Cyber Threat Alliance, Inc.
1001 19th Street North, Suite 1200
Arlington, Virginia 22209

Cyber Threat Alliance Comments on Distributed Threats Report

The Cyber Threat Alliance (CTA) appreciates the opportunity to provide feedback on the draft "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and other Automated, Distributed Threats." CTA currently encompasses 14 member companies, including Checkpoint, Cisco, Eleven Paths, Fortinet, IntSights, McAfee, Palo Alto Networks, Rapid 7, RSA, Reversing Labs, Saint Security, SK Infosec, Sophos, and Symantec.

CTA strongly supports the overall thrust of the report. Botnets represent a clear threat to the digital ecosystem, but the threat they pose can be substantially mitigated through coordinated action, as the report suggests. As such, this report provides a strong framework for coordinated action between governments and the private sector. However, we believe the report could be made stronger by prioritizing the proposed steps, identifying more concrete actions to achieve the goals, and expanding the role for cybersecurity companies. In support of this overarching feedback, we would offer the following specific comments on the report:

1) Comment: The report acknowledges that the majority of compromised devices in recent botnets have been located outside the U.S. We recommend acknowledging that this situation represents an on-going shift that will continue and even accelerate as other countries digitize.

   Reason: Since the majority of distributed threats will emanate from overseas, the report should use this fact to reinforce the need to address the threat through partnerships that extend internationally.

2) Comment: The definition of "infrastructure" on pages 9-10 should include cybersecurity companies as a key player in dealing with the threat from automated, distributed attacks.

   Reason: The role of cybersecurity companies in mitigating the threat from automated, distributed attacks is currently limited in the report. The report focuses on actions to mitigate DDoS traffic or other malicious activity that is already occurring. Cybersecurity companies play a key role in the ecosystem by striving to prevent malware infections from occurring in the first place through their cybersecurity tools and by the rapid sharing of technical indicators new malware and botnets are discovered. Furthermore, cybersecurity companies play a key role in preventing reinfection of devices when coordinated botnet takedown actions are taken. As we mention later in our comments, botnet takedowns are only effective when performed in coordination with the cybersecurity community to reduce reinfection rates.

Cyber Threat Alliance, Inc.
1001 19th Street North, Suite 1200
Arlington, Virginia 22209

3) Comment: On page 14, the report argues that "Organizational procurement policies must ensure that security lifecycle issues figure prominently in procurement decisions, so insecure products are not added to the mix." CTA recommends that the last clause be reworded to read, "so that the most secure products available are favored or if insecure devices must be bought to meet mission requirements, compensating controls are put in place."

   Reason: In many cases, "secure" products are not available in the marketplace, but the organization still has a mission need for those items. Therefore, procurement policies should require that if an insecure device must be bought, the acquiring organization must have a plan for managing or mitigating the risk that comes with that device.

4) Comment: The report should acknowledge that part of the reason distributed threats thrive is that the cost of the malicious activity is not borne by either the manufacturer nor the user of IOT devices. Therefore, effectively addressing the botnet threat will include creating incentives for these two groups to support increased cybersecurity on these devices.

   Reason: Unlike previous botnet targets, neither the manufacturer nor the device owner suffers adverse consequences from botnet activity. For example, if a botnet hijacks an internet connected thermostat, the manufacturer does not typically lose business as a result, so it has no incentive to make future thermostats more secure. Similarly, the thermostat continues to work properly and effectively for the owner, so the owner has no incentive to address the issue. We will need to create incentives for manufacturers and owners to support increased security for these devices.

5) Comment: On page 17, the report states that the vast majority of home and small business owners are unaware of cybersecurity risks. CTA recommends that this sentence be reworded to read "The majority of home and small business owners do not fully understand the risks associated with all their connected devices or how to mitigate those risks."

   Reason: As drafted the sentence probably overstates the public's lack of awareness. Almost everyone is aware that cybersecurity is a problem. Where the awareness breaks down is how the threat potentially affects an individual or small business directly. Therefore, we recommend re-wording the sentence to reflect where the lack of awareness actually consists of.

Cyber Threat Alliance, Inc.
1001 19th Street North, Suite 1200
Arlington, Virginia 22209

6) Comment: The report should prioritize the five goals and the subsequent actions should identify concrete recommendations and tasks to specific entities to achieve the goals.

