M³AAWG Messaging Malware Mobile Anti-Abuse Working Group

April 4, 2023

Sent via email to *cmareview@homeoffice.gov.uk*

M³AAWG Comments on Review of the Computer Misuse Act 1990: consultation and response to call for information (accessible)

I. Introduction and Context

The Messaging Malware Mobile Anti-Abuse Working Group (M³AAWG) appreciates the opportunity to submit comments in response to the above referenced consultation.

M³AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 institutional members worldwide, we bring together stakeholders in the online community in a confidential yet open forum, developing best practices and cooperative approaches for fighting online abuse.

We applaud the UK government's interest in tackling online abuse and cybercrime. There are some areas where technical consideration may require careful execution or a light touch. In particular, we would like to note the technical, organizational, and procedural challenges and complexities that must be taken into account when legislating in this area. Considerable collateral damage may result from scoping requests too broadly. We elaborate on this below. Therefore, as an overall recommendation, we urge the UK government to liaise with key security and anti-abuse groups including M³AAWG and its partner organizations[1] as well as key UK-based and international industry stakeholders.

II. Regarding "Domain name and IP address takedown and seizure"

With regard to takedowns, the consultation document states:

> One of the simplest ways of dealing with the criminal use of domain names is to require the registrar responsible for the creation of the domain name to remove it from the list of registered domains. This will prevent anyone from accessing the website, and prevent criminals from misusing it. The power would also apply to seizing IP addresses as criminals can (and do) on occasions just use IP addresses in their malware.

While we sympathize with the goal of identifying a simple and effective solution for mitigating malicious domains and IPs, this approach can cause problems in practice. Complexities and nuances must be appropriately considered. We recommend that the UK government continue their dialogue with relevant industry players to align on a feasible approach.

We urge you to consider these specific complicating factors:

[1] M³AAWG Partner Organizations may be found at https://www.m3aawg.org/our-partners.

Collateral damage is hard to avoid. Domain names and IP addresses may be shared by multiple parties. This means that one user may be engaging in nefarious and/or unlawful behavior while other users sharing a domain or IP may be innocent, law-abiding third parties. Furthermore, the offending behavior might be a result of a successful resource takeover (e.g. hijacking) rather than the result of malicious action by any registered resource user. Failure to consider collateral damage to innocent third parties may cause unexpected (and often unacceptable) side effects. For example:

- In 2014, Microsoft, in an effort to combat malware, seized 23 domains from No-IP, the world's largest free dynamic DNS provider.[2] Unfortunately, in doing so, they inadvertently caused collateral damage to "nearly 5 million subdomains (or hostnames) and unintentionally took down service to 1.8 million innocent No-IP customers."[3]
- Other parties, such as some reverse proxy service providers,[4] may **intentionally** exploit a "human shield" business model. That is, some reverse proxy service providers interpose reverse proxy servers between the public internet and concealed backend customer servers, intentionally interleaving and comingling diverse groups of customers in order to obfuscate ownership and interdomain relationships that may exist, and to make it difficult to localize (and to block or surgically take down) the specific domains and IPs that may ultimately be associated with a particular bad actor.

Criminals move faster than due diligence. Any process meant to tackle maliciously used domains or IP addresses must recognize the agility of online criminal perpetrators. Enforcement efforts should take into account the amount of time and effort required by bona fide providers when performing due diligence on taking down resources versus the ability of malicious providers to deflect such processes and/or to warn affected criminals.

For example, a malicious actor will face little trouble in quickly redirecting resources via DNS (assuming the usual TTLs[5]), especially when employing the services of abuse-tolerant providers. Furthermore, if one domain gets taken down, criminals may swiftly substitute a (potentially previously prepared) replacement domain. The process to take down a domain cannot take days or weeks to play out. To be effective, any attempt at taking down a specific IP or domain must be able to run at a speed equal to (or preferably faster than) the speed of the abusers, ensuring that abusers can't simply execute more crisply than the defenders combating them.

This need for speedy action has been noticed many times in the past but may present considerable challenges, even for well-meaning, abuse-aware providers. To mention just a few examples:

---

[2] Dynamic DNS providers, as used in this context, allow users with non-static IP addresses (typically, residential IPs temporarily assigned via DHCP) to point a convenient and unvarying domain name at whatever IP may currently be assigned for their use. This enables the customer to host a personal web server or other server infrastructure despite the fact that they don't have a static IP address.

