**Framework on Domain Generating Algorithms (DGAs)**
**Associated with Malware and Botnets**

## Objective

The objective of this framework is to develop a common understanding of the problems facing law enforcement (LE) and registry operators in combating malware or botnets associated with domain generating algorithms (DGAs) at a large scale. It intends to explain how domain names can support malware and botnets through these DGAs, and the unique mitigation practices that are essential to addressing the resulting DNS Abuse. This framework has been jointly drafted by the Governmental Advisory Committee Public Safety Working Group (PSWG) and the Registries Stakeholder Group (RySG) The framework is voluntary and non-binding  and does not reflect any consensus policy affecting gTLD registries.

## Scope

This framework addresses the role of both registries and law enforcement in handling  malware and botnet[1] infrastructure using the Domain Name System, specifically as a result of illegitimately used DGAs. DGAs are often employed by botnet command & control ("C&C" or "C2") infrastructure to maintain persistent control of botnets, but the framework need not be limited to DGA referrals - it may also be used in the handling of non-algorithmic large lists of domains employed by botnets and malware.

## Summary

DGAs are often used by criminals to prevent their online activity being detected. DGAs are computer programs that automatically generate domain names, usually using a long random collection of numbers and letters. This is done at scale and pace to allow the criminals to move between different domain names to continue their activities, for example to distribute malware - malicious software to disrupt computers or gain access to private/sensitive information or systems. The intention is to evade security countermeasures that are designed to prevent criminals from reaching victims, such as blocking the domain on a network. These types of attacks tend to be large scale and well organised with significant consequences for victims.

There are limited but effective ways that registries and law enforcement can work together to address DGAs associated with malware or botnets – usually by reserving or creating the domain name. The options available may require the registry to seek certain approvals from ICANN.  As a result it is important that LE  provides as much advance time and evidence as possible to the registry operator and keeps an open dialogue on cooperation. The LE should also consider the time period for which action is required (i.e. months, years, indefinitely). In some circumstances a Court Order may also be necessary or useful to facilitate action.

[1] Botnets are networks of computers infected with malware, which are under the control of a cybercriminal. Botnets allow criminals to harvest sensitive information from infected computers, such as online banking credentials and credit card information. A criminal can also use a botnet to perform cyberattacks on other computer systems, such as denial-of-service attacks.

## Context: Problems Associated with Large Scale Malware and Botnets

Criminal use of DGAs poses unique challenges to LE and private sector anti-abuse efforts. Simply put, DGAs enable criminals to tell their botnet to check a long list of domains for instructions - the catch being that at any given point in time in the future, there is only one specific domain to check, as determined by the algorithm. Criminals do not need to register all of the domains generated by the algorithm, as the criminal's use of any one of the domains at the specific point in time designated by the algorithm, may be enough for the criminal to regain control of a botnet after LE seizure.

*First Real World Example, Conficker (2008-09)*

The Conficker worm was a self-replicating virus that exploited a vulnerability found in the then-current Microsoft Windows Operating System. Conficker malware was able to use networks to inject code into both home and business computers. It was also malware that was able to prevent detection by attaching itself into a program or software on an infected computer and disabling Windows Automatic Update, Windows Security Center, Windows Defender and Windows Error Reporting.[2] Infected computers then used a domain generation algorithm (DGA) to create a daily list of domain names.

The worm was discovered by a number of security research organizations in collaboration with the US intelligence community who brought the issue to several gTLD and ccTLD operators including Neustar, Verisign, Afilias, and PIR). A Conficker Working Group (later called the Conficker Cabal) composed of members from each of the above organizations was formed to decrypt the DGA, analyze the traffic and find infected hosts. To support the efforts to monitor the traffic, the TLD registries began to preemptively register domain names generated through the DGA. This would serve two purposes, (a) prevent Conficker infected hosts from communicating with the command and control bot , and (b) direct traffic to sinkhole hosts where the Conficker bot could be further monitored and analyzed.

