Written Testimony of
Alex Stamos
Vice President of Information Security
Yahoo! Inc.
Before the Senate Homeland Security and Government Affairs
Permanent Subcommittee on Investigations
"Online Advertising and Hidden Hazards to Consumer Security and Data Privacy"
May 15, 2014

Introduction

Chairman Levin, Ranking Member McCain, and distinguished members of the subcommittee, thank you for convening this hearing and for inviting me to testify today about security issues relating to online advertising. I appreciate the opportunity to share my thoughts and to discuss the user-first approach to security we take at Yahoo.

My name is Alex Stamos, and I am Yahoo's Vice President of Information Security and Chief Information Security Officer. I joined Yahoo in March. Prior to that I served as Chief Technology Officer of Artemis Internet and co-founded iSEC Partners. I have spent my career building and improving secure, trustworthy systems, and I am very proud to work on security at Yahoo.

Yahoo is a global technology company that provides personalized products and services, including search, advertising, content, and communications, in more than 45 languages in 60 countries. We strive to make these daily habits inspire and entertain our users. As a pioneer of the World Wide Web, we enjoy some of the longest lasting customer relationships on the web. It is because we never take these relationships for granted that 800 million users each month trust Yahoo to provide them with Internet services across mobile and web.

One reason I joined Yahoo is that from the top down, the company is devoted to protecting users. Building and maintaining trust through secure products is a critical focus for us, and by default all of our products should be secure for ***all*** of our users across the globe.

Achieving security online is not an end state; it's a constantly evolving challenge that we tackle head on. At Yahoo, we know that our users rely on us to protect their information. We also see security as a partnership; we want to educate our users to be mindful of their own security habits, and we provide intuitive, user-friendly tools and security resources to help them do so.

Malware is an important issue that is a top priority for Yahoo. While distribution of malware through advertising is one part of the equation, it's important to address the entire malware ecosystem and fight it at each phase of its lifecycle. It is also important to address security more broadly across the Internet.

I outline in my testimony below several specific ways Yahoo is fighting criminals and protecting our users, including: focusing on security in the advertising pipeline and sharing threats; leading the fight on email spam; operating a bug bounty program; and working to fully encrypt 100 percent of Yahoo's network traffic.

Internet Advertising Security and the Fight Against Malware and Deceptive Ads

Internet advertising security is an important focus for us. Yahoo has built a highly sophisticated ad quality pipeline to weed out advertising that does not meet our content, privacy or security standards. In January of this year we became aware of malware distributed on Yahoo sites and immediately took action to remove the malware, investigated how malicious creative copy bypassed our controls, and fixed any vulnerabilities we found. The malware impacted users on Microsoft Windows with out-of-date versions of Java, a browser plugin with a history of security issues, and was mostly targeted at European IP addresses. Users on Macs, mobile devices, and users with up-to-date versions of Java, were not affected.

As I mentioned earlier, the malware ecosystem is expansive and complex. Advertising is only one method of distribution, and distribution is only one part of the problem. Vulnerabilities that allow an attacker to take control of user devices through popular web browsers like Internet Explorer, plugins like Java, office software and operating systems, are large parts of the problem. Malware is also spread by tricking users into affirmatively installing software they believe to be harmless but is, in fact, malicious.

We successfully block the vast majority of malicious or deceptive advertisements with which bad actors attack our network, and we always strive to defeat those who would compromise our customers' security. This means we regularly improve our systems, including continuously diversifying the set of technologies and testing systems to better emulate different user behaviors. Every ad running on Yahoo's sites or on our ad network is inspected using this system, both when they are created and continuously afterward.

Yahoo also strives to keep deceptive advertisements from ever reaching users. For example, our systems prohibit advertisements that look like operating system messages, because such ads often tout false offers or try to trick users into downloading and installing malicious or unnecessary software. Preventing deceptive advertising once required extensive human intervention, which meant slower response times and inconsistent enforcement. Although no system is perfect, we now use sophisticated machine learning and image recognition algorithms to catch deceptive advertisements. This lets us train our systems about the characteristics of deceptive creatives, advertisers and landing sites so we detect and respond to them immediately.

We are also the driving force behind the SafeFrame standard. The SafeFrame mechanism allows ads to properly display on a web page without exposing a user's private information to the advertiser or network. Thanks to widespread adoption, SafeFrame enhances user privacy and security not only in the thriving marketplace of thousands of publishers on Yahoo, but around the Internet.

