FRAMING BRIEF: IMPROVING THE WORKFLOW OF FIGHTING BOTNETS: HANDLING ALGORITHMICALLY GENERATED DOMAINS (AGDs)

REF: 22-105 | October 4, 2022

A Botnet (short for "robot network") is a network of servers and devices that have been targeted and infected by malware to put the network under the control of a single attacking party. The attacking party can use the computers on its botnet to carry out coordinated criminal action. The scale of a botnet enables the attacker to perform wide-spread malicious actions, such as phishing, spam delivery or even denial of service attacks.

In parallel, Domain Generating Algorithms ("DGAs"), contained in various families of malware, periodically generate a large number of domain names across multiple registries that can be used as rendezvous points with command and control servers. These domains are thus referred to as Algorithmically Generated Domains ("AGDs"). The large and complex networks created by DGAs make shutting down botnets difficult.

Cracking a Domain Generating Algorithm (DGA) allows law enforcement and security experts to anticipate the universe of domains that can be used by a particular botnet and to then disable it by registering and then blocking or sinkholing[1] the domains. However, the enormous number of domain names generated by DGAs and the rapid pace at which botnets operate demand significant coordinated action among law enforcement, domain name registries, CERTs and regulators - often on a global scale, making remediation and mitigation a growing transnational challenge.

In this context, this framing brief seeks to address some cooperation and coordination challenges arising in the mitigation of botnets at a global scale and identify key questions that need to be addressed. The first part of this Outcome (Current Approach and Its Limitations) provides a brief outline of the way tackling AGD botnets is currently undertaken, and in particular identifies the role of different actors in the process and the challenges of the existing cooperation measures. The second part (Potential Avenues for Moving Forward) identifies possible measures that may aid the speedy mitigation of threats. Finally, the third section (Additional Elements for Consideration) documents where further dialogue and cooperation is required as well as key structuring questions that need to be clarified.

1. THE CURRENT APPROACH AND ITS LIMITATIONS

The current system of dealing with AGDs presents three distinct challenges: 1) the heavy legal procedures that law enforcement authorities need to follow, 2) the applicable rules of ICANN, 3) the limits of transnational coordination.

1.1. ON LEGAL PROCEDURES

Typically, law enforcement authorities have to obtain court orders to secure full and complete participation by several affected registries and their preventive registration of these domains. In most cases, whether an Operator will require a court order depends on the laws of their home jurisdiction, their anti-abuse policies as well as the specific actions requested to remediate the botnet (i.e. mere domain registration/reservation vs. sinkholing). Even when local law does not mandate securing a court order, some Operators will nonetheless

[1] European Union Agency for Cybersecurity (ENISA) defines sinkholing as "a mechanism aimed at protecting users by intercepting DNS request attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address.

require them to sinkhole such domains. In that regard, modalities of cooperation and action often differ between Generic Top Level Domains (gTLDs) and Country Code Top Level Domains (ccTLDs).

The requirement for a court order for any action is even more complex when an Operator is not located within the jurisdiction of the law enforcement authority. In cases where remediation efforts involve operators in more than one country or ccTLD operators, multiple Mutual Legal Assistance Treaties (MLATs) often need to be used to ensure coordinated global action. Yet, MLAT processes are lengthy and procedurally burdensome. In cases where MLATs are not already in place, direct voluntary cooperation from registries is necessary and in many cases Operators require a foreign court order to be domesticated, which adds time and complexity to the remediation process.

1.2. ON APPLICABLE RULES OF ICANN

In parallel, ICANN registry agreements explicitly prohibit Generic Top Level Domains (gTLDs) registries from registering domains on their own and require the payment of a fee to ICANN for each name registered. As a consequence, gTLD registries need to use the so-called Expedited Registry Security Requests (ERSR) process to inform ICANN of the impending law enforcement action against the botnet and seek ICANN's permission to register the AGD domains and avoid incurring the corresponding ICANN fees.

In theory, each registry must file its own ERSRs and await ICANN's approval before taking action, but some relaxation of the practice has been progressively implemented, albeit informally. ICANN reviews and approves each such request on an individual basis. Moreover, each ERSR submission contains a description of the upcoming highly sensitive law enforcement initiative and is therefore submitted confidentially. This process is complex and makes coordination among affected gTLD registries difficult.

1.3. ON TRANSNATIONAL COORDINATION

Given the size of botnets and their capacity to impart geographically broad-ranging harm, speed, coordination and secrecy are key to their remediation. However, in the current landscape there are no clearly established pre-existing coordination mechanisms or processes between law enforcement authorities, ICANN and other relevant stakeholders, particularly in establishing the bona-fides of the botnet. Additionally, the existence of the botnet must be validated and at present, there is no central authority/institution fulfilling this important function. In the absence of such a validating mechanism, law enforcement authorities outside the operators' jurisdiction(s) have to demonstrate the threat and rely on time-consuming legal processes to enable a coalition to act globally.

