Statement of

Craig D. Spiezle

Executive Director & Founder

OTA
Online Trust Alliance

Testimony before the

Senate Committee on Homeland Security & Government Affairs

Senate Permanent Subcommittee on Investigations

Emerging Threats to Consumers within the Online Advertising Industry

May 15, 2014

Chairman Levin, Ranking Member McCain, and members of the Committee, good morning and thank you for the opportunity to testify before you today.

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, empowering users to control their data and privacy, while promoting innovation and the vitality of the internet.

I am testifying to help provide context to the escalating privacy and security threats to consumers resulting from malicious and fraudulent advertising known as malvertising.

As outlined in Exhibit A, malvertising increased over 200% in 2013 to over 209,000 incidents generating over 12.4 billion malicious ad impressions.[1] The impact on consumers is significant. This past January Yahoo experienced an incident resulting in over 300,000 malicious impressions in a single hour. Approximately 9% or 27,000 unsuspecting users were compromised. For these consumers, the infection rate was 100%.

This is not an isolated case. Cybercriminals have successfully inserted malicious ads on a range of sites including Google, Microsoft, Facebook, Wall Street Journal, New York Times, Expedia, Major League Baseball, (MLB) and others.[2, 3, 4]

The threats are significant, with the majority known as "drive by downloads". A drive by is malicious software which runs when a user innocently visits a web site – with no

[1] OTA data analysis based on incidents reported via data providers including RiskIQ, Zedo, The Media Trust, DoubleClick malvertising group and other sources, factoring in daily site traffic and life of exploit.

[2] http://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-malvertising-infrastructure/

[3] http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-banners-target-expediacom-and-rhapsodycom/

[4] http://www.scmagazineuk.com/major-league-baseball-website-hit-by-malvertising-that-may-potentially-impact-300000-users/article/246503/

interaction or clicking required.[5] This threat is not new; malvertising was first identified over seven years ago, yet to-date, little progress has been made.

The impact of malvertising ranges from capturing personal information to turning a device into a bot where essentially a cybercriminal can take over that device and use it in many cases to execute a distributed denial-of-service attack (DDoS) against a bank, government agency or other organization.[6] Just as damaging is the deployment of ransomware which encrypts a user's hard drive, demanding payment to be unlocked. Users' personal data, family photos and health records can be destroyed and stolen in seconds.

In the absence of secure online advertising, an impossibly task given today's fragmented advertising ecosystem, the integrity of the internet is at risk. Not unlike pollution in the industrial age, in the absence of regulatory oversight and meaningful self-regulation, these threats continue to grow. The development of coal mining and the use of steam power generated from coal is without doubt the central, binding narrative of the nineteenth century. Jobs were created and profit soared, but the environment soon felt the full impact of industrialization in the form of air and water pollution. Today we are approaching similar cross roads which are undermining the integrity of the internet.

Facing the onslaught of threats, a disturbing trend has emerged with enterprises opting to block all third-party advertising viewed by their employees. This follows users who have been installing ad blockers such as Ad Block Plus and No Script to similarly block all ads.[7, 8] While these tools may help maximize security and privacy, they marginalize the vitality of advertising which supports the sites and services which consumers and business depend on.

[5] A drive by download is malicious code which executes against a device by simply visiting a site, with no interaction and installs malware. A social engineered exploit is in the form of a pop up or dialog box which attempts to convince a user to take action including downloading a fraudulent update.

[6] http://en.wikipedia.org/wiki/Ransomware_(malware)

[7] https://adblockplus.org/en/internet-explorer

[8] http://noscript.net/

How does malvertising occur?

Since the first banner ads appeared twenty years ago, online advertising and complexity has progressed exponentially.[9] The industry has moved from sites having independent ad sales teams to a complex ecosystem of ad sellers, aggregators and buyers. Stakeholders include advertisers and ad agencies who create ads through a complex arbitrage of ad exchanges, ad networks and demand side platforms (DSP), where ultimately the display ad or ad banner is served through programmatic ad buying. (Exhibit B)[10] [11] A typical ad goes through five or six such intermediaries before being served.