We also actively work with other companies through our participation in a number of industry groups, including the Interactive Advertising Bureau's (IAB) Ads Integrity Taskforce, which aims to create a higher level of trust, transparency, quality and safety in interactive advertising. We have proudly joined TrustInAds.org, a group of Internet industry leaders that have come together to protect people from malicious online advertisements and deceptive practices. We also participate in groups dedicated to preventing the spread of malware and disrupting the economic lifecycle of cybercriminals, including the Global Forum for Incident Response and Security Teams (FIRST), the Anti-Phishing Working Group, the Underground Economy Forum, the Operations Security Trust Forum (Ops Trust) and the Bay Area Council CSO Forum.

Leading the Fight on Email Spam

While preventing the placement of malicious advertisements is essential, it is only one part of a larger battle. We also fight the rest of the malware lifecycle by improving ways to validate the authenticity of email and by reducing financial incentives to spread malware. Spam is one of the most effective ways malicious actors make money, and Yahoo is leading the fight to eradicate that source of income. For example, one way spammers act is through "email spoofing". The original Internet mail standards did not require that a sender use an accurate "From:" line in an email. Spammers exploit this to send billions of messages a day that feign to be from friends, family members or business associates. These emails are much more likely to bypass spam filters, as they appear to be from trusted correspondents. Spoofed emails can also be used to trick users into giving up usernames and passwords, a technique known generally as "phishing".

Yahoo is helping the Internet industry tackle these issues. Yahoo was the original author of DomainKeys Identified Mail or DKIM, a mechanism that lets mail recipients cryptographically verify the real origin of email. Yahoo freely contributed the intellectual property behind DKIM to the world, and now the standard protects billions of emails between thousands of domains. Building upon the success of DKIM, Yahoo led a coalition of Internet companies, financial institutions and anti-spam groups in creating the Domain-based Message Authentication, Reporting and Conformance or DMARC standard. You can read about this standard and the companies behind it at DMARC.org. DMARC provides domains a way to tell the rest of the Internet what security mechanisms to expect on email they receive and what actions the sender would like to be taken on spoofed messages.

In April of this year, Yahoo became the first major email provider to publish a strict DMARC reject policy. In essence, we asked the rest of the Internet to drop messages that inaccurately claim to be from yahoo.com users. Since Yahoo made this change another major provider has enabled DMARC reject. We hope that every major email provider will follow our lead and implement this common sense protection against spoofed email. DMARC has reduced spam purported to come from yahoo.com accounts by over 90%. If used broadly, it would target spammers' financial incentives with crippling effectiveness.

Incentivizing Sharing: The Bug Bounty Program

Part of keeping our users' data secure is building trustworthy products. To this end, Yahoo operates one of the most progressive bug bounty programs on the Internet, details of which can be viewed at bugbounty.yahoo.com. Our bug bounty program encourages security researchers to report possible flaws in our systems to us via a secure web portal. In this portal we engage researchers and discuss their findings. If their bug turns out to be real, we swiftly fix it and reward the reporter with up to $15,000. In an age where security bugs are often auctioned off and then used maliciously, we believe it is critical that we and other companies create an ecosystem where both burgeoning and established security experts are rewarded for reporting, and not exploiting, vulnerabilities.

Encryption Across Yahoo

Yahoo invests heavily to ensure the security of our users and their data across all of our products. In January, we made encrypted browsing the default for Yahoo Mail. And as of March of this year, domestic and international traffic moving between Yahoo's data centers has been fully encrypted. Our ongoing goal is to enable a secure encrypted experience for **all of our users**, no matter what device they use or from which country they access Yahoo.

Conclusion

I want to restate that security online is not, and will never be, an end state. It's a constantly evolving, global challenge that our industry is tackling head on. Threats that stem from the ad pipeline, or elsewhere, are not unique to any one online company or ad network. And while bad actors pose real threats, we are strongly dedicated to staying ahead of them.

Yahoo fights for user security on multiple fronts. We partner with other companies to detect and prevent the spread of malware via advertising and pioneered the SafeFrame standard to assure user privacy in ad serving. We have led the industry in combating spam in phishing with DKIM and DMARC. We continuously improve our product security with the help of the wider research and security communities. Finally, we are the largest media publisher to enable encryption for our users across the world.

Yahoo will continue to innovate in product security. We will continue to integrate secure development practices into our software lifecycle. We will continue to view user trust and security as top priorities.

Thank you for the opportunity to testify.