In January 2009, the TLD registries approached ICANN seeking a waiver of all domain name fees associated with the names that were re-registered. ICANN agreed to not only waive the fees, but to also coordinate with ccTLD operators that were also impacted by Conficker to have them begin the process of preemptively register domain names in their respective ccTLDs. Subsequently, in February 2009, Microsoft announced the Conficker Cabal along with a $250,000 reward for information leading to the arrest and conviction of the writers of the Conficker worm.[3] In March and April 2009 a number of ccTLDs agreed to cooperate with the

[2] See https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf

[3] Microsoft Collaborates With Industry to Disrupt Conficker Worm (Microsoft offers $250,000 reward for Conficker arrest and conviction.), Microsoft, 12 February 2009, archived from the original on 15 February 2009, retrieved 22 September 2009

Conficker Cabal and pre-register domain names, including .ca, .cl, .ch, .pl, and many others. By mid-2009 all domain names generated by Conficker A had been successfully locked or pre-emptively registered, rendering its update mechanism ineffective. Ultimately, three Ukranians were arrested in relation to Conficker, but there are no records of them being prosecuted or convicted. A Swede was also arrested and sentenced to 48 months in prison in the United States after pleading guilty. [4]

*Real World Example 2: Avalanche*

A more recent example is the 2016 action by an international coalition of partners (public and private sector) that dismantled the criminal infrastructure platform known as 'Avalanche'[5]. Avalanche was a criminal botnet used as a delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns; conservative estimates put the number of Avalanche victims at more than 3,000,000 globally. Avalanche infrastructure was designed to use DGAs to provide resiliency in the face of takedown efforts. The Avalanche mitigation operation, led by the Public Prosecutor's Office Verden and the Lüneburg Police (Germany) in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, used (and was the largest ever example of) a sinkhole to combat a botnet.

The operation included close cooperation from over 40 top-level domain registries globally (both gTLDs and ccTLDs). In all, approximately 800,000 domain names were seized, blocked and/or sinkholed each year of the operation's existence (2016-2019). And yet, Avalanche's use of DGAs persists and has since required LE to go before the courts on an annual basis to refresh authority for seizure of the (very large) list of domains expected to be generated by the DGA that year, In turn, LE must then again provide the collaborating registry operators with those seizure orders requiring their action on an annual basis to prevent the dangerous domains from being made available to the public. Thus, it can be seen that the use of a *single* DGA by criminal actors creates a *perpetual* obligation and burden to those seeking to preserve the integrity of the DNS system against its abuses by malware/botnet operators. Without improvements to the method by which LE and registries address the DGA risk (such as those proposed by this Framework), mitigative action alone may not be sustainable.

## Recommended Practices for Registry Operators in Addressing Security Threats from Unregistered Domain Names

As set forth in the Framework for Registry Operators to Respond to Security Threats (the "Security Framework"), Registry Operators have a limited number of technical options they can utilize when they have identified a security threat. When it comes to addressing un-registered domain names that were generated by or will later be part of a DGA (or a known list of to-be

[4] See "The Work that Nearly Ate the Internet", New York Times (29 June 2019) by Mark Bowden https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html.

[5] https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

created domains engaged in DNS Abuse), the primary objective is to prevent resolution of these domain names to avoid victimization of end users. Registry operators can use certain tools, such as **reserving** or **creating** the domain name, but other options also exist. In this framework we discuss reserving or creating a domain name as they are the typical tools involved in addressing DGAs.

### *Reserving a Domain Name*

When a law enforcement agency or other trusted source provides a registry operator with a list of domains that have not yet been created but are algorithmically certain to be created and engage in distribution of malware or serve in a botnet, a registry may mitigate the threat by reserving the domain name. Under their Registry Agreements with ICANN, Registry Operators have flexibility to reserve unregistered domain names without prior permission from ICANN. These reserved names are prevented from being created by a third party, meaning that when the domains are set to be created as part of malware or a botnet, that create command will fail because the name is on a registry reserve list.

### *Creating a Domain Name*

Similar to reserving a domain name, a registry operator can, instead, create that domain name. When an algorithm (or an individual) seeks to register a domain to engage in malware or botnets, the create will fail. Creating a domain has a benefit that is not achievable under reservation, in that once the domain name is created, the registry operator can "sinkhole" the domain. Sinkholing is when the registry redirects the nameservers of the domain, which allows for law enforcement to help identify victims of the malware or those who have machines participating in a botnet.

Unlike reservation, however, there are restrictions in the Registry Agreement that prohibit a registry from taking this action without certain permission. Section 2.9 of the Base Registry Agreement requires that all domain name registrations must be done through an ICANN accredited registrar. Similarly, section 6.1 of the Base Registry Agreement requires a per transaction fee to ICANN for all domains created. Some malware or botnet families can have tens of thousands of domains, meaning responsible and cooperative action by the registry to assist law enforcement by registering the dangerous domain names could be very expensive to the registry operator.