The most common tactic to run a malicious ad is the criminal going directly to an ad network, selecting a target audience and paying for an ad campaign. In the absence of reputational checks or threat reporting among the industry, once detected and shut down by one ad network, they simply "water fall" or roll over to other unsuspecting networks to repeat variations of similar exploits.

Other tactics are illustrated in Exhibit C. They include impersonating legitimate advertisers or ad agencies, taking over an employee's user account, actions by rogue employees and the hacking of ad servers compromising existing ads and directly inserting malicious ads.[12]

Increasingly ads are purchased through an automated process as illustrated in Exhibit D. These systems without human inaction have increased from 38% of total display advertising in 2012 to a forecast of 73% in 2015. While this automation offers significant efficiencies, it lacks robust circuit breakers to detect fraudulent advertisers.[13] [14]

[9] http://www.wired.com/2010/10/1027hotwired-banner-ads/

[10] If browser or device cookies are disabled or if a user has enabled anti-tracking mechanisms, they will be served a contextual ad versus one based on the browser habits or profile. If a user turns on "Do Not Track" and the site respects the setting, they would most likely receive contextual based ads.

[11] http://onlineadvertisingecosystem.com/

[12] http://www.tripwire.com/state-of-security/vulnerability-management/analyzing-cve-2013-4211-openx-ad-server-remote-code-execution-vulnerability/

[13] http://cmsummit.com/behindthebanner/

[14] http://www.adotas.com/2014/05/watch-200-milliseconds-the-life-of-a-programmatic-ad-impression/

The impact of these threats has increased significantly. Criminals are becoming experts in targeting and timing, taking advantage of the powerful tools and data available to internet advertisers. They are data driven marketers with precision to reach vulnerable segments of society or high net worth audiences. This have been enabled to choose the day and time of exploits as well as the type of device they choose to target.

In the absence of policy and traffic quality controls, organized crime has recognized malvertising as the "exploit of choice" offering the ability to be anonymous and remain undetected for days.

Industry & Self-Regulatory Efforts

Recognizing the threats of malvertising, in December 2007, DoubleClick, later acquired by Google, established a mailing list which remains today as one of the primary methods of malvertising data sharing. In 2010, OTA established what is now the Advertising and Content Integrity Group, (ACIG), focused on security and fraud prevention best practices. This group of diverse stakeholders leverages a proven model of threat mitigation.[15] This group has since published white papers including a risk evaluation framework and remediation guidelines.[16, 17] These efforts are a small but first step to combat malvertising, reflecting input from leaders including Google, Microsoft, PayPal, Symantec, Twitter and interactive advertisers, web sites and ad agencies.

Last June, StopBadware, a non-profit organization, launched a parallel effort known as the Ads Integrity Alliance. In January 2014, this initiative disbanded due to its members' "desire to refocus their resources on aggressively defending industry practices to policy groups and regulatory bodies".[18]

[15] https://otalliance.org/resources/botnets/index.html
[16] https://otalliance.org/resources/malvertising.html
[17] https://otalliance.org/docs/Advertising%20Risk%20Evaluation%20Framework.pdf
[18] https://www.stopbadware.org/blog/2014/01/20/stopbadware-steps-down-as-leader-of-the-ads-integrity-alliance

In the wake of this group's demise, TrustInAds.org was launched last week. According the site, its focus is public policy and raising consumer awareness of the threats and how to report them.[19]

Unfortunately no amount of consumer education can help when users visit trusted web sites that are serving malvertising. Consumers cannot discern good vs malicious ads or how their device was compromised. Focusing on education after the fact is like the auto industry telling accident victims whom to call after an accident from a previously known manufacturing defect, instead of building security features in the cars they sell and profit from.

Other industry efforts have been focused on click fraud, fraudulent activities that attempt to generate revenue by manipulating ad impressions. Click fraud is focused on the monetization and operational issues facing the industry. While efforts to address these issues are underway, do not be confused—click fraud is not related to malvertising's harmful impact on consumers. Click fraud affects websites and advertisers. Malvertising affects consumers.

What is Needed?

OTA proposes a holistic framework addressing five key areas: Prevention, Detection, Notification, Data Sharing and Remediation. Such a framework should be the foundation for an enforceable code of conduct or possible legislation.

