

News Release

For Immediate Release

Unabhängige Studie der Georgia Tech zeigt die besten Methoden, um Kunden über einen Bot-Angriff zu informieren

SAN FRANCISCO, CA--(Marketwire - February 21, 2013) - Ein Bot, von dem angenommen wird, dass er 14 Mio. Dollar an rechtswidrigen Gewinnen erzielte, verwandelte sich in eine einmalige Lernmöglichkeit, indem er wichtige Einsichten lieferte, wie die Online-Community am besten vor Schadsoftware gewarnt und wie Kunden mit infizierten Rechnern unterstützt werden können. Auf der 27. Hauptversammlung der M3AAWG in San Francisco gaben Forscher der Georgia Tech am Dienstag im Rahmen einer Präsentation die Ergebnisse einer Studie bekannt, die auf den Reaktionen der Branche gegenüber dem DNS Changer-Trojaner basierte und Empfehlungen zur Eindämmung künftiger Malware enthielt.

Die 'DNS Changer Remediation Study' führte unter den wirksamsten Methoden zur Benachrichtigung von Kunden mit infizierten Systemen u.a. folgende Maßnahmen an: Telefonanrufe, Hinweise auf Rechnungen sowie die Weiterleitung der Benutzer zu speziellen Webseiten. Die Forscher Wei Meng und Ruian Duan arbeiten unter der Leitung von Professor Wenke Lee von der Georgia Tech School of Computer Science und waren ebenfalls der Meinung, dass "aktive" Warnungen durch soziale Medien für die Beseitigung von Malware nützlich sein können. Im Rahmen dieses Ansatzes haben Websites wie z.B. Google die Benutzer direkt über ihre Browser-Fenster darüber informiert, dass sie infiziert wurden. Diese Vorgehensweise erwies sich als effizienterer Ansatz zur Motivierung der Benutzer, ihre Systeme zu desinfizieren, wohingegen passive Warnhinweise in allgemeinen Posts oder Nachrichtenartikeln auf Plattformen der sozialen Medien weniger beachtet wurden.

"Soziale Medien können eine wichtige Rolle bei der Warnung der Benutzer vor Infizierungen ihrer Systeme und der Eindämmung von Schadprogrammen spielen. Wir sind davon überzeugt, dass der Implementierung aktiver, direkter Benachrichtigungen in einer früheren Phase des Verfahrens eine besondere Bedeutung zukommt", betonte Lee. Die Wissenschaftler untersuchten sowohl die verschiedenen Arten von Alerts für die Endanwender als auch die Anstrengungen der Netzbetreiber, ihre Kunden bei der Desinfizierung ihrer Systeme zu unterstützen, wobei Walled Gardens, DNS-Umleitungen, Antivirus-Software und Programme zur Entfernung von Schadsoftware zum Einsatz kommen. Laut Angaben von M3AAWG-Vorstand Michael O'Reirdan besteht ein Teil der Herausforderungen, denen die Branche im Bereich von Bots gegenübersteht, darin, zu bestimmen, wie die Benutzer schnell und glaubhaft darüber benachrichtigt werden, dass ihre Systeme betroffen sind, und wie dann technisch nicht versierte Kunden bei der Säuberung betroffener Rechner unterstützt werden können.

O'Reirdan ergänzte: "Die Reaktion der Branche auf die DNS Changer-Schadsoftware zeigte deutlich, wie gut Konkurrenten und Anbieter zusammenarbeiten können, wenn die Sicherheit ihrer Kunden auf dem Spiel steht. Zudem war es eine ausgezeichnete Möglichkeit, die unterschiedlichen Ansätze, die die Unternehmen zur Unterstützung ihrer Kunden entwickelt haben, auf objektive Weise zu untersuchen und die wichtige Rolle zu erkennen, die wir alle beim Schutz der Internet-Nutzung spielen. Außerdem zeigte sich, dass die aktive Mitwirkung der Anbieter von Anti-Malware- und Sicherheits-Tools, der Social-Media-Plattformen, der Strafverfolgungsbehörden, der Anbieter von Betriebssystemen sowie der Anbieter von Heimnetzwerk-Technologien von entscheidender Bedeutung war. Letztendlich wurde klar, dass es der Zusammenarbeit des gesamten Internet-Ökosystems bedarf, um die Endbenutzer zu schützen."