### *Expedited Registry Security Request Process (ERSR)*

The ERSR[6] is a process available for gTLD registries to inform ICANN of a "present or imminent security incident to their TLD and/or the DNS to request a contractual waiver for actions it might take or has taken to mitigate or eliminate an Incident." Since ccTLD registry operators do not have Registry Agreements with ICANN, the permissions sought from an ERSR are not required

[6] https://www.icann.org/resources/pages/ersr-2012-02-25-en

for a ccTLD operator (though each ccTLD operator may have its own or different restrictions). Through the ERSR process, a gTLD Registry Operator can request ICANN waivers and create the domains itself and without ICANN fees. There may be circumstances in which a Registry Operator must act to mitigate a botnet or malware immediately, even prior to obtaining permissions through an ERSR. ICANN's ERSR page contemplates such a situation and states, in part, "in some extraordinary instances registries may be required to take immediate action to prevent or address an Incident. In cases of such Incidents, registries should submit an ERSR as soon as possible so ICANN may respond with a retroactive wavier if appropriate". ICANN understands the issues created by dealing with DGAs, malware, and botnets at scale and works cooperatively with registries on these ERSR requests.

Due to the nature (i.e., volume and potential activation time) of some large scale malware and botnet threats, and the contractual implications of an ERSR, a Registry Operator should consider these factors to determine the scope of a given ERSR, e.g., narrow or broad, in response to a request from LE. An example ERSR request to address a DGA is included here as Appendix 1: Model Expedited Registry Security Request Process for reference.

*General Cooperation*

Whichever mitigation path is implemented, the registry operator and law enforcement point of contact should work together and have an open channel of communication regarding the time of implementation, any issues that arise during the mitigation, and any after action steps that are necessary on either side (for example LE may assist the registry in providing information for the registry's after action report associated with an ERSR waiver).

## Recommended Practices for Law Enforcement in Working with Registry Operators to Mitigate these Threats

When LE approaches a registry regarding mitigating a threat such as that identified in a DGA, it should be mindful of the logistical and administrative burdens involved on the registry side. Ideally, a LE request to a registry should be a component of a well thought-out, comprehensive abuse disruption strategy that also considers a remediation plan and victim notification. To this end, LE should be sure to allow as much lead in time as practicable for the registry to account for both (i) any necessary permissions required from ICANN; and (ii) the actual implementation of the mitigation, which may involve thousands of domain names for a single registry operator or setting up sinkhole servers, some managed by third parties, to enable victim notification.

Similarly, any requested (or mandated if in the case of a Court Order) mitigation should be tailored to avoid unnecessary impacts on the registry; this is particularly true for the length of the mitigation. In the example of a DGA, if a subset of domains are expected to be a potential threat for a matter of months, LE should be sure to communicate this window to the registry so that it can have the domains reserved or created for that relevant window and not in perpetuity.

LE should also have an understanding that there may be instances when a Court Order will be necessary for a registry to implement certain mitigations.

*Understanding the Role of Court Orders*[7]

Mitigation of malware and botnets associated with a DGA has a number of complications.

Certain factors may make it *more likely* that a particular registry operator requires a Court Order to effectuate a certain mitigation of a DGA, including:

*Domain Seizures.*

Where LE requests the **seizure** of an existing domain (one already registered by a third party registrant), it should be understood that any voluntary action by the registry operator may impact the legal exposure they face. Thus, a registry operator may require that such requests are accompanied by Court Order of competent jurisdiction, not only to protect the registry, but also to ensure that due process rights are observed.

*High Value Names.*

Registries, as businesses whose inventory of domain name strings may have value based on criteria unique to the registry, may have to consider that value as part of choosing the action to be executed.

There are also some factors that might make a registry operator *less likely* to require a Court Order in order to effectuate a particular mitigation, including:[8]

*Reserving Unregistered Domains*

Where LE requests a registry operator to reserve unregistered domains, such action will usually have a much smaller impact on the legal rights of third parties, and therefore is more likely to be actionable without a Court Order.

*General Requirements to Action based on Terms of Service:*

Availability of evidence of a security threat, where backed by LE request is helpful to registry operators in assessing the requested mitigation, as well as the potential to act without a Court Order. Requests from law enforcement authorities will help substantiate registry action without a

[7] In this instance, “court orders” should be interpreted to include any lawful legal instruments issued by an authorized governmental agency (a.k.a. “legal process”) that have a binding effect on the registry to take actions so directed, but which may vary in name by issuing nation and/or agency.

