Store, generando un cumulativo di $ 25 miliardi di fatturato per sviluppatori di app e giochi fino ad oggi. Tuttavia, la scala dei mercati app più sicuri rende estremamente difficile evitare che il malware di tanto in tanto possa essere distribuito. Così come l'e-commerce è migrato verso l'ambiente cellulare, i malfattori e truffatori sono stati pronti ad adeguarsi.

MINACCE PARTICOLARI E MIGLIORI PRATICHE

SICUREZZA DELL'APP STORE

Gli smartphone possono essere compromessi con l'installazione di un nuovo software, spesso ottenuto da un negozio controllato dal produttore del sistema operativo del telefono (OS). Nel 2014, Symantec ha rilevato che il 17 per cento (oltre 160 mila) delle applicazioni Android erano in realtà malware sotto mentite spoglie[l]. In una revisione delle 100 applicazioni sanitarie in App Store, il 20 per cento trasmetteva le credenziali utente senza crittografia, oltre la metà (52 per cento) non aveva visibile nessuna politica sulla privacy e, in media, ogni app contattata cinque domini Internet (in genere un mix di servizi pubblicitari e di analisi).[li]

Alcuni fornitori di sistemi operativi e di negozi di app hanno la capacità di rimuovere le applicazioni dannose dal telefono dell'utente se questa applicazione è stata originariamente ottenuta dalla loro negozio app. Altre applicazioni dannose saranno respinte prima di entrare in negozio se violano le politiche di sicurezza stabilite dal negozio stesso.

Apple ha messo in atto restrizioni ancora maggiori per le applicazioni e per gli sviluppatori prima di consentire l'accesso al loro App Store. Il negozio Google Play ha una politica di accettazione più aperta e fa più affidamento sulla rimozione di applicazioni accettate che si rivelano essere dannose e / o in violazione delle politiche del negozio.

Quando un consumatore acquista uno smartphone, l'accesso agli app store non ufficiali è in genere disabilitato; il telefono è limitato ad una ristretta cerchia di negozi app "ufficiali" (ad esempio, del produttore del sistema operativo e dell'operatore di telefonia mobile). I dispositivi mobili che utilizzano il sistema operativo Android hanno una impostazione chiamata "Origini sconosciute" con una casella di controllo per autorizzare l'installazione di applicazioni provenienti da altre fonti. L'utente può riconfigurare i telefoni Android per consentire la connessione ad app store non ufficiali o alternativi. I dispositivi Apple richiedono un processo tecnicamente più difficile denominato "jailbreaking"; tuttavia, agli utenti meno esperti, il jailbreaking viene offerto come un servizio a basso costo in molti punti vendita. Anche per accedere ad app store alternativi legittimi come l'Amazon Appstore, questa opzione può avere bisogno di essere selezionata. Purtroppo in seguito il telefono è aperto all'installazione di eventuali origini sconosciute. Gli utenti possono quindi essere più facilmente indotti a installare malware. Lo scrittore di malware ottiene un pass gratuito senza supervisione da qualsiasi negozio ufficiale app una volta che l'accesso agli app store non ufficiali viene abilitato.

Ci sono anche nuovi modi per i truffatori per eludere le restrizioni degli app store anche se il telefono è configurato utilizzare solo l'app store ufficiale. I browser web dei dispositivi mobili possono essere usati per installare applicazioni mobili HTML5, che visualizzano una icona sulla schermata iniziale del dispositivo che assomiglia ad un app installata da un app store. Gli aggressori possono sfruttare le vulnerabilità nel browser che viene fornito con il dispositivo mobile o in browser alternativi che l'utente può scegliere di installare. I collegamenti dal browser alle funzioni native del dispositivo come fotocamera, microfono, la tastiera e la posizione geografica possono

essere utilizzati da un criminale per ottenere i dati personali e le attività in corso degli utenti del dispositivo mobile.

Il login con username / password che ogni dispositivo mobile utilizza per accedere all'app store e autorizzare gli acquisti è un punto di vulnerabilità significativo. Una volta in possesso di queste credenziali, i criminali possono provocare perdite finanziarie e installare spyware. Entrambi i sistemi operativi mobili di Apple e Google attualmente richiedono lo stesso nome utente e password come chiavi di accesso per l'app store e tutti gli altri servizi tra cui computer i portatili, l'archiviazione di file sul cloud, i contatti, il calendario e la posta elettronica. Se un username e una password un tempo avrebbero consentito al malintenzionato di accedere solo all'account di posta elettronica di un abbonato, ora le stesse credenziali forniscono l'accesso all' app store. In più casi, gli utenti si sono trovati i computer portatili e i telefoni senza più nessun dato dopo che i criminali hanno ottenuto queste informazioni chiave. Diverse terze parti offrono una protezione anti-virus per alcuni cellulari e cercano di testare tutte le nuove applicazioni presenti negli app store contro attività pericolose o dolo.

MIGLIORI PRATICHE PER IL SETTORE E IL GOVERNO PER GLI APP STORE:

1. "Neutralità dell'applicazione": Consenti agli utenti, agli operatori di rete o ad altri soggetti di fiducia di specificare esplicitamente app store di "fiducia" aggiuntivi, e forse il livello di fiducia associato a ciascuno. Questo consente ai consumatori di scegliere tra altri app store degni di fiducia senza esporli al rischio di scaricare app a provenienti da fonti sconosciute.
2. Identificare applicazioni con potenziale malevolo tramite scansioni di sicurezza rigorose prima di consentirle nell'app store, invece di basarsi sui reclami successivi.
3. Fornire avvertimenti, controlli e formazione agli utenti per ridurre i casi di utenti ingannati a seguire le istruzioni fraudolente per oltrepassare le misure di sicurezza.
4. Migliorare le politiche di sicurezza per i meccanismi di reimpostazione della password degli app store per evitare che i criminali possano ottenere le credenziali agli app store che non appartengono a loro.
5. I telefoni possono essere bloccati per accedere solo agli app store ufficiali come forma contro la competizione. Mentre i consumatori possono essere ben protetti con questo modello, esso invita i consumatori ad utilizzare soluzioni che introducono falle di sicurezza (ad esempio, il jailbreaking, il "rooting" o lo sblocco i dispositivi). Le politiche che permettono o assistono nel blocco dell'app-store devono essere soppesate con l'impatto delle falle di sicurezza create dal sblocco.
6. Incoraggiare gli app store a diventare membri di centri di analisi sulle minacce online e di botnet, in modo che possano beneficiare di analisi, avvisi e segnalazioni provenienti da questi centri. Le applicazioni dannose possono quindi essere rilevate, contrassegnate ed eliminate nel modo più rapido possibile.
7. Fornire meccanismi che consentono agli utenti di segnalare le applicazioni potenzialmente dannose.

MALWARE PER DISPOSITIVI MOBILI

Le applicazioni dannose, conosciute come malware per dispositivi mobile, esistono per Android, iOS, Windows Phone, Symbian (Nokia) e dispositivi Blackberry. Attualmente la maggior parte dei malware mobile è indirizzato verso la piattaforma Android in aree con abbondante uso di app store non ufficiali.

La maggior parte del malware è - o sembra essere - un'applicazione utile, ed è distribuita su siti web o attraverso app store non ufficiali. Spesso, i promotori di malware corrompono applicazioni legittime inserendo del codice "cavallo di Troia". Pertanto, gli utenti possono installare queste applicazioni modificate, inconsapevoli che contengono codice dannoso. I criminali stanno utilizzando sempre di più la pubblicità digitale come veicolo per diffondere malware; questo è noto come “Malvertising”. Inoltre 2014 ha visto la nascita del "SMS Worm " che si propaga tramite SMS attraverso elenchi di contatti telefonici infetti. I destinatari sono indotti a cliccare sul link malevolo contenuto all'interno dell’ SMS, che porta allo stesso exploit. Se installano l'exploit poi loro contatti riceveranno lo stesso SMS dannoso rendendo questo vettore di attacco altamente virale.

In genere il malware esegue azioni che generano entrate economiche per gli attaccanti. Gli schemi di monetizzazione diretta causano la perdita finanziaria diretta alla vittima e comprendono applicazioni dannose che possono eseguire una vasta gamma di funzioni, tra cui: l'invio di messaggi SMS premium ad un numero registrato dagli aggressori; il download di contenuti a pagamento (pay-per-download); il clic sui collegamenti di tipo pay-per-click; l’ effettuare chiamate in uscita ai numeri di telefono a pagamento; l’intercettazione delle credenziali di online banking e la richiesta di un pagamento come riscatto per sbloccare i dispositivi delle vittime. Gli aggressori possono anche generare entrate indirettamente attraverso la raccolta di numeri di telefono per lo spam SMS, raccogliendo i dati del dispositivo e degli utenti per il marketing, per la visualizzazione di annunci pubblicitari, per la vendita di applicazioni spyware commerciali e utilizzare il dispositivo infetto per generare valute criptate. Inoltre, le applicazioni spyware commerciali consentono a chi le usa di monitorare una persona di interesse e raccogliere i dati utente e del dispositivo come i messaggi SMS, le e-mail, la posizione e i registri delle chiamate.

Qui di seguito sono elencati degli esempi degni di nota di malware per Android, BlackBerry e iOS.

Oleg Pliss Attack (2014): L'attacco Oleg Pliss utilizza un attacco compromesso iCloud per bloccare gli utenti dall’accesso al loro iPhone.

Slocker.A (2014): Slocker.a è apparentemente il primo esempio di crittazione file ransomware (con l’obiettivo di chiedere un riscatto) per dispositivi mobili. Crittografa i file di dati utente su dispositivi Android, e quindi richiede un pagamento per la chiave di decrittazione.

SMScapers (2013 – ad oggi): Questo malware appare sotto le spoglie di un app per adulti ed è diffusa attraverso spazi pubblicitari a pagamento per

i dispositivi mobili. Addebita di nascosto gli utenti i costi di invio di un SMS verso un numero premium e sopprime la notifica per i relativi SMS in arrivo. La campagna ha colpito prevalentemente il Regno Unito anche se l'applicazione della normativa ha contribuito ad un netto calo di tale attività. La campagna è stata suddivisa in venti diversi soggetti giuridici aggiungendo quindi complessità al processo di applicazione. La campagna continua ad essere viva in altri 15 paesi.[lii,liii]

Worm.Koler (2014 ad oggi): Il 2014 ha visto l'ascesa di ransomware per Android, dove sono emersi numerosi esempi quali ScareMeNot, ScarePackage e ColdBrother. Gli Stati Uniti hanno visto Worm.Koler diffondersi via SMS ai contatti memorizzati su cellulari infetti. L'exploit blocca anche le vittime dall'accesso al loro dispositivo con un falso allarme dell'FBI affermando che dei contenuti illegali sono stati trovati nel proprio cellulare. Essi sono quindi incoraggiati a pagare una multa per evitare accuse penali e liberare i loro cellulari.

DeathRing (2014 to present): DeathRing prevalentemente si rivolge all'Asia ed è il malware che tenta di sollecitare dati sensibili alle vittime mediante la visualizzazione di un SMS falso. Il vettore di attacco è unico in quanto il malware sembra essere installato in fabbrica suggerendo che i criminali si sono infiltrati ad un certo punto della catena di fornitura.

MIGLIORI PRATICHE PER IL SETTORE E IL GOVERNO PER PROTEGGERE DAL MALWARE PER MOBILE:

1) Educare i consumatori, utilizzando annunci di servizio pubblico, pagine web, opuscoli e altri mezzi di comunicazione per effettuare le seguenti operazioni:
   a) Ottenere applicazioni solo da mercati di applicativi affidabili che eseguono verifiche sulle applicazioni o dagli sviluppatori o direttamente da ben conosciuti fornitori di applicazioni.
   b) Guardare con attenzione e capire le schermate relative alle autorizzazioni, ai contratti di licenza dell'utente finale, alle politiche sulla privacy e ai termini del contratto, durante l'installazione di nuove applicazioni.
   c) Mantenere le restrizioni di sicurezza di default sul dispositivo, e non effettuare il jailbreaking del dispositivo (il jailbreaking è discusso in dettaglio sotto).
   d) Installare software per la localizzazione remota e per il blocco, in modo da facilitare il recupero e la protezione dei dati nei telefoni smarriti o rubati. Ad esempio, l'IMEI (International Mobile Equipment Identity) è un codice di 15 o 17 cifre che identifica univocamente un telefono cellulare. Il codice IMEI può consentire ad una rete GSM o UTMS (Universal Mobile Telecommunications Service) di impedire ad un telefono smarrito o rubato di effettuare chiamate.
   e) Installare ed eseguire il software di sicurezza per dispositivi mobili su tutti i terminali.

2) Sviluppare servizi per permettere ed incoraggiare i consumatori a praticare la segnalazione di applicazioni sospette.
3) Incoraggiare, automatizzare e facilitare il backup dei dati del telefono sul cloud e / o su supporti di memorizzazione personali (ad esempio, un PC).
4) Valutare l'uso di soluzioni di sicurezza per dispositivi mobili come i browser sicuri, le soluzioni di gestione dei dispositivi mobili (MDM), ambienti di test ("sandbox") per dispositivi mobili aziendali e applicazioni di prevenzione della perdita dei dati per ridurre al minimo il rischio di infezione e l'impatto conseguente.

   Un ottimo esempio di educazione dei consumatori sulle migliori pratiche per cellulari è stato creato da Ofcom e può essere trovato qui:

   http://consumers.ofcom.org.uk/files/2014/1394750/using-apps-safely-and-securely.pdf

MINACCE MISTE

I dispositivi mobili sono ora impiegati nel processo di autenticazione a più fattori per accessi ad account molto importanti. Un esempio della minaccia mista relativa all'autenticazione a due fattori occorre quando un utente visita un sito web finanziario sul proprio computer desktop e accede con un nome utente e una password, come è sempre stato fatto in passato. Ma ora la banca richiede un ulteriore passo all'utente prima di accedere al proprio account: si riceve una chiamata o un messaggio di testo sul proprio telefono cellulare con un codice che l'utente quindi digiterà nel browser Web del computer desktop. Questo passo in più è stato aggiunto perché molti computer desktop degli utenti sono infettati da malware che ha fornito la propria password di accesso ai servizi bancari ai criminali. I criminali hanno dimostrato di essere persistenti nell'attaccare ogni nuovo metodo di protezione. Ora hanno bisogno di compromettere sia le password di accesso ai servizi finanziari degli utenti che il loro telefono cellulare, ed essere in grado di mettere in relazione le due cose.

Questo rende i telefoni un obiettivo ancora più prezioso per i criminali da compromettere e controllare. Questo controllo può essere fisico, come nel caso di furto del telefono dal proprietario, o compiuto in remoto con il software di spionaggio per il dispositivo mobile. In entrambi i casi, le minacce miste richiedono uno sforzo maggiore da parte dei criminali e probabilmente verranno indirizzate verso gli account o i sistemi di maggior valore.

Le applicazioni dei dispositivi mobili sono utilizzate anche come generatori di token, come ad esempio i codici a sei cifre che eravamo abituati a vedere solo su dispositivi fisici emessi singolarmente per generare chiavi di autenticazione a due fattori, come ad esempio Google Authenticator e Amazon AWS Virtual MFA.

A seconda punto di accesso dei criminali, questi possono essere in grado di osservare il contenuto del traffico da e per alcuni dispositivi mobili e ottenere i codici di autenticazione. Questo è il caso di codici inviati via e-mail, che alcune banche offrono come opzione. Il traffico SMS non è crittografato.

La mancanza di una struttura con la quale condividere informazioni riguardanti le minacce miste può a sua volta essere vista come una minaccia; permette un gran numero di exploit che potrebbero altrimenti essere evitati. Quello che è necessario è di elaborare e attuare strategie e strutture che coinvolgono dipartimenti tecnici, la politica, le forze dell'ordine, e le persone giuridiche in diversi paesi.

MODIFICARE I DISPOSTIVI MOBILI

Molti produttori di apparecchiature originali (OEM) e operatori di rete mobile (MNO) creano ambienti informatici mobili sicuri per mantenere la stabilità del dispositivo, la sicurezza, e sostenere un'esperienza dell'utente positiva. In molti casi, la modifica di questi ambienti crea vulnerabilità di sicurezza che possono

Esempio: Zeus Mitmo (Man in the middle / mobile)

Zeus è un'applicazione cavallo di Troia che infetta computer Windows e tenta di rubare informazioni bancarie tramite la registrazione della battitura nel browser accoppiata ad un sistema di cattura delle informazioni immesse nei moduli. I meccanismi tipici per la proliferazione di Zeus sono stati le attività di "drive-by download" e tentativi di phishing atti a attirare l'utente verso un sito malevolo. Il primo avvistamento è avvenuto circa nel 2007 e ha ricevuto molti aggiornamenti che hanno aumentato la sua raffinatezza, di recente di può essere sfruttato per attaccare i dispositivi mobili. Questo aggiornamento va a beneficio del malware Zeus dal momento che molte aziende tra cui istituzioni finanziarie stanno ora utilizzando gli SMS come un secondo vettore di autenticazione, per fare in modo che avere sia il nome utente e la password on-line non siano sufficienti nel processo di furto di identità. L'evoluzione della minaccia di questo vettore consente un'alternativa progettata da una banda di Zeus: infettare il dispositivo mobile e leggere tutti i messaggi SMS che vengono consegnati. Lo scenario è descritto di seguito.

