October 4, 2019

What's trending on NP Privacy Partner

The difference between adverts and badverts, Facebook throws the book at thousands of app developers and more. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

Adverts or badverts: The difference, though important, may be difficult to discern

A "badvert" is a false advertisement that has been coded to redirect the user to malicious content. Known as maladvertising in the infosecurity community, badverts generate revenue for the attacker by redirecting the user to a page that delivers genuine advertisements that the coders behind the original, legitimate advertisement did not otherwise intend the user to see. It is also quite common for the page to which the user is redirected to contain malicious software (also known as malware), which is a term used to generally refer to computer viruses or software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from the victim's hard drive.

One particularly prolific badvertising attacker is eGobbler, which has undertaken several wildly successful badvertising campaigns. The first truly newsworthy badvertising campaign by eGobbler resulted in roughly 500 million legitimate advertisements being compromised on the iPhone in only ten days in April 2019. The attacker, or more likely attackers, found a vulnerability in the Google Chrome application for iOS that allowed them to bypass pop-up blockers and redirect unsuspecting users to the badvert sites. Security researchers later concluded that eGobbler had been behind a campaign that resulted in the corruption of over 1.1 billion advertisements. Security researchers believe that eGobbler may be an organized criminal venture, as the attacker has been able to locate software vulnerabilities specific only to certain applications on certain devices and quickly exploit those vulnerabilities with expert efficiency. Researchers are attempting to run test environments on various devices to spot eGobbler campaigns in the early stages. This is an increasingly difficult task as the attackers have begun exploiting software loopholes that render "sandboxing"[1] measures useless as a defense against badvert campaigns.

How can you protect yourself?

Security research teams constantly monitor applications and devices for potential maladvertising threats. Once discovered, these teams report the vulnerabilities to in-house security teams at companies such as Google and Apple. The Google and Apple teams then develop protections to the vulnerabilities and release those protections in patches.[2] Therefore, you should ensure that your

operating systems and browsers are completely up to date and capturing the latest patches released by the development teams. For example, the eGobbler loophole discussed above was corrected in the iOS 13 release on September 19. – *Wesley Gangi*

[1] Sandboxing refers to a software management strategy that detects potentially malicious code and executes that code behind the scenes without causing harm to the user's device or network.

[2] A patch is an update to computer software that is designed to fix specific issues with that software.

Your business may be liable for years-old website images

A recent case before the United States Court of Federal Claims provides a good reminder to keep track of images on your website and all webpages, because copyright infringement claims may be lurking. We address this issue in detail in an Alert available here. – *Troy K. Lieberman*

Social Media

Facebook throws the book at thousands of app developers for failing to comply with its privacy policy

Facebook has suspended tens of thousands of applications ("apps") as a result of its ongoing investigation, which began in March 2018 following the Cambridge Analytica controversy.

The now obsolete Cambridge Analytica was a political consulting firm that made a Facebook app through which they were able to collect data from over 87 million Facebook users. Although Facebook had a policy in place that prohibited the sale of its user data, Cambridge Analytica sold it anyway.

After its initial investigation, Facebook flagged about 400 apps that presented possible privacy issues. Fast forward a year and a half later, Facebook has now suspended tens of thousands of apps. Two such examples of the apps suspended include myPersonality and any apps associated with South Korean analytics company, Rankwave. In a company blog post, Facebook Vice President of product partnerships, Ime Archibong, stated the app developers for Rankwave refused Facebook's request to participate in an audit while the app myPersonality was found to share information with researchers and companies with only limited protections in place.

Archibong expressed, however, that the recent suspension "wasn't necessarily an indication that these apps were posing a threat to people."

"In a few cases, we have banned apps completely. That can happen for any number of reasons including inappropriately sharing data obtained from us, making data publicly available without protecting people's identity[,] or something else that was in clear violation of our policies," Archibong wrote.

The suspension of these apps likely follows the result of Facebook's settlement with the Federal Trade Commission ("FTC") earlier this year. In a separate case, Facebook was fined a record-breaking $5 billion for mishandling user privacy. Part of its settlement with the FTC requires that a privacy committee be independently created and also requires Facebook to exercise greater oversight over

third-party apps. This includes "terminating app developers that fail to certify they're in compliance with Facebook's platform policies or fail to justify their need for specific user data," according to the FTC. *–Jenny L. Holmes*

Special thanks to Martha Medina for her contributions to this post.

TCPA

The fight against robocalls

In recent years, telemarketers have used technology to pester consumers with prerecorded calls that are unwanted, frequently deceptive, and total in the hundreds of millions, nationally. If you answer the phone, and hear a recorded message instead of a live person, it is a robocall. Many of these are probably scams. Oftentimes, these robocalls are run by scammers using autodialed, prerecorded messages to target unsuspecting consumers to steal money, personal information, or both.

To get consumers to answer these robocalls, scammers often fake the name and number that shows up on your Caller ID. This practice is called spoofing. Common methods of spoofing include using local phone numbers, known as neighbor spoofing, or numbers that resemble those of government agencies and legitimate businesses to fool consumers into thinking that a call is legitimate.

In 2018, in the United States alone, there were 47.8 billion robocalls, an increase of 56.8% over 2017. The U.S. Federal Communications Commission (FCC) receives 200,000 complaints each year reporting robocalls—the largest consumer complaint that the agency deals with regularly. As such, the FCC has made combatting unlawful robocalls and Caller ID spoofing its top consumer protection priority. To help resolve these issues, the FCC recently introduced new rules regarding Caller ID authentication. Additionally, service providers are implementing new technology that will prevent Caller ID spoofing by authenticating Caller ID from the point a call originates and passing along the validation to the Caller ID displayed on a consumer's phone.

These technology standards are known as the SHAKEN/STIR Caller ID Authentication Framework. The FCC is rapidly attempting to qualify these capabilities. Chairman Ajit Pai recently hosted a summit focused on the industry's implementation of the technology. The FCC has also issued enforcement actions totaling over $240 million against three telemarketers for apparent Caller ID spoofing. It is also working with industry groups that share information among carriers and providers to help trace the traffic of illegal calls to the originating provider.

Consumers can take self-help measures to lessen the number of robocalls they receive, such as:

Ignoring calls from unknown numbers and letting them go to voicemail.

- If you answer a call and the caller claims to be from a legitimate company or organization, hang up and call back using a valid number found on their website.
- If you answer and the caller asks you to press a button to stop receiving calls, just hang up.
- Be aware that Caller ID showing a local number no longer means that it is a local caller.
- File a complaint with the FCC Consumer Complaint Center.
- Register your telephone numbers in the National Do Not Call Registry. – *Justin Smith*

For more information, please contact:

- Wesley Gangi at **wgangi@nixonpeabody.com** or 312-977-4478
- Troy K. Lieberman at **tlieberman@nixonpeabody.com** or 617-345-1281
- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
- Justin Smith at **jssmith@nixonpeabody.com** or 401-454-1027

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team