2. POTENTIAL AVENUES FOR MOVING FORWARD

There are a few avenues where progress may be made in securing speedy cooperation in tackling botnets, particularly around 1) Scope of action (particularly on the distinction between reservation of names for mitigating the botnet vs. sinkholing and prosecuting) and 2) Evergreen ERSRs for gTLDs.

2.1. DISABLING VS. STUDYING THE BOTNET

A key criterion for Operators to act to remediate botnets is clarity regarding the action required from them. Sinkholing domains demand a higher threshold for action than simply creating or reserving domain names to disable the botnet. The choice of actions available include, but may not be limited to:

Disabling: Operators can effectively contribute to disabling a botnet by merely reserving[2] names identified through the algorithm, provided such reservation is consistent with the Operator's terms of service. This method offers efficiency and rapid action in that it requires neither a court order, nor an ERSR (for gTLD Operators). However, unlike the full registration of the names, the "disablement through reservation" method may limit later ability to study the behavioral aspects of the botnet and thus hinder efforts to identify and/or prosecute the perpetrators of the botnet; only registration of the names allows to sinkhole them and conduct the necessary analysis.

Sinkholing: Where the goal is to study the botnet, identify and/or prosecute its perpetrators, registration and sinkholing of domain names is thus the preferred method. As noted above, this often implicates court orders and MLAT procedures. Particularly where Operators are asked to create domain names and redirect them to third parties (e.g. law enforcement), Operators may insist on a court order since such activity closely mimics formal legal seizure mechanisms.

A hybrid approach, combining sinkholing and disabling may also be undertaken. For example, a majority of AGDs may be disabled by reserving or registering the domains while a few are sinkholed in order to study and gather evidence.

Reservation and registration of a domain are two different actions with different implications for the operators and may also impact individual operator's metrics and reputation depending on the action taken. When domains are registered as part of the remediation action, clarity on how long to keep the domains registered and who bears the costs are important. Operators also cooperate with the Registrar of Last Resort (RoLR)[3] but in some instances domain registration as part of the remediation action may be preferred to be done by the registries themselves rather than by the RoLR on the administrative and costs grounds. Instances where domains are left in limbo and remain on the books (either registered or reserved) for indefinite periods of time should be avoided.

2.2. EVERGREEN ERSRS (FOR GTLDS)

So-called "evergreen language" refers to wording in an agreement or a court order which permits an Operator to take recurring action on the same basis upon the provision of additional information (e.g. new lists of names).

In the ERSR context, it may manifest in two scenarios. First, an individual ERSR granted to an Operator may include evergreen language, authorizing the Operator to continue to take action against a given botnet and any subsequent instance of the same botnet, without the Operator having to file a new ERSR. It may also arise in the context of a specific agreement between a given Operator and ICANN vis a vis the handling of botnets, allowing the Operator to take immediate action against botnets with only post-hoc notification to ICANN. Both scenarios offer greater speed and efficiency for the Operator in remediation efforts.

Evergreen language is also used in court orders to allow both the proponent of the order (e.g. private companies, law enforcement) and the Operators to continue remediation efforts for the life of the botnet, without the need to start fresh court proceedings when additional domain names need to be added to the remediation action.

[2] For more information on reserving domain names, see ICANN's "About Reserved Names and Name Collision Occurrence Management"

[3] The Registrar of Last Resort (RoLR) is a non-profit organization that seeks to quarantine malicious domains. For more information see: https://www.rolr.eu/index.en.html

The length of action, in both the above cases, is determined by the DGA as it specifies a target set of domains as rendezvous points during specific time periods, typically a day to a week. When action is taken, it is important to block the domains for as long as the DGA specifies while accounting for differences in time-zones, i.e. time-slop factor. However, there are broader questions that need to be addressed with regards to how long registered and sinkholed domain names are retained by Operators and costs associated with the maintenance of such domain names in the Operators books.

3. ELEMENTS FOR FURTHER CONSIDERATION

Additional elements would benefit from further deliberation, particularly on: 1) how to facilitate a global emergency response mechanism 2) how to secure cooperation of ccTLD operators, and how to address questions pertaining to 3) name collisions, and 4) secrecy.

3.1. EVERGREEN ERSRS (FOR GTLDS)

At present, there is no specific structure to foster or facilitate the indispensable coordination - especially across multiple jurisdictions - among the various actors (i.e. law enforcement, courts, ICANN, CERTs, ccTLD regulators and domain registries) to ensure the precise and efficient action in botnet takedown initiatives. Currently, DGAs are typically identified by law enforcement in a particular jurisdiction who must then begin each time the process of informing key stakeholders and securing their cooperation to remediate the botnet, including through cumbersome MLAT processes. There are currently no universally accepted protocols that predicate who to approach and the standard of proof required if an entity or an individual (e.g. a researcher or Trusted Notifier) seeks to remediate a botnet. There is also a lack of structures and mechanisms to coordinate subsequent action across actors and jurisdictions.