Die Daten, die in der Studie zur Feststellung der Infizierungs- und Säuberungsraten verwendet wurden, wurden in anonymisierter Form von bedeutenden ISPs aus aller Welt bereitgestellt, wobei die DNS Changer Working Group

(DCWG) die Daten an das Forscherteam des Georgia Tech Information Security Center (GTISC) weiterleitete. Um die verschiedenen Benachrichtigungsarten und die Schlichtungsverfahren klassifizieren zu können, verschickten die Forscher Umfragen an die Netzbetreiber und fragten sie, wie sie die Kunden benachrichtigten, die von der DNS Changer-Malware betroffen waren und welche Schlichtungsverfahren die einzelnen ISPs konkret einsetzten, um ihre Kunden bei der Säuberung ihrer Rechner zu unterstützen. Laut Lee erhielten jene ISPs, die keinerlei Maßnahmen hinsichtlich der Malware einleiteten, den Wert zugeteilt, von dem ausgehend die Messung der Wirksamkeit der anderen Ansätze durchgeführt wurde.

Zwischen 2007 und 2011 setzte der DNS Changer-Trojaner bei Internet-Suchen an und leitete die Webbrowser infizierter Computer auf betrügerische Websites weiter, wobei die vom Rove Digital-Werbenetzwerk betriebenen betrügerischen DNS-Server verwendet wurden. Wenn die betrügerischen DNS-Server jedoch zu dem Zeitpunkt vom Netz genommen worden wären, als die vermeintlich verantwortlichen Esten verhaftet wurden, dann hätten betroffene Nutzer keinen Zugang mehr zum Web gehabt. Die DCWG war eine Gruppe, die die Strafverfolgungsbehörden hinsichtlich der Auswirkungen beriet, die Strafverfolgungsmaßnahmen auf die Endanwender haben könnten. Die DCWG half zudem beim Betrieb und der Überwachung der "sauberen" DNS-Server, die vom November 2011 bis zum Juli 2012 infolge der Verfügung eines US-Gerichts vom Internet Systems Consortium (ISC) auf legale Weise betrieben wurden. Dies bedeutete, dass Millionen von Benutzern darüber informiert wurden, dass ihre Rechner infiziert waren und gesäubert werden mussten - statt plötzlich den Zugriff auf das Internet zu verlieren.

Die vollständige Fassung der 'DNS Changer Remediation Study' ist auf der M3AAWG-Website unter https://www.maawg.org/sites/maawg/files/news/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf verfügbar.

Über die Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

Die Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) stellt einen Zusammenschluss mehrerer Unternehmen dar, die gemeinsam gegen Bots, Malware, Spam, Viren, Denial-Of-Service-Attacken und ähnliche Online-Angriffe vorgehen. M3AAWG (www.M3AAWG.org) repräsentiert über eine Milliarde Postfächer einiger der größten Netzbetreiber weltweit. Dabei setzt M3AAWG auf die gesamte Erfahrung seines globalen Mitgliedernetzwerks, um mit Hilfe von Technologien, Zusammenarbeit und politischen Maßnahmen gegen Angriffe auf bereits bestehende Netzwerke und neue Dienste aktiv vorgehen zu können. Sie informiert außerdem Entscheidungsträger weltweit über technische und operative Probleme im Zusammenhang mit Online-Missbrauch und Messaging. Die M3AAWG hat ihren Sitz in San Francisco im US-Bundesstaat Kalifornien und beschäftigt sich mit den Anforderungen des Marktes. Sie wird von größeren Netzbetreibern und Messaging-Anbietern unterstützt.

M3AAWG-Vorstand: AT&T (NYSE: [T](#)); Cloudmark, Inc.; Comcast (NASDAQ: [CMCSA](#)); Constant Contact (NASDAQ: [CTCT](#)); Cox Communications; Damballa, Inc.; Eloqua; Facebook; France Telecom (NYSE und Euronext: [FTE](#)); Google; PayPal; Return Path; Symantec; Time Warner Cable; Verizon Communications und Yahoo! Inc.

M3AAWG-Vollmitglieder: 1&1 Internet AG; Adaptive Mobile Security LTD; Adobe Systems Inc.; AOL; BAE Systems Detica; Cisco Systems, Inc.; Dynamic Network Services Inc.; Email Sender and Provider Coalition; Genius; iContact; Internet Initiative Japan (IIJ NASDAQ: [IIJ](#)); Mailchimp; McAfee Inc.; Message Systems; Mimecast; Nominum, Inc.; Proofpoint; Scalify; Spamhaus; Sprint; und Twitter.

Die gesamte Mitgliederliste steht unter <http://www.m3aawg.org/about/roster> zur Verfügung.

Medienkontakt:

Linda Marcus, APR, 1+714-974-6356, LMarcus@astra.cc, Astra Communications