- L'attaccante ruba sia il nome utente e la password per l'accesso on-line utilizzando un malware (Zeus 2.x).
- L'attaccante infetta il dispositivo mobile dell'utente costringendolo a installare un'applicazione dannosa via SMS o tramite il malware che si finge una legittima applicazione bancaria o di produttività.
- L'attaccante accede con le credenziali rubate utilizzando il computer dell'utente come socks / proxy ed esegue una specifica operazione che richiede l'autenticazione SMS.
- Un SMS viene inviato al dispositivo mobile dell'utente con il codice di autenticazione. Il software dannoso in esecuzione nel dispositivo inoltra l'SMS ad un altro terminale controllato dall'utente malintenzionato.
- L'attaccante inserisce il codice di autenticazione e completa l'operazione.

Gli hacker quindi possono utilizzare queste informazioni per controllare i conti bancari delle vittime ed effettuare trasferimenti non autorizzati

esporre le informazioni dell'utente, consentire il furto di servizio sotto forma di telefonate non autorizzate o messaggi di testo, abilitare il controllo remoto delle risorse del dispositivo come microfoni o telecamere per ascoltare o vedere senza la conoscenza dell'utente, oppure consentire l'esecuzione di una lunga serie di altre attività non autorizzate.

Ci sono numerose tecniche per modificare l'hardware e il software di un dispositivo, ma tre delle modifiche più note sono "jailbreaking", "rooting", e "sblocco".

JAILBREAK DI UN DISPOSITIVO

Con il termine "Jailbreaking" si intende quando qualcuno elimina i controlli incorporati in un dispositivo. Il fabbricante può utilizzare controlli OEM per far rispettare le autorizzazioni dell'applicazione, proteggere le aree critiche del file system del dispositivo, forzare le applicazioni ad effettuare l'autenticazione con il dispositivo, far rispettare la complessità della password e molte altre funzioni di gestione e di amministrazione.

Perché la gente effettua il jailbreak dei dispositivi? Una ragione è che, anche con centinaia di migliaia di applicazioni disponibili, alcune persone vogliono versioni personalizzate o modificate di queste. In alcuni casi, una applicazione modificata può costare meno dell'applicazione ufficiale (ma potrebbe violare il diritto d'autore); tuttavia, l'applicazione meno costosa può contenere anche contenuti dannosi.

ROOTING DI UN DISPOSITIVO

Il Jailbreak consente all'utente di eliminare i controlli, ed eleva l'accesso degli utenti per ottenere i privilegi di root ad un dispositivo che, alla fine, concede all'utente tutti i privilegi del sistema operativo. Il "rooting" di un dispositivo consente all'utente i privilegi più alti di un sistema operativo.

Perché la gente effettua il "rooting" di un dispositivo? Oltre a consentire il caricamento di applicazioni personalizzate o non autorizzate eludendo i controlli, l'accesso di root consente a un utente di modificare i componenti e le funzionalità, o di sostituire completamente il sistema operativo su un dispositivo. Alcuni sistemi operativi per dispositivi mobili si basano su una versione di UNIX con un ridotto set di comandi, alterando il sistema operativo gli utenti possono liberare spazio di archiviazione eliminando funzioni non necessarie per la maggior parte degli utenti di dispositivi mobili. Il rooting di un dispositivo potrebbe anche consentire a un utente di caricare comandi aggiuntivi, se lo desidera.

SBLOCCO DI UN DISPOSITIVO

Gli operatori di rete mobile (MNO) possono sovvenzionare le vendite di telefoni cellulari nell'ambito di un contratto che richiede l'uso della rete dell'operatore stesso per un periodo di tempo. Per aiutare a prevenire le frodi e il furto, gli operatori spesso utilizzano un mezzo tecnico conosciuto come "blocco" per limitare l'uso del telefono cellulare alla propria rete. Un dispositivo in genere può essere sbloccato inserendo un "codice di sblocco" unico fornito da un operatore su richiesta o in seguito alla risoluzione di un impegno contrattuale. I consumatori possono anche

trovare o acquistare un codice di sblocco on-line. Se hanno ottenuto il codice da terze parti, gli utenti corrono il rischio di perdere le informazioni personali o di trovarsi del malware installato da un fornitore inaffidabile.

MIGLIORI PRATICHE PER GLI INDIVIDUI RIGUARDANTI LE MODIFICHE DEI DISPOSITIVI MOBILI:

1. Effettuare il Jailbreak, il rooting e lo sblocco dei dispositivi non sono attività consigliate a chi cerca un dispositivo standard stabile con il supporto del produttore a lungo termine in quanto può introdurre vulnerabilità sconosciute per l'utente.
2. Non utilizzare servizi non ufficiali di "terze parti" per sbloccare i dispositivi

MIGLIORI PRATICHE PER IL SETTORE E IL GOVERNO PER LE MODIFICHE DEI DISPOSITIVI MOBILI:

1. Sviluppare e promuovere l'educazione dei consumatori e la consapevolezza dei rischi che si corrono nel modificare i dispositivi mobili
2. Creare protezioni più forti contro la sostituzione delle impostazioni dei produttori
3. Condurre appropriate campagne per l'applicazione della legge contro i promotori degli abusi delle piattaforme mobili.

MINACCE BANDA BASE

Ci sono diverse tipi di minacce per la "banda base". Alcune possono comportare la creazione di una rete GSM (Global System for Mobile communications) illecita che attiri i dispositivi di connettersi ad esso. Altri possono comportare attacchi in cui messaggi appositamente predisposti tentino di sfruttare falle di sicurezza nei dispositivi mobili. Con la crescita della ricerca a basso costo e installazioni GSM fuorilegge, queste minacce hanno proliferato.

Tradizionalmente, la gestione di un rete GSM ha richiesto un investimento significativo, che ha reso impraticabile la ricerca al di fuori delle grandi istituzioni, limitando la scoperta e lo sfruttamento di attacchi basati sulla rete. Ad esempio, per falsificare una rete GSM, un utente malintenzionato avrebbe bisogno di operare una "Base Transceiver Station" (BTS). Quando la tecnologia GSM è stata implementata, gli attacchi basati sulla rete contro i dispositivi finali non costituivano una preoccupazione, per questo motivo i telefoni non

Attacchi Banda Base

L'attaccante creerà una Base Transceiver Station (BTS) fraudolenta in prossimità della Stazione Mobile (MS) che vuole colpire. La BTS fraudolenta trasmette messaggi informativi di sistema che annunciano la disponibilità di una rete alla quale la stazione mobile presa di mira è disposta a connettersi. Poiché il criterio principale per la ricezione di rete è la potenza del segnale, l'attaccante può forzare la Stazione Mobile a connettersi alla stazione di base falsa semplicemente trasmettendo con un segnale più forte della stazione base legittima. Ciò non avverrà istantaneamente, ma il processo può essere accelerato mediante un "jammer GSM" per confondere in maniera specifica la frequenza delle BTS legittime. Questo scenario è molto simile a quello utilizzato dai collettori "International Mobile Subscriber Identity" (IMSI). Dal momento che il GSM non fornisce sempre autenticazione reciproca, non vi è alcuna protezione contro le BTS fasulle.

erano tenuti ad autenticare le reti alle quali si attaccavano. Recentemente, tuttavia, software gratuito open-source come OpenBTS ha permesso a chiunque di creare la propria rete GSM ad una frazione del costo delle attrezzature "carrier-grade", portando gli studi sulla sicurezza GSM alla portata sia dei ricercatori di sicurezza che dei criminali.

MIGLIORI PRATICHE PER IL SETTORE E IL GOVERNO PER PROTEGGERE DALLE MINACCE DELLA BANDA BASE:

Nel momento in cui I carrier adottano le nuove tecnologie (es. 3G e 4G/LTE), i terminali dovrebbero essere obbligati ad autenticare l'infrastruttura del carrier alla quale si collegano.

1. I fornitori di servizi possono lavorare con i produttori dei terminali per informare gli utenti quando il terminale apre una sessione che non utilizza autenticazione reciproca. Questo potrebbe allertare l'utente della possibile minaccia.

ABUSO DEL SERVIZIO PREMIUM (A SOVRAPREZZO)

Normalmente offerti come servizi per le applicazioni vocali e testuali addebitati su un conto telefonico prepagato o postpagato di un abbonato, i servizi a sovrapprezzo includono oroscopi una tantum e ricorrenti di tipo "pay-per-call", donazioni per catastrofi ed emergenze, crediti di gioco, servizi di consigli e chat, SMS mensili di consigli d'amore e una vasta gamma di altri sistemi.

MODELLO DI BUSINESS PREMIUM:

Il desiderio di creare un diffuso ecosistema di applicazioni facili da sviluppare ha portato ad ambienti di fatturazione lunghi e complessi con i vari modelli di condivisione dei guadagni, come il tipico percorso per l'abbonamento a servizi a pagamento per US $ 9.99 / mese SMS, che sono sfruttabili a scopo criminale (illustrato di seguito).

In questo esempio, un operatore di rete mobile consente ad "aggregatori SMS" indipendenti di ottenere l'instradamento ad una serie di "numeri brevi" (numeri di telefono di solito con 4-7 cifre instradabile all'interno di una parte della rete di telefonia globale). L'aggregatore poi vende connettività mobile SMS "a due vie" ad un proprietario dell'applicazione oroscopo conosciuto come un fornitore di contenuti. Il fornitore di contenuti paga una commissione per-abbonamento ad un affiliato di pubblicità. I soggetti interessati prossimi possono essere solo vagamente correlati.

I soggetti interessati e le relazioni diventano progressivamente più problematiche verso il lato destro del diagramma. In un certo numero di casi, i fornitori di contenuti permettono relazioni esclusivamente via internet e male autenticate con gli affiliati di pubblicità per facilitare la possibile smentita dello spamming e/o delle frodi proprie o dei loro affiliati. Meccanismi di pagamento quasi anonimi come i trasferimenti alle banche straniere, denaro virtuale tramite internet non regolamentato o meccanismi di pagamento on-line

Malware per Servizi Premium

Phonepay Plus, l'autorità di regolamentazione britannica dei servizi a sovrapprezzo, ha emesso multe di £ 330.000 in dicembre 2014 a tre diverse società dopo aver scoperto che stavano usando malware mobile per generare spese ai proprietari di telefoni Android. Il malware era contenuto in applicazioni scaricate automaticamente senza il consenso degli utenti quando hanno visitato specifici siti web per adulti. Una volta installato gli utenti potrebbero inavvertitamente avviare una sottoscrizione cliccando in un qualsiasi punto dello schermo. L'applicazione avrebbe quindi inviato messaggi di testo nascosti a tariffa maggiorata in modo che il proprietario non avrebbe visto evidenza di questi messaggi nella registro del proprio telefono.

abbassano le barriere e consentono lo spam per facilitare le frodi.

Le truffe di servizi a sovrapprezzo esistono da molti anni, ma l'aumento della penetrazione dei servizi di telefonia mobile, l'evoluzione dei dati mobili, e la creazione di un ecosistema del crimine informatico globale hanno portato ad un aumento del numero e della varietà di attacchi. La frode può avvenire in quasi ogni fase dei processi di servizio o di pagamento, dall'ingannare l'utente a sottoscrivere o a utilizzare inavvertitamente un servizio, da un affiliato che rivendica abbonamenti fasulli, fino ad arrivare al malware per dispositivi mobili che manda clandestinamente messaggi per servizi premium senza che il sottoscrittore ne sia a conoscenza.

Un comune exploit coinvolge un truffatore che crea un numero Premium e fa uno squillo o invia un messaggio di testo ad una vittima, nella speranza di adescarla a rispondere. Questo porta il chiamante ad un servizio "pay-per-call" senza il suo consenso. All'ordine del giorno sono stati anche abbonamenti non autorizzati, "infarciti" da "consigli d'amore" a sovraprezzo o altri servizi di messaggi di testo da affiliati e / o fornitori di contenuti.

Questo ha portato molti aggregatori SMS ad implementare una verifica secondaria, di solito aggiungendo un messaggio di conferma o PIN scambiato tra l'abbonato SMS e l'aggregatore. Ma anche questi sono stati sfruttati; per esempio, il malware Android GGTracker invia una richiesta di sottoscrizione SMS ed il messaggio di conferma senza che gli abbonati ne siano a conoscenza. [liv]

Falsificare l'identità dell'abbonato, tramite l'accesso non autorizzato alle reti di segnalazione o un exploit della crittografia, costituisce ancora un altro metodo per commettere frodi di questo tipo.

MIGLIORI PRATICHE PER IL SETTORE E IL GOVERNO PER LA PROTEZIONE CONTRO LE TRUFFE A SOVRAPREZZO:

La frode delle tariffe a sovrapprezzo è simile a molti altri tipi di crimine informatico ed è quindi adeguatamente coperta da una serie di tecniche comuni, tra cui auto-protezione, l'educazione e la tutela dei consumatori e le misure anti-malware.

Molti operatori di telefonia mobile hanno creato un servizio di segnalazione per consentire agli abbonati di segnalare SMS di spam inoltrando ili messaggio ad un numero breve (ad esempio, 7726, che corrisponde a "spam"). Molti governi e le agenzie di polizia responsabili per lo spam SMS in alcuni paesi hanno creato i propri numeri per la segnalazione come il 1909 in India, 33700 in Francia e 0429 999 888 in Australia.

Specifiche misure di protezione contro le truffe delle tariffe a sovraprezzo includono la difesa iniziale, le azioni dei partner e una conferma addizionale.

1. **I reclami ai TSP o alle autorità di regolamentazione:** Incoraggiare la presentazione di reclami da parte dei consumatori. Queste denunce permettono ai TSP di identificare la fonte delle minacce ed implementare meccanismi di difesa che consentono la diagnosi precoce,

prima che il denaro sia stato trasferito. Includendo e applicando le clausole anti-abuso nei loro termini e condizioni, i TSP e le piattaforme di servizi a tariffa speciale possono fermare i pagamenti ai criminali prima che si verifichino. Il TSP è avvertito in una fase iniziale attraverso reclami, può tutelare i propri termini e condizioni, minando così il business case del criminale. Allo stesso modo, le denunce alle autorità di regolamentazione e alle autorità di controllo forniscono ricche informazioni che possono portare all'applicazione della legge contro i truffatori.

2. **Azioni dei Partner per quanto riguarda le Relazioni e i Pagamenti:** La frode dipende dalla sottrazione di denaro verso una località nascosta e / o non rintracciabile. I soggetti interessati possono proteggersi richiedendo la piena identificazione, la qualificazione e l'autenticazione degli altri soggetti, utilizzando meccanismi di pagamento affidabili o ritardando il pagamento per un periodo sufficiente.
3. **Conferme Supplementari:** Poiché molti degli exploit coinvolgono comunicazioni confuse o falsificate tra i soggetti interessati coinvolti nella catena dei pagamenti, le notifiche e le conferme tra parti più affidabili possono permettere di prevenire o di individuare rapidamente la frode. Esempi di questo sono un aggregatore SMS o un operatore di rete mobile che conferma l'abbonamento con l'utente piuttosto di fare affidamento esclusivamente alle asserzioni di chi è a valle del flusso di pagamento.

SPAM SU DISPOSITIVI MOBILI (MOBILE SPAM)

Il seguente scenario descrive la recente attività di spamming internazionale e dimostra il ruolo critico della collaborazione internazionale, in particolare quella tra carrier, vitale per la difesa contro gli abusi delle reti e degli abbonati.

Carrier A e B operano in paesi diversi; entrambi i paesi hanno molte persone che parlano la stessa lingua. Lo spam originato dalla rete del Carrier A rappresenta la maggior parte dello spam in entrata nella rete del Carrier B. Il Carrier A traccia lo spam nella sua rete mediante la segnalazione di spam verso numeri brevi e attraverso l'analisi dei log del server di messaggistica. Il Carrier B ha anche lui la segnalazione dello spam verso i numeri brevi, ma *non* raccoglie i numeri originari dei messaggi che vengono segnalati come spam. Il Carrier B, tuttavia, eseguire la scansione anti-spam sul traffico dei messaggi. Di conseguenza, la rete del Carrier B raccoglie informazioni sulle origini e sul contenuto dello spam.

Carrier A e Carrier B vengono a conoscenza separatamente dello spam originato dalla rete del Carrier A che viene ricevuto dal Carrier B. Il Carrier A termina lo spammer che si identifica sulla propria rete, ma solo se ha ricevuto un certo volume di segnalazioni di spam per quello specifico numero di provenienza. Così, fino a quando uno spammer sulla rete del Carrier A invia solo ai numeri al di fuori della rete di Carrier A, può inviare spam illimitato agli abbonati del Carrier B, in quanto:

a) Il Carrier A non potrà mai ricevere le segnalazioni spam dai propri abbonati, il suo requisito per attivare un blocco; e

b) Non c'è condivisione di informazione per contrastare gli spammer internazionali

In assenza di condivisione dei dati tra gli operatori, gli spammer possono operare abbastanza liberamente *all'interno di un determinato paese*, se hanno la cura di inviare lo spam solo agli abbonati di operatori *diversi da quello della rete su cui essi hanno i loro account*.