[3] "No-IP Takes Stock of Toll on Customers from Microsoft's Service Takedown," Cision PR Newswire, July 2014, https://www.prnewswire.com/news-releases/no-ip-takes-stock-of-toll-on-customers-from-microsofts-service-takedown-267149251.html)

[4] When a customer uses a reverse proxy service, the IP address of the customer's actual server is replaced by the IP of a reverse proxy server operated by the reverse proxy service provider, and that IP will be shared by an assortment of other randomly selected customers. In addition, the name servers the customer previously used get replaced by the name servers of the reverse proxy service provider. Those name servers will be shared by an assortment of other randomly selected customers. The actual SSL/TLS certificate the customer may have used may also be replaced with a new shared and anonymous certificate, and so on. Thus, identifying individual users/resources in a timely manner may be difficult.

[5] A domain's TTL ("time to live") is the recommended time that a domain name is meant to be cached on recursive resolvers worldwide. These values are normally measured in seconds. Long TTLs minimize load on backend servers and may allow distributed recursive resolvers to keep rolling through brief interruptions to authoritative name servers, but require patience when changing values in response to a reconfiguration, outage, or other difficulty. Shorter TTLs allow quicker changes, if needed, but result in more cache misses (and thus more DNS refresh traffic), and may result in a site becoming unreachable if the site's name isn't cached and the authoritative nameservers become non-responsive for any reason.

- Fast Flux Domains, where malicious content is replicated and rotated across a large pool of botted broadband consumer hosts using domains with short domain TTLs. See for example, the ICANN "Fast Flux Hosting Report."[6]
- The response of the Pirate Bay team to UK blocking demands directed at a particular domain name.[7]

Processes and necessary information needed to conduct takedowns must be considered, and should ideally be developed in partnership with relevant parties. Furthermore, law enforcement training needs should be taken into account so that requests are complete and made to the right party.[8]

Consider a cyber sanctions list for extra-territorial registries offering domains under country code top level domains (ccTLDs): Some registries may be domestic (i.e., UK-based), and thus subject to UK law and UK legal processes. Other registries may be required to follow local laws and processes in non-UK jurisdictions. This does not necessarily indicate an unwillingness to support UK law enforcement efforts, but rather lawful behavior by these parties. However, when dealing with recalcitrant or abuse-enabling parties in international locales, authorities may need to consider alternative, indirect approaches. One such approach might be a new cyber sanctions list modeled on existing (non-cyber-focused) sanctions lists. These include, among others:

- The **Australian** Consolidated Sanctions List[9]
- The Consolidated **Canadian** Autonomous Sanctions List[10]
- The **EU** Consolidated Financial Sanctions List[11]
- The **Inter-American Development Bank** Sanctioned Firms and Individuals List[12]
- The **UK** Sanctions List[13]
- The **UN** Security Council Consolidated Sanctions List[14]
- The **US** Specially Designated Nationals and Blocked Persons List[15]
- The **World Bank** Listing of Ineligible Firms and Individuals[16]

Is removal from the list of registered domains the right action? The consultation document proposes "requir[ing] the registrar responsible for the creation of the domain name to remove it from the list of registered domains." The intent is clear, but the proposed process may be flawed. If a registrar were simply to "remove [a domain] from the list of registered domains," that domain would normally then become immediately available for **re-registration**, either by the party that originally registered it or by an alert third party. Thus, it might be better to require that the domain be put on clientHold EPP status so that it is removed from the DNS,[17] and that it be locked so that the registrant cannot make changes to it.

---

[6] "Final Report of the GNSO Fast Flux Hosting Working Group," August 2009, http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf

[7] https://proxybay.github.io/; "How Effective is the UK Pirate Bay Blockade?" TorrentFreak, May 2018, https://torrentfreak.com/how-effective-is-the-uk-pirate-bay-blockade-180527/

[8] It is an unfortunate reality that many abuse reports and law enforcement requests are incomplete and thus not actionable, or are sent to the wrong party altogether, slowing down not only the response time for the specific case but also affecting abuse response overall by consuming time and resources.

[9] https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list

[10] https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng)

[11] https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en

[12] https://www.iadb.org/en/transparency/sanctioned-firms-and-individuals

[13] https://www.gov.uk/government/publications/the-uk-sanctions-list

[14] https://www.un.org/securitycouncil/content/un-sc-consolidated-list

[15] https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists)

[16] https://www.worldbank.org/en/projects-operations/procurement/debarred-firms

[17] The clientHold status effectively makes the domain unresolvable. https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.