In this environment, it would be beneficial to explore an 'Emergency Response Mechanism' (informal or formal) to foster exchange of lessons learned and best practices, but also to set protocols and procedures that foster rapid coordination on a case by case basis. This could entail an ad hoc body or even a stand alone entity with representatives from the various actors and stakeholders typically involved, serving as a point of contact for law enforcement and security experts around the world. Furthermore, depending on the body's composition and the standard of due-process that it would follow, it could also potentially serve as an authoritative mechanism to evaluate the evidence and validate the threat that would encourage Operators to voluntarily take certain actions based on their terms of service. The composition of the body and its structure, mandate and operating modalities would of course be critically important to provide legitimacy and instill confidence in its assessments.

As an alternative, or in addition, it could be considered, if it were conducive, for ICANN to play a more proactive role in the process of coordinating cooperation in tackling botnets, particularly in the case of gTLD operators. In such cases, ICANN could, upon receipt of reliable information about a botnet and its remediation efforts, notify relevant registries and prompting the affected registries to submit ERSRs, perhaps having an expedited or simplified ERSR procedure in such instances.

3.2. CCTLDS & ROLE OF CERTS

Actions by ccTLD Operators are strongly predicated by the applicable national legal framework of the country in which the ccTLD operates and their own anti-abuse policies. The plurality of ccTLD operators and the corresponding diversity of the legal norms applicable to them significantly complicates securing in a timely manner their cooperation on a case by case basis as this would imply multiple MLAT procedures. Two avenues that could be considered in this regard could include:

a) Role of national CERT/CSIRTs: In most cases, ccTLD operators have streamlined cooperation mechanisms with their national 'Computer Emergency Response Team' (CERT) or 'Cyber Security Incident Response Team' (CSIRT). Securing their cooperation in both validating the threat as well as streamlining communications with local ccTLD operators may be an avenue for speedy remediation of the botnet.
b) Acting pursuant to Operator's Anti-Abuse Policies: Secondly, most DNS Operators, including ccTLDs have broad anti-abuse policies that may empower them to act on technical abuse[4]. Depending on the type of action required and subject to robust threat validation processes, some ccTLDs may choose to voluntarily act based on their anti-abuse policy. Coordination and communication with the national CERTs would further strengthen this approach.

3.3. NAME COLLISION

An element of complication arises when the cracked DGA generates domain names that have been previously registered. This is known as collision.[5] It is important to note that while DGAs may generate already registered domains, they rely heavily on unregistered ones. For example, of the 800,000 domains that were part of the Avalanche botnet, less than 1% were already registered. However, given that even one single active domain may allow the attacker to communicate and control the botnet, collision poses a tremendous security and due process challenge. It requires the identification of whether the domain was maliciously registered in advance by the attacker, and if not would require securing either the cooperation of the registrant or taking invasive action against the domain. If a court order requires seizure of all DGA generated domains, there are chances that some innocent domains registered in good faith may also be affected. Instances of collision also happen when, for example, a domain sinkholed by researchers is seized by security agencies. Such instances of collision show that cooperation and coordination between relevant stakeholders is a challenge and could be improved.

3.4. SECRECY

Secrecy is the cornerstone of a successful mitigation strategy for botnets. This also has implications for the remediation action strategies as mass sinkholing or a wide disabling operation may reveal to the perpetrator that the DGA has been cracked. If the attackers become aware that their DGA has been compromised, it may allow them to change the parameters of the DGA (i.e. generate more random domain names or even in some cases change the DGA itself). Therefore any action necessitates a significant level of secrecy requiring many actors to operate on a strict 'need to know' basis. This is in conflict with the significant degree of cooperation needed among numerous actors, with the often long preparation phase for any mitigating action, and in some cases with applicable due-process in the case of name collisions. Furthermore, this has implications for any form of validation mechanism that may be envisaged. Additionally, many operators and security researchers would not disclose their operational policies and mechanisms, in order to prevent attackers gaining knowledge of them to game the system.

[4] For definitions of DNS Abuse, see Domains & Jurisdiction Operational Approaches Criteria A: Types of Abuses

[5] The term is understood differently from the ICANN context which covers names that are outside of the DNS system as, according to the definition, a collision occurs when an attempt to resolve a name used in a private namespace results in a query to the public DNS (see more here: https://www.icann.org/resources/pages/name-collision-2013-12-06-en#overview)