RFC RESPONSE:

Promoting Stakeholder Action Against Botnets and Other Automated Threats

National Telecommunications and Information Administration, U.S. Department of Commerce

13 July 2017

I. BACKGROUND

In response to the U.S. Department of Commerce, National Telecommunications and Information Administration's (NTIA) Request For Comment (RFC) on *Promoting Stakeholder Action Against Botnets and Other Automated Threats* [1], CrowdStrike offers the following views. We commend the focus on this critically important issue in the 11 May *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* [2] and this follow through effort. The articulated intent, to "lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the Internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)" is timely and appropriate.

As a leading provider of cybersecurity threat intelligence, services, and endpoint protection software, CrowdStrike has a unique vantage on this topic. The organization has assisted in multiple botnet investigation, disruption, and takedown efforts, notably against the GameOver Zeus and Kelihos botnets [3] and actively monitors emerging threats along these lines. Some of the lessons learned during those efforts are captured herein. This comment does not seek to address every issue raised in the RFC; it is limited to areas for which CrowdStrike may offer particular insights.

II. QUESTIONS

1. *What works:* What approaches (*e.g.,* laws, policies, standards, practices, technologies) work well for dealing with automated and distributed threats today? What mechanisms for cooperation with other organizations, either before or during an event, are already occurring?

Most counter-botnet efforts involve cooperation by an ad hoc group of law enforcement, technology, cybersecurity, research, nonprofit, and academic organization representatives. The composition of these groups and their membership changes depending on the specific threat, but a few entities with highly specialized expertise or that hold a privileged place in the IT ecosystem are often represented. These groups are agile, quickly organizing actors with relevant skills, authorities, equities, and insights to tackle a botnet.

Such ad hoc groups usually are informal, and trust is established on the basis of introduction or affiliation. From participants' point of view, essential elements include: discretion, a clear objective, equitable contributions across membership, and interaction in the context of a peer relationship. Non-government members generally participate on a pro bono basis. These entities are among the clearest positive examples of functional cybersecurity information sharing and public-private partnership.

Botnets are often quite unique, and the most sophisticated require comprehensive analysis and cooperation from a broad group of stakeholders to address. Takedown efforts may require seizure, dismantlement, or disruption of command and control (C2) mechanisms, and must be carefully sequenced. Mistakes and failures could comprise the operation and hobble future efforts, so execution tends to be slow and deliberate.

2. *Gaps:* What are the gaps in the existing approaches to dealing with automated and distributed threats? What no longer works? What are the impediments to closing those gaps? What are the obstacles to collaboration across the ecosystems?

Without concerted action, the botnet problem will not be solved in the near term, as law enforcement and the security community lack the incentives and resources to respond to every instance. Botnets often exploit common vulnerabilities, so successfully combatting one botnet may mean its nodes are later simply compromised by a different botnet. Therefore, resources and efforts should be carefully prioritized. Factors like virulence, application or potential application for malicious ends (e.g., observed usage in severe distributed denial of service (DDoS) attacks is more urgent than usage for SPAM distribution), or persistence might inform prioritization schemes. Moreover, there should be a process for expediting community efforts to combat particularly dangerous examples.

Unfortunately, security talent is not evenly spread across affected industry sectors, therefore impairing botnet response capabilities. Additional dedicated investigative and prosecutorial resources with subject matter expertise and a clear mandate would help regularize counter-botnet activities and help increase success rates.

At present, no entity has the mandate or capacity to help remediate compromised machines. Common practice is to notify Internet Service Providers (ISPs) when Internet Protocol (IP) addresses they serve are associated with botnets, and they in turn notify the victims. This notification process is handled differently throughout the ecosystem, but it is clear that many machines are never remediated. Universal botnet reporting protocols, victim notification processes, and expedited network mitigation techniques are necessary to ensure botnets cannot wreak sustained havoc like today's ad hoc responses to an automated threat.

3. *Addressing the problem:* What laws, policies, standards, practices, technologies, and other investments will have a tangible impact on reducing risks and harms of botnets? What tangible steps to reduce risks and harms of botnets can be taken in the near term? What emerging or long term approaches may be promising with more attention, research, and investment? What

are the public policy implications of the various approaches? How might these be managed, balanced, or minimized?

CrowdStrike proposes that the security and law enforcement community bring more energy to this fight. A serious commitment from law enforcement and the security community to attempt to take down one botnet every week would be a "game changer." Moreover, it should be the policy of the U.S. government to deny a safe haven to botnet operators on U.S. Internet infrastructure, such as U.S.-based web hosting companies. These goals are ambitious relative to the status quo, but not impossible. Ultimately, focusing on such initiatives would provide a powerful organizing principle for decision makers across government and industry, going well beyond botnets and automated threats to catalyze a seismic shift in cybersecurity.

