Response & Commentary to

The DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Request for Comment

Draft Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

[Docket No. 180103005-8005-01]
RIN 0660-XC040

FASTER FORWARD

Akamai Technologies, Inc.

11111 Sunset Hills Road
Suite 250
Reston, VA 20190

Primary Contact:

Tom Ruff
VP Public Sector
Akamai Technologies
703-621-4027
thruff@akamai.com

Technical Contact:

Micah Maryn, CISSP
Senior Solutions Engineer
703-963-1577
mimaryn@akamai.com

Introduction

Akamai is pleased to respond to the Department of Commerce, National Telecommunications and Information Administration, Request for Comment on the *Draft Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* ([Docket No. 180103005-8005-01] RIN 0660-XC040).

Akamai Response

The Draft Report includes several goals and actions which, over time, may have an impact on the ease of bot-net proliferation. The report does define current challenges and future goals fairly well, and presents several actions to encourage improved security in development and manufacturing using standards, policies, and other market incentives.

However, the Draft Report does lack goals and actions related to the mitigation of attacks. Most of the report is focused on using standards and policies in some way to eliminate the potential for large bot net-infections. There is very little information and no recommendations for making networks more resilient to attack. While encouraging better security among manufacturers is important, this is a long term goal. There needs to be near term goals and actions directed at preventing attacks from highly distributed bot-nets from impacting critical infrastructure.

The report touches on this on page 11, paragraph 1:

> *The current best practices involve employing a hybrid approach that uses both local filtering and off- premise capacity-increasing DDoS defense tools. However, best practices are at times expensive, difficult to manage, and require skilled staff; they are also typically built around past crises, making it difficult to argue for a large amount of excess capacity, for example, until under attack.*

Akamai agrees, a hybrid approach is needed, that includes security layer within the enterprise, at the border, and into the cloud. But, Akamai disagrees that such an approach needs to be expensive, difficult to manage, or have excess in capacity.

A Cloud-based security layer can be dynamically scalable, easily managed, and adaptable. Moreover, in order to have the resiliency to mitigate the kinds of attacks that highly distributed bot-nets are capable of invoking, requires a highly distributed security layer.

Key Recommendation:

Additional Goal: Improve Network Resiliency of Critical Infrastructure Networks. In order to ensure the availability and integrity of Critical Infrastructure, it is necessary that such networks have additional capacity and layers of security to ensure operations during the largest of bot-net attacks. Critical Infrastructure networks should be strongly encouraged to deploy Cloud Based security tools and services, which are able to provide dynamic scalability and a distributed layer of defense to mitigate the threats from highly distributed bot-nets.

Whenever applicable, Critical Infrastructure networks should invest in cloud security solutions with the capabilities of mitigating attacks as far upstream from the Critical infrastructure's networks and as close as possible to the source. These solutions will provide increased and dynamic scalability far beyond what is possible with origin side or ISP investment.

Akamai Responses to RFC Questions

The following section includes Akamai's direct responses to the questions posed in the RFC solicitation.

1. **The Ecosystem:** Is the Report's characterization of risks and the state of the current Internet and communications ecosystem accurate and/or complete? Are there technical details, innovations, policy approaches, or implementation barriers that warrant new or further consideration?

   The current draft's definition of "infrastructure" is too broad. The high level definition of infrastructure as "the technology and organizations that enable connectivity, interoperability, and stability", is accurate. However, the security considerations and challenges of the different components of infrastructure are different.

   The practical capabilities of appliances (routers/switches) differ from the capabilities an ISP could provide. Approaches to securing host environments are different for cloud hosted, physical hosted, and hybrid environments.

   By separating out the components of infrastructure, the report would be able to detail where within the infrastructure (devices, ISP, DNS, etc.) specific improvement be made. This should provide better clarity on recommendations as well as illustrating how "the complexity of modern infrastructure, with key tools and players interspersed through the ecosystem," requires a multi-layered approach to security.

2. **Goals:** Are the Report's stated goals appropriate for achieving a more resilient ecosystem? Do the actions support the relevant goals? In aggregate, are the actions sufficient to significantly advance the goals?