MIGLIORI PRATICHE PER IL SETTORE E IL GOVERNO PER LA PROTEZIONE CONTRO LO SPAM SUI DISPOSITIVI MOBILI:

Dialogo e condivisione dei dati: Gli spammer sfruttano le vulnerabilità dei fornitori di servizi in merito alle politiche anti-abuso, alle difese e alle conoscenze. Una delle lezioni più importanti apprese dalla proliferazione delle e-mail di spam su internet fin dalla sua infanzia nel 1993 ad oggi, quando lo spam rappresenta ormai circa il 90 per cento di tutto il traffico internet relativo alla posta elettronica, è che quando i partecipanti dell'ecosistema condividono le informazioni, il gioco cambia per gli spammer. Il dialogo tra carrier e la condivisione dei dati che coinvolgono i fornitori di terze parti, come ad esempio gli sviluppatori di tecnologia e gli enti del settore, è vitale per proteggere l'ecosistema mobile dallo spam e dalla migrazione degli strumenti e delle tecniche a disposizione degli spammers, affinate su internet da un decennio o più, verso un mondo di dispositivi mobili sempre più basato su IP e già interconnesso a livello globale.

Mentre i seguenti punti non sono critici per la collaborazione tra i fornitori di servizi, essi sono utili per contrastare gli spammer e possono essere acquisiti attraverso le segnalazioni di spam:

Informazione	Note
Numero di cellulare dal quale proviene lo spam	MSISDN (il numero univoco associate con un terminale di un abbonato) o IMSI (il numero univoco della SIM card)
Numero di segnalazioni Spam ricevute	Richiede che siano raccolte e correlate
Numero di segnalatori Spam unici	Utile ma non critico
Rete dell'emittente dello spam	Derivato dalla ricerca

Si noti che nessuno degli elementi identificati sopra fornisce dati personali sul segnalatore dello spam. Le informazioni vengono raccolte solo sul numero segnalato come emittente dello spam.

Come nell'esempio del Carrier A e B precedente, la condivisione degli elementi indicati sopra aiuta a combattere lo spam all'interno di un determinato paese tanto quanto lo fa oltre i confini nazionali.

Ci sono vantaggi e rischi per la condivisione internazionale inter-carrier di dati selezionati tra le segnalazioni di spam. I vantaggi includono la possibilità di rimediare ai reclami degli abbonati spontanei. La condivisione dei dati e il dialogo anti-spam tra gli operatori facilita anche i loro sforzi per monitorare, raffinare, e far rispettare i propri termini d'uso e policy. Infine, la condivisione dei dati è in grado di fornire la prova avvalorante per le decisioni sul blocco dell'operatore, così come per le forze dell'ordine e per gli attori coinvolti nella regolamentazione. La collaborazione internazionale tra carrier verso questi obiettivi renderà più difficile per gli spammer mobili la possibilità di nascondersi.

D'altra parte, ci sono problemi legali, di privacy e di sicurezza che devono essere affrontati in sede di attuazione di qualsiasi collaborazione internazionale in questo ambito. Attualmente queste preoccupazioni costituiscono un impedimento alla collaborazione transfrontaliera. Alcuni hanno notato, tuttavia, che questi problemi di privacy sono ingiustificati perché 1) le segnalazioni Spam sono sottoposte spontaneamente dagli abbonati, 2) non è necessario includere informazioni personali identificabili (PII), nel condividere i dettagli della segnalazione, e 3) non è fondamentale includere il contenuto dei messaggi nella condivisione dei dati della segnalazione. (Condividere il contenuto del messaggio può aumentare il rischio di condivisione accidentale delle informazioni personali dei segnalatori o delle persone che non siano lo spammer. Tuttavia, il contenuto dei messaggi segnalati come spam può anche essere utile per identificare e bloccare lo spam.)

In sintesi, la condivisione internazionale tra carrier di taluni elementi cambia il gioco per gli spammer in quanto lascia loro un minor numero di posti dove nascondersi. La condivisione dei dati richiederà il dialogo e il consenso sui dati da condividere, così come precisi formati per lo scambio di dati tra i partecipanti all'ecosistema.

Il settore dovrebbe anche cercare di informare il personale delle forze dell'ordine quando vengono a conoscenza di comportamenti illeciti sulle loro reti e sui loro sistemi. Il coordinamento con le

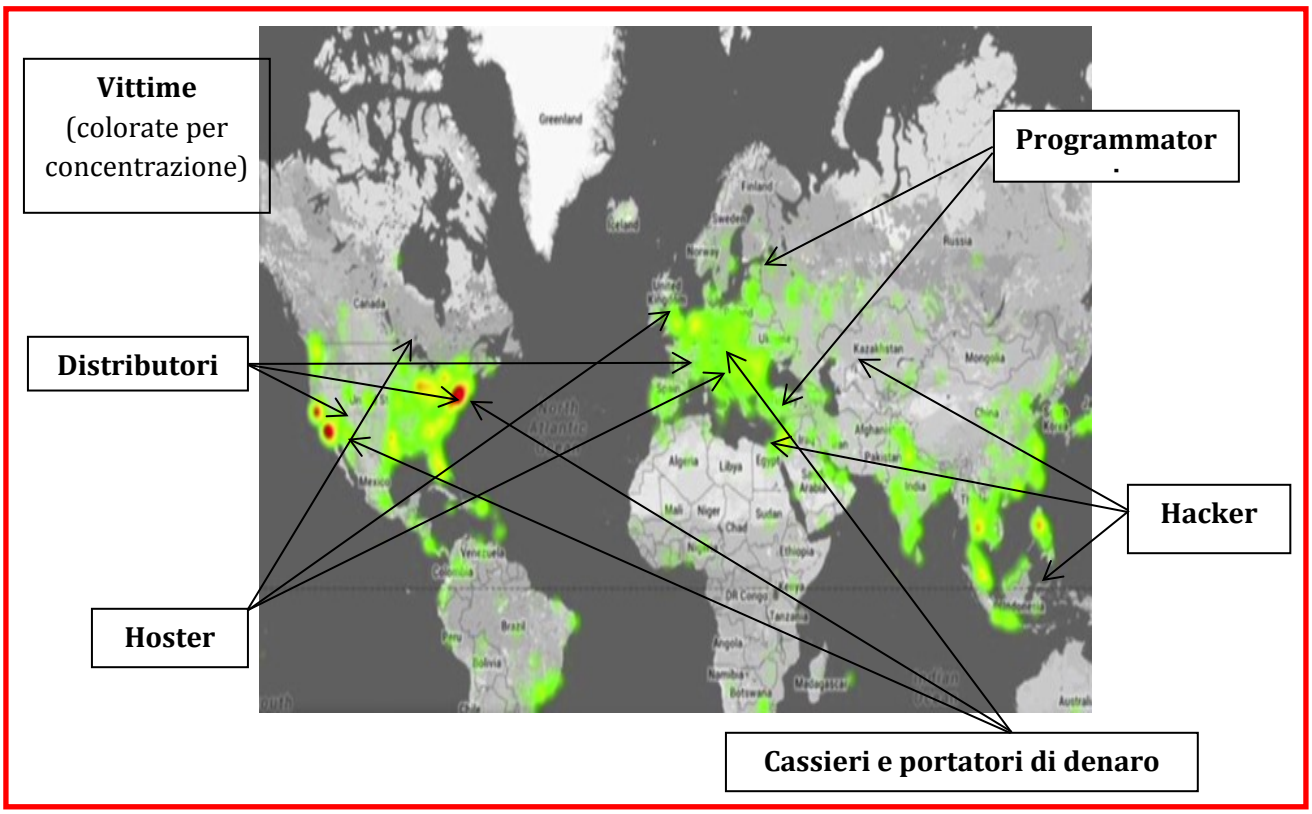
forze dell'ordine, sia sul lato penale che normativo, spesso può consentire di arrivare alla fonte della minaccia, e scoraggia ulteriormente gli altri dal porre in essere tali comportamenti.

CRESCITA DEGLI EXPLOIT TRANSFRONTALIERI

Mentre le nazioni affrontano gli attacchi interni e le minacce, gli attaccanti rivolgono la loro attenzione altrove per identificare e sfruttare le vulnerabilità internazionali. Ad esempio, la campagna di spam "iPad / iPhone gratuita" del Nord America ha originariamente colpito gli Stati Uniti. I carrier canadesi e statunitensi hanno implementato le difese tecniche per bloccare lo spam inviato ai loro abbonati. Gli aggressori hanno rapidamente notato ciò e hanno iniziato l'invio di SMS di spam agli abbonati canadesi da telefoni basati negli Stati Uniti, eludendo in tal modo le difese. Casi simili esistono in frodi, phishing, malware e spyware. Nella maggior parte dei casi (ad esempio la difesa da spam e malware), si è scoperto che fermare l'abuso alla fonte è necessario, in quanto le nazioni che ricevono potrebbero non essere in grado di identificare l'abuso nascosto all'interno di flussi di comunicazione ad alto volume. Come Internet, le reti di comunicazioni per la telefonia mobilie sono globali e richiedono un approccio di difesa internazionale e la collaborazione internazionale.

CONSIDERAZIONI INTERNAZIONALI

I criminali informatici hanno una forte preferenza per operare in un ambiente transnazionale. Ad esempio, un venditore illegale on-line di pillole che vive negli Stati Uniti potrebbe inviare spam pubblicitario di quei farmaci da un computer compromesso in Brasile, facendo puntare i potenziali acquirenti ad un sito web con un nome di dominio russo (mentre fisicamente il sito è situato in Francia). I pagamenti con carta di credito per gli ordini possono venire processati tramite una banca in Azerbaijan, con gli ordini spediti da un sito in India, e i proventi incanalati verso una banca di Cipro. I criminali sanno che operando in questo modo, molti fattori complicano ogni indagine ufficiale per i loro crimini on-line, e riducono la loro probabilità di essere scoperti. Questi fattori includono la mancanza di cooperazione, le differenze da una giurisdizione all'altra, ed il costo delle indagini internazionali.



Giurisdizione e cooperazione internazionale
Le forze dell'ordine non hanno poteri illimitati. In particolare, un funzionario di polizia di una città o di un paese normalmente non avrà giurisdizione per citare in giudizio i documenti o arrestare un criminale oltre la propria giurisdizione. Le indagini transfrontaliere richiedono una cooperazione internazionale tra le agenzie di polizia nazionali e internazionali, un processo che può coinvolgere processi formali spaventosamente complessi, per non parlare del tempo e le risorse necessarie. Le complicanze associate a questi processi possono ritardare le indagini, o renderne impossibili alcune.

COPERTURA DI LEGGE E PRECEDENTE DELLA COMMON LAW
Un'attività che è illegale in una giurisdizione potrebbe non essere illegale altrove. Ad esempio, alcuni paesi non hanno leggi in materia dello spam via e-mail, né hanno criminalizzato la diffusione di malware. In altre giurisdizioni, il sistema legale potrebbe non essere in

Esempio: Truffa del call center indiano
Fino a 60.000 persone nel Regno Unito recentemente sono diventate le vittime di una truffa multi-milionaria di un call center indiano e di un prestito online. Gli investigatori ritengono che il numero di persone vittima di truffe sui prestiti la rende una delle più grandi truffe mai realizzate nel Regno Unito. Al suo apice, più di 1.000 persone al giorno che avevano legittimamente cercato prestiti non garantiti con le banche e le società finanziarie sono state oggetto di pubblicità telefonica non desiderata ("chiamate a freddo") dal call center in Nuova Delhi - con circa 100 persone al giorno che sono state indotti a sottoscrivere e pagare una “tassa di elaborazione” per garantire liquidità inesistente. Secondo la polizia indiana sono state rubate almeno 10 milioni di £.

grado di tenere il passo con un flusso costante di nuovi, chimicamente diverse ma equivalenti, farmaci. In altri casi, una legge può essere ufficiale, ma il paese può non avere alcun precedente per perseguire con successo coloro che hanno violato quella legge. Ciascuna di queste condizioni sono sfide alle forze dell'ordine e alla collaborazione.

COSTI DELLE INDAGINI INTERNAZIONALI

Tutto ciò che riguarda l'operatività internazionale costa alle forze dell'ordine di più rispetto al lavorare a casi strettamente locali. Se un ricercatore ha bisogno di viaggiare in un paese straniero, il biglietto aereo e gli altri costi di viaggio possono essere notevoli. Le agenzie a corto di liquidi possono quindi semplicemente non essere in grado di permettersi di lavorare a casi con aspetti internazionali.

Ironia della sorte, se è costoso per un funzionario di polizia lavorare ad un crimine che ha aspetti internazionali, i criminali informatici sono spesso in grado di acquistare beni o servizi illegali all'estero via internet a prezzi stracciati. Ad esempio, un autore di talento di malware proveniente da una nazione economicamente depressa potrebbe essere disposto a scrivere malware che farà milioni di dollari di danni per poche centinaia di dollari. Queste condizioni danno ai criminali informatici un incentivo sostanziale al lavoro transfrontaliero, e molti in effetti lo fanno.

MIGLIORI PRATICHE PER IL SETTORE E IL GOVERNO RIGUARDANTI LE PROBLEMATICHE TRANSFRONTALIERE:

1. **Collaborazione:** Il cuore di una efficace difesa internazionale è la collaborazione. In primo luogo, enti governativi e non governativi nelle nazioni interessate devono prendere coscienza del problema. Successivamente, la collaborazione è necessaria per elaborare e attuare strategie e strutture di difesa che coinvolgano la tecnica, la politica, le forze dell'ordine e le persone giuridiche in diversi paesi. Le principali sfide nel raggiungimento della collaborazione necessaria includono l'identificazione del giusto insieme di forum e l'ottenere adeguata partecipazione.
2. **Condivisione delle Minacce/Abusi:** Lo scambio di informazioni sulle minacce e sugli abusi è essenziale per combattere le sfide transfrontaliere. Mentre sono necessarie comunicazioni da uomo a uomo, l'ampiezza e la scala degli abusi (ad esempio, i miliardi giornalieri di messaggi di spam e di phishing) dettano la necessità di approcci automatizzati. Anche in questo caso, perché sia attuato con successo un quadro internazionale automatizzato, si devono prendere in considerazione gli ostacoli alla diffusione e all'adozione, tra cui la frammentazione tra i molti sistemi diversi; le diverse esigenze funzionali di diverse nazioni (tra cui ostacoli giuridici e le questioni tecniche / tecnologiche) e le diverse esigenze dei diversi carrier. Un quadro generale per lo scambio di informazioni sugli abusi dovrebbe anche sostenere modelli peer-to-peer e server centralizzati ed identificare i protocolli sia di formato che di trasferimento.
3. **Formazione:** Per riconoscere e rispondere alle minacce mobili i professionisti e le forze dell'ordine devono essere aggiornati sui trend e sulle minacce emergenti.

MINACCE TELEFONIA VOCALE

L'AMBIENTE DELLA TELEFONIA VOCALE

I consumatori hanno molte scelte per quanto riguarda le chiamate vocali telefoniche: il cavo telefonico, il wireless, le fonti alternative (ad esempio, il computer). Queste chiamate possono attraversare la Public Switched Telephone Network (PSTN) tramite Time Division Multiplexing (TDM), Voice over Internet Protocol (VoIP), o una combinazione del TDM e del VoIP. La telefonia via internet si riferisce all'integrazione dei servizi di telefonia con le reti di computer. In sostanza, il processo converte i segnali vocali analogici che venivano tradizionalmente inviati tramite rete fissa in segnali digitali. Questi segnali vengono trasmessi via Internet e poi riconvertiti in segnali vocali analogici.

Il Session Initiation Protocol (SIP) è un protocollo di comunicazione per la segnalazione e il controllo di sessioni di comunicazione multimediali ed si trova di soliuto in applicazioni di telefonia Internet o VoIP.

Il Time Division Multiplexing (TDM) è un metodo di trasmissione e ricezione di segnali indipendenti su un flusso di segnale comune mediante interruttori sincronizzati a ciascuna estremità della linea di trasmissione.

Il numero di abbonamenti di telefonia fissa in tutto il mondo ha raggiunto il picco nel 2006 ed è diminuito ogni anno da allora. Per esempio, gli abbonamenti di telefonia fissa sono stati poco meno di 1,11 miliardi nel 2014, in calo da oltre 1,14 miliardi nel 2013. Allo stesso tempo, il numero di abbonamenti di telefonia mobile-cellulare è in aumento in tutto il mondo e si sta rapidamente avvicinando il numero di persone sulla terra. Gli abbonamenti cellulari hanno raggiunto quasi i 7 miliardi per la fine del 2014, corrispondente ad un tasso di penetrazione del 96 per cento, ma i tassi di crescita hanno raggiunto il livello più basso di sempre (del 2,6 per cento a livello mondiale), che indica che il mercato si sta rapidamente avvicinando ai livelli di saturazione.

