REPORT

McAfee
Together is power.

Trojans, Ghosts, and More Mean Bumps Ahead for Mobile and Connected Things

What lies ahead for 2017

Trojans, Ghosts, and More Mean Bumps Ahead for Mobile and Connected Things

The meaning of mobile threats has changed significantly over the past year and is continuing to evolve and expand along with the nature of mobile devices, as adversaries experiment with different attack vectors and monetization efforts. Mobile means not just smartphones, but all manner of devices from the Internet of Things (IoT), many of which interact with or are controlled by smartphone apps.

Mobile means not just smartphones, but all manner of devices from the Internet of Things (IoT), many of which interact with or are controlled by smartphone apps.

Threat means ransomware, banking Trojans, bots, spyware, apps that trick the user into sending premium messages, and a variety of other malware looking to steal private information or money from the user. This is a global issue, spanning most countries that have a significant smartphone user base. Different countries have different threat profiles, depending on the nature of mobile phone usage in the country (see map on page 3). App store curators are increasing their efforts to identify and block malware from getting onto user devices, but with millions of apps available, some malicious ones are still making it through the screening process.

With the exception of root exploits, most mobile threats are steadily growing. In this report, we explore three of the most significant threats to the privacy and security of mobile devices and their users:

- The extension of ransomware into mobile and connected devices
- The invisible threat of dead apps that have been removed from an app store for privacy or security violations only after being downloaded
- The rich and vulnerable targets that are being exploited in the universe of IoT devices

Mobile Threat Landscape Activity Map

Source: McAfee Mobile Threat Research, 2016

Ransomware—Not Just a PC Problem Anymore

The rise of ransomware was unprecedented in 2016 and is predicted to continue its domination in 2017 and beyond. Not only are PC's experiencing ransomware at an unprecedented rate, but other connected devices are seeing vulnerabilities being identified that make them vulnerable to this strain of malware. Users should not forget that ransomware has no boundaries and devices including mobile phones and IoT devices such as smart-home devices, ICS/SCADA equipment, automobiles, and medical equipment to name a few will continue to see their share of vulnerabilities being displayed in very public settings demonstrating how ransomware can infect such devices.

A recent example of ransomware targeting mobile devices was "Charger" that was found in January 2017 and bundled with EnergyRescue.[1] The malicious snooping app was briefly available on Google Play and targeted Android devices before being pulled. "Charger" demanded 0.2 Bitcoins and threatened to sell the victim's personal information on the black market if the ransom was not paid.

Ransomware holding Industrial Control System or SCADA equipment hostage has not made a breakthrough in the industry yet, but a pair of researchers from Georgia Institute of Technology at this year's RSA Conference in San Francisco demonstrated the attack scenario.[2] They showed it was possible to take control of a simulated water treatment plant and cause a programmable logic controller (PLC) to display false information, shut off valves, and increase chlorine levels unless a ransom was paid.

Researchers in the past year have also shown that automobiles are not immune to being controlled by someone other than the driver. Researchers from McAfee's Advanced Threat Research Group at last year's BlackHat security conference demonstrated a ransomware attack on an automobile infotainment system.[3] The simulated

Although PC's will continue to see the bulk of ransomware attacks in 2017, other connected devices are starting to gain momentum.

attack showed that the automobile's computer system could be taken over and display a ransom note demanding payment to release its grip on the car.

Connected medical devices are also susceptible to ransomware attacks and this year could be the year we see medical devices such as insulin pumps, heart monitors, and pacemakers along with other hospital equipment become targets by threat actors.[4] Many of these devices have weak or non-existent security and could be a financial sweetspot for ransomware developers.

Although PC's will continue to see the bulk of ransomware attacks in 2017, other connected devices are starting to gain momentum. Ransomware will continue to evolve as the threat actors exploit new ways to make money especially as more devices come online.

Ghosts in the Phone

Dead apps need recall notices like other defective products

According to **Statista**, there are more than 2 million apps in each of the major app stores, and store curators **proudly talk** about the substantial precautions they are taking to review submitted apps for malware or privacy violations. However, malicious apps sometimes find a way through the initial screening process and are caught only after they have been downloaded onto mobile devices by unknowing consumers. Once identified as malicious, McAfee® Mobile Threat Research has found that the apps are removed silently from the store without any external communications. Many other apps are removed because they have been abandoned by the developer, also without notice.