1. Prevention – Focused on the development and adoption of controls, systems and safeguards. Networks need to know who their advertisers are and have methods do identify outliers who may have malicious or fraudulent intent. Stakeholders who fail to adopt reasonable best practices and controls should bear the liability and publishers should reject their ads.

[19] http://trustinads.org/index.html

2. <u>Detection</u> – There is no perfect security, but circuit breakers must be in place to help detect abnormal ad behavior. Continuous monitoring is required with 24 /7 incident response teams and abuse desks to both detect and notify stakeholders.

3. <u>Notification & Data Sharing</u> - Escalation paths are needed to share threat intelligence, report abuse and take down threats. Standardized abuse reporting formats and metrics need to be established not unlike those used in the anti-spam and online abuse communities.

4. <u>Remediation</u> – Resources need to be allocated to taking down threats, including addressing any security vulnerabilities in the ecosystem and the user's device that have been compromised.

5. <u>Recovery</u> - Assistance to be provided to users whose devices and accounts have been compromised.

In parallel, operational and technical solutions need to be explored. Ideally we will have solutions where publishers would only allow ads only from networks who vouch for the authenticity of all of the ads they serve, and web browsers will render only such ads that have been signed and verified from trusted sources. It is recognized that such a model would require systemic changes; yet they would increase accountability, protecting the long term vitality of online advertising and most importantly the consumers.

In summary, as a wired society and economy we are increasingly dependent on trustworthy, secure and resilient online services. As observed in every area of our nation's critical infrastructure, we need to recognize that fraudulent businesses, cybercriminals and state sponsored actors will continue to exploit our systems.

For some, malvertising remains a "Black Swan Event", rarely seen but known to exist. For others it is the elephant in the room that no one wants to acknowledge.

Today, companies have little if any incentive to disclose their role or knowledge of a security event, leaving consumers vulnerable and unprotected for potentially months or years, during which time untold amounts of damage can occur. Failure to address these threats suggest the needs for legislation not unlike State data breach laws, requiring mandatory notification, data sharing and remediation to those who have been harmed.

As learned from the Target breach, it is the responsibility of a company and its executives to implement safeguards and to heed the warning of the community. The same standards should apply for the ad industry. We must work together, and openly disclose and mediate known vulnerabilities, even at the expense of short-term profits.

It is important to recognize there is no absolute defense against a determined criminal. OTA proposes incentives to companies who adopt best practices and comply with codes of conduct. They should be afforded protection from regulatory oversight as well as frivolous lawsuits. Perceived anti-trust and privacy issues must be resolved to facilitate data sharing to aid in fraud detection and forensics.

Trust is the foundation of every communication we receive, every web site we visit, every transaction we make and every ad we view. Now is the time for action and collaboration, moving from protective silos of information to multi-stakeholder solutions combating cybercrime.

I look forward to your questions.