Entro la fine del 2014, il numero di abbonamenti di telefonia mobile a banda larga, ha raggiunto 2,3 miliardi a livello globale, quasi 5 volte maggiore rispetto a solo sei anni prima (nel 2008). Gli abbonamenti a banda larga su dispositivi mobili erano 2,1 miliardi nel 2013. La penetrazione della banda larga fissa continua a crescere, anche se lentamente (al 4,4 per cento a livello globale nel 2014). Poiché i servizi stanno diventando sempre più accessibili, l'adozione della banda larga fissa ha mostrato una forte crescita nel 2013, ci sono stati quasi 700 milioni di abbonamenti a banda larga fissa, corrispondente ad un tasso di penetrazione globale del 9,8 per cento.

Il numero di utenti di Internet a livello globale avrà raggiunto quasi 3 miliardi entro la fine dell'anno 2014, dai 2,7 miliardi di persone nel 2013.[lv]

Con la crescita diffusa della telefonia via Internet, è fondamentale che l'infrastruttura di supporto di questa tecnologia rimanga sicura e disponibile. Una piccola quantità di "downtime" ha il potenziale per costare alle aziende milioni di dollari in ricavi persi e problemi di supporto ai clienti.

MINACCE VOIP

Questa sezione fornisce una semplice tassonomia delle minacce di telefonia vocale, che copre i problemi che riguardano i sistemi voce e Unified Communications (UC) e le migliori pratiche per

prevenire e porre rimedio a queste minacce. Questa sezione si concentra sulla voce, ma le minacce possono influenzare altre forme di comunicazione, inclusi video e messaggistica. Queste minacce sono per lo più applicabili alle imprese, ma possono colpire anche i fornitori di servizi, le piccole imprese e consumatori.

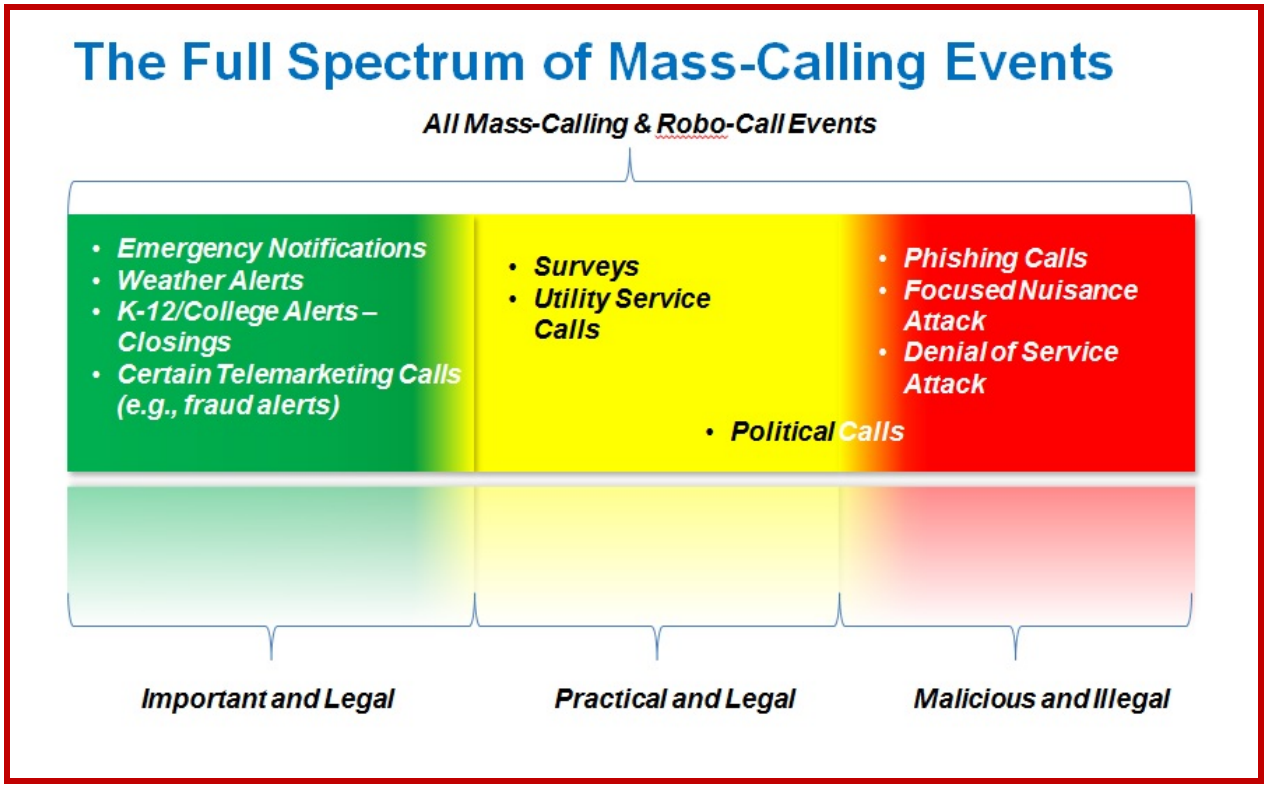
ROBOCALLING

Robocalling, ovvero utilizzare sistemi di selezione automatica per effettuare chiamate vocali, è una forma sempre più problematica di abuso del servizio voce. Viene utilizzato in genere per le chiamate relative a vendite, marketing o sondaggi. Per esempio, quando viene condotto un sondaggio un messaggio pre-registrato può chiedere alla persona che risponde di premere un tasto corrispondente alla risposta scelta. Un altro uso comune è per le notifiche di emergenza, annunci, o promemoria. Questo è spesso utilizzato dai funzionari di Pubblica Sicurezza tramite un sistema chiamato Emergency Notification System (ENS). Il Robocalling, però, è anche comunemente usato per truffare i consumatori o per altri scopi illegali.

Negli Stati Uniti, ad esempio, le robocall riguardano in modo particolare i clienti di rete fissa, che vengono spesso presi di mira dai venditori senza scrupoli e dai truffatori. [lvi] Le robocall sono state in cima tra le denunce per frodi al consumo da parte della FTC nel 2014. Recentemente, i carrier hanno iniziato a registrare un numero crescente di reclami da parte dei clienti wireless. Ad esempio, la truffa "singolo squillo" è stata recentemente introdotta con lo scopo di indurre i clienti a per comporre inavvertitamente numeri internazionali a pagamento.[lvii] Sono anche comuni le chiamate di adescamento (phishing) specificamente finalizzate ad ottenere l'accesso ad informazioni private personali e finanziarie, spesso definito come vishing.

Truffe a singolo squillo: Gli utenti di telefonia mobile ricevono chiamate automatizzate da numeri di telefono con prefissi che imitano i numeri nazionali, ma sono in realtà associate a numeri internazionali a pagamento. Queste chiamate automatizzate di solito terminano dopo uno squillo, non dando il tempo dei consumatori di rispondere alla chiamata invogliandoli a richiamare. I clienti che richiamano indirizzano traffico aggiuntivo verso questi carrier stranieri e il truffatore può ricevere una parte delle spese di terminazione (o possibilmente addebiti premium) che il prestatore di servizi straniero ottiene dal carrier del cliente wireless.

Le Robocall vengono spesso utilizzate per sopraffare sia i clienti di rete fissa che wireless clienti con attacchi di tipo Denial of Service Telefonico (TDOS) creando chiamate in massa che impediscono di porre a termine le chiamate legittime.



MIGLIORI PRATICHE PER COMBATTERE LE ROBOCALL:
I carrier o i venditori di terze parti possono offrire degli strumenti e delle soluzioni per combattere le Robocall. Non esistono soluzioni, però, per eliminare tutte le robocall non desiderate o illegali.

Honeypot: Una Honeypot (vaso di miele) è una trappola per rilevare, deviare o contrastare tentativi di utilizzo non autorizzato di una rete o di un sistema. In generale, le honeypot imitano un computer, dati o una rete, ma in realtà sono isolati, protetti e monitorati. Sono costruite specificamente come esche per gli attaccanti. Una volta adescati, i malfattori possono essere monitorati e controllati.

Raccolta dati e Analisi: L'informazione rappresenta uno strumento potente nel prevenire robocall. Attraverso la raccolta di informazioni sul flusso normale del traffico in una particolare rete e combinando questi dati con strumenti di analisi per identificare gli schemi di chiamata sospetti basati su volumi, instradamento, destinazioni, durate e tassi di completamento delle chiamate, i fornitori sono in grado di identificare e analizzare i modelli di chiamata sospetti per identificare le robocall illegali. Si possono utilizzare queste informazioni per creare blacklist per bloccare le chiamate provenienti da determinati numeri, o whitelist, che contengono le chiamate che possono essere ricevute. Una volta che un modello robocall viene identificato, gli operatori di rete e le autorità preposte alla tutela possono utilizzare tecniche di rintracciamento (traceback) per identificare e perseguire i responsabili.

Customer Premises Equipment (CPE): Sono disponibili strumenti forniti sia dai carrier che dai fornitori di terze parti per gestire le chiamate ricevute sui telefoni. I tipi più comuni di comprendono:

- ***ID Chiamante:*** L'ID chiamante visualizza il numero che sta chiamando. I clienti possono utilizzare questa tecnologia ben nota per filtrare le chiamate provenienti da fonti sconosciute. I servizi e i dispositivi di blocco di chiamata si basano sulle informazioni dell'ID chiamante trasmesse con le chiamate in entrata per bloccare le chiamate provenienti da numeri presenti nella lista nera.

- ***Dispositivi CAPTCHA[lviii]:*** passano alcune chiamate attraverso menù studiati per eliminare i chiamanti non umani.[lix]

- ***Applicazioni:*** i clienti wireless possono scaricare una varietà di applicazioni che utilizzano la funzionalità ID chiamante per rifiutare o filtrare chiamate da numeri di telefono che le applicazioni identificano come sospetti basandosi su varie tecniche come algoritmi di crowd-sourcing o blacklist.[lx] Gli utenti possono inoltre usufruire di funzionalità integrate nei loro smartphone che permettono loro di decider quali chiamate faranno suonare i loro cellulari e quali no.

- ***Identificazione a Chiave Pubblica/Privata:*** questo sistema è stato sviluppato per autenticare l'indirizzo del chiamante o la rete associata al chiamante.

Regimi normativi: Molte imprese hanno usato la telefonia per promuovere le campagne di marketing. La maggior parte dei regimi "Do Not Call" vietano robocall a meno che il consumatore non abbia acconsentito a ricevere tali chiamate dal chiamante. Inoltre, il fastidio del consumatore per colpa di sollecitazioni indesiderate ha portato molte nazioni a regolare tutte le chiamate commerciali, con alcune giurisdizioni che operano in regime "Do Not Call" di tipo opt-in (ad esempio la Germania, l'Austria e Israele) e molti operano in regime di tipo opt-out (alcuni volontari, alcuni obbligatori). In paesi come l'Australia, il Canada e gli USA, i registri nazionali di numeri da non chiamare sono integrati da ulteriori leggi per telemarketing che comunemente includono regole sui tempi di chiamata, sull'identificazione del chiamante (CLI) e sulle informazioni obbligatorie.

Le sanzioni possono essere significative e, insieme all'alto rischio di danni alla reputazione, sono state fondamentali nel garantire che le società responsabili abbiano politiche e procedure per garantire la loro conformità.

La rete internazionale "Do Not Call", parte del "London Action Plan", ha istituito un forum annuale e una conferenza periodica prevedendo la discussione di problemi comuni ed emergenti nella gestione delle chiamate telemarketing non richieste a livello globale e le opportunità per una applicazione della legge in maniera collaborativa.

Standard di settore: I fornitori di servizi, gli enti che definiscono gli standard del settore, e le agenzie di polizia hanno lavorato in modo cooperativo e in modo indipendente per mitigare questi

tipi di chiamate illegali. I fornitori di servizi e gli enti privati stanno sviluppando o hanno già sviluppato servizi e funzionalità a disposizione dei consumatori per combattere robocall illegali[lxi] e devono continuare a sviluppare e implementare questi standard.

I fornitori di servizi dovrebbero anche prendere in considerazione il miglioramento del loro primo livello di uffici commerciali o degli altri call center in ingesso, l'accesso on-line per i clienti, così come i centri di riparazione e di supporto tecnico, e dovrebbero educare il proprio personale sulle caratteristiche dell'ID del chiamante, sugli usi legittimi dello spoofing delle chiamate e sulle falsificazioni malevole conosciute al momento.

Alcuni provider potrebbero considerare l'istituzione di specifici "Annoyance Call Bureau" (Uffici per le chiamate non desiderate) o di team di sicurezza per affrontare problemi come questi. I clienti che continuano ad avere preoccupazioni dopo il loro contatto con il personale di primo livello o le risorse online possono essere indirizzati a tale gruppo per ottenere ulteriore assistenza a seconda dei processi specifici dei provider. I clienti possono essere invitati a condividere le informazioni pertinenti quali le date e gli orari nelle quali hanno ricevuto le chiamate contraffatte e altre indicazioni appropriate per l'indagine sulle chiamate. Gli uffici per le chiamate non desiderate o i team di sicurezza sono in grado di fornire attività preziose per affrontare questi problemi, come ad esempio:

- La fornitura e il controllo di apparecchiature per effettuare il tracciamento delle chiamate sui servizi di telefonia dei consumatori,
- Il tracciamento, la traduzione e l'identificazione delle origini delle chiamate tramite un ufficio di commutazione centrale e sistemi di analisi e monitor della rete.
- L'utilizzo di sistemi di fatturazione, indirizzi e servizi per identificare le origini delle chiamate, quando possibile,
- Lavorando direttamente con i carrier di lunga distanza e locali, con i fornitori di comunicazione senza fili e di altro tipo e i dipartimenti degli uffici per le chiamate non desiderate
- Lavorando con le forze dell'ordine per rilasciare le informazioni concernenti i soggetti identificati e
- Contattando i soggetti identificati per conto dei clienti quando necessario per risolvere i problemi dalle chiamate di minacce o fastidiose fino alle chiamate generate automaticamente dai computer, quelle falsificate, gli invii massivi di fax e tutte le altre tipologie di chiamate non desiderate identificate dai clienti.

Applicazione della legge: Mentre i regimi di conformità alle normative possono coprire le chiamate indesiderate effettuate dalle imprese legittime, non sono un deterrente sufficiente per coloro che cercano di ingannare il pubblico. In questi casi, una ferrea applicazione della legge è spesso l'unico mezzo per affrontare questi abusi. Alcune nazioni hanno preso una posizione aggressiva per quanto riguarda l'uso della telefonia, sia tramite VoIP o altri mezzi, atto ad indurre in

errore i consumatori. Il perseguimento dei casi ai sensi delle leggi a tutela dei consumatori sia nei procedimenti civili che penali ha portato a sanzioni sostanziali e pene detentive. Per affrontare pienamente il problema delle frodi del telemarketing è essenziale che le forze dell'ordine, il settore e le autorità di regolamentazione continuino a rintracciare e perseguire i truffatori il cui utilizzo di un ID chiamante falsificato e di chiamate automatizzate ha causato frodi di centinaia di milioni di dollari in tutto il mondo.

ATTACCHI DI TIPO DENIAL OF SERVICE TELEFONICO (TDOS)

Il TDoS è un attacco mirato a rendere inutilizzabile il sistema telefonico di una società o di un servizio pubblico. Saturando un numero di telefono dall'esterno o addirittura la totalità dei canali di comunicazione dell'impresa, gli aggressori possono impedire rapidamente tutte le chiamate in entrata e in uscita. Gli attacchi TDOS sono molto simili a quelli di Denial of Service Distribuito (DDoS) effettuati verso siti web. Gli aggressori tengono in ostaggio il sistema telefonico e rendono indisponibile il sistema fino a quando la vittima non paga una determinata somma.

Per avviare un attacco TDoS, l'attaccante deve avere accesso a diversi canali di comunicazione o più account Session Initiation Protocol (SIP) (di solito hackerati). Successivamente utilizzano macchine per chiamate automatizzate per chiamare contemporaneamente e ripetutamente uno o più numeri di telefono della vittima. Gli "Strumenti" o i "kit" per effettuare gli attacchi TDoS sono facilmente disponibili su Internet. E' anche molto facile, per persone senza scrupoli, commissionare un tale attacco. Questo tipo di attacco avviene normalmente a scopo di interruzione, estorsione, o per coprire le frodi.

MIGLIORI PRATICHE TDOS:

Application Layer Gateway:

E' importante che le aziende di tutte le dimensioni proteggano i propri sistemi VoIP e di telefonia. I sistemi VoIP sono come qualsiasi altro sistema di reti di computer e quindi richiedono una protezione dalle stesse tipologie di attacchi informatici di qualsiasi altro server di rete. Mentre i firewall legacy possono avere problemi nel gestire correttamente le esigenze specifiche dei sistemi VoIP, molti dispositivi di sicurezza moderni sono dotate di Application Layer Gateway (ALG) progettati specificamente per gestire i protocolli specifici del VoIP. Alcuni di questi ALG possono anche fornire funzionalità di sicurezza specifiche per il VoIP, come ad esempio impedire la raccolta di informazioni sull'elenco degli account SIP o impedire a livello di rete gli attacchi DoS.