The security concern is the lack of transparency from app store companies about which apps have been removed, and why. Even though these apps are no longer available, they are not deleted or deactivated on devices. If they were removed due to policy violations, such as copyright or piracy, the affected content owners may have been notified, or at a minimum the damage has been stopped from spreading further. However, if they were removed due to previously undetected malware or privacy issues, users who downloaded these apps are still at risk.

In the past year, McAfee Mobile Threat Research has identified more than 4,000 apps that were removed from Google Play without notification to users. Currently, there is no consistent or centralized reporting available. Telemetry data collected by McAfee Mobile Threat Research show that more than 500,000 devices still have these apps installed and are active. These users, and the organizations they work for, are still exposed to any vulnerabilities, privacy risks, or malware contained in these dead apps.

One recent example is a password stealing App, distributed on Google Play as a Trojanized version of Instagram. The app is marketed as a set of tools and utilities that will help users gain Instagram followers and analyze usage data. The malware leads the user to a phishing website with a simple design that makes it difficult to distinguish between the legitimate and the fake, easily capturing the user's credentials.

Malicious apps sometimes find a way through the initial screening process and are caught only after they have been downloaded onto mobile devices by unknowing consumers.

In the past year, McAfee Mobile Threat Research has identified more than 4,000 apps that were removed from Google Play without notification to users.

Source: McAfee Mobile Threat Research, 2016.

Another example is a Trojanized photo app called I Love Filter, downloaded more than 1 million times, according to Google Play statistics (see figure at left). At first sight it looks like another free app to add filters to user photos. However, as soon as it is opened the app requests the user to "confirm upgrade to VIP." The Trojan triggers a subscription to SMS services by sending a text message to premium-rate numbers. The subscription continuously charges the user until a request to cancel text messages is submitted. In addition to this fraudulent behaviour, injected code in the Trojanized app can download other apps to the compromised device that carry out additional attacks.

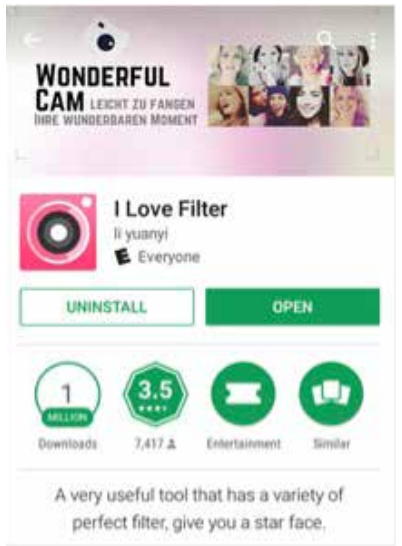
The app is rated 3.5 out of 5.0 on Google Play, showing that the rating system is not enough to go on when it comes to evaluating apps and threats.

Many commercial products are subject to consumer protection regulations that require customers to be notified, and sometimes products to be recalled, when safety issues are discovered. For example, defects in automobile parts or manufacturing are commonly recalled or safety notices issued. There was the recent recall of the Samsung Galaxy Note 7 due to risk of fire or explosion.

Dead and malicious apps are not yet in the same personal risk category as contaminated food or exploding mobile phones. However, they do pose a security risk, and the continued growth and integration of smart phones and IoT devices, in areas such as healthcare, transportation, and energy, suggests that it is only a matter of time before a security risk becomes a threat to physical safety.

App stores do a good job at screening out bad apps, but they are not able to detect and prevent 100% of the malicious code from making it onto phones. With 4,000 apps being removed in the past year, it's time for app store curators to notify those users impacted to help keep them secure and protect their privacy. Pay close attention to the apps that you are downloading and research the developer and reviews about any app before installing it.

Security software is available for phones, similar to that for PCs, which adds additional protection beyond that provided by the operating system and the app store screening. Look for a security tool that can identify apps which are no longer on the store and, even better, can provide some information on why they were removed.



Source: *McAfee Mobile Threat Research, 2016*

The continued growth and integration of smart phones and IoT devices, in areas such as healthcare, transportation, and energy, suggests that it is only a matter of time before a security risk becomes a threat to physical safety.

Finally, voice your opinion to app store vendors about public disclosure of apps that are removed from the store, and the reasons behind the removal. Product recall and safety notices are a common feature of consumer products and should be extended to mobile apps.

Little Things Can Make Big Things Happen

Mobile malware developers are increasingly targeting IoT devices

There are more than 2 billion smartphones around the globe, making them a rich target for malware authors and other cyber attackers. However, a richer target is emerging. McAfee estimates that there are already more than 15 billion IoT devices in operation,[5] and this number is growing rapidly. Not only are there more of these devices, but the manufacturers have also prioritized their operations for convenience and time-to-market, often leaving the devices more vulnerable to compromise than mobile phones.