The future of botnet prevention and broader cybersecurity is dependent upon shifting security responsibilities away from vulnerable end user victims to those best able to help. It is necessary to enhance centralized mitigation efforts, but the problem must be addressed at all levels. Specific to infrastructure, it is critically important for network operators to heed to the security community's call for the adoption of anti-spoofing measures such as BCP38, BCP84, and SAC065 to prevent source address spoofing, which plays a significant role in denial of service reflection and amplification attacks. Whereas, for end users, vendor managed, next generation endpoint security solutions, like CrowdStrike's Falcon platform, can leverage advanced endpoint detection and response (EDR), machine learning, and managed threat hunting to detect and defeat adversary activity without relying upon the end user to patch software, quarantine malware, or report suspicious machine behavior. This is particularly important because not all botnets have an architecture or C2 that is susceptible to a centralized means of dismantlement. Peer-to-peer (P2P) botnets, for example, present unique challenges in this regard.

Recent gains in traditional endpoint protection soon may be offset by the adoption of vulnerable Internet of Things (IoT) devices. This is a complex phenomenon in and of itself but one for which the threat vector may be mitigated by injecting transparency into the marketplace. For example, the use of device security ratings may inform consumers as they make their purchases. Equipped with such information, major retailers might consider flagging items that appear to have poor security, or not carry them at all, in order to enhance vendor accountability for enhanced security practices.

4. *Governance and collaboration:* What stakeholders should be involved in developing and executing policies, standards, practices, and technologies? What roles should they play? How can stakeholders collaborate across roles and sectors, and what should this collaboration look like, in practical terms?

Botnets affect a wide range of stakeholders, from Internet infrastructure providers such as ISPs, domain name registries and registries, and hosting providers to victimized individuals and organizations unwittingly providing attack vectors, as well as responding law enforcement organizations. These stakeholders can be flexibly incorporated into the ad hoc working groups that exist today. Most major organizations have formal security teams that can coordinate, although maturity and capacity vary

greatly across different organizations. The ability to bring new organizations into the fold is important because, for example, new web services or platforms are frequently leveraged by botnets for C2, and coordinating with a newly-implicated firm's security team may be essential for a successful takedown effort. From stakeholders' vantage, expertise—and in the case of government stakeholders specifically, authorities—are generally varied and specific enough to minimize the need for formal roles.

From an institutional standpoint, the absence of a standing organization may hinder process formalization or compromise the capture of institutional knowledge. To these ends, there is probably room for a strengthened architecture for counter-botnet efforts. Previous "lessons learned" documents and papers summarize a variety of different options for how to achieve this, and some existing entities hold informal leadership roles in this space. Enhanced capacity to maintain current points of contact, strengthen relationships between stakeholders, develop institutional knowledge across disparate efforts, and allocate resources would help. This may require additional resources.

5. *Policy and the role of government:* What specific roles should the Federal government play? What incentives or other public policies can drive change?

The most important thing the Federal government can do in this area is to approach the issue with more urgency (e.g., to carry out one major takedown per week as proposed above.) Within the interagency process, relevant government entities should be tasked to report on what it would take to meet this operational tempo. Those answers should inform institutional changes, a review of relevant authorities, resourcing questions, and so on. From the government's perspective, another incentive to move more aggressively would be to head off periodic instances of vigilantism, which have the potential to erode norms, cause damage, or create strategic instability.

Balancing a more aggressive counter-botnet policy against the need to dedicate resources toward combatting other threats, like targeted intrusion activity, is critically important. Achieving a policy this ambitious therefore requires "scaling up" investigatory talent at the government's disposal. This can be achieved through enhancing the existing federal workforce or supplementing it. Effectively leveraging outside expertise is important, particularly given that many private institutions are willing to cooperate with and assist these efforts on a pro bono basis. Notably, cybersecurity information sharing concerns are abated in this context, where questions of liability and competition issues part and parcel to targeted intrusion activity do not apply.

As in other areas, attribution plays an important role in combating botnets. The ability to hold perpetrators accountable is key to meaningful change. For example, the fourth attempt to disrupt the Kelihos botnet was ultimately successful because the criminal actor was arrested in tandem with a technical operation. Even targeted publicity against bad actors is useful. The FBI's "Cyber's Most Wanted" program is a powerful example of how to increase the costs to perpetrators even as they remain inaccessible to law enforcement. Rewards appear to be underutilized in this context. The $3 million offered for information leading to the arrest and/or conviction of Evgeniy Bogachev [4] of the GameOver Zeus botnet complicates his efforts to travel internationally, utilize the international financial system, and participate in the loosely-affiliated criminal networks common in high-end cybercrime

schemes. More broadly, it is important to focus on extracting intelligence from and disrupting criminal coordinating ecosystems.

