12 February, 2018

Via email to: counter_botnet@list.commerce.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

Attn: Evelyn L. Remaley,
Deputy Associate Administrator

Re: Comments for draft report on automated threats

Dear Ms. Remaley:

The draft work, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, seems a well considered effort to raise awareness and initiate actions that will ultimately lead to safer public networks and reduced losses for both government and private enterprises.

While the report does not specifically exclude any relevant category, we believe that public interest will be served to make the report more comprehensive by including the details for a newer category of unwanted automation threatening nine-figure dollar losses at one large civilian federal agency. Although the details of this pervasive and ongoing threat are confidential, the federal agency will most likely brief other government personnel in a private meeting and we would be pleased to arrange an introduction. We can also arrange for numerous fortune 100 companies facing the same threat to provide private briefings on their experiences. Understandably, none of these organizations are willing disclose the details of their attacks in a way that publicly attributes themselves as victims.

Putting aside any possible briefings, in the pages that follow, we propose to introduce two additions to the report to make it a more comprehensive. The nature of the threat and details about its operation are self-evident in the proposed additions.

Proposed change: additional technical domain of *Applications*:

Applications are the systems and software that deliver an experience to a consumer such as websites, web services, and mobile apps and their corresponding API endpoints that enable them.

Many applications are inherently vulnerable to fraud, breach, and denial-of-service via the intended user experience. Generating traffic that fully conforms to expected norms within the infrastructure and enterprise network technical domains, the attacker manipulates the user experience of an application to achieve unwanted and potentially deleterious outcomes.

Perhaps the most notorious case for application automation is the credential stuffing attack where the attacker, using arbitrary lists of stolen credentials, iterativley tries each credential set on an application until discovering which credentials work. Empirical data from current victims show an average success rate of around 1%. The success cases are then used to take over the breached accounts for fraudulent purposes.

Applications may be subject to denial of service (DoS) such as purposely using wrong passwords to lock out a large number of accounts and burdening the customer support function to restore access to legitimate customers. Another type of DoS attack exercises computationally expensive functions such as filling the shopping cart on an e-commerce application or operating a locator function to find stores or business partners within a geographical radius. [Not to be confused with network, HTTP, and SSL/TLS denial of service discussed under the infrastructure technical domain, these attacks are well-formed and fully complaint at the infrastructure layers. Further, they often achieve denial of service without transaction rates considered onerous or even unusual for the infrastructure technical domain.]

Motivated attackers of the application technical domain typical use botnets that are highly distributed among the IP addresses that normally patronize the same application and they limit their rates to normal levels of traffic, rendering IP reputation and rate throttling within the infrastructure and enterprise network technical domains ineffective. Instead the applications must be remediated or employ special anti-automation mitigations. The most well-known mitigations are turing tests (e.g. CAPTCHA), although their utility has waned in recent years due to advances in the attacker's use of machine learning.

Proposed change: additional action for protection of applications:

Action 2.x Stakeholders and subject matter experts, in consultation with NIST, should lead the development of a CSF Profile for Prevention of Application Automation.

The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) version 1.0 was developed by NIST with extensive private sector input. The CSF provides a flexible approach to managing cybersecurity risk that incorporates industry standards and best practices, is sufficiently general to allow for broad applicability in a variety of environments, and has been widely accepted by industry. The CSF may be supplemented by Framework Profiles, which apply the Framework components to a specific situation. In particular, profiles may be used by industry sectors to document best practices for protection against specific threats.

Through consultation with NIST, stakeholders including industry, academic and other subject matter experts should partner to develop a CSF Profile for Prevention of Application Automation, focusing on the desired state of organizational cybersecurity to remediate or mitigate application automation vulnerabilities. The profile would help enterprises identify opportunities to improve anti-automation mitigations and aid in cybersecurity prioritization by comparing their current state with the desired target state. The profile would likely include multiple levels to support industry sectors with different resilience requirements. Government stakeholders should participate in the development to ensure the profile is broadly applicable enough to contribute to a CSF Profile for Prevention of Application Automation.

If you would like to learn more about application automation attacks, two good sources with an academically sound discussion include:

> *Polymorphism as a Defense for Automated Attack of Websites*, X. Wang, et al., Springer, 2014
> (Section 2, providing a background on automated attacks is the most relevant part.)
>
> *OWASP Automated Threat Handbook*, Wason and Zaw, OWASP Foundation, 2016

I have attached both to the same email as this letter. (Shape purchased unlimited redistribution rights for the Springer paper and the OWASP document is freely shared on their website.)

Finally, if you find any of this interesting, I am at your disposal to discuss further and/or to help you integrate the concepts into your report.

Kindest regards,

Marc Hansen

Enclosures: Springer paper and OWASP handbook

cc: Derek Smith,
      CEO, Shape Security