   Reason: CTA agrees with the goals and actions laid out in the report. However, the report lacks any explicit prioritization of the five goals. If the group's study identified any true linchpins among the actions and goals that would have an outsized effect on solving the identified problems, it would be useful to call attention to them and prioritize those actions. We understand that coordinated activity is required across all of the goals, but as currently written, it is unclear where efforts should be focused in the short-, mid-, and long-terms. From CTA's perspective, we believe that the following actions would provide the greatest benefits in the short-term and should be prioritized in the following order:
   - Action 2.1 (with comments below incorporated)
   - Action 2.2
   - Action 4.1 (with comments below incorporated)
   - Action 2.5
   - Action 2.4 (with comments below incorporated)

   Additionally, the actions as identified are clearly useful for achieving the goals. However, the draft report often leaves unclear what specific groups should be tasked or have ownership with ensuring that the actions are moving forward and making progress. The report would benefit from including recommendations for organizations to lead the actions and timelines for their implementation.

   Alternatively, the report could acknowledge that prioritization, identification of leads, and establishing timelines would form the core of an implementation plan for the report's goals and actions.

7) Comment: The report makes several allusions to the role of information sharing in mitigating botnet threats and other malicious activity. While CTA certainly supports those assertions, the report should make clear that effective information sharing does not just mean sharing technical indicators, but also encompasses sharing information about threat context, business operations, best practices, threat awareness, vulnerabilities, etc. In addition, the type of information sharing an organization shares should reflect its overall business operations and not every organization needs to be sharing or trying to consume technical indicators. Whenever possible and reasonable, organizations should look for opportunities to encourage their cybersecurity providers to enable automated ingestion of indicators to speed up cybersecurity, or if they are able to consume technical indicators themselves, seek such automation internally. Throughout the report, the role of cybersecurity companies in information sharing, in coordination with ISPs and governments, should be emphasized.

Reason: Most organizations have difficulty producing or consuming technical indicators for themselves (large banks are the exception, not the rule). Instead of trying to get every organization to produce or consume technical cybersecurity information, certain key players in the ecosystem need to be the focus of the technical indicator sharing, such as cybersecurity companies, telecommunications companies, such as the ISPs, and large IT service providers. Other organizations need to focus on sharing intelligence and information directly relevant to their business operations that helps the company make risk-informed cybersecurity decisions. We note that this line of thought already appears in the report in some places, such as on page 18 regarding how devices should be engineered with users' behavior (or lack of good security behavior) in mind and include processes to automatically update software.

Examples:

- Page 12, first paragraph at top of page. Technical indicator information sharing should not necessarily be extended to "smaller, less well-funded, or niche players," but instead should focus on the cybersecurity companies and ISPs that provide services to those players and can act on their behalf. Smaller, less capable organizations need different information, more focused on the specific threats they face and the actions they need to take on their networks.
- Page 28, Action 2.1. This action should include cybersecurity companies. For example, "Internet service providers and their peering partners, in coordination with cybersecurity companies, should…" Inclusion of cybersecurity companies in this action would accurately reflect the role these companies play in threat intelligence and development and distribution of technical indicators. Once these indicators are shared amongst cybersecurity companies and ISPs, these organizations can use them to protect their customers.

8) Comment: Action 4.1 should not be focused exclusively on sharing information with law enforcement and should expand to cover increasing information sharing with the network defense community, which includes cybersecurity companies and government Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs).

   Reason: As written, the Action only takes into account the law enforcement equities in what can be done with the information that is shared regarding automated, distributed threats. While law enforcement actions are important for disrupting malicious cyber activity, they are not the only actions necessary to address distributed threats over the long-run. Cybersecurity companies and

Cyber Threat Alliance, Inc.
1001 19th Street North, Suite 1200
Arlington, Virginia 22209

ISPs can take actions on their networks to counter threats outside of or in coordination with law enforcement actions that will likely bring a more holistic solution to the problem. For example, law enforcement actions may help with taking down a botnet, but they often do not mitigate the vulnerabilities that allowed the botnet to be established in the first place.

9) Comment: We understand Action 2.4 encourages entities to continue collaborating on the enhancement of standardized information sharing protocols; however, we recommend more explicitly stating the intent of the Action. Further, we recommend considering the "Report on Securing and Growing the Digital Economy" written by the Commission on Enhancing National Cybersecurity. Specifically, Recommendation 2.1 and its associated Actions in the Commission's report includes language that may provide helpful context when further developing Action 2.4.

   Reason: As written, the purpose and desired outcome of Action 2.4 is unclear. For instance, the language stating "…to enhance information-sharing protocols to meet stakeholder needs and establish international standards…" is vague. Further, the language is unclear as to who is the stakeholder – private and/or public sectors, specific segments of these sectors, international partners, and/or all of the above.

Sincerely,

J. Michael Daniel
President & CEO
Cyber Threat Alliance