Thank You

Exhibit A – Malvertising Trends

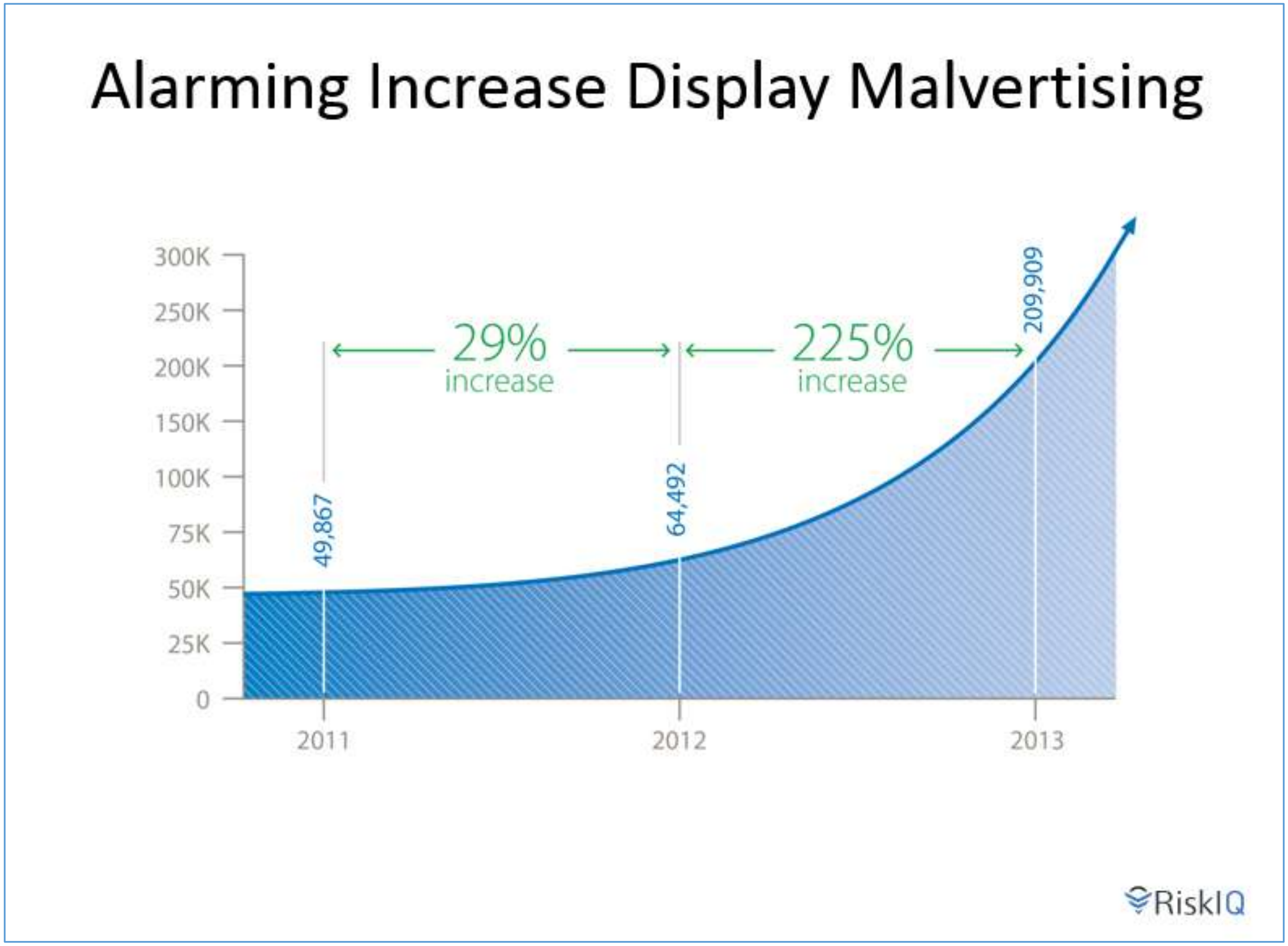


