Online Trust Alliance

Written Testimony

Craig D. Spiezle, Executive Director & Founder
Online Trust Alliance

Before the
Senate Judiciary Committee's
Subcommittee on Crime & Terrorism

Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks

July 15, 2014

Chairman Whitehouse, Ranking Member Graham and members of the Committee, thank you for the opportunity to testify before you today. I also would like to thank you for your leadership in focusing attention to this important topic which is impacting users and businesses throughout the country.

My name is Craig Spiezle. I am the Executive Director and President of the Online Trust Alliance. OTA is a 501c3 non-profit, with the mission to enhance online trust and empower users, while promoting innovation and the vitality of the internet.

My background includes over a decade focusing on fighting online abuse, security and privacy threats. I have worked on a range of technologies and practices including developing and advancing anti-spam standards, anti-phishing technologies and introducing privacy controls providing users the ability to control the collection and use of their personal data.

OTA collaborates with several leading organizations fighting online abuse including the Anti-Phishing Working Group, (APWG), CA/Browser Forum, Center for Democracy and Technology (CDT), Email Service Provider Coalition, (ESPC), the Identity Theft Council, InfraGard, the International Association of Privacy Professionals (IAPP), the London Action Plan, Merchant Risk Council, StopBadware and others.

Botnets and associated cybersecurity exploits pose a significant risk to users, businesses and governments around the world. Increasingly bots are deploying key loggers and ransomware driving identity theft and bank account take-overs holding user's personal data, photo and health records hostage. Consumers innocently visiting trusted web sites are being compromised by malicious ads known as malvertising, while other bots are being used to cripple banking sites and make government services inaccessible.

It is important to recognize fighting bots is not just a domestic activity. Any effort requires a strategy to address international networks as cyber criminals intentionally operate beyond our borders. Criminals are leveraging the jurisdictional limitations of law enforcement and are proving to be nimble and innovative. They collaborate, share data and tools and often operative with impunity. Left unabated, they are a significant threat or our nation's critical infrastructure, to our economy and to users' privacy.

In my testimony I will discuss the following key areas:

1. Status of industry efforts
2. Need for a multifaceted anti-bot strategy
3. Role of takedown and law enforcement
4. Threat intelligence & data sharing
5. Privacy safeguards

Industry Efforts

Efforts to help combat botnets have been embraced by a range of public and private efforts. As an example, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), a FCC Federal advisory committee, last year developed a voluntary U.S. Anti-Bot Code of Conduct for ISPs, (ABC for ISPs). [1] [2] This code, modeled on efforts originally developed in Australia and Japan, has been publicly supported by ATT, Century Link, Comcast, Cox Communications and others. This code is an important example of the industry's ability to self-regulate.

In parallel, OTA has facilitated several multi-stakeholder efforts and working groups. These include publishing remediation and notification best practices and anti-bot guidelines for hosters and cloud service providers.[3] [4] [5] Adoption of these best practices by ISPs and other intermediaries will pay dividends helping protect users and aid in the remediation of their devices, data and privacy.

Multifaceted Strategy

Fighting botnets requires a holistic and global multi-stakeholder strategy. As outlined in Exhibit A, OTA advocates a five prong anti-bot framework including: Prevention, Detection, Notification, Remediation and Recovery. The Exhibit outlines a partial list of tactics and counter measures, which underscores the need for increased industry collaboration, research and two-way data sharing with the public and private sectors.

[1] http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv

[2] http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

[3] https://otalliance.org/system/files/files/resource/documents/ota_botnet_notification_whitepaper2012.pdf

[4] https://otalliance.org/system/files/files/best-practices/documents/ota_2013_botnet_remediation_best_practices.pdf

[5] https://otalliance.org/resources/botnets

Law Enforcement & Takedown Efforts

Law enforcement efforts are an important component to fighting online threats serving three major functions; 1) disrupting command and control hosts used by cybercriminals to run their botnets, 2) gathering evidence and intelligence and 3) bringing criminals to justice.[6]

Law enforcement can't fight today's sophisticated cyber criminals alone. They need help from industry partners. Similarly, the private sector can't fight cyber criminals without help from law enforcement. A trusted partnership is required. Noteworthy examples of collaboration is the DNS Changer takedown, impacting four million computers located in over 100 countries and similar efforts led by Microsoft and Symantec.[7]

Botnet take-downs and related efforts need to be taken with care and respect to three major considerations: 1) the risk of collateral damage to innocent third parties, 2) errors in identifying targets for mitigation and 3) respecting users' privacy. For example, taking down an entire web hoster because they have a handful of bad customers may be an example of unacceptable collateral damage. At the same time hosters and ISPs cannot hide behind bad actors and must take reasonable steps to help prevent the harboring of criminals and enabling cybercrime activity.

It is important to note that other anti-abuse tactics run similar risks including the unintended sharing of personal and sensitive information. The ISP and the anti-spam community continually fight spam which unfortunately can result in the blocking of legitimate senders. Bot traffic has been misidentified by ISPs and security vendors have temporarily blocked and re-directed residential users' internet access. Web browsers run the risk of misidentifying phishing sites and AV solutions can mistakenly block downloads and web content. Recognizing these risks, the public and private sector must establish

[6] http://en.wikipedia.org/wiki/Botnet

[7] http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

risk assessment procedures while staffing 24/7 remediation and escalation processes to remediate any unintended business and user impact.

Data Sharing

Data sharing between law enforcement and industry colleagues has the promise of being one of the most impactful tools in our arsenal. Data sharing must be reciprocal, with law enforcement providing data back to industry. Effective sharing requires exchanges that are dynamic and assure confidentiality. While today such sharing is occurring within individual sectors, expanded collaboration is needed between sectors such as retail, financial services and advertising networks. In the absence of this collaboration, cybercriminals move from one industry to another, sending malicious spam one day and perpetrating click-fraud and malvertising the next.[8]

Several industries have stood up Information Sharing and Analysis Centers (ISACs). These provide the ability to share data with each other, accelerating the deployment of best practices and threat detection capabilities.[9]

Privacy Controls & Considerations

The privacy landscape is rapidly evolving in the US, EU and other countries, ranging from the "right to be forgotten" and "Do Not Track", to restrictions on data sharing with third parties. Unfortunately threat intelligence data can often contain personally identifiable information, (PII). This underscores the importance that privacy be at the foundation of all fraud prevention and data sharing practices. Safeguards must be established including traffic monitoring by ISPs and data sharing among intermediaries including banks, websites and the AV community with law enforcement. Parties need to adhere to the FTC's Fair Information Practice Principles (FIPPS) and related sectorial regulations and adopt de-identification practices.[10]

[8] http://www.businessinsider.com/study-bots-will-waste-116b-in-ad-spend-in-2014-2014-1
[9] http://www.isaccouncil.org/
[10] http://en.wikipedia.org/wiki/FTC_Fair_Information_Practice

These privacy concerns can be easily addressed. When data is collected and used exclusively for threat detection, entities should be afforded "safe-harbor", providing that the data collected and shared is not used or retained for any other purpose. Conversely, industry needs assurances that law enforcement will not use such data for purposes other than fighting cybercrime.

Shared Responsibility

Every stakeholder has a responsibility to take action against these threats. We need to work together, be nimble and innovative. Progress has been with some ISPs and hosters, but a renewed focus and greater commitment from industry is required. As the Internet of Things, the smart grid and wearable technologies becomes prevalent, we need to look beyond the desktop. For example today mobile devices are increasingly being targeted by bots. This requires a renewed focus and investment from the mobile community including the role of app platforms and OS providers to increase the scrutiny and vetting of apps they host.

Summary

In summary, it is important to recognize there is no absolute defense against determined criminals. They will continue to exploit our systems and users, requiring all stakeholders and intermediaries to take action. We have a shared responsibility to increase investments in data sharing and adopt privacy enhancing practices, while finding new approaches to work with law enforcement and expand international cooperation.

Working together we can make the internet more trustworthy, secure and resilient while promoting innovation.

Thank you and I look forward to your questions.

Exhibit A – OTA Anti-Botnet Framework