   The goals stated in the report are focused primarily on prevention of proliferation of bot-nets through creation of standards and policies. While the recommendations are valid for a long term approach to preventing bot-net threats, they are not practical for near term solutions for three reasons:

   1. The time it takes to develop and publish standards and policies
   2. Ability to ensure compliance to standards and policies, especially when applied to an international market.
   3. Does not address the current number of devices and bot-net infections already in existence.

   What the report is missing are recommendations for building resiliency for mitigation of bot-net attacks. Two recommendations which should be added.

   1. Reinforce the IT modernization goals of EO 13800
   2. Recommended actions for improving network resiliency with tools and services available today.

   EO 13800 lays out a plan for modernizing federal IT infrastructure. IT modernization key building resiliency against massive bot-net attacks. Modernization is not just updating systems and infrastructure. Modernization includes modernizing the approach to operations to include continuous development and enhancement, a DevOps approach. The threat landscape is dynamic. Vulnerabilities are not always detected until later, sometimes after they have been exploited. Therefore it is critical that networks and network owners have the flexibility to develop and deploy new mitigations and defenses.

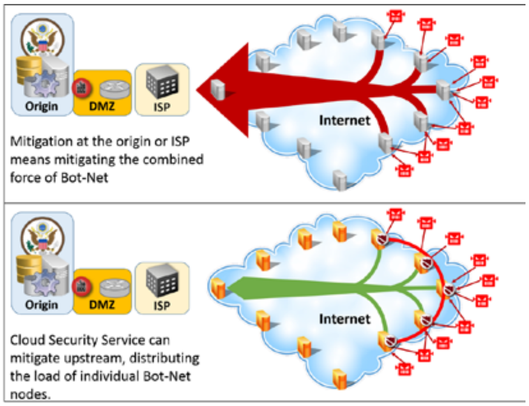
The report needs to include recommendations for improving network resiliency today, identifying tools, approaches, and services which have been proven to be successful in mitigating large scale bot-nets.

When dealing with automated and distributed threats, security solutions and mitigations need to be able to scale rapidly to meet that threat. ISPs do not have the scalability to match the amount to traffic that can be quickly generated by these attacks. In order to be scalable to match distributed threats, the mitigation tools and solutions also need to be distributed.

The report needs to include recommendations for the use of cloud based security solutions which are able to mitigate attacks closer to the individual bot-net nodes, and further upstream from the target networks and ISPs. The solutions include:

- Cloud based network scrubbing solutions that can inspect traffic up stream and mitigate threats before they can impact the target network
- Cloud Based application layer firewalls that can inspect and mitigate inbound application layer traffic upstream from the host environment with dynamic scalability.
- Cloud based DNS services that can mitigate and absorbed large volumetric attacks
- Content Delivery Networks that offload the amount of inbound traffic, absorbing volumetric spikes and preventing the host environment from being overwhelmed.

These are commercially available solutions today that have been proven as effective tools and solutions for mitigation of large scale bot-net attacks.


Origin
DMZ
ISP
Internet
Mitigation at the origin or ISP means mitigating the combined force of Bot-Net
Origin
DMZ
ISP
Internet
Cloud Security Service can mitigate upstream, distributing the load of individual Bot-Net nodes.

With respect to information sharing, the report outlines several approaches to information sharing of threat intelligence, attacks, and other network monitoring between commercial entities and ISPs. The report does acknowledge potential defaulting in gain such cooperation, including legal concerns for entries to share such information.

In addition to pursing approaches to improve information sharing, the report should also consider commercially available threat intelligence services which are able to aggregate similar, and sometimes more detailed information. In fact, the National Cybersecurity and Communications Integration Center (NCCIC) is currently aggregating threat intelligence and information about active threats and vulnerabilities from multiple commercial providers

3. **Stakeholder Roles:** How can specific actions be refined for efficacy and achievability? What actors, inside the Federal government, in the private sector, and across the global community, can be instrumental in the successful accomplishment of these activities? Who should play a leadership role; and where and how? What stakeholders are key to particular successes?

   Start with what can reasonably be controlled. Within the federal government, it would be easy to define specific security standards for network devices and policies baseline measures for building resiliency DDoS mitigation.

   The government should make an effort to ensure that vendors supplying network connected devices are following common sense secure engineering and prioritize procurement from vendors or manufacturers that adopt secure engineering standards and certifications.

