REPORT

McAfee
Together is power.

Mobile Threat Report

The Next 10 Years

McAfee Mobile Threat Report Q1, 2018

Criminal Quest for Money Could Make 2018 the Year of Mobile Malware

Imagine the logistical difficulty of physically moving millions of dollars. In the film "Brewster's Millions," Monty Brewster, the character played by Richard Pryor, is presented with three vast mountains of cash after accepting the challenge of spending $30 million in 30 days to inherit $300 million. Today he could just use his smartphone, and if he took the challenge using cryptocurrency in late 2017, all he would have to do is spend a little over 1,500 Bitcoin.

Herein lies the opportunity, but also articulates the risk. Your phone is not just a phone. It is a rich computing environment that includes potentially your children's inheritance, your digital persona, and the keys to your home or the keys to your entire digital life—including all the connected things in your home. As a result, it's not just mobile malware that we need to be aware of. The mobile platform itself has become the perfect illustration of physical and digital convergence. With reports of armed men holding up cryptocurrency traders and exchanges, it is an important lesson that not all mobile threats are digital.

As we look into this year's edition of the *McAfee Mobile Threats Report*, there are some significant trends that demonstrate just how these platforms are being targeted. One trend is the growth in mobile malware. However, not all malware is created equally, and we detail the targeted use of mobile threats to identify political dissidents.

If you follow McAfee Labs blogs and threats feeds, you will have noticed some analysis by our Mobile Research team that identified the transition by a significant threat actor to the mobile platform. This was the first time we saw this outfit, whose objective was to impact potential defectors by targeting a religious group in South Korea. Of course, the threat does not end there. A short few weeks later, another campaign targeted dissidents in the region.

Before we give too much away, please enjoy our *Mobile