Exhibit B – Interactive Advertising Ecosystem

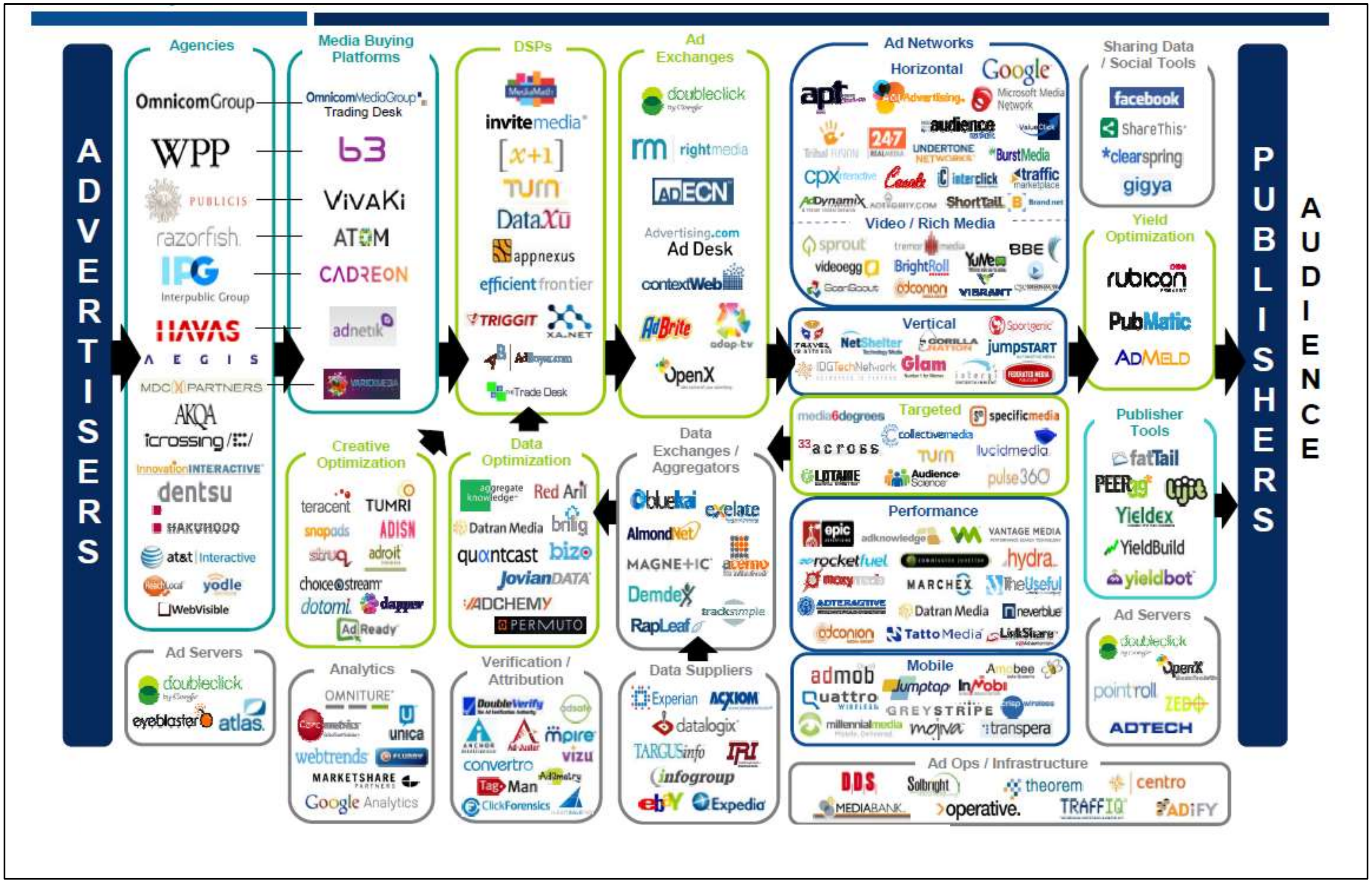
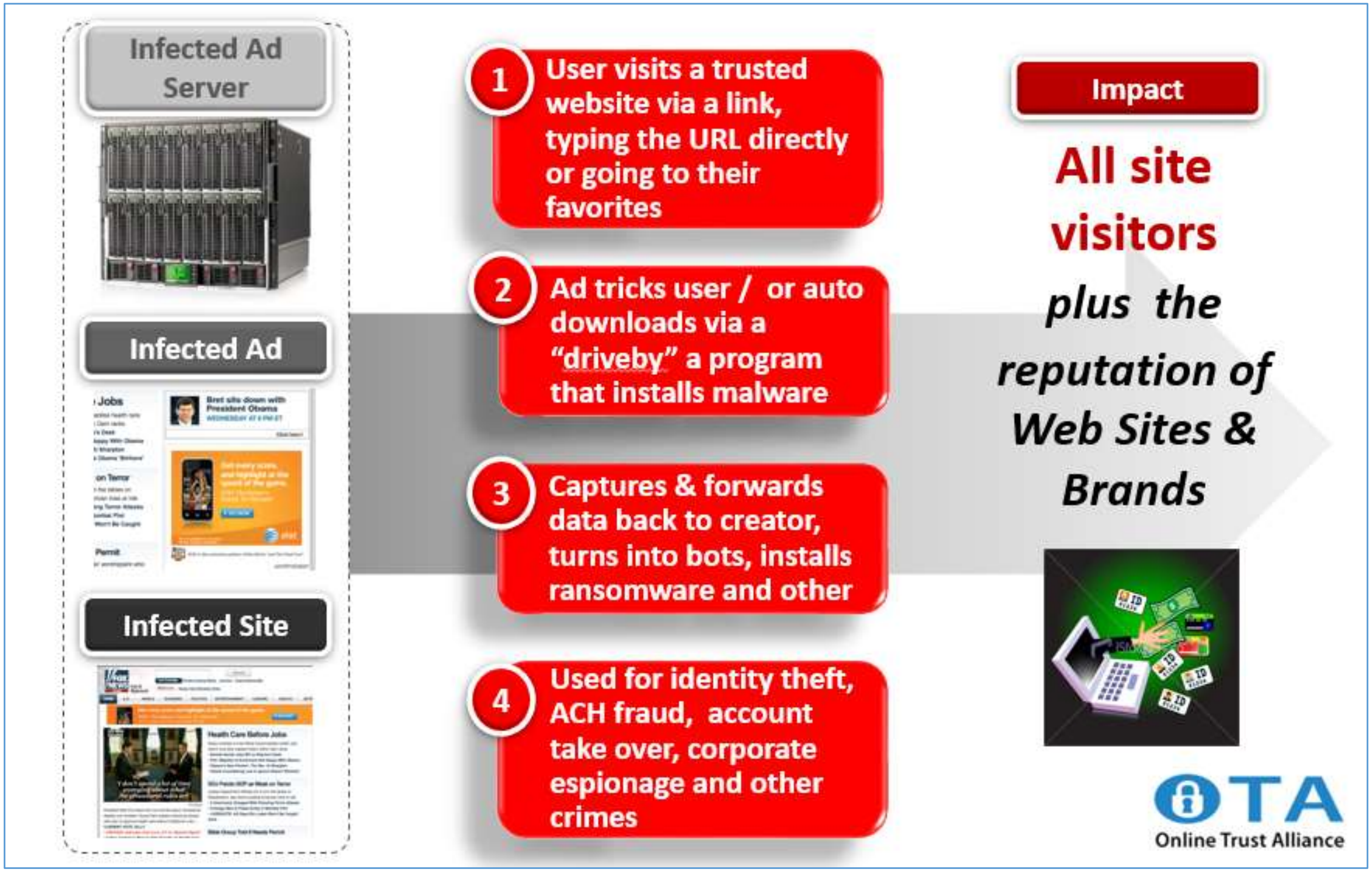