III. Regarding the seizure of IP addresses

From the context of the consultation, we understand seizing an IP address to constitute one of the following special cases:

a) Denying a criminal actor ongoing access to particular IP addresses that may have been hardcoded in a piece of malware (as may be done in creating an IP-based botnet C&C [command and control] server)

b) Tunneling traffic for a given IP address to an alternative location (e.g., to sinkhole a botnet C&C server),

c) Seizing portable, customer-controlled address space (e.g., entire routable CIDR netblocks), or

d) Recovering hijacked IP address space that has been used without the permission of the original registrant.

If this is the correct understanding of the proposal, we recommend clarifying that intent. Otherwise, impracticable approaches might be considered in scope, such as seizing individual dynamic IPs from a DHCP address pool, or seizing an individual IP or small CIDR range from a much larger netblock and then routing that single IP or small CIDR range internet-wide via BGP.[18]

In modern routing practice, routers will likely ignore such more-specific BGP announcements, as they are often spurious or malicious in nature. Furthermore, the possibility of seizing IPs outside the UK scope of control will be very limited and may result in criminals moving IP addresses out of the UK, should action be taken there. In contrast to the DNS, which is hierarchical by design, there are no points of control within the addressing system. The RIRs merely record allocations; they do not control usage in any practical way.

IV. Regarding "Prevent domain name creation"

The consultation document states:

> There are cases where it is possible to predict that certain domain names will be created for criminal purposes—perhaps to mimic a business or a government department—for the purpose of committing fraud. We believe that there would be benefits to requiring the UK Registry not to register defined domain names to prevent this sort of fraud or other criminal activity.

It should be noted that Nominet, operator of the .uk top level domain, implemented sound anti-abuse practices years ago. Nominet performs analysis at the point of domain creation, preventing the creation of domain names that meet certain criteria. The analysis performed by .uk is both automated and human in order to reduce the risk of false positives.

While our reading indicates that this point refers to the .uk ccTLD only, we note that operators of generic top level domains (gTLDs) are already broadly empowered to do blocking of this sort. Section 2.6 of the 2017 ICANN base registry agreement[19] reads (emphasis added):

> **2.6 Reserved Names.** Except to the extent that ICANN otherwise expressly authorizes in writing, Registry Operator shall comply with the requirements set forth in Specification 5 attached hereto ("Specification 5"). **Registry Operator may at any time establish or modify policies concerning Registry Operator's ability to reserve (i.e., withhold from registration or allocate to Registry Operator, but not register to third parties, delegate, use, activate in the DNS or otherwise make available) or block additional character strings within the TLD at its discretion.** Except as specified in Specification 5, if Registry Operator is the registrant for any domain names in the registry TLD, such registrations must be through an ICANN accredited registrar, and will be considered Transactions (as defined in Section 6.1) for purposes of

[18] Routes more specific than an IPv4 /24 tend to not propagate due to ISP filtering for various reasons, including technical limitations.

[19] https://www.icann.org/en/registry-agreements/base-agreement.

calculating the Registry-level transaction fee to be paid to ICANN by Registry Operator pursuant to Section 6.1.

Section 2.8 further provides (emphasis added):

> 2.8 **Protection of Legal Rights of Third Parties. […] Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD**. In responding to such reports, Registry Operator will not be required to take any action in contravention of applicable law.

The consultation also specifically makes reference to "Domain Generation Algorithms (DGAs)," noting that they "give criminals an asymmetric advantage – since criminals only have to control one domain each day – whilst law enforcement may have to control hundreds or thousands of possibilities each day."

This statement is true, but it understates potential challenges of this approach. On the one hand, various registries are already blocking DGA domains proactively and with success. On the other hand, such approaches are necessarily limited in scale, sophistication, and scope. A single DGA can create and test thousands of possible domains from a potential candidate pool of a million or more DGA domain name targets per day. Depending on various factors, the quality and timeliness of preemptive blocking may vary; here law enforcement must take steps to ensure that their requests are complete and based on a correct analysis of the relevant DGA. Otherwise, this approach is likely to have little to no effect. Furthermore, rule clashes may become likely, if, for example, DGAs were to rely on dictionary word combinations. Here, candidate DGA domains might have been registered already, or might clash with legitimate names. That said, preemptive measures are extremely useful and should be pursued. However, the limitations of this approach should be discussed and aligned with affected parties.