Proteggere I Servizi Essenziali

La "Canadian Interconnection Steering Committee" (CISC) ha valutato il tema degli attacchi di tipo Denial of Service telefonici nei gruppi di lavoro per i servizi di emergenza e ha proposto le migliori pratiche per la protezione dei sistemi essenziali.http://www.crtc.gc.ca/public/cisc/nt/NTCO0570.docx

Segnalazione alle forze dell'ordine:

Gli attacchi TDoS hanno il potenziale per rendere indisponibili infrastrutture critiche compresi i servizi di emergenza, di pronto intervento e gli ospedali. Questo può sollevare questioni di

sicurezza nazionale e non appena viene rilevato un attacco deve quindi essere riportato all'autorità competente.

Falsificazione delle Chiamate (Call Spoofing)

Lo spoofing del numero chiamante è un metodo per falsificare le informazioni relative all'origine del chiamante. Anche se non è un attacco di per sé è comunemente utilizzato per mascherare l'identità di un utente malintenzionato o per effettuare attacchi più efficaci. Attraverso tale spoofing, i truffatori prendono di mira i consumatori con chiamate che sembrano provenire dal paese o dal prefisso del consumatore, o da una fonte per lui attendibile. Alcuni chiamanti hanno utilizzato numeri associati con le agenzie governative e hanno falsificato funzionari del governo per truffe in materia fiscale e sull'immigrazione. Spesso la fonte di queste chiamate è da un continente diverso, aggiungendo una maggiore complessità per rintracciare e bloccare le frodi.

Segnalazione / Blocco selettiva (*09)
I codici di servizio verticali, come ad esempio * 09, dovrebbero essere definiti dal settore per consentire ai consumatori di avviare facilmente la cattura automatica e l'analisi delle informazioni di rete relative a chiamate indesiderate. Questo sistema funziona permettendo ad un consumatore, che riceve una chiamata telemarketing fraudolenta o un altro tipo di chiamata indesiderata, di riagganciare e premere *09 per segnalare le informazioni complete della chiamata al proprio carrier, alle forze dell'ordine, alle autorità di regolamentazione e anche per bloccare automaticamente future chiamate da quel numero.

Migliori Pratiche per la Prevenzione dal Call Spoofing:

Legislazione contro le frodi:
Generalmente dovrebbe essere universalmente illegale trasmettere informazioni di identificazione del chiamante fuorvianti o inesatte con l'intento di frodare, causare un danno, o ottenere ingiustamente qualcosa di valore.[lxii]

Negli Stati Uniti, ad esempio, il "Truth in Caller ID Act" del 2010 proibisce lo spoofing, o la falsificazione volontaria del numero di telefono o del nome visualizzato per mascherare l'identità del chiamante per *scopi nocivi o fraudolenti*.[lxiii] Questo tipo di definizione permette l'uso dello spoofing per fini non ingannevoli, ad esempio l'uso di numero dell'ufficio del medico quando chiama dalla sua linea privata.

Educazione dei Consumatori: La fiducia dei consumatori nel sistema telefonico è a rischio con l'aumento della falsificazione del Caller ID e delle chiamate automatizzate. Per proteggere i consumatori da frodi e altri danni che si basano sull'uso improprio della piattaforma telefonica, le agenzie governative hanno lanciato campagne di informazione. Ad esempio, la US Federal Trade Commission (FTC) ha pubblicato avvisi sui propri siti web, blog post e promosso i loro sforzi nell'applicazione della legge per aumentare la consapevolezza dei consumatori circa le robocall e la falsificazione dell'ID chiamante.[lxiv] Favorire una maggiore consapevolezza dei consumatori circa l'uso dello spoofing può contribuire a ridurre il danno risultante che può derivare da frodi promosse attraverso questa tecnica. Gli sforzi nell'educazione dei consumatori dovrebbero anche

aumentare la consapevolezza relativa ai vari strumenti che i consumatori possono utilizzare per proteggersi da chiamate indesiderate.

SERVIZI HOSTING E CLOUD

I servizi cloud e hosting rappresentano uno dei cambiamenti recenti più significativi nella tecnologia dell'informazione. Le aziende sono eccitate dalla possibilità di controllare meglio i costi, aumentare l'agilità e di disinvestire dalla complessa infrastruttura IT. Le preoccupazioni per la sicurezza e la perdita del controllo diretto stanno, tuttavia, soffocando l'adozione e la crescita di questa nuova tecnologia.

Le minacce online e dei dispositivi mobili sono in aumento per quando riguarda l'hosting e servizi cloud. Secondo un recente articolo su The Economist, il mercato globale dei servizi di cloud computing dovrebbe raggiungere 176 miliardi di $ nel 2015. Questo importo rappresenta ancora una piccola parte della spesa IT complessiva, ma la spesa per l'hosting e per i servizi cloud è in rapida crescita. Attualmente, la maggior parte delle altre parti del settore sono stagnanti o addirittura in declino, ma entro il 2017 la spesa per il Cloud si prevede raggiunga un totale di 240 miliardi di $ all'anno.[lxv]

Questa sezione categorizza tipi di hosting e delinea le aree di preoccupazione. Essa fornisce uno sguardo al panorama delle minacce attuali per gli ambienti di hosting online e Cloud e un breve sguardo alle soluzioni utilizzate per contrastare tali criticità.

TIPOLOGIE DI HOSTING

I provider di hosting facilitano il funzionamento di Internet e gestiscono gli ingranaggi che lo fanno funzionare. I provider di hosting variano in dimensione da imprese individuali alle imprese a livello mondiale note in tutto il mondo. Ciò che differenzia i fornitori di infrastrutture Internet da altri aspetti di Internet è il loro relativo anonimato. Queste aziende generalmente operano dietro le quinte per facilitare l'uso di Internet per tipologie di imprese così diverse come può essere una lavanderia a secco locale o una banca globale.

TIPOLOGIE DI INFRASTRUTTURE INTERNET

Il mercato dei servizi di infrastrutture Internet si comprende meglio guardando le tipologie sottostanti utilizzate per fornire servizi per l'utente finale. Queste si dividono in tre componenti:

- **Struttura**: La struttura, comunemente indicata come data center, è l'edificio fisico alla base di un provider di infrastruttura Internet. Esso può essere di proprietà del fornitore di infrastrutture o gestito da terzi. Questa struttura ospita i router e gli switch che si collegano a Internet insieme ai server - fisici e virtuali - che ospitano i contenuti, i dati e le applicazioni.

- **Server fisico**: Il server fisico è situato in un armadio o in un rack collocato nel data center. E' dove vengono archiviati e protetti i contenuti e le applicazioni.
- **Server virtuale:** Il server virtuale è una partizione virtualizzata di un server fisico. Il server virtuale agisce e si comporta esattamente come un server fisico con una differenza marginale, in termini di prestazioni. Un singolo server può letteralmente ospitare fino a decine di server virtuali.

I provider di hosting possono essere generalmente collocate in una delle cinque categorie principali:

i. Hosting condiviso

ii. Hosting gestito standard

iii. Hosting gestito complesso

iv. Infrastruttura Cloud

v. Colocation

CATEGORIA DI INFRASTRUTTURE INTERNET

Hosting Condiviso: L'hosting condiviso è uno spazio condiviso su un server fisico senza isolamento tra gli utenti e senza una allocazione delle risorse definita. Le risorse limitate di un server fisico sono condivise - spesso in modo non uniforme - tra tutti i clienti che risiedono su di esso. I provider possono letteralmente ospitare centinaia di clienti su un singolo server.

L'hosting condiviso è comunemente utilizzato per pubblicare i contenuti statici o dinamici del sito web. Le piattaforme di blogging come WordPress e semplici applicazioni di e-commerce sono spesso eseguiti in ambienti di hosting condiviso e sono attivati tramite installazioni automatiche.

Le organizzazioni che fanno un uso di risorse molto limitato usano l'hosting condiviso per comunicare e costruire una presenza su Internet. L'hosting condiviso in genere costituisce il livello più basso del mercato delle infrastrutture. Gli utilizzatori tipici sono: i consumatori, le piccole imprese, gli uffici domestici, e i blogger.

Hosting Gestito Standard: Un fornitore di infrastrutture che fornisce hosting gestito di tipo standard tipicamente affitta server fisici dedicati (a volte indicato come “il ferro”) o server virtuali ospitati in strutture data center del provider di infrastrutture. I clienti in genere affittano le risorse del server con un contratto prestabilito.

Nei casi di hosting gestito di tipo standard, i clienti hanno accesso root al server e in genere lo gestiscono in autonomia. Il fornitore di infrastrutture offre un livello base di supporto e gestisce alcuni ma limitati compiti di gestione come la manutenzione hardware, i backup e l'installazione di sistema operativo e del software del server web.

Il server vero e proprio è di proprietà del fornitore e affittato al cliente. Come risultato, il cliente non dovrà affrontare un ciclo di aggiornamento IT. Potrà semplicemente passare a un altro server che si adatta alle sue esigenze. Di solito non paga per gli aggiornamenti hardware, né ha alcun obbligo di rimanere sul server affittato.

L’hosting gestito standard è progettato per soddisfare configurazioni e carichi di lavoro relativamente semplici. Le piccole imprese in genere utilizzano l’hosting gestito standard come alternativa all’acquisto e all'installazione di risorse IT.

Hosting Gestito Complesso: L’hosting gestito di tipo complesso si applica sia ai server dedicati fisici che ai server virtuali. Ci sono molte somiglianze tra hosting gestito standard e complesso, ma la differenza fondamentale è il livello di supporto amministrativo e ingegneristico per il quale il cliente paga. Queste differenze sono dovute sia alla maggiore dimensione e alla maggiore complessità della distribuzione dell'infrastruttura. Il fornitore di infrastruttura interviene per prendere in consegna la maggior parte della gestione.

L’hosting gestito di tipo complesso richiede una vasta gamma di competenze e capacità nelle aree di amministrazione dei sistemi, gestione di database, sicurezza, controllo, gestione dei log, disaster recovery e backup. I servizi di gestione possono anche estendersi a livello dell’applicazione, anche se questo tende ad essere piuttosto raro al di fuori delle applicazioni aziendali più standard. Una tipica distribuzione di hosting gestito avrà una serie di dispositivi aggiuntivi, tra cui i database, applicazioni e server Web, firewall e bilanciatori di carico. Invece di memoria locale, i clienti spesso utilizzano memoria collegata alla rete o “storage area network” (SAN). Essi potranno anche acquistare i servizi di backup e di replica o impostare strategie di disaster recovery. Alcuni fornitori di infrastrutture aumentano le loro offerte standard, fornendo servizi di consulenza che vanno al di sopra e oltre al livello di servizi standard di gestione.

Quando si tratta di hosting gestito complesso, l’hosting tende ad essere limitato ad un piccolo numero di applicazioni rispetto al totale di quelle che effettivamente esistono all'interno dell'azienda. L’hosting gestito è per molti versi utilizzato come un'estensione del data center locale.

L’hosting gestito complesso viene utilizzato per configurazioni e carichi di lavoro grandi e complessi. E' anche un’opzione quando le organizzazioni hanno bisogno di attività molto specifiche

e specializzate come la sicurezza e la “compliance”. L’hosting gestito è una alternativa all'acquisto e all’installazione di risorse IT e ha una componente di risparmio sui costi. E' un modo per alleviare il carico di lavoro del personale IT interno e liberare risorse.

Infrastruttura Cloud: L’infrastruttura Cloud è fondamentalmente una forma più flessibile e scalabile di server di hosting virtuale. La caratteristica fondamentale di un'infrastruttura cloud è la disponibilità delle risorse. La dimensione di un server può essere aumentata o diminuita immediatamente oppure entro un brevissimo lasso di tempo. Così, invece di una certa quantità di risorse, l'utente finale può regolare la capacità dell’infrastruttura in funzione della domanda (o della sua mancanza). In genere, il cloud si fattura su base oraria, ma incomincia ad essere fatturato anche in incrementi di minuto per minuto, consentendo in tal modo il consumo di basato sull’utilità.

Il Cloud è anche altamente resistente senza singoli punti di vulnerabilità. Le risorse cloud sono mobili e possono automaticamente effettuare il “failover” su di un altro host fisico. Possono essere riavviate ovunque e in qualsiasi momento tramite l’apposito set di strumenti e di funzionalità. Questa flessibilità consente cloud per essere integrato in ambienti ibridi in qualsiasi data center, sia in outsourcing o in locale.

Colocation: La colocation rappresenta la fornitura di capacità dei data center per le organizzazioni che necessitano di un luogo fuori sede per ospitare o "collocare" server, dispositivi di archiviazione e di rete che possiedono e gestiscono. Gli elementi di base della colocation sono lo spazio, l’alimentazione, il raffreddamento e la connettività Internet. Nel modello di colocation, il cliente ha accesso ad un'area designata all'interno di una struttura in cui si può installare i dispositivi che possiede o che ha affittato. Molti fornitori di colocation offrono la gestione remota e servizi di monitoraggio. Alcune fornitori affittano apparecchiature ai clienti.

La realtà del settore delle infrastrutture Internet può diventare più complessa in quanto i limiti dei servizi delle infrastrutture tendono a mischiarsi. Ad esempio, la linea di demarcazione tra hosting gestito standard e complesso è sempre meno chiara dato che i fornitori si spingono verso categorie di mercato superiori e si espandono verso i servizi a valore aggiunto. Lo stesso si può dire per la linea tra hosting gestito - nella varietà dei server virtuali - e l’infrastruttura cloud. Un certo numero di offerte di hosting di server virtuali assomigliano all’infrastruttura cloud. Queste potrebbero non avere tutte le caratteristiche del cloud, ma potrebbero far vedere abbastanza per confondere la linea di demarcazione e creare alcune zone d'ombra.

IL PANORAMA DELLE MINACCE

Di seguito è riportato un elenco dei tipi di abuso più comunemente osservati tra i fornitori di servizi hosting e cloud. L'elenco non pretende di essere completo e potrebbe cambiare nel tempo.

- **Spam (in uscita)**: Con spam si intende qualsiasi e-mail elettronica commerciale indesiderata o non richiesta. I fornitori dovrebbero garantire che gli utenti finali seguano le Migliori Pratiche Correnti per gli speditori indicate dal M^{3}AAWG[lxvi]. I provider di hosting

vorranno anche iscriversi al maggior numero di segnalazioni di Feedback Loop che riescono a processare.

- **Spamvertising (reindirizzamento e payload)**: Lo "Spamvertising" si verifica quando l'utente finale di un fornitore di hosting incarica un terzo per pubblicizzare la propria presenza sul Web. La maggior parte delle segnalazioni di spam sono causate dagli utenti finali che inviano e-mail ai potenziali clienti per tentare di vendere qualche prodotto o servizio sopravvalutato. I fornitori che ricevono una di queste denunce sono probabilmente nel flusso in quanto mittenti del messaggio di posta elettronica o host del sito pubblicizzato.
- **Phishing in uscita (hosting e in ingresso per le credenziali dei clienti)**: Il phishing avviene soprattutto quando l'account di un utente finale è stato compromesso, quasi sempre a causa di script obsoleti gestiti da utenti finali. Un sito di phishing è un sito fraudolento che pretende di essere una società legittima, come una banca, una compagnia di carte di credito, o PayPal e che spinge l'individuo ad inserire informazioni riservate. I phisher quindi hanno tutto il necessario per frodare l'individuo. (Vedere la sezione Phishing e Social Engineering per ulteriori informazioni.)
- **Pagine violate o deturpate (hostate sul client)**: Mentre le denunce di phishing spesso rientrano in questa categoria, non tutti gli account violati sono utilizzati per il phishing. Alcuni possono essere semplicemente deturpati e i dati degli utenti finali danneggiati o distrutti. Frequentemente gli hacker possono anche iniettare codice dannoso o caricare bot che sono impostati per causare ulteriori problemi come compromettere siti, download nascosti o reindirizzare ad altri contenuti dannosi. Le terze parti e le forze dell'ordine analizzano questi eventi e forniscono informazioni su come ripristinare i siti violati. La maggior parte degli account sono compromessi a causa di installazioni CMS (Content Management System) obsolete quali Joomla o WordPress.
- **Materiale pedopornografico (hostato sul client)**: Per una corretta gestione di queste problematiche fare riferimento alle Migliori Pratiche Comuni sulla gestione del materiale pedopornografico pubblicate dal M^3AAWG (https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Disposition_CAM-2015-02.pdf).
- **Copyright e questioni di proprietà del marchio / intellettuale (hostate sul client)**: Per la legge statunitense online sul copyright vedere http://www.copyright.gov/reports/studies/dmca/dmca_executive.html. In altre giurisdizioni si applicano regimi di copyright diversi.
- **Denial of Service Distribuito e altro traffico ostile in uscita:** Mentre il servizio cloud o i fornitori di hosting possono avere protezioni migliori rispetto alle imprese individuali più piccole, questi fornitori di servizi possono anche soffrire di un rischio maggiore di attacchi DDoS rispetto alle altre imprese on-line, perché, in effetti, aggregano il rischio di tutti i loro clienti. Un attacco ad un cliente può influenzare gli altri e potenzialmente l'intera struttura di hosting a causa della forte dipendenza da infrastruttura condivisa.
- **Iscrizioni dannose:** gli hacker costruiscono una botnet utilizzando solo account di tipo

“prova gratuita” e "freemium" su servizi applicativi di hosting on-line. Gli hacker quindi utilizzano un processo automatizzato per generare indirizzi di posta elettronica unici e sottoscrivere i servizi con questi account gratuiti *en masse*, assemblando una botnet basata sul cloud costituita da migliaia di computer.