   Applying similar standards to the private sector would be more difficult. Rather, the federal government needs to actively participate with private sector and industry working groups. This would enable direct government input in establishing standards and policies, development of solutions and policies for reducing cyber risk of national IT infrastructure (public and private). Furthermore, many industry working groups are international, so participation would be a step toward international goals.

   DHS's National Cybersecurity and Communications Integration Center (NCCIC) has been effective in aggregating threat intelligence and disseminating information about active threats and vulnerabilities. Acting as the primary federally centralized organization for cyber security, it is now effectively collaborating with 64 private and 11 federal agencies.

   It is recommended that investment into the NCCIC should continue toward improving the efficiency and capabilities of the NCCIC.

4. **Road map:** What information can help the government and stakeholders delineate a road map for achieving these goals? How should implementation be phased to optimize resources and commitments? Which actions are of highest priority, or offer opportunities for near term progress? Which actions depend on the completion of other actions? Are there known barriers that may inhibit progress on specific actions?

   For building a road map the government should identify near term and long term goals. Near term goals should ones that are higher priority and more easily obtainable.

   Using currently available solutions to build resiliency against highly distributed bot-nets is probably the most important and feasible shorter goal. As stated in our response to Question 2, there are multiple solutions available today that are proven to be successful in mitigating these kinds of attacks.

   The educational recommendations contained within the report are also easily obtainable. Because so many consumer market devices are targeted for bot-net infections, information campaigns targeting the consumer audience would improve consumer awareness to the importance of securing these devices. Such an educational campaign would help prevent future bot-net proliferation without having to wait for standards to be created.

   Many of the report’s recommendations and actions are long term goals. These recommendations are focused on preventing proliferation of bot-nets through standards and policies. Completion of these goals are depended upon a time consuming process for creation and publication of new standards and policies.

5. **Incentives:** What policies, innovations, standards, best practices, governance approaches, or other activities can promote market-based solutions to the challenges and goals discussed in the report? Are there specific incentive ideas beyond the market-based approaches discussed in the report (e.g., procurement, multistakeholder policy development, R&D, best practices, and adoption & awareness efforts) that demand new consideration or exploration?

   It's very difficult for the US Government to regulate any industry market without legislation. Furthermore, such legislation would have almost no impact on many foreign markets. In other words, there's no way that regulations within the US are going to prevent the proliferation of insecure devices in other countries.

   Most successful market changes occur when it is profitable for companies to do so. Consumer awareness will help drive manufactures and developers to have more secure products.

   And the federal government is also a consumer within this marketplace, a rather large consumer. As the federal government completes research and begins issuing standards and policy requirements for connected devices, manufactures and developers will want to ensure their products will be within compliance guidelines.

6. **Further Activities:** What additional specific actions can improve the resilience of the Internet and communications ecosystem? What partners can drive success for these activities?

   There needs to be additional recommendations for tools, solutions, and services that will enhance offload and scalability to mitigate the impact of highly distributed Bot-nets.

7. **Metrics:** How should we evaluate progress against the stated goals?

   There's three metrics that should be considered based on the various goals.

   For standards and policies, progress should be measured on successful agreement and industry adoption.

   Another metric to monitor is the proliferation of bot-net infections. This will help demonstrate the effectiveness of standards and education with respect to prevention.

   Finally, we need to monitor the impact of future bot-net attacks. The ultimate goal here is to build resiliency, therefore, success should be measure by successful mitigations. i.e. attacks that are mitigated without impact upon the targeted networks.

About Akamai

Operational since 1998, Akamai is the largest and most robust Content Delivery and Cloud Security Platform, providing enterprises across the globe secure, high-performing user experiences on any device, anywhere.