V. Regarding "Use of the power"

The consultation states:

> A request to take down, seize or prevent the creation of a domain name would be served on the relevant party who was in control of the domain, such as the Registry (who create it and ensure that only one instance of it exists), a Registrar (who effectively leases it) or the Registrant (who rents it and deploys their content).

For the sake of clarity, we understand "take down" here to mean a suspension, which technically means setting the domain's EPP status to "clientHold" or "serverHold." We also understand that seizing a domain can take two forms:

- Changing the registration information associated with the given domain, so that the registrant changes to a new party, or
- Redirecting traffic by
    - Changing the name servers, or
    - Maintaining the name servers but changing the IP addresses that they point to.

With regard to takedowns as we understand them in the passage above, only the registrars and the registries have the technical ability to change the EPP status variables of suspended domain names. Asking a malicious actor to suspend their own malicious domain does not make sense. Suspension requests should be sent to either registrars or registries, or to both. In most cases, the registrar will be the best positioned stakeholder to implement the suspension of the domain, given that they have a direct relationship with the registrant. In other cases, as when a malicious campaign uses many domains registered across many registrars, but only a few top level domains, it may be more appropriate for the registries to modify the EPP status and set it to "serverHold."

Changing the name servers (or the IP addresses that they point to) can only be implemented by the parties that manage the DNS for each particular domain. This can be either the registrar itself, a hosting provider (which can be a different company), or yet another separate stakeholder, a DNS service provider. It must be ensured that these requests are routed to the correct party.

Registrants and registrars cannot "prevent the creation of a domain" except by registering each domain themselves (and paying any associated fees). Domain registrars can decide not to create the domains requested by their customers if they have reason to believe that the domains will be created for a malicious purpose. If they do that, however, the registrars' customers might look for another domain registration provider without such anti-abuse controls.

Registries will usually be the only parties technically positioned to fulfill the stated objective of preventing the creation of malicious domains. However, law enforcement has to have certainty that the strings they want to prevent from being registered will in fact be malicious, and that the analysis deciphering the DGA algorithm was correct.

Finally, we note that registrants are often effectively unknown and unreachable, and that at least some registrars compete for business on their willingness to let registrants be totally anonymous, up to and including offering cryptocurrency payment options. Hoping that registrants or even some non-cooperative registrars will be responsive to governmental requests may be a recipe for disappointment, and may often be dependent on the extra-territorial effect of the powers granted to law enforcement and the jurisdiction in which the registrars are located.

The consultation also states:

> A request to seize control of an IP address would be served on a network provider that controls that IP address. They might be required to tunnel that IP to another in the control of law enforcement or other trusted party.

This statement requires clarification: A network address block might be **allocated or delegated** to one party (as documented in IP Whois), given to a second party for their **use** (and then potentially subsequently further redelegated hierarchically), and **routed** by yet another party. Thus, the IP Whois data might be absent altogether, redacted, out-of-date, or otherwise inaccurate. The business relationships between the owner of the netblock and the party (or parties) subsequently authorized to use that netblock may be non-public (or at least not determinable by querying Whois data), including for wholly legitimate businesses and relationships.

This basically leaves law enforcement and other relevant parties with little option but to seek satisfaction from the party publicly seen routing the netblock containing the IP of interest. Not only does this put considerable burden on that party; in some cases, they may be located in a region hostile to Western interests in general, or be hostile to the UK in particular. In others, the party routing the netblock may be under-resourced and overwhelmed,[20] may struggle with English language requests, may do business in a region where corruption is endemic, or may not bother replying. Thus, seizure of IP addresses may prove difficult – in at least some cases. Therefore, we suggest that the UK government engage with the Numbers Community, including RIPE, AFRINIC, APNIC, ARIN, and LACNIC, and key players like ISPs to align on a feasible approach.

Furthermore, not all IP addresses match to one device or service, as in the case of Anycast addresses as well as shared IP addresses. Taking control of such an address would have wide-ranging effects.

VI. Regarding Specific Question 8

> Q8. Should multiple domains / IP addresses feature on one application or will separate applications be required?

We believe that related domains (or related IP addresses) should be consolidated on a single application if that is feasible and does not lead to an overbroad request. Even a small IPv4 /24 netblock has 256 IPs, while a IPv6 /64 netblock has 2^64=18,446,744,073,709,551,616 addresses. IP-by-IP documentation of such large resource spaces would be technically and logistically difficult, if not impossible.