MAGGIORI AREE DI PREOCCUPAZIONE

Installazioni CRM Vulnerabili/Non aggiornate:

Considerando che ci sono più di 67 milioni di siti WordPress, che rappresentano il 23 per cento di tutti i siti web[lxvii], in tutto il mondo - e che gli editori stanno utilizzando la piattaforma per creare blog, siti di notizie, siti aziendali, riviste, social network, siti sportivi e altro ancora - non è sorprendente che molti criminali abbiano gli occhi puntati sul come ottenere l'accesso a questo Content Management System (CMS). Ad esempio, Drupal, una piattaforma di CMS in rapida crescita, è stato preso di mira nel 2014 tramite software di terze parti installato sull' infrastruttura stessa di Drupal.org.

Non è solo la popolarità di questi sistemi che li rende obiettivi ambiti. Molti dei siti su questi server, anche se attivi, sono stati abbandonati dai loro proprietari. Ci sono verosimilmente milioni di blog abbandonati e domini acquistati non utilizzati, ed è probabile che molti di questi siti siano stati compromessi dai criminali informatici. Gli esperti di sicurezza Cisco prevedono che il problema non potrà che peggiorare nel momento in cui sempre più persone dai mercati emergenti di Internet nel mondo creano un blog o un sito web, solo per lasciarlo inutilizzato successivamente.

L'uso diffuso di plugin, che sono progettati per estendere la funzionalità di un CMS e per alimentare i video, animazioni e giochi, è stato dimostrato essere un vantaggio per i criminali informatici che cercano di ottenere l'accesso non autorizzato alle piattaforme. Ad aggravare questo problema molti plugin non sono più aggiornati dai loro autori e costringono coloro che li utilizzano e dipendono da questi a non aggiornare la loro installazione corrente per non perdere il lavoro o la funzionalità sul loro sito. Molte compromissioni di CMS osservate dai ricercatori Cisco nel 2013 si possono far risalire a plugin scritti nel linguaggio web di scripting PHP che sono stati progettati male e senza aver in mente la sicurezza.

Le statistiche raccolte dalla società di sicurezza Sucuri mostrano un totale di 3143 vulnerabilità in WordPress in 15 diverse categorie.[lxviii] Con questa quantità di vulnerabilità, i consumatori di WordPress hanno iniziato a mantenere il loro software aggiornato ma oltre il 30 per cento dei siti WordPress sta ancora utilizzando la versione 3 o inferiore[lxix], lasciando tali siti aperti allo sfruttamento da parte di soggetti malintenzionati.

Attacchi DDoS:

Poiché gli attacchi DDoS sono stati a lungo considerati una "notizia vecchia" in termini di tecniche di criminalità informatica, molte imprese erano fiduciose che le misure di sicurezza che avevano messo in atto potessero fornire una protezione adeguata. Tale fiducia è stata recentemente scossa da attacchi DDoS su larga scala nel 2012 e 2013, tra cui l'operazione Ababil, che è stato indirizzata a diverse istituzioni finanziarie e che, molto probabilmente, ha avuto una motivazione politica.

I leader del settore avvertono che gli attacchi DDoS dovrebbero essere una delle maggiori preoccupazioni di sicurezza per le organizzazioni del settore pubblico e privato perché si ritiene che campagne future possano essere ancora più ampie. Le organizzazioni, in particolare quelle che

operano o che hanno interessi in settori che sono già obiettivi primari come i servizi finanziari e l'energia, hanno bisogno di essere eccezionalmente prudenti. Dal 2010 al 2013 le interruzioni non pianificate a causa di attacchi DDoS sono aumentate dal 2 al 13 per cento in totale[lxx]. In realtà, un confronto tra il quarto trimestre del 2013 e il 2014 ha mostrato che attacchi DDoS sono aumentati del 90 per cento, sottolineando che gli attacchi sono sempre in aumento.[lxxi] Il costo medio totale di queste interruzioni è aumentato da 613.000 a 822.000 $ nello stesso periodo di tempo.[lxxii]

Alcuni attacchi DDoS hanno preso una piega preoccupante. Essi sono stati utilizzati per distogliere l'attenzione da altre attività criminali, come la frode telematica. Questi attacchi possono sopraffare il personale delle banche, evitare che i clienti ricevano le notifiche di trasferimento fondi, e impedire ai clienti di denunciare le frodi. Le istituzioni finanziarie sono raramente in grado di recuperare le loro perdite finanziare. Un attacco simile, che ha avuto luogo il 24 dicembre 2012, ha preso di mira il sito di un istituto finanziario regionale della California e ha contribuito a distrarre i funzionari della banca dall'espropriazione di un conto online di uno dei suoi clienti, facendo guadagnare ai ladri più di 900.000 $.

L' approfondimento rapido della competenza nel compromettere i server ospitanti servirà solo a rendere più facile per i criminali informatici lanciare attacchi DDoS e rubare dalle organizzazioni scelte. Con la requisizione di una parte dell'infrastruttura di Internet, i malfattori possono usufruire di un'ampia larghezza di banda, predisponendosi per lanciare un grande numero di campagne importanti. Questo sta già accadendo: nel mese di agosto del 2013, il governo cinese ha riferito che il più grande attacco DDoS che abbiano mai visto ha reso inutilizzabile l'Internet nella Cina per circa quattro ore.

Anche gli spammer stanno usando attacchi DDoS per colpire le organizzazioni che ritengono essere un ostacolo alla loro generazione di entrate. Nel marzo 2013, l'ente non-profit Spamhaus (che tiene traccia degli spammer e ha creato la lista di blocco Spamhaus, un elenco di indirizzi IP sospetti) è stato il bersaglio di un attacco DDoS che ha temporaneamente reso inagibile il suo sito web e ha rallentato il traffico Internet in tutto il mondo. Gli aggressori sarebbero stati affiliati con CyberBunker dei Paesi Bassi, un fornitore di hosting con i termini d'uso molto permissivi, e STOPhaus, che ha pubblicamente espresso la sua avversione verso le attività di Spamhaus. L'attacco DDoS è avvenuto dopo che il servizio Spamhaus, ampiamente utilizzato, ha incluso CyberBunker sulla sua lista nera.

Server Mal configurati in Ambienti Non Gestiti:
Con l'avvento del Cloud, gli utenti hanno ora la possibilità di creare e impostare un intero server in una frazione del tempo che era prima necessario con hardware fisico. Questo ha permesso agli utenti di essere in grado di creare facilmente la propria infrastruttura con poca o nessuna conoscenza su come funzionano i sistemi predisposti. Anche se questo cambiamento ha dato agli utenti la possibilità di fare molto di più di quello che facevano prima, ha aperto una nuova sfida nel prevenire e nel fermare l'abuso di questi sistemi.

Molti dei server virtualizzati e non gestiti non vengono mantenuto con la circospezione che era già presente nel mondo dell'hardware fisico gestito. I sistemi operativi e i programmi non vengono aggiornati correttamente (o per niente) per affrontare aggiornamenti di sicurezza e vulnerabilità. Le autorizzazioni sono raramente modificate o sono impostate in modo che chiunque abbia accesso al server può apportare modifiche, lasciando un server con una porta aperta verso il mondo esterno suscettibile di attività dannose.

Alcuni programmi utilizzano metodi di comunicazione sia in entrata che in uscita che, se non configurati correttamente, possono lasciare un server come un'arma utilizzabile per attacchi DDoS riflessi, login SSH, SQL injection, ed altri attacchi che hanno la capacità di rendere inutilizzabili i sistemi oggetto di attacco per una notevole quantità di tempo. Inoltre, questi errori di configurazione permettono ai malintenzionati di accedere ai siti o alle informazioni ospitate sul server provocando il furto dei dati, la creazione di siti di phishing e l'hosting di malware.

Il monitoraggio di questi sistemi mal configurati e mal aggiornati è un compito enorme per le società che fanno l'hosting di questi server quindi poco viene fatto per questi sistemi fino a quando non vengono compromessi.

MIGLIORI PRATICHE

Prevenzione:

1) **Esaminare i clienti prima che causino problemi**: i fornitori di hosting sono in balia delle peggiori pratiche dei loro clienti. I fornitori devono mettere in atto un processo di valutazione per identificare in modo proattivo i clienti malevoli prima che intraprendano attività abusive. Fare sforzi per selezionare i clienti buoni per la società di hosting stessa è un altro modo per preservare la sicurezza dell'ambiente di hosting.
2) **Obbligare i clienti a mantenere i software aggiornati:** Il mancato aggiornamento del software, hardware o firmware dell'ambiente è una delle cause primarie di abusi nell'hosting. I contratti con i clienti dovrebbero specificare che i clienti dovranno fare del loro meglio per mantenere i loro sistemi aggiornati.
3) **Addestrare il personale a contatto con i clienti per la sensibilizzazione alla sicurezza:** I team a contatto con i clienti, come il supporto, le vendite e il marketing non affrontano la maggior parte delle sfide quotidiane che sono la norma per i team anti abuso o di sicurezza. La formazione dovrebbe fornire a questi team la consapevolezza di quando dire ad un cliente o ad un prospect che le sue pratiche non rispettano i termini d'uso o la politica di utilizzo consentita del sistema che stanno utilizzando o di quello su cui stanno cercando di predisporre un ambiente.
4) **Impedire gli abusi ai bordi della rete:**
    a) Prendere in considerazione sistemi hardware di "intrusion detection" (IDS).
    b) Utilizzare sistemi di scansione software e firewall.
    c) Promuovere l'utilizzo di firewall per applicazioni web.
    d) Utilizzare l'assegnazione dei diritti a più livelli per i clienti di valore.
    e) Contrattare con i clienti per proteggere la sicurezza.
    f) Massimizzare il contatto con i clienti e proteggere l'identità del cliente.

g) Incoraggiare l'utilizzo di password robuste da parte i clienti.
h) Utilizzare le migliori pratiche in materia di reti IPv6: IPv6 offre così tanti indirizzi che non vi è alcuna necessità - e nessuna ragione - per condividere un singolo indirizzo IP tra più clienti. La pratica migliore è quella di assegnare ad ogni cliente uno spazio separato /64 di indirizzi IPv6. Anche sui più piccoli sistemi condivisi fisicamente ogni cliente e ogni sito web dovrebbe avere un indirizzo univoco. Questo rende più facile monitorare la fonte di abuso, rende possibile per i destinatari di abusi bloccare il cliente incriminato senza bloccare tutti gli altri sullo stesso host, e può rendere più facile sospendere e rinnovare il servizio quando necessario.
i) I fornitori di hosting devono mantenere forti pratiche e sistemi di sicurezza interna. Tutte le misure raccomandate sopra sono inutili se i malintenzionati possono indovinare le password usate dal personale del provider. I provider di hosting devono essere conformi agli standard PCI.

Rilevamento e identificazione:

1) **Utilizzare identificatori dei clienti riservati:** Le società di hosting dovrebbero creare un identificatore univoco per ogni specifico cliente. Questo identificatore deve essere comprensibile solo alla società di hosting ed essere incomprensibile a terzi. Questo mantiene la riservatezza dell'identità del cliente ma dà la società di hosting un modo semplice ed efficace per identificare i clienti.

2) **Creare "role account" per domini di rete:** Gli indirizzi email "role account" e quelli specificati dalla RFC come prassi devono essere creati per ogni dominio e dominio cliente predisposto su una rete.

3) **Mantenere accurati record per lo SWIP e per il WHOIS dell'IP:** Le aziende di hosting dovrebbero mantenere chiare e precise voci per il loro Registro Internet Regionale (RIR) per quanto riguarda l'allocazione dello spazio IP, tra cui le sotto-allocazioni maggiori di una /27 per i clienti. Questi elenchi WHOIS dovrebbero includere "role account" funzionali alla segnalazione abusi.

4) **Impostare telemetria interna che segnala lo stato della rete:** Gli esempi includono,
   a) Scansioni automatiche della rete,
   b) Analisi del traffico e
   c) Monitor per filtrare lo spam in uscita.

5) **Rendere la segnalazione abusi semplice:** I fornitori di hosting devono fornire servizi al pubblico per segnalare gli abusi che essi percepiscono provenire dalla rete in questione. I fornitori devono quindi rispondere a tali segnalazioni e agire di conseguenza. I provider di hosting dovrebbero mantenere i canali di comunicazione ridondanti per tenere conto del fallimento di un qualsiasi canale.
   a) E-mail,
   b) Telefono,

c) Messaggistica instantanea (chat),
d) Sistemi di ticketing,
e) Rapporti di stato dei siti web e
f) Presenza sui social media.

6) **Rispondere prontamente alle lamentele:** Le segnalazioni individuali dovrebbero avere un messaggio di risposta automatica (AUTO-ACK) con una specificità tale da essere separate dalle altre osservazioni che il denunciante ha fatto. Essi dovrebbero includere la segnalazione iniziale, un numero di ticket originale e qualsiasi altra informazione che assicurerà all'utente che il reclamo è stato ricevuto ed è in fase di gestione.

7) **Considerare di designare segnalatori di fiducia:** Gli autori delle segnalazioni possono essere di alta qualità e ad alta priorità. Tali fonti possono essere sia interne che esterne. È opportuno prevedere un servizio di corsia prioritaria, pur mantenendo i livelli di priorità specificati. Ad esempio, un contatto di una DNSBL (Domain Name System Blacklist) ampiamente utilizzata può essere designato come un segnalatore prioritario, anche se un reclamo di spam da quella fonte rimarrebbe ovviamente meno significativo di un problema DDoS verificatosi nello stesso momento.

8) **Predisporre Feedback Loops (FBL) e report automatici:** Gestire gli FBL sottoscrivendo i programmi FBL aiuta i fornitori ad evitare di essere listati nelle DNSBL, limita il danno alla reputazione e consente al personale di gestire proattivamente i clienti abusivi e abusati (compromessi).

9) **Implementare Metriche di Confronto:** Stabilire metriche sistematiche affinché siano utilizzate da parte dei fornitori di hosting permette ai fornitori di hosting e alle forze dell'ordine di identificare efficacemente l'abuso e confrontare i dati con tutto il settore. [lxxiii]

Rimedio:
Le priorità di rimedio forniscono alle società di hosting e ai clienti le linee guida per risolvere i problemi. Le raccomandazioni per quanto riguarda la priorità dei reclami dovranno anche tener conto della gravità e serietà dell'abuso e la portata di un determinato problema. Inoltre, devono essere prese in considerazione la fonte della segnalazione e la gravità del danno alla reputazione della società di hosting e del cliente. Una campagna di spam di massa può essere di priorità maggiore rispetto alla presenza di una botnet dormiente. Deve essere fatta una valutazione caso per caso dei problemi che possono far cambiare il livello di priorità per un determinato fornitore o di un determinato cliente.

Rispondere rapidamente ai problemi di alto profilo / alta priorità:
La maggior parte dei reclami ricevuti da qualsiasi società di hosting richiedono solo un avviso di ricevimento. Alcuni casi, tuttavia, quali i reclami di alto profilo, le richieste di chiusura immediata e la rimozione dalle blacklist, richiedono una attività aggiuntiva. Il cliente o l'agenzia che ha effettuato la segnalazione devono essere inizialmente contattati per comunicare che il problema è in corso di

gestione. Dovrebbero essere ricontattati quando il problema è stato risolto. Dovrebbero essere necessarie comunicazioni multiple solo se ci sono problemi persistenti o eccezionali. Comunicare in modo proattivo quando si verificano eventi a livello del settore o aziendale.

Nel caso di un compromesso serio o di una vulnerabilità che potrebbe mettere più clienti o un gruppo specifico di clienti a rischio, dovrebbe essere sviluppato un piano di comunicazione per renderli consapevoli del problema e fornire istruzioni generali su come risolverlo. Se la violazione ha coinvolto l'accesso a dati personali, dovreste sapere quali sono i vostri obblighi sono in conformità ai requisiti regionali o nazionali, tra cui l'ambito della comunicazione alle persone interessate e l'avviso alle appropriate autorità giudiziarie. Tali comunicazioni devono essere inviate in modo tempestivo. Inoltre il personale di supporto deve essere messo al corrente del problema e avere le istruzioni appropriate per risolvere la questione con i clienti che hanno bisogno di assistenza.