[8] To be clear, this Framework only addresses mitigation of malware and botnets at scale, which are both well settled forms of DNS Abuse. Any referral from LE to a registry for any Website Content Abuse issue is outside the scope of this Framework.

Court Order, but evidence of the claimed threat remains important to demonstrate that any actions taken are capable of being considered both necessary and proportional in the circumstances and were not arbitrary.

Where LE is not in a position to provide evidence to ground such actions (e.g., potential interference with ongoing investigations), that may make a registry operator more likely to require a Court Order to effectuate a particular mitigation.

*Ongoing Cooperation from Registry Operator*

Having an ongoing and cooperative relationship between a registry operator and  LE in its jurisdiction can often facilitate a smoother and  prompt mitigation of DGAs (or other DNS Abuse) for all parties involved. Each registry is likely to have slightly different practices and procedures for intaking LE requests to mitigate these threats, so having an understanding of those practices may enable LE to tailor  requests in such a way that is administratively more efficient for LE and may not ultimately necessitate Court Order.

## Appendix 1: Model Expedited Registry Security Request Process

**Description of the Incident**:

THIS SUBMISSION IS CONFIDENTIAL --

[REGISTRY OPERATOR] has been approached by a law enforcement agency working in [REGISTRY OPERATOR]'s jurisdiction regarding [MALWARE/BOTNETS] propagated through a domain generating algorithm ("DGA Domains"). [INSERT DESCRIPTION OF ANY APPLICABLE COURT ORDER].

[REGISTRY OPERATOR] seeks a waiver of: (1) ICANN fees under the [TLD] Registry Agreement for creation of DGA Domains in order to mitigate malware and/or botnets; and (2) contractual requirements that prohibit [REGISTRY OPERATOR] from acting as its own registrar when [REGISTRY OPERATOR] is creating those domains. [REGISTRY OPERATOR] would rely on this waiver and provide ICANN with an after action report shortly after all DGA domains created pursuant to this waiver.

**How did you learn of the Incident you described**?

The DGA Domains were reported to [REGISTRY OPERATOR] by a law enforcement agency.

**What action(s) will you or did you take to respond to the Incident**?

Once a waiver is obtained from ICANN, [REGISTRY OPERATOR] will act to mitigate DGA Domains. The domains that do not already exist will be created by the [REGISTRY OPERATOR] in a special projects account, and will then be locked, suspended or sinkholed. If the domains already exist, [REGISTRY OPERATOR] will ensure that the domains are given the same protocols.

**Estimated duration of Incident (if available)**:

Indefinite.

**What contractual relief is requested and what are the relevant section(s) of the TLD Registry Agreement?**

Section 2.9 of the Registry Agreement ("RA") prohibits [REGISTRY OPERATOR] from acting as its own registrar. In order to address DGA domains, [REGISTRY OPERATOR] will have to register the DGA Domains. [REGISTRY OPERATOR] seeks a waiver of this provision of the RA to allow [REGISTRY OPERATOR] to act as registrar for all DGA Domains that will be registered within the [TLD] gTLD.

Sections 6.1(a)(ii) and 6.3(b) of the Registry Agreement require [REGISTRY OPERATOR] to pay ICANN a Registry-Level Fee “equal to the number of annual increments of an initial or renewal domain name registration. . . during the applicable calendar quarter multiplied by US $0.25.” Section 6.3(b) provides that [REGISTRY OPERATOR] shall pay a transactional component of the Variable Registry-Level Fee (as defined by the Registry Agreement) “specified by ICANN. . . but shall not exceed US $0.25 per domain registration per year.” [REGISTRY OPERATOR] requests a waiver of all fees associated with the registration of DGA Domains.

**Estimated duration of waiver for contractual relief (if applicable):**

[REGISTRY OPERATOR] respectfully requests that the waivers contemplated by this ERSR be effective so long as such waivers pertain to DGA Domains. For the avoidance of doubt, [REGISTRY OPERATOR] respectfully requests that the terms of any waiver granted by ICANN allow for automatic continuation of the waiver in the event [REGISTRY OPERATOR] is notified of additional DGA Domains to be acted upon.

Specifically, for the sake of operational efficiency for both [REGISTRY OPERATOR] and ICANN, [REGISTRY OPERATOR] requests that to the extent there are additional DGA Domains to be registered, then upon notification of the same to ICANN, together with all available supporting documentation, any waiver issued pursuant to this ERSR will apply, such that the filing of a new ERSR shall not be necessary.

**Do you have information about other TLDs that may be affected by the Incident you described? If so, who are they and what have you communicated to them?**

[Incident specific]