[20]From empirical observation we believe that at least some cyber criminals target vulnerable providers that they know will struggle to respond.

Furthermore, different (and sometimes unknown) parties may be responsible for different parts of IP address blocks, particularly large IP address blocks controlled by cloud service providers. They may not be able to effectively or efficiently document IP address usage.

Thus, we suggest that a single application may be used for one or more CIDR netblocks, assuming that either:

- The same party controls all netblocks in the application per IP Whois, or
- The same party routes all the netblocks in the application per industry routing data (such as BGP data from Oregon Routeviews, or BGP data from https://bgp.he.net/).

As to domain names, we suggest that multiple domains may be listed on a single application, provided that:

- In the case of applications provided to a registry, all domains are from TLDs controlled by that registry,
- In the case of applications provided to a registrar, all domains are in the registrar's own domain portfolio, or
- In the case of applications provided to a domain registrant, all domains are registered to that same registrant.

Furthermore, we note that many requests to providers are misdirected, and urge that appropriate processes and training of relevant parties are ensured to limit the number of non-actionable requests that take away time and resources from actionable requests.

In addition, for print-format applications, requesters should also provide a list of domains in machine-readable form (such as a CSV or JSON file), electronically conveyed (e.g., via encrypted email, on a thumbdrive, via secure file transfer, etc.).

Another issue that presents itself is the scope of requests. If abuse is registered from one address within a IPv6 /64 network controlled by one actor, for example, would the seizure apply to the whole network or only the specific address? Here again, that address may be compromised by hackers, it might be controlled by a tenant or subscriber of the registered registrant, or the network might indeed be wholly malicious. Considerable complexity is present and options will have to be carefully chosen to avoid overbroad application or collateral damage.

VII. Regarding "Power to preserve data"

The consultation states,

> There are very few offences where it would not be conceivable that electronic evidence could be required as part of an investigation, and it is therefore essential that law enforcement agencies are able to require the preservation of existing data by a data owner to prevent that data being deleted. Preservation would require the data to be retained by the system owner in an unaltered state, pending a decision on whether a formal request for seizure of the data by a law enforcement agency should be made to a court.

A wide variety of data may potentially be targeted, including (but not limited to):

- Account-related records (account owner of record, address where service is delivered, date of initial subscription, method of payment, service[s] provisioned and date thereof, equipment provided [if any], other authorized users, etc.
- Access detail records (DHCP IP lease details, authentication data [server logins], etc.)
- IPFix ("Netflow") data
- DNS queries and responses, ideally with the IP address where the queries originated
- Web proxy cache server log data
- Email messages (sent, received-but-unread, read, in-the-trash but not yet actually deleted)
- Other files on a user's account
- Full traffic (packet) captures.

Some of this data may be compact, already routinely retained for business or technical purposes, and may be of limited sensitivity. Other data may potentially be voluminous, or incredibly privacy sensitive, even if it is only defined as metadata. Providers should not be required to build out new collection capabilities, nor be compelled to routinely collect and preserve entire categories of data not currently collected and preserved. Only data that is directly needed to address particular criminal or national security incidents and only the use of existing collection mechanisms should be in scope for this new capability.

We urge the UK government to consider approaches and measures that ensure that such requests are actionable, meaning that all requests are complete, specific, and clear, especially when it comes to the technical detail and data sought, and are addressed to the right entity and therein to an officer with appropriate authority.

With regards to preservation of digital evidence in an international context, we note that the United Kingdom is a party to the Budapest Cybercrime Convention and participates in the 24/7 Network that was created pursuant to Article 35 of the Convention, with the purpose of facilitating international requests for the preservation of digital evidence according to articles 29 and 30. Any powers given to law enforcement in this regard should be aligned with the Budapest Convention and foster cooperation and collaboration between theM3 members of the 24/7 Network.

Conclusion

Thank you for the opportunity to submit these comments. We welcome the opportunity to engage as needed to answer any questions during this process. M^{3}AAWG urges the UK government to consider our comments and suggestions. We are happy to respond to further questions as well. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,

Amy Cadagin
Executive Director, Messaging Malware Mobile Anti-Abuse Working Group
comments@m3aawg.org

P.O. Box 9125
Brea, CA 92822