Affrontare efficacemente i clienti problematici:

1) Confermare la validità della segnalazione.
2) Informare il cliente della compromissione. Includere eventuali istruzioni verificate al cliente che potranno aiutare per la risoluzione del problema.
3) Fornire al cliente i Termini e Condizioni pertinenti ed eventuali regolamenti governativi applicabili che potrebbero essere stati violati e hanno causato la notifica di violazione o la sospensione del servizio. In questo modo, il contratto con il cliente rimane intatto. La notifica al cliente protegge la società di hosting da problematiche di potenziali clienti o di segnalatori esterni che potrebbe tradursi in contenzioso.
4) Accordare al cliente del tempo per porre rimedio al problema o, se c'è un contratto in corso, dare il tempo al provider di provvedere al rimedio del problema per proprio conto.
5) Confermare che la segnalazione è stata risolta.
6) Chiudere l'incidente. Se necessario, avvisare il segnalatore che il problema è stato risolto. Sospendere il servizio ai clienti che non rispondono.

MOLESTIE ONLINE

Non passa giorno che i media on-line e quelli tradizionali non riportino una qualche forma di molestia on-line. Anche se si va da azioni fastidiose a quelle terribilmente serie, è chiaro che, se i servizi Internet diventano sempre più disponibili in tutto il mondo, così anche il problema delle molestie on-line aumenterà frequenza. Le molestie on-line possono andare dai messaggi on-line o dalle immagini digitali imbarazzanti o crudeli, alle minacce on-line, il bullismo e commenti negativi, allo stalking attraverso e-mail, siti web, social network e messaggi di testo.

Ogni fascia di età è vulnerabile alle molestie online, che è un problema crescente nelle scuole nei campus universitari e anche sul posto di lavoro. Le molestie online sono diventate un problema perché Internet fornisce un qualche anonimato, che è attraente per gli aggressori in quanto la loro intimidazione risulta difficile da rintracciare. Purtroppo le voci, le minacce e le foto possono essere diffusi su Internet molto rapidamente.

Ci sono stati tentativi con diversa attuabilità per regolare[lxxiv] e anche scrivere leggi[lxxv, lxxvi] per affrontare alcuni aspetti della questione, ma nel complesso si tratta di una zona che è, ad ora, onnipresente ed ha bisogno di un ulteriore esame e un migliore sviluppo della pratica.

Di seguito un elenco delle varie forme di molestie on-line e, a seguire, alcune semplici linee guida su come evitare molestie.

Catfishing – Un profilo falso viene impostato su siti di incontri e social media per attirare una potenziale vittima in una relazione on-line per poi truffarla ed estorcere denaro.

Molestie tramite Annunci (Craigslist)– Gli annunci vengono creati sostenendo che una persona è alla ricerca di sesso o di altri comportamenti personali atipici con le risposte impostate per arrivare al numero di telefono di casa o all'indirizzo e-mail della vittima.

Cyberbullismo – Fondamentalmente cyberstalking, ma legato più ai bambini e ai ragazzi molestati dagli altri studenti attraverso siti web, siti di social media, bacheche, applicazioni per e-mail o per smartphone e sms.

Cyberstalking – Quando allo stalker è stato chiesto di fermarsi e continua a contattare ripetutamente la vittima on-line. Questo può assumere molte forme, e-mail, messaggi o commenti su siti web, bacheche, SMS commenti e post attraverso applicazioni smartphone, ecc.

Doxing – Trovare informazioni personali su un individuo, quindi pubblicarle on-line, compreso l'indirizzo di casa, numero di telefono di casa, numero di cellulare, indirizzo di lavoro e il numero di telefono, informazioni di parenti, ecc. [lxxvii]

Impersonificazione – Quando un utente crea profili on-line o account usando il nome, le foto e informazioni identificative di un'altra persona e poi la pubblica post come quella persona. Questo può essere usato per screditare la vittima o, in alcuni casi, come un primo passo verso attività fraudolente a scopo di lucro. Ad esempio, rubando foto e informazioni da un profilo di social media e creandone uno nuovo, un malintenzionato può confondere amici e parenti della vittima e

contattarli con uno schema del tipo “stranded traveller”[lxxviii], in cui la persona sostiene di aver viaggiato da qualche parte ma ha perso il loro portafoglio. Gli amici più vicini hanno più probabilità di cadere in questa truffa e inviare denaro perché credono che il profilo finto sia reale.

Mobbing – Quando un gruppo di utenti si rivolge ad uno o più individui come una "banda" perseguitando e molestando nella speranza di cacciarli via Internet, farli espellere da scuola o fare loro perdere l’occupazione. [lxxix]

Outing – Rivelare il fatto (o l’accusa) che qualcuno è gay, lesbica, trans-genere o condividere on-line senza il permesso informazioni sui feticismi, condizioni mediche e altro.

Furto di Identità Online – Rubare informazioni personali per prendere il controllo dell'identità o per vendere le informazioni in modo che possano essere utilizzate in modo fraudolento al fine di ottenere carte di credito o altri strumenti finanziari, come prestiti o mutui.

Recensioni Vendicative – Pubblicare commenti falsi o molto critici a siti come ripofferport.com. Queste possono anche assumere la forma di pubblicazioni di informazioni personali e giudizi su una persona su siti come thedirty.com.

Porno Vendicativo – Pubblicare foto o video semi-nudi/nudi su siti web e altri forum senza il consenso dell’interessato. Come con altri metodi di molestie on-line, la maggior parte degli autori tentano di mantenere l'anonimato mentre sono impegnati nella vendetta porno tramite la creazione di account di posta elettronica gratuiti o falsi profili per pubblicare in merito alle loro vittime.

Sexting – Foto o video semi-nudi/nudi vengono condivisi online tramite applicazioni come Snapchat, Instagram, Vine o siti web come Facebook. Mentre il sexting di per sé non costituisce una molestia on-line, può diventare molestia se le foto vengono inviate ai destinatari che non vogliono o se il destinatario a sua volta le ri-distribuisce.

SWATting – Effettuare una chiamata simulata alla polizia per richiedere un intervento armato, di solito dal Team SWAT. [lxxx] Questo a volte prende a volte la forma di un allarme bomba falso o una falsa segnalazione di una presa di ostaggi armata.

Trolling – Gli utenti online che tentano di incitare la reazione con la pubblicazione di commenti intenzionalmente marginali o aggressivamente maleducati. Questo a volte comprende i “troll” assunti come, per esempio, gli individui associati a campagne politiche possono essere pagati per incitare argomenti o inviare punti di vista risibilmente estremi dei loro avversari per screditarli.

Migliori Pratiche per limitare le molestie on-line[lxxxi]:

Limita i posti dove si pubblicano informazioni personali: Essere consapevoli di chi può accedere alle informazioni di contatto o ai dettagli sui tuoi interessi, abitudini o sull'occupazione per ridurre l'esposizione agli aggressori. Ciò può limitare il rischio di diventare una vittima e può rendere più facile identificare l'aggressore se vieni preso di mira.

Evita di intensificare la situazione: Rispondendo con ostilità si rischia di provocare l'aggressore. A seconda delle circostanze, prendere in considerazione di ignorare il problema. Spesso, bulli e aggressori traggono vantaggio dalla reazione delle loro vittime. Se voi o il vostro bambino ricevete messaggi elettronici indesiderati, siano essi messaggi SMS o email, valutate di cambiare l'indirizzo di posta elettronica. Il problema si può fermare. Se si continua a ricevere messaggi al nuovo account, ci possono essere gli estremi per intraprendere un'azione legale.

Documenta il cyberbullismo: Tenere traccia di tutte le attività on-line (e-mail, pagine web, messaggi di social media, ecc.) comprese le date e gli orari relativi. Mantenere sia una versione elettronica che una copia stampata.

Segnala bullismo alle autorità competenti: Se tu o tuo figlio siete molestati o minacciati, segnalate l'attività alle autorità locali. La polizia locale o quella nazionale sono spesso buoni punti di partenza. C'è una distinzione tra libertà di parola e reati punibili. Le forze dell'ordine e gli avocati possono aiutare a chiarire le implicazioni legali. Può anche essere opportuno segnalarlo a funzionari della scuola che possono avere politiche diverse per trattare le attività che coinvolgono gli studenti.

Possiedi la tua presenza online: Quando disponibile, imposta le impostazioni di privacy e di sicurezza sui siti web al livello che si ritiene adeguato per la condivisione delle informazioni. Ad esempio, modifica le impostazioni dei tuoi siti di social media per limitare la visibilità di tutti i messaggi "solo agli amici". E ' corretto limitare le modalità di condivisione delle informazioni.

Utilizza password robuste e domande di verifica: Non riutilizzare le password tra i siti. Se avete difficoltà a ricordare le password, utilizzare un gestore di password, come IPassword (Agilebits) e utilizza l'autenticazione a due fattori quando possibile sui social media e per account di posta elettronica. Se pubblichi informazioni personali sui social media come la tua scuola elementare e il nome da nubile di tua madre, usa risposte diverse per domande di verifica che possono essere richieste dal vostro istituto finanziario, in modo che le risposte non possono essere determinate facilmente. Inoltre, invece di usare le informazioni personali reali, considera la scelta di una frase senza senso che puoi ricordare e usala per tutte queste domande (ad esempio, il nome da nubile della madre: Batman)

Più sicuro per me, più sicuro per tutti:
Quello che fai online può influenzare tutti - a casa, al lavoro e in tutto il mondo. Praticare buone abitudini online avvantaggia la comunità digitale globale.

Educa la tua comunità: Ci sono molte risorse disponibili che possono aiutare a scoraggiare il cyberbullismo. Fornite tramite le autorità governative[lxxxii]

CONCLUSIONE

Negli ultimi anni, il contesto delle minacce online e mobili è cambiato radicalmente, destinate ad una gamma sempre più ampia di individui, aziende e reti. L'emergere di nuove tecnologie permette lo sviluppo di attacchi più sofisticati sfruttando le vulnerabilità attraverso una gamma più ampia di servizi, canali e piattaforme.

I metodi tradizionali per affrontare le minacce online, con software anti-virus, firewall, e campagne di educazione continuano ad essere una parte importante della difesa. Il malware e le botnet che sono emersi in questi ultimi anni si sono trasformati per evitare il rilevamento e la cura. Per far fronte a queste nuove ed emergenti minacce, la comunità internazionale deve entrare maggiormente nell'ecosistema Internet e sviluppare ina maniera collaborativa approcci multi-sfaccettati e multi-laterali per combatterle.

Questo rapporto fornisce raccomandazioni sulle migliori pratiche per i consumatori, il settore e governi per affrontare le minacce sulla rete e sui dispositivi mobili. Queste includono le raccomandazioni per i consumatori ad essere più proattivi nel mettere in sicurezza i propri dispositivi; per i service provider ad implementare tecnologie e pratiche di sicurezza raccomandate senza indugio; per i governi a garantire che ambienti normativi e legislativi moderni siano in atto e applicati e di lavorare con le organizzazioni internazionali per promuovere sforzi di collaborazione.

Queste raccomandazioni sono una serie di strumenti per gestire le minacce on-line, mobili e vocali. Tuttavia, le minacce descritte in questo rapporto sono solo un'istantanea della situazione delle minacce di oggi. Mentre le attività online cambiano, l'uso del mobile computing cresce e gli utenti di Internet e le imprese cambiano le loro risposte e le difese al le minacce esistenti, queste minacce si sposteranno e si adatteranno a sfruttare le nuove vulnerabilità e a perseguire nuovi obiettivi.

Mettendo in pratica queste raccomandazioni si avrà un approccio multilaterale concertato. A tal fine, gli autori di questo rapporto incoraggiano fortemente l'OCSE e altre organizzazioni internazionali ad unirsi al M^{3}AAWG e al LAP e di impegnarsi con le organizzazioni che governano e amministrano le infrastrutture di Internet. Inoltre, al fine di stare al passo con la minaccia ambientale che cambia, tutte le organizzazioni interessate dovrebbero cominciare a collaborare più attivamente nel monitoraggio delle minacce e nell'attuazione di nuove misure, se necessarie, per affrontarle.

- **Truffa 419:** così chiamata a causa del codice penale nigeriano Capitolo 38, sezione 419 che affronta la frode. "Qualsiasi persona che, con qualsiasi falsa pretesa e con l'intento di frodare, ottiene da un'altra persona qualsiasi cosa in grado di essere rubata o induce qualsiasi altra persona a fornire a chiunque qualsiasi cosa che possa essere rubata, è colpevole di un crimine, ed è responsabile della reclusione per tre anni. " Queste sono le famose e-mail del principe nigeriano o altri sistemi in cui è richiesto di spendere soldi in cambio di ricchezze incalcolabili alla fine dello schema.

- **Frode di pagamento anticipato:** le e-mail che propongono il pagamento anticipato, tra cui un pagamento supplementare, per i servizi offerti. Nella forma più comune, viene richiesto di inviare il pagamento a terzi. Dopo che la terza parte liquida questo pagamento, il pagamento originale si scopre essere contraffatto e ritirato dal conto in banca della vittima.

- **Border Gateway Protocol (BGP):** il protocollo che effettua le decisioni di base del routing su Internet. Mantiene una tabella di reti IP o "prefissi" che designano rete la portata e la capacità della rete tra sistemi autonomi. [1]

- **Cache:** archivio di informazioni utilizzate di recente in un luogo al quale si può accedere in maniera estremamente veloce. Ad esempio, un browser Web utilizza una cache per memorizzare sul disco rigido le informazioni che riguardano i siti web visitati di recente. Poiché l'accesso al disco rigido del computer è molto più veloce dell'accesso a Internet, il caching dei siti web può accelerare la navigazione Web in modo significativo. [2]

- **Distributed Denial of Service (DDoS):** un tipo di cyber-attacco volto a schiacciare o comunque compromettere la capacità del sistema di destinazione di ricevere informazioni e interagire con qualsiasi altro sistema. Per esempio, inviando uno o un numero elevato di messaggi indesiderati per impedire ad un server o aduna rete di funzionare correttamente.

- **Drive by Download:** il download involontario di software per computer da Internet. Un utente può autorizzare un download senza capirne le conseguenze, come nel caso di un programma eseguibile contraffatto, oppure il download può avvenire tutto senza la consapevolezza dell'utente. [3]

- **E-mail Service Providers (ESP):** una società che fornisce servizi di posta elettronica ad altre aziende. Questi servizi possono includere la raccolta il mantenimento di elenchi di indirizzi e-mail, l'invio di e-mail di massa agli indirizzi negli elenchi, la rimozione di indirizzi errati, e la gestione dei reclami e delle segnalazioni di abuso causate dall'invio massivo di email.

- **Firewall:** un hardware e / o un dispositivo software su un computer che controlla l'accesso tra una rete privata e una rete pubblica come Internet. Un firewall è progettato per fornire una protezione bloccando l'accesso non autorizzato al computer o alla rete.