Exhibit C – How Malvertising Works



Infected Ad Server

Infected Ad

Infected Site

1 User visits a trusted website via a link, typing the URL directly or going to their favorites

2 Ad tricks user / or auto downloads via a “driveby” a program that installs malware

3 Captures & forwards data back to creator, turns into bots, installs ransomware and other

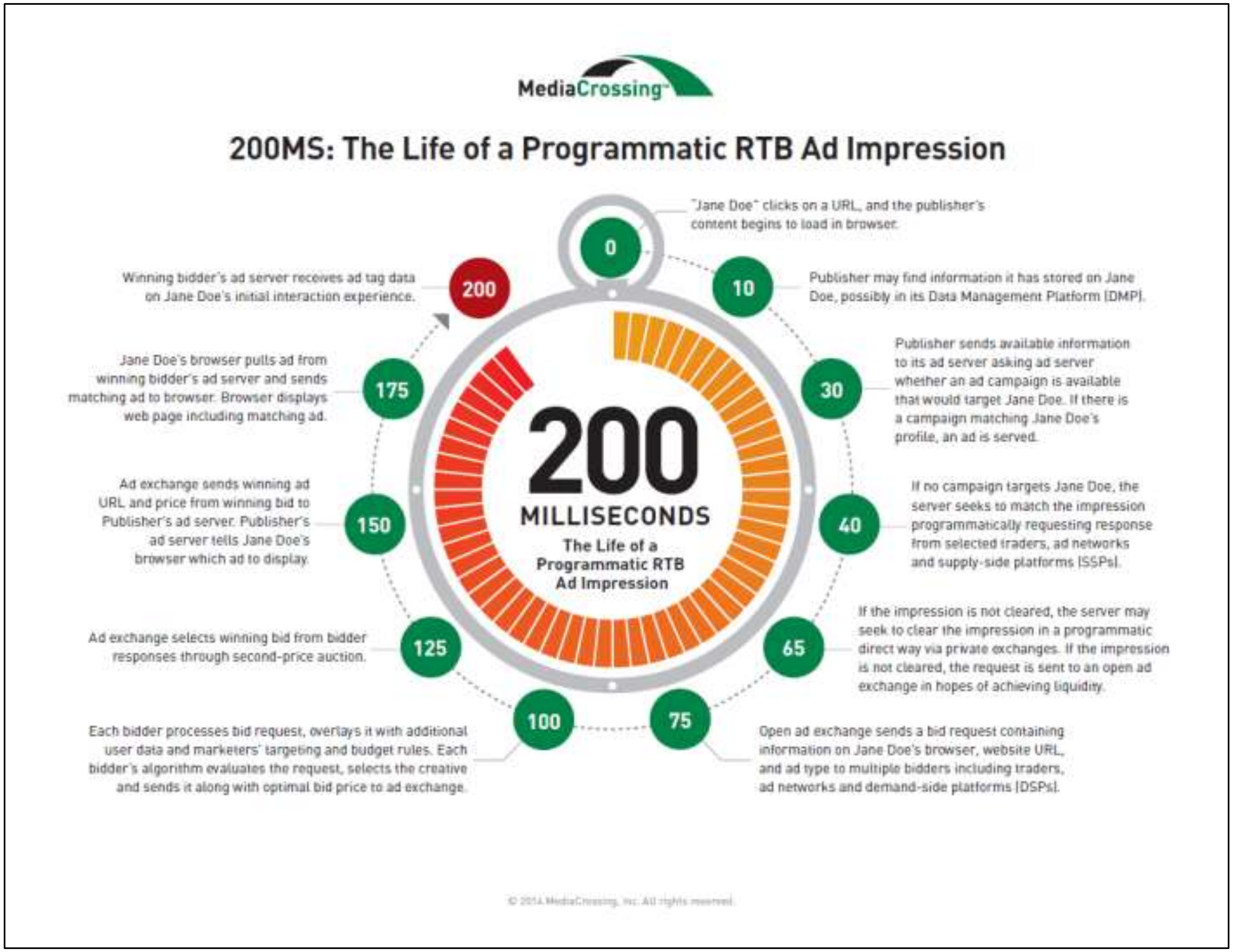
4 Used for identity theft, ACH fraud, account take over, corporate espionage and other crimes

Impact

All site visitors *plus the reputation of Web Sites & Brands*

OTA Online Trust Alliance

Exhibit D – Programmatic Ad Buying



200MS: The Life of a Programmatic RTB Ad Impression

0 – "Jane Doe" clicks on a URL, and the publisher's content begins to load in browser.

10 – Publisher may find information it has stored on Jane Doe, possibly in its Data Management Platform (DMP).

30 – Publisher sends available information to its ad server asking ad server whether an ad campaign is available that would target Jane Doe. If there is a campaign matching Jane Doe's profile, an ad is served.

40 – If no campaign targets Jane Doe, the server seeks to match the impression programmatically requesting response from selected traders, ad networks and supply-side platforms (SSPs).

65 – If the impression is not cleared, the server may seek to clear the impression in a programmatic direct way via private exchanges. If the impression is not cleared, the request is sent to an open ad exchange in hopes of achieving liquidity.

75 – Open ad exchange sends a bid request containing information on Jane Doe's browser, website URL, and ad type to multiple bidders including traders, ad networks and demand-side platforms (DSPs).

100 – Each bidder processes bid request, overlays it with additional user data and marketers' targeting and budget rules. Each bidder's algorithm evaluates the request, selects the creative and sends it along with optimal bid price to ad exchange.

125 – Ad exchange selects winning bid from bidder responses through second-price auction.

150 – Ad exchange sends winning ad URL and price from winning bid to Publisher's ad server. Publisher's ad server tells Jane Doe's browser which ad to display.

175 – Jane Doe's browser pulls ad from winning bidder's ad server and sends matching ad to browser. Browser displays web page including matching ad.

200 – Winning bidder's ad server receives ad tag data on Jane Doe's initial interaction experience.

© 2014 MediaCrossing, Inc. All rights reserved.