BlackRidge Technology International, Inc.
5390 Kietzke Lane, Suite 401
Reno, NV 89511
www.blackridge.us
February 12, 2018

John Hayes
CTO and Founder, BlackRidge Technology
jhayes@blackridge.us

BlackRidge Technology Comments to the Draft *Report To the President On Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*

BlackRidge Technology appreciates the opportunity to provide comments on the draft *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* ("Report").

In order to ensure that the Report's description of the ecosystem and challenges is more complete, BlackRidge recommends that the National Telecommunications and Information Administration (NTIA):

- Emphasize the role of device identity and authentication in mitigating risk from automated threats such as botnets; and
- Recognize mitigation approaches that prevent botnets from discovering exploitable IOT devices to compromise and recruit.

Weak identity and access management of IOT devices is a major attack vector routinely exploited by botnets and other automated threats that needs to be specifically called out and emphasized in the Report. Many IOT devices use standard default usernames and passwords that are identical for every device and are often not changed by the device owner. Moreover, these devices do not have identity primitives and cannot be uniquely identified. This combination of vulnerable usernames and passwords and a lack of unique identity make the devices easy targets for exploitation by a botnet.

Using traditional IT methodologies of assigned identity for IOT devices also introduce significant management complexities (to include secure storage, database management, and policy enforcement), expense, risk of compromise and scalability challenges. In addition, many IOT devices lack other basic security protections like secure boot and secure upgrade that will

increase risk over their extended lifecycle. While the state-of-the-art is advancing rapidly and IOT devices with identity and a hardware root of trust are becoming viable, a change in paradigm across the ecosystem will take many years to implement.

As a less costly and near-term alternative, the Report should reference approaches that prevent botnets from discovering new exploitable devices to infect. By cutting off botnets at the first pass, organizations are able to better manage risk associated with the inherent identity and access management weaknesses associated with IOT devices.

One example of a capability that prevents device discovery is Transport Access Control (TAC). TAC blocks unauthorized traffic at the first packet of a TCP/IP session in the transport layer of the open system interconnection (OSI) stack, which prevents botnets from discovering and infecting new IOT devices. By cutting off communication prior to establishing a TCP/IP session, TAC effectively disrupts the cyber kill chain at the earliest possible moment. The ability to stop a botnet at the transport layer of the open system interconnection (OSI) model prior to establishing a communication channel conceals network assets from scanning and discovery -- essentially rendering the network invisible to the botnet.

TAC works by imposing identity and authentication onto the network, combining non-interactive authentication (authentication before any response is made to a network authentication request) and network identity in a fully automated fashion. Inserting identity into the first packet of a TCP/IP session to communicate a requester's identity across the network allows cloud and network services to determine the identity of the requester before responding to the TCP/IP request and block unauthorized, anonymous traffic at the very first packet.

While not a silver bullet, TAC has the ability to significantly reduce the size and impact of a botnet. This revolutionary capability addresses a critical security flaw in the TCP/IP protocol and there is currently no other mechanism for blocking botnet scanning and reconnaissance without also blocking legitimate users.

Recommended Report Edits

To better incorporate the concepts of identity and authentication, Blackridge recommends adding the following bolded and underlined sentence on page 17 and on page 36 as follows:

> Hardware roots of trust and trusted execution technologies are now a component of many off-the-shelf computing platforms. Future products will need to leverage these technologies to demonstrate authenticity and integrity at initial deployment and throughout the period of use. Modern development techniques rely on a combination of open source and commercially available components. To meet future security demands, such components must be traceable through the supply chain and offer greater

assurance. **Device identity, coupled with authentication, must be available operationally to enhance transport, application and data-level protections.** (page 17)

Critical infrastructure and industrial applications of IoT present significantly higher risks to the nation than home applications. These devices are also deployed in very different environments, supported by professional administrators. The lightweight assessment mechanism envisioned in Action 5.1 would not offer a sufficient level of assurance for these customers, and additional features are likely to be required. Assessment features such as device authentication, hardware roots of trust, or managed update functions would require direct interaction with products, if not review of source code. **Device identity, coupled with device authentication must be available operationally to enhance transport, application and data-level protections** (Action 5.2 page 36).

To incorporate approaches that prevent botnets from discovering exploitable IOT devices, BlackRidge recommends adding the bolded and underlined phrases to Action 3.3 on page 32 and to add an additional Action 3.5 as follows:

Action 3.3 Enterprises should migrate to network architectures that facilitate **prevention,** detection, disruption, and mitigation of automated, distributed threats.

A variety of effective anti-DDoS products and services are currently available, and innovative new products (such as those described in Action 3.1) have recently emerged. However, most enterprises have architected their networks for simplicity and performance rather than security. In combination with the CSF Profile for DDoS Prevention and Mitigation, enterprises have an opportunity to re-architect their networks to isolate insecure devices **and prevent their discovery by unauthorized actors**, manage communication flows, and generally enhance the resilience of the ecosystem.

Action 3.5 Encourage the development and deployment of anti-scanning and anti-reconnaissance technologies that can be applied to both legacy IPv4 and modern IPv6 environments.

Network scanning and reconnaissance enable the discovery of computers and devices that may be compromised and incorporated into botnets. The use of anti-scanning technologies at the enterprise, device, home and small business router levels can thwart the discovery of exploitable IOT devices and prevent their recruitment into a botnet.