- **Global System for Mobile Communication (GSM):** uno standard sviluppato dalla European Telecommunications Standards Institute (ETSI) per descrivere i protocolli per le reti cellulari digitali di seconda generazione (2G) utilizzate dai telefoni cellulari. [4]

- **Ingress filtering:** una tecnica usata per fare in modo che i pacchetti in entrata siano in realtà provenienti dalle reti da cui sostengono di essere da bloccando i pacchetti provenienti da falsi indirizzi IP. [5]
- **International Association for Assigned Names and Numbers (ICANN):** coordina gli identificatori univoci, tra cui il Domain Name System (DNS), gli indirizzi Internet Protocol (IP), l'allocazione dello spazio, l'assegnazione dell'identificatore di protocollo, la gestione dei domini di primo livello (Top-Level) generici (gTLD) e nazionali (ccTLD) e la gestione delle funzioni dei root server.[6]
- **Money Mule: u**na persona che trasferisce il denaro o la merce rubata da un paese all'altro, sia di persona, tramite un servizio di corriere, o per via elettronica. I "money mule" online in genere esistono come risultato del phishing o delle truffe di malware. [7]
- **Nodo:** nella comunicazione di dati, un nodo di rete fisico può essere una attrezzatura per i circuiti di terminazione (DCE) come un modem, un hub, un bridge o uno switch; o un'apparecchiatura terminale dati (DTE), quale un ricevitore digitale telefonico, una stampante o un computer host, ad esempio un router, una workstation o un server.
- **JavaScript:** Un linguaggio di scripting che permette agli autori di creare pagine web interattive
- **Phishing:** un tentativo di ottenere informazioni personali per rubare l'identità o altre informazioni sensibili come numeri di carte di credito o coordinate bancarie a scopo di frode. Ad esempio, un messaggio di posta elettronica può sembrare provenire dalla banca del ricevente chiedendo di visitare un sito web per confermare i dettagli del conto, ma invece indirizza a un sito web falso in cui vengono raccolte le informazioni personali.
- **SMShing - phishing via SMS or text message:** un link che porta ad un sito web fraudolento viene inviato via SMS o il messaggio indirizza il destinatario a chiamare un numero di telefono dove l'attacco di social engineering continuerà.
- **Spoofing**: fingere di essere un'altra persona o organizzazione per far sembrare che un messaggio email o una telefonata provenga da una parte diversa dalla sua origine reale.
- **Domini di Primo Livello (Top-Level Domains - TLD):** i TLD sono al livello più alto nella gerarchia del Domain Name System di Internet e rappresenta l'ultima parte del nome di dominio. Ad esempio, nel nome di dominio www.example.com, il dominio di primo livello è .com. La responsabilità per la gestione della maggior parte dei domini di primo livello è delegata ad organizzazioni specifiche dalla Internet Corporation for Assigned Names and Numbers (ICANN), che gestisce la Internet Assigned Numbers Authority (IANA), ed ha il compito di mantenere la zona DNS principale.
- **Typosquatters:** si affidano ad errori, come errori di digitazione fatti dagli utenti Internet quando si inserisce un indirizzo web nel browser. Se un utente accidentalmente dovesse inserire un indirizzo web errato potrebbe essere portato ad un sito alternativo di proprietà di un cybersquatter. Una volta nel sito del typosquatter, l'utente può anche essere indotto a pensare

che quello sia in realtà il sito reale attraverso l'uso di loghi, layout del sito web o contenuto copiato o simile.[8]

- **VoIP**: l'instradamento di conversazioni vocali via Internet. E' diverso rispetto ad una telefonata, fatta dal telefono di casa o dell'ufficio che passa attraverso la rete telefonica pubblica commutata.
- **Vishing - phishing via Voice over IP:** viene effettuata una chiamata al destinatario, spesso utilizzando una funzionalità VoIP comune per impostare un falso ID chiamante, chiedendo al ricevente di visitare un sito web o chiamare un numero di telefono dove l'attacco di social engineering continuerà. Diversi schemi comuni includono "Supporto tecnico Microsoft", inadempimenti fiscali scaduti, oppure "verrà arrestato se non pagherà una multa."
- **Web injection:** un tipo di exploit di sicurezza in cui l'attaccante aggiunge codice in una casella di un modulo Web per ottenere l'accesso alle risorse o apportare modifiche ai dati. Le caselle di inserimento sono in genere utilizzate per l'autenticazione degli utenti, tuttavia la maggior parte moduli Web non hanno meccanismi in atto per bloccare un input diverso dai nomi e dalle password. A meno che non vengono prese queste precauzioni, un utente malintenzionato può utilizzare le caselle di inserimento per inviare la propria richiesta al database, che potrebbe consentire loro di scaricare l'intero database o interagire con esso in altri modi illeciti. [9]

[i] DCWG, http://www.dcwg.org/

[ii] Conficker Working Group, http://www.confickerworkinggroup.org/

[iii] WinFixer, Wikipedia, http://en.wikipedia.org/wiki/WinFixer

[iv] Symantec, 2015 Internet Security Threat Report, Volume 20, http://www.symantec.com/security_response/publications/threatreport.jsp

[v] McAfee, McAfee Labs 2014 Threats Predictions, http://www.mcafee.com/ca/resources/reports/rp-threats-predictions-2014.pdf

[vi] Microsoft, Download Center, http://www.microsoft.com/en-us/download/details.aspx?id=44937

[vii] Secunia, http://secunia.com/vulnerability_scanning/personal/

[viii] PCMag, "The Best Password Managers for 2015", http://www.pcmag.com/article2/0,2817,2407168,00.asp; PCMag, "You Can't Remember Good Passwords, So You Need a Password Manager", http://securitywatch.pcmag.com/security-software/332153-you-can-t-remember-good-passwords-so-you-need-a-password-manager

[ix] PCMag, "The Best Free Antivirus for 2015", http://www.pcmag.com/article2/0,2817,2388652,00.asp

[x] Internet Engineering Task Force (IETF), "Recommendations for the Remediation of Bots in ISP Networks", http://tools.ietf.org/html/rfc6561

[xi]Aquilina, James, Eoghan Casey, and Cameron Malin, Malware Forensics: Investigating and Analyzing Malicious Code, Elsevier, Inc., 2008.

[xii] Safe Code, http://www.safecode.org

[xiii] M[3]AAWG, "ABCs for ISPs", https://www.m3aawg.org/abcs-for-ISP-code

[xiv] National Security Agency, Security Configuration Guides, http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

[xv] National Vulnerability Database, "National Checklist Program Repository", http://web.nvd.nist.gov/view/ncp/repository

[xvi] Verizon, 2014 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2014/

[xvii]*Ibid.*

[xviii] APWG, "APWG Phishing Attack Trends Reports", https://apwg.org/resources/apwg-reports/

[xix] APWG, "APWG Global Phishing Survey 1H2014: Trends and Domain Name Use", http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf

[xx] RSA, "2014 Cybercrime Roundup", www.emc.com/collateral/fraud-report/h13929-rsa-fraud-report-jan-2015.pdf

[xxi] Center for Strategic and International Studies, "2014 McAfee Report on the Global Cost of Cybercrime", http://csis.org/event/2014-mcafee-report-global-cost-cybercrime

[xxii] O'Connor, Fred, PCWorld, "Monetising Medical Data is Becoming the Next Revenue Stream for Hackers", March 21, 2015

[xxiii] IT Governance, "123 Million Health Care Records Breached so far this Year", March 26, 2015, http://www.itgovernanceusa.com/blog/123-million-health-care-records-breached-so-far-this-year/

[xxiv] Sender Policy Framework, "Project Overview", http://www.openspf.org/

[xxv] DKIM.org, http://dkim.org/

[xxvi] ICANN, http://www.icann.org/

[xxvii] DMARC, http://dmarc.org

[xxviii] In most western countries, financial institutions will reimburse consumers for fraud losses that were made through the financial institution.

[xxix] McAfee, "McAfee Labs Report Highlights Success of Phishing Attacks with 80% of Business Users Unable to Detect Scams", September 4, 2014, http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx

[xxx] SANS, "Building an Effective Phishing Program", http://www.securingthehuman.org/media/resources/presentations/STH-Presentation-PhishingYourEmployees.pdf

[xxxi] Stop. Think. Connect., "Resources", www.stopthinkconnect.org/resources/

[xxxii] StaySafeOnline.org, "National Cyber Security Awareness Month", https://www.staysafeonline.org/ncsam/

[xxxiii] APWG, "How to Redirect a Phishing Site Web Page to the APWG.ORG Phishing Education Page", http://phish-education.apwg.org/r/how_to.html

[xxxiv] Anti-Phishing Working Group (APWG), apwg.org

[xxxv] Messaging Malware Mobile Working Group, m3aawg.org

[xxxvi] Online Trust Alliance, otalliance.org
[xxxvii] Merchant Risk Council, merchantriskcouncil.org
[xxxviii] Forum of Incident Response and Security Teams, first.org
[xxxix]FBI, "DNS Changer Malware" November 9, 2011, http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf
[xl] RFC Editor, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", May 2000, http://www.rfc-editor.org/info/bcp38
[xli] RFC Editor, "Ingress Filtering for Multihomed Networks", March 2004, http://www.rfc-editor.org/info/bcp84
[xli] https://www.arin.net/policy/nrpm.html
[xlii] RFC Editor, "Ingress Filtering for Multihomed Networks", March 2004, http://www.rfc-editor.org/info/bcp84
[xliii] https://www.arin.net/policy/nrpm.html
[xliv] Counterpoint, "Market Monitor: Handset and Spartphone Markets Q4 2014", January 29, 2015, http://www.counterpointresearch.com/marketmonitor2014q4
[xlv] The Realtime Report, "Mobile Comemerce: Online Retail Sales from Mobile Devices Double in Last Year", May 3, 2012, http://therealtimereport.com/2012/05/03/mobile-commerce-online-retail-sales-from-mobile-devices-double-in-last-year/
[xlvi] Corra, "Mobile Shopping Trends by Device", February 3, 2015, http://corra.com/mobile-ecommerce-trends-2015
[xlvii] GSMA Intelligence, "Global Data", https://gsmaintelligence.com/
[xlviii] Worldometers, "Current World Population", http://www.worldometers.info/world-population/
[xlix] IDC, Llamas, Ramon, Anthony Scarsella, William Stofega, "Worldwide Mobile Phone 2015-2019 Forecast and Analysis", April 2015, http://www.idc.com/getdoc.jsp?containerId=prUS23455612 (iscrizione richiesta)
[l] Symantec, "Internet Security Threat Report", April 2015, Volume 20, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA- internet-security-threat-report-volume-20-2015-social_v2.pdf
[li] *Ibid.*
[lii] Australia, Bulgaria, Belgium, France, Germany, Ghana, Greece, Ireland, Kenya, Netherlands, USA, South Africa, Spain, Sweden, Switzerland
[liii] Lookout, "2014 Mobile Threat Report," https://www.lookout.com/static/ee_images/Consumer_Threat_Report_Final_ENGLISH_1.14.pdf
[liv] Bibat, Aerol, "GGTracker Malware Hides as Android Market", Android Authority, June 21, 2011 http://www.androidauthority.com/ggtracker-malware-hides-as-android-market-17281/
[lv] ICT, "Statistics", http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
ICT, "ICT Facts and Figures, The World in 2014", http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf; http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf
[lvi] *Compare for example:* 47 U.S.C. § 227(b)(1)(A)(iii) *with* 47 U.S.C. § 227(b)(1)(B) and 47 U.S.C. § 227(b)(2)(B).
[lvii] FCC, "'One Ring' Phone Scam," *available at* http://www.fcc.gov/guides/one-ring-wireless-phone-scam.
[lviii] CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart"
[lix] See for e.g., T-Lock Call Blocker – Version N2, http://hqtelecom.com/callblocker?gclid=CMmt_raT6cECFc1_MgodhnEAWg; CPR Call Blocker Product Page, http://www.cprcallblocker.com/purchase.html; Digitone Call Blocker Plus, http://www.digitone.com; and Sentry Dual Mode Call Blocker, http://www.plugnblock.com/?gclid=CJmKkbaT6cECFSFgMgodJRIAGA; Privacy Corp Caller ID Manager, http://www.privacycorps.com/products/.
[lx] Weisbaum, Herb, "Want to get rid of those $#%@ robocalls? There's an app for that," http://www.cnbc.com/id/101758815#.
[lxi]Alliance for Telecommunications Industry Solutions, "Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document," https://www.atis.org/docstore/product.aspx?id=26137
[lxii] Prepared Statement of The Federal Trade Commission Before the United States Senate Committee on Commerce, Science and Transportation, Subcommittee on Consumer Protection, Product Safety, and Insurance on 'Stopping Fraudulent Robocall Scams: Can More Be Done?', Washington, DC, July 10, 2013 ("Senate Hearing"), , http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=c1eec086-3512-4182-ae63-

d60e68f4a532&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2013

[lxiii] *Truth in Caller ID Act*, 47 U.S.C. § 227(e); cf. 16 C.F.R. Part 310.4(a)(8).

[lxiv]Federal Trade Commission, "Robocalls Gone Wrong", https://www.consumer.ftc.gov/media/video-0027-robocalls-gone-wrong

[lxv] The Economist, "The Cheap, Convenient Cloud," April 18, 2015, http://www.economist.com/news/business/21648685-cloud-computing-prices-keep-falling-whole-it-business-will-change-cheap-convenient?fsrc=scn/tw/te/pe/ed/thecheapconvenientcloud

[lxvi] M[3]AAWG, "M[3]AAWG Sender Best Common Practices, Version 3, Updated February 2015," https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[lxvii] http://w3techs.com/technologies/history_overview/content_management/all/y

[lxviii] https://wpvulndb.com/statistics

[lxix] http://w3techs.com/technologies/details/cm-wordpress/all/all

[lxx] http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 13

[lxxi] http://www.stateoftheinternet.com/resources-web-security-2014-q4-internet-security-report.html

[lxxii] http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 14

[lxxiii] Noroozian, A. et al., "Developing Security Reputation Metrics for Hosting Providers, http://www.tudelft.nl/fileadmin/Faculteit/TBM/Onderzoek/Publicaties/hosting-metrics.pdf

[lxxiv] Twitter boss vows to crack down on trolls and abuse: http://www.theguardian.com/technology/2015/feb/26/twitter-costs-dealing-abuse-harassing-dick-costolo

[lxxv] Suicide of Rehtaeh Parsons: https://en.wikipedia.org/wiki/Suicide_of_Rehtaeh_Parsons

[lxxvi] Granby, Quebec, Canada moves to fine people insulting police on social media: http://www.cbc.ca/news/canada/montreal/granby-moves-to-fine-people-insulting-police-on-social-media-1.3045816

[lxxvii] 4chan Bullies Fitness Guru Scooby Off YouTube With Doxxing and Threats: http://newmediarockstars.com/2013/07/4chan-bullies-fitness-guru-scooby-off-youtube-with-doxxing-and-threats-video/

[lxxviii] How I got caught up in a 'stranded traveller' phishing scam: http://www.theguardian.com/money/2013/nov/13/stranded-traveller-phishing-scam

[lxxix] How One Stupid Tweet Blew Up Justine Sacco's Life: http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html?_r=0

[lxxx] The World Has No Room For Cowards: http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/

[lxxxi] Stay Safe Online, https://www.staysafeonline.org/stay-safe-online/for-parents/cyberbullying-and-harassment

[lxxxii] From the US FTC, https://www.consumer.ftc.gov/articles/0028-cyberbullying ; Nigeria, http://www.mamalette.com/parenting-3/cyber-bullying-nigerian-parents-need-know/; ACMA, http://www.cybersmart.gov.au/Schools/Cyber%20issues/Cyberbullying.aspx; RCMP, http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm; South African Police Service, http://www.saps.gov.za/child_safety/teens/cyber_bullying.php;

Steering Committee

Andre Leduc, Manager, National Anti-Spam Coordinating Body, Industry Canada

Alyson Hawkins, Policy Analyst, Industry Canada

Christina Adam, Policy Analyst, Industry Canada

Jerry Upton, Executive Director, Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

Lisa Foley, Policy Analyst, Industry Canada

Neil Schwartzman, Executive Director, CAUCE.org

Contributors

Alex Bobotek, Lead, Mobile Messaging Anti-Abuse Strategy and Architecture, AT&T

Amy Hindman, Principal Engineer, Verizon

Betsy Broder, Counsel for International Consumer Protection, Federal Trade Commission

Bruce Matthews, Manager, Anti-spam Team, Australian Communications & Media Authority

Carlo Catajan, iCloud Mail & iMessage Anti-Abuse, Apple Inc.

Carlos Alvarez, Sr. Manager, Security Engagement, SSR Team, ICANN

Chris Boyer, Assistant Vice President, Global Public Policy, AT&T

Christian Dawson, President, ServInt and Chairman, i2Coalition

David Jevans, Chairman, Anti-Phishing Working Group (APWG)

Eric Freyssinet, Ministère de l'intérieur, France

Foy Shiver, Deputy Secretary-General, APWG

Francis Louis Tucci, Manager, Network Repair Bureau, Verizon Wireless

Frank Ackermann, M³AAWG Public Policy Committee Co-chair

Gary Warner, Director of Research in Computer Forensics, University of Alabama at Birmingham

Jay Opperman, General Manager, CSP, Damballa

Jayne Hitchcock, President, WOAH

Jeff Williams, Dell SecureWorks

Jessica Malekos Smith, Student, UC Davis School of Law

John Levine, President, CAUCE.org

Jonathan Curtis, Norse Corporation

Justin Lane, Anti-Abuse Manager, Endurance International

Karen Mulberry, ISOC

Lee Armet, Senior Investigator, TD Bank Group

Mary Retka, Director, Network Policy, CenturyLink

Matthew Bryant, Ofcom

Matthew C Stith, Manager, Anti-abuse, Rackspace Hosting

Michael Hammer, American Greetings

Michael O'Reirdan, Comcast Fellow

Patrick Tarpey, Ofcom

Paul Vixie, CEO, Farsight Security

Peter Merrigan, Government of New Zealand

Phil Shih, Structure Research

Richard Feller, Hedgehog Hosting

Rod Rasmussen, President and CTO, Internet Identity (IID)

Sanjay Mishra, Distinguished Member of Technical Staff, Verizon

Sara Roper, Manager Information Security, CenturyLink

Sid Harshavat, Symantec

Steven Champeon, Enemieslist

Terry Zink, Program Manager, Microsoft

TR Shaw, SURBL

Venkata Atluri, Associate Professor, Alabama A&M University

Participants

Adam Panagia, Adria Richards, Alexander Falatovich, April Lorenzen, Autumn Tyr-Salvia, Bill Wilson, Bulent Egilmez, Chris Lewis, Dave Crocker, David Dewey, David Levitt, Donald McCarthy, Donald Smith, Dylan Sachs, Eric Chien, Franck Martin, Hein Dries-Ziekenheiner, Jacek Materna, Jack Johnson, Jared Mauch, Jean Marie Norman, John Cunningham, Julia Cornwell McKean, Kaio Rafael, Karmyn Lyons, Ken Simpson, Lucas Moura, Mark Collier, Matteo Lucchetti, Michael Shoukrey, Mustaque Ahamad, Nabeel Koya, Nitin Lachhani, Olivier Caleff, Patricia B. Hsue, Paul Ebersman, Peter Cassidy, Raymond Choo, Richard Clayton, Richard Gane, Rudy Brioche, Sid Harshavat, Steve Jones, Steven M. Wernikoff, Suresh Ramasubramanian, Toni Demetriou, Trent Adams, Will Clurman