SUMMER 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss relevant case law on smartphones, evidentiary value in cases and the increasing security threat from mobile malware.

Mobile Malware: Cybercriminals Increasingly Sophisticated Attacks

Of thriller writers Michael Crichton, James Rollins, or Stephen King – who wrote the following line:

"Considering the aforementioned modular architecture and privileged access to the device, the malware can create literally anything."

Sorry, trick question. The above quote isn't pulled from fiction. Unfortunately, that frightening line was authored by Kaspersky Labs researchers who evaluated a new strain of mobile malware called the Triada Trojan (http://securityaffairs.co/wordpress/45187/malware/triada-trojan-android-trojan.html). The implications of the phrase "create literally anything" are chilling, and therefore, reviewing mobile malware is a wise response. Following our discussion, we'll offer some suggestions to keep your mobile devices safer.

Platform Preference of Cybercriminals

The platform of choice is slightly different for each cyber threat actor, including nation states, competitors, organized criminals, terrorists, hacktivists and insiders. But as you read this article, which is drafted to highlight the malware antics of cybercriminals, imagine the implications of each cyber threat actor harnessing the "creative" powers of mobile malware. Globally, the Android platform dominates the mobile device market. Some estimates place Android as holding over 85% of the worldwide mobile device platform market, up to 2 billion devices on approximately 500 carriers. Cybercriminals are practical opportunists with an eye toward making money. They understand economies of scale; they know that the billions of Android devices are replete with opportunity.

In addition, the architecture of the Android platform, designed to allow users to download applications from multiple app stores, increases the chances that malware will slip through

Android's security protocols. With the exception of jail-broken iPhones, Apple requires all apps to be downloaded from their app store – a single point source which Apple can screen and control more easily. Notably, both Apple and Google's Google Play Store check apps for malware prior to public release.

This isn't to say that iOS-based mobile devices cannot be infected with malware. iOS is susceptible, especially as cybercriminals increase their sophistication and stealthiness. This is even truer for jail-broken iOS devices, wherein privilege escalations are achieved by removing software restrictions – basically taking the locks off, including the security controls. However, given the prevalence of Android-based mobile malware targeting, our focus will be on those devices, and the malware currently considered to be the most advanced, the Triada Trojan stable of viruses.

Everything Starts with a Zygote

In Android terms, the Zygote is the base process from which all other applications are launched. Control the Zygote and you control the device. The Triada Trojan is a strain of rooting virus that modifies the Zygote so that the Trojan will be installed in each new app installed on the device, creating superuser privileges for itself. There are various trojan viruses under the Triada name, all of them with various capabilities. For reading ease, we're going to refer to Triada Trojan viruses in the singular, as Triada. All of the following functions are confirmed as part of the Triada group, but depending on the virus variant some may not occur.

Triada doesn't simply patch the Zygote to install the Trojan on new apps for the sake of replicating itself. Triada is capable of modifying application functions and replacing them, including URL substitutions with browsers, redirecting traffic. This is true for all Triada viruses.

Triada's first mission is to collect data and send it to a Command and Control Server. The data collected includes device identification, operating system version, a list of applications installed, mobile country code, and mobile carrier identification. With this information sent, the malware begins its work, often by waiting ten minutes after installation so that mobile device users won't notice what happens next.

Continuing to work in stealth mode, Triada shuts off various notifications and sounds. That's often the first change in device functions that users notice. The reason Triada disables sounds is that the next phase of its attack requires Triada to send and receive SMS messages. Triada will receive a new SMS message from the Command and Control Server, including a new SMS destination address. In the event that Triada can't find a network connection, it's designed to seek out SMS addresses among encrypted data in local configuration files.

Once the SMS messaging function is altered, Triada takes control of the SMS functions of other applications, primarily targeting apps with an in-app purchase function. The goal here is to reroute the money from any in-app purchases to the Triada developer. Triada may also prevent the purchaser from receiving whatever it was they intended to buy, thus stealing from the mobile device user. Gaming apps are popular targets of Triada developers because in-app purchases are easy and inexpensive. As of this point, rerouting the SMS transactions are the only known way by which Triada developers are collecting money, however, with seemingly unlimited functionality, it may not be long until other methods are discovered.

An exceptionally malevolent aspect of Triada is that it resides almost exclusively in RAM, making detection difficult. There is no ransomware demand, no wiping process announcing its presence. The infection occurs during the installation of an app, and then continues replicating with each

new installation.