At the core of Akamai's solutions is the Akamai Intelligent Platform™, the largest, most distributed, FedRAMP accredited cloud infrastructure on the Internet. Consisting of more than 233,000 servers in over 130 countries and within more than 1,600 networks around the world, Akamai sits within one network hop of 85% of all client users (malicious and non- malicious actors), delivering over 30 terabits of traffic and over 3 trillion interactions daily. Akamai supports thousands of organizations, including:

- 60 percent of Global 500 & Fortune 500 companies
- The top 30 media & entertainment companies
- All 20 top global e-commerce sites
- 18 of the top 20 world's largest asset managers
- 8 of the top 10 world's largest FinTech firms
- Thirteen of the top 15 largest auto manufacturers
- Nine of the top 10 global pharmaceutical companies
- Six of the top seven computer manufacturers
- All of the top anti-virus companies
- All branches of the U.S. military
- Multiple Federal agencies within every cabinet level department

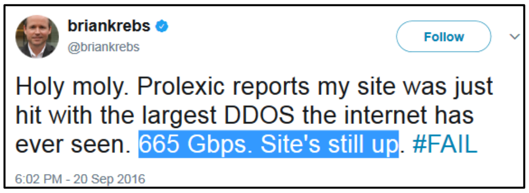
Akamai’s government experience includes over 100 government agencies and a presence within each of the 15 cabinet level departments. In addition to our product solutions, several agencies have implemented customized which leverage our insight and intelligence capabilities.

Akamai extends the security perimeter to the edge providing unmatched reliability, security, and visibility. Using this far reaching visibility to monitor current Internet conditions and activities enables Akamai to aggregate real time threat intelligence, which is then applied to further strength the security of our customers and enhance our cloud security solutions. Real-time data feeds of our threat intelligence are also available and are currently being used by several federal agencies.

Using the reach of our platform, our extensive threat intelligence, and our practical experience with active mitigation, Akamai has been successful in mitigating hundreds of attempted DDoS and application-layer attacks. Akamai has mitigated at least one major attack per week for years. Major trends are discussed in our quarterly *State of the Internet Report* (the most recent report, Q1-2017, has been included as Attachment 1). Some notable events mitigated by Akamai include:

- September 11, 2001- flash mobs and loss of major Internet connections inside the World Trade Center crippled news sites, the sites delivered by Akamai continued to be operational.
- July 2009- Akamai defended numerous US Government, commerce, and financial services sites from a multi-day 124-Gbps DDoS coming from a bot-net within South Korea (likely attributed to North Korea) with no operational impact.
- December 2010- Akamai defended several of its customers against a highly-contested hacktivist campaign known as Operation Avenge Assange.

- September 2016- Akamai successfully mitigated one of the largest attacks ever seen, in excess of 665 Gbps targeting security blogger, Brian Krebs.[1]



briankrebs
@briankrebs

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

6:02 PM - 20 Sep 2016

Twitter @briankrebs 9/20/2016

In addition to our core platform and threat intelligence capabilities, Akamai has assembled a team of security experts who are proactively engaged in increasing the security posture of our customers and our platform. Akamai operates five Security Operations Centers around the world maintaining 24x7 operations to support our customers during any security event. We also have teams dedicated to the analysis of the massive amounts of data aggregated to identify emerging threats and develop successful mitigations.

Akamai staff are certified across industry domains, such as CISCO networking certifications, Project Management certificates (e.g. PMP), and Security certifications (CISSP, GWAPT, GSLD, CEH, GPEN, etc.) to name a few. In addition, Akamai and Akamai employees actively participate with several working groups to solve problems like botnets, incident response, cloud security, and law enforcement (complete list in Appendix 2). Most recently, Akamai's CEO, Dr. Tom Leighton, and CSO, Andy Ellis, participated in the White House Technology Summit.[2]

Finally, Akamai has been a strong partner in support of information sharing both within the public and private sectors. Akamai is a member of Financial Services Information Sharing and Analysis Center (FS-ISAC), including providing cloud security services for the protection of the FS-ISAC web sites[3], and an active partner with the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC)[4]

[1] Many media outlets inaccurately reported that Akamai had dropped Krebs due to the impact on our platform. krebsonsecurity.com had been protected pro bono by our Prolexic scrubbing solution for 4 years (prior to and after Akamai acquired Prolexic). In that time, the Prolexic solution mitigated around 269 attacks (Source: Krebs 11/22/2016). We have included some links to articles which more accurately describe the events which led to that decision.

1. Motherboard.com interview with Brian Krebs
2. Boston Globe 9/23/2016

[2] NBC News: Tech Titans Meet at the White House

[3] https://www.fsisac.com/about/PoweredByAkamai

[4] https://www.dhs.gov/national-coordinating-center-communications