The Federal government should utilize its significant purchasing power to incentivize better security practices and technologies from all industries. Specifically, the Federal government can incorporate anti-botnet best practices and state of the art cybersecurity standards into its purchase requirements for software and hardware, such as endpoints, routers, and any devices that could serve as a botnet attack vector. A concerted, focused effort to increase and enforce such standards can have a positive impact on the cybersecurity posture of industries and contractors seeking government business, thereby more broadly providing positive externalities to non-government consumers. However, recent history, such as with regard to IPv6 adoption, demonstrates that the Federal government must scrutinize its vendors to distinguish between the purported *capabilities* of a product or service and the actual, proven deployment of requisite technologies.

6. *International:* How does the inherently global nature of the Internet and the digital supply chain affect how we should approach this problem? How can solutions explicitly address the international aspects of this issue?

Combatting global botnets and automated threats requires a high degree of collaboration across foreign government, industry, and nongovernmental partners. Linguistic, legal, and policy differences always have the potential to pose challenges. But in practice, cooperation works reasonably well, particularly on an industry-to-industry basis.

Mutual legal assistance treaty enhancements or reforms might speed international law enforcement efforts, increasing the rate of successful arrests. Whether through increased staffing or other means, it is necessary to ensure that MLATs can be prioritized and processed rapidly when digital evidence is involved. Given the near consensus on the need to combat botnets, particularly relative to inherent challenges in addressing targeted intrusion activity, governments have the opportunity to utilize counter-botnet initiatives as confidence building measures between technical agencies. It is important to make progress on this issue now, as the window for action may be closing. Over past few years, nation state actors have increasingly leveraged botnets generally and DDoS attacks specifically. In some instances, CrowdStrike has observed state actors piggybacking on traditional criminal botnet infrastructure, searching compromised hosts for information or access of potential interest, sometimes only in highly-localized areas. Such developments may eventually complicate international cooperation or narrow the base of potential participants.

Globally, domain names often play a role in the command-and-control of botnets. Consequently, it is important for the Federal government to use its influence in the Internet Corporation for Assigned Names and Numbers (ICANN) Governmental Advisory Committee (GAC) to advocate for policies that incentivize domain name registries and registrars to play a proactive role in preventing malicious registrations before they are used for botnet infrastructure. Moreover, the Federal government should encourage all parties involved in ICANN's multistakeholder community to collaborate on an anti-botnet initiative.

7. *Users:* What can be done to educate and empower users and decision makers, including enterprises and end consumers?

Decision makers should study past counter-botnet efforts and codify lessons learned. CrowdStrike supports continued user education, but recognizes that there are limitations on the extent to which users can protect themselves, and security practitioners should be careful not to victim-blame. In parallel, the community should place greater emphasis on victim notification and cleanup efforts, even if that inconveniences users. Relying on the eventual "decay" of infected hosts is a weak solution; as we approach the 10 year anniversary of the advent of Conficker, variants still appear to infect a million or more nodes. The problem will not just go away over an acceptable timeframe. As threats become more sophisticated, the burden falls increasingly on tech companies, security providers, and enterprises, in some instances enabled by governments.

As with other common problems, it is critical to move away from the failing status quo model of victim self-help and post-damage mitigation to a future in which those most capable of protecting infrastructure and endpoints are empowered and incentivized to stop botnets and the automated threats of tomorrow. A winning strategy depends on prioritizing the issue, enhancing law enforcement resources, encouraging industry best practices, promoting device security transparency, and shifting toward vendor managed next generation cybersecurity technologies.

III. FURTHER INFORMATION

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. CrowdStrike's core technology, the CrowdStrike Falcon™ platform, stops breaches by preventing and responding to all attack types – both malware and malware-free. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify three crucial elements: next-generation AV, endpoint detection and response (EDR), and a 24/7 managed hunting service — all powered by intelligence and uniquely delivered via the cloud in a single integrated solution.

Falcon uses the patent-pending CrowdStrike Threat Graph™ to analyze and correlate billions of events in real time, providing complete protection and five-second visibility across all endpoints. Many of the world's largest organizations already put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 health care providers, and three of the top 10 energy companies. CrowdStrike Falcon is currently deployed in more than 176 countries.

We Stop Breaches. Learn more: www.crowdstrike.com.

IV. NOTES

[1] https://www.federalregister.gov/documents/2017/06/13/2017-12192/promoting-stakeholder-action-against-botnets-and-other-automated-threats.
[2] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.
[3] See: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware and https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.
[4] https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev/@@download.pdf.

###