IoT attacks took center stage on October 21, 2016, when a botnet using compromised IoT devices, primarily webcams, flooded the Internet with up to 1.2 Terabits per second of data in the largest distributed denial of service (DDoS) attack ever recorded. Analyzing the code behind this attack, McAfee Labs found that simple brute-force password cracking was used to gain access to the devices, with each newly compromised device joining up to find others to infect, as detailed in the forthcoming **March 2017 McAfee Labs Threats Report**. Ultimately, more than 380,000 devices were infected with the Mirai virus in a very short period, according to McAfee Labs telemetry. Highly-connected countries were the most infected, with the U.S. and South Korea facing an infection rate of around 15%.

We have been watching IoT attacks for several years and over the past year have seen the infection rates grow by roughly 20% every quarter. The success of the Mirai attack has not only encouraged others, but also made the code readily available to reuse and learn from. There are now four to six major IoT cyber incidents every quarter big enough to make headlines, most of which are DDoS attacks. Dark web markets are offering IoT botnets of various sizes for rent, and the number of offerings increased 50% in the last quarter, bringing rental prices down substantially. Many smaller attacks have been documented, but these are mostly from people playing with the tools and using them against a personal target.

The major weaknesses being exploited are hardcoded or default passwords and keys used by manufacturers or firmware developers, many of which remain unchanged by consumers after installation. The username and password combinations used in the brute force attacks are disturbing in their simplicity: 12345, 54321, 11111, admin, password, and default are all represented, as are vendor names and product model numbers. We have already identified five mobile malware families that are targeting Smart TVs using these same techniques. Fixing these vulnerabilities requires updating the firmware

on the device. However, that is a time-consuming task, even if it is automatic, when the number of devices are measured in the millions. If updating the firmware is a manual process, most users are not even aware that updates are needed, let alone how to do it.

There is an enormous variety of IoT devices currently being sold, with many more on the horizon, covering almost every industry. It is apparent that most manufacturers have little to no experience in implementing effective security controls and are wandering unprepared into a very hostile environment. Based on the early success of IoT cyberattacks, it may be necessary for regulatory bodies, such as the U.S. FTC, to set minimum security standards. For example, requiring unique passwords for each device, similar to how software companies generate product activation keys, would most likely have stopped or at least slowed down the Mirai botnet infection. Secure boot functions and trusted execution environments protect the firmware and make it difficult for unauthorized sources to insert new code.

DDoS was just the start of the IoT attack cycle. We expect to see new attack vectors and objectives emerge as more malware authors realize the potential of IoT devices. Spam bots and ransomware targeting IoT devices will likely be quick evolutionary steps, as cybercriminals look for ways to monetize their efforts. Back-end services will also come under threat as hackers look for ways to jump from devices into other, more lucrative systems.

Much of the work necessary to protect IoT devices is the purview of the manufacturers and firmware developers. Consumers and businesses can protect themselves in similar ways they have already learned for computers: changing default passwords, using firewalls to block unused ports, and keeping device software up to date. Continue to pay close attention to mobile phone security, as in most cases data from the devices in your home flows through your smartphone and targeting infection to, from, or through the phone is a very real possibility.

Summary

Wearables, webcams, smart TVs, and numerous other consumer and commercial IoT devices have joined smartphones as targets for cyberattacks. Whether looking to extort ransoms, steal banking credentials, collect personal information, or use as part of a botnet, mobile threats are continuing to grow and adapt as they look for the best payoff. Direct attacks on mobile phones make up the largest share of these threats, but we expect that ratio to change over the next year, as more attackers discover the potential and easy vulnerability of many IoT devices. Smartphone developers, app store curators, device manufacturers, and security vendors will need to work closely together, transparently share threat intelligence, and rapidly address security vulnerabilities to keep this marketplace healthy.

It is apparent that most manufacturers of IoT devices have little to no experience in implementing effective security controls and are wandering unprepared into a very hostile environment.

1. https://arstechnica.com/security/2017/01/ransomware-app-hosted-in-google-play-infects-unsuspecting-android-user/
2. http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls
3. http://www.zdnet.com/article/ransomwares-next-target-your-car-and-your-home/
4. http://www.zdnet.com/article/the-state-of-medical-device-security-today-and-beyond/
5. http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com