A Growing Population

In 2016, Kaspersky Labs identified staggering numbers of malicious mobile malware installations topping 8.5 million. Over 100,000 were mobile banking malware installations and over a quarter million were ransomware. During October and November 2016 alone, more than 50 applications on Google Play's service were identified as carrying two strains of the Ztorg Android rooting virus accounting for over 100,000 installations. One of the most popular apps that hid the Ztorg virus was designed as a Pokemon GO user guide that was downloaded more than half a million times over the course of 2016.

Other viruses that popped up in 2016 included TrojanSpy, which sought user names and passwords for Instagram accounts; TrojanPSW, which collected user data from social media networking sites; and, several ransomware viruses which rendered devices inoperable until the ransom was paid.

SpyDealer is a recently identified rooting virus with a penchant for stealing data from more than 40 apps including Facebook, Skype, Android's Native Browser, and Firefox's Browser. Perhaps the most concerning functions of SpyDealer may be its ability to answer incoming phone calls from a specific number, spying on the device user by recording phone calls, audio, and video, taking photos and screenshots, and monitoring the device's location via GPS. Fortunately, Google Play Protect has protections against SpyDealer available.

Last Year's Vaccine Versus This Year's Flu

Much like the yearly influenza virus, mobile malware viruses evolve into different and more virulent strains. The Triada Trojan isn't the first rooting virus strain to infect mobile devices – it's just the most advanced to date. Again, like the dreaded flu and the researchers who create vaccines based on current strains, mobile device security experts do the same – they create malware protection by responding to what they find. As recently as early July 2017, Google Play announced that another set of infected apps was removed from distribution through their service.

In light of the threat, what can mobile device users do to protect themselves from malware installations?

First, keep operating systems updated. Perhaps not surprisingly, many infected mobile devices are running on back-leveled operating systems. Patches, bug fixes, and security updates are released in a continuing cycle and neglecting the operating system invites vulnerability. Keeping your mobile device operating system current is the first line defense against mobile malware.

Second, consider installing a trusted antivirus software program recommended by your IT department. Be cautious and make sure that the protection you're adding is fully vetted and comes from a reliable, well-rated source. The app eVestigator was pulled from the Google Play store after the app, which advertised that it would seek out malware, was reported to be vulnerable to remote code execution.

Third, resist the temptation to jail-break or root mobile devices. The same privilege escalation that allows the user to change permissions also creates a crack through which sophisticated hackers can slip. Users tempted to root their Android phones may also find that they have inadvertently voided the manufacturers' warranties. Apple warns that any jail-broken iPhone that cannot be restored to factory settings will be considered warranty voided.

Fourth, use an official app store. Apple's App Store and Google Play routinely detect and respond to malware threats. Sideloading, downloading apps via websites and other app stores, is an easy way for malware to infect a mobile device under the guise of a legitimate app. When you find an app that peaks your interests, check to see if the app is available on your mobile device's trusted app store. If it's not offered there, proceed with extreme caution, if at all.

Fifth, know the signs of malware infection. Watch for changes in device settings that appear randomly. As stated above, one of the Triada's first steps is to turn off SMS notifications and sounds. Be aware of your mobile device's performance – slow processing, rapid battery consumption, and freezing can be symptoms of a malware infection. URLs that mysteriously redirect may be a sign of browser hijacking malware.

Finally, if you can't curb the impulse to make an in-app purchase, watch to make sure the transaction is completed. A rerouted transaction-SMS, especially one that interrupts the delivery of your purchase, can be evidence that malware is operating on your device. Malware that specifically targets banking transactions gained popularity in 2016 and continues to evolve in 2017. Most users don't verify the legitimacy of SMS addressed used by installed apps, and cybercriminals rely on that to reroute funds.

Mobile malware can be difficult to detect because developers are using legitimate apps to cloak the dissemination of viruses. With increasing sophistication, mobile malware is operating more frequently in processes that are invisible to users, even controlling what users see and hear. Like a thrilling novel where a mutant virus takes control of its host, mobile malware developers are creating scarier threats with each new strain, and cybersecurity heroes are racing the clock to stop them. Ultimately, as scary as malware can be, it's simply one type of mobile security threat that must be managed in concert with a more comprehensive security plan, which should be designed, implemented and enforced with the use of experts and include systems beyond mobile.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

Black Hat USA
Las Vegas, NV: July 22-27, 2017

ILTACON 2017 Annual Educational Conference
Las Vegas, NV: August 13-17, 2017

PFIC 2017 Cyber Symposium
Pittsburgh, PA: August 18, 2017

Today's General Counsel, "The Exchange" eDiscovery
Houston, TX: September 13-14, 2017

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) 2017 Midyear Meeting
San Diego, CA: September 18-19, 2017

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: