Online Trust Alliance

Via email to mary_robertson@hsgac.senate.gov

June 18, 2014

Ms. Mary Robertson
Chief Clerk
U.S. Senate Homeland Security and Governmental Affairs Committee
Permanent Subcommittees on Investigations
223 Hart Senate Office Building
Washington, D.C. 20510-6250

Re: Supplement Questions from Senator Johnson

Dear Ms. Robertson,

Thank you for your request to provide additional insights responding to the May 15th Hearing "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy". Since the Hearing the impact of malvertising continues to grow. Ransomware and related threats deployed by malvertising is on the rise, with high profile sites such as the Disney, Facebook and the FIFA World Cup sites impacting innocent site visitors.[1, 2, 3]

The Online Trust Alliance (OTA) agrees with the industry that ad networks are under attack. Cybercriminals and fraudulent businesses have recognized the advertising ecosystem provides a highly scalable infrastructure to target and exploit consumers, businesses and government services simultaneously. The lack of security controls and low adoption of best practices makes ad networks soft targets and ripe for abuse. Yet when faced with the facts, industry trade groups continue to defend their practices and attempt to shift accountability to others.[4, 5]

Consumer's expectation of safety offline should be not different when online. A consumer visiting a shopping mall, has an expectation that systems are in place to help deter, detect and mitigate threats. While such incidents may be infrequent, mall owners and merchants have recognized the need to collaborate, invest in security staff, surveillance systems and training of first responders. Retailers work with law enforcement, share data with other merchants and report incidents. Although there is no guarantee of physical security against determined criminals, similar safeguards are needed online to help protect online consumers from malvertising.

---

[1] Malicious website ads lead to ransomware
http://www.computerworld.com/s/article/9248886/Malicious_major_website_ads_lead_to_ransomware?source=CTWNLE_nlt_security_2014-06-06

[2] Malvertising scheme uses Flash exploit to profit from World Cup buzz
http://www.scmagazine.com/malvertising-scheme-uses-flash-exploit-to-profit-from-world-cup-buzz/article/351289/

[3] http://www.fifa.com/worldcup/index.html

[4] http://netchoice.org/catch-criminals-dont-pass-buck/

[5] http://trustinads.org/about.html

In response to Senator Johnson's questions;

1. Given the enormous free market incentive to make sure malvertising does not drive consumers away, why is regulation from other organizations or government entities necessary?

   In the absence of meaningful self-regulation and an enforceable code of conduct governing the integrity of online advertising, the need for regulatory oversight is fast becoming warranted. In a perfect world, industry would recognize the long-term impact and be willing to address the vulnerabilities of their business models. Yet due to the inability of consumers and publishers to correlate an incident to a specific ad, the advertising industry is not realizing reputational harm. Unfortunately consumers have little if any visibility to know how, where and when they have been compromised by a malicious ad.

   In the near decade since the threat of malvertising was identified, the general response from industry has been one of dismissing the threat and attempting to discredit those who have raised the alarm.

   Society and our economy are increasingly reliant on web services funded by advertising. The knowledge of this dependency by cybercriminals is placing the Nation's critical infrastructure at risk. Inaction suggests the need for regulatory oversight, not unlike what is being demanded of network providers. Recently the Federal Communications Commission Chairman Tom Wheeler called on industry to step up cybersecurity measures or face new regulations. He called on ISPs and carriers to take the lead in ensuring their networks are secure against cyber-attacks.[6]

   As outlined in my testimony, we must work towards a framework addressing five key areas: Prevention, Detection, Notification, Data Sharing and Remediation. It is important that remediation be addressed. One such idea is industry establish a "super fund" offering remediation to impacted consumers. A victims' fund could cover financial losses, provide technical support along with reimbursement from ransomware. Such a program would instill consumer trust and serve as an incentive for networks and their trade groups to invest in prevention and detection technologies and operational procedures.

2. What can governments do to combat cybercriminals responsible for malvertising? What about cybercriminals generally?

   Malvertising is not unique to other forms of cybercrime plaguing critical infrastructure. It is being driven by sophisticated organized criminals operating outside of our borders with a great deal of anonymity and immunity from many of the countries they operate from. Without formal data sharing mechanisms, law enforcement efforts are limited. With only partial and unstructured data sharing, law enforcement lacks a 360 degree view of the threat landscape.

   In the aftermath of the Target breach, the advertising and banking industries formed an Information Sharing and Analysis Center (ISAC) to foster data sharing and adoption of best practices. Other mechanisms such as: InfraGard, a partnership with the FBI and the private sector; the Homeland Security Information Network; and the adoption of STIX (Structured Threat Information Expression) should be considered as part of required incident reporting.[7] [8] [9]

---

[6] http://online.wsj.com/articles/fcc-urges-an-industry-led-approach-on-cybersecurity-to-protect-u-s-communications-networks-1402594627?mod=WSJ_TechWSJD_NeedToKnow&cb=logged0.681783548510998

[7] http://stix.mitre.org/

[8] https://www.infragard.org/

[9] http://www.dhs.gov/homeland-security-information-network

Combined they would facilitate threat intelligence sharing with both other industry sectors and law enforcement, providing an early warning system and aid in shutting down criminal networks. The biggest factor impacting law enforcement today is that malvertising incidents remain largely unreported and what data that is being shared is typically unstructured and incomplete.

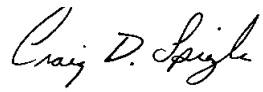
Recently U.S. Security and Exchange Commissioner Aguilar made a plea to public companies for mandatory incident reporting. He stated, "It is possible that a cyber-attack may not have a direct material adverse impact on the company itself, but that a loss of customers' personal and financial data could have devastating effects on the lives of the company's customers and many Americans."[10] The same obligation should apply to the interactive advertising industry. In the absence of such reporting, law enforcement's and stakeholder's efforts to fight malvertising will remain stymied.

Such data sharing should protect reporting parties from oversight and include controls to prevent personal identifiable information and competitive data from being shared outside of law enforcement. The National Cyber-Forensics & Training Alliance (NCFTA) is a public-private partnership where threat intelligence data is shared with law enforcement and back to partipating stakeholders with such privacy and confidential provisions.[11]

In summary, as our society and economy are increasingly reliant upon the internet and advertising-supported services, we have a shared responsibility to harden our systems. The OTA favors the adoption of an enforceable code of conduct and mandatory reporting over regulation.

As cybercriminals remain determined and in the absence of meaningful security controls, we can only expect the impact to consumers and our economy to grow. OTA looks forward to working with the Committee and industry to help fight these abuses and threats.

Respectfully,



Craig Spiezle
Executive Director & President
Online Trust Alliance

Cc: Jack Thorlin, Daniel Goshorn

[10] http://www.reuters.com/article/2014/06/10/sec-cybersecurity-aguilar-idUSL2N0OR13U20140610
[11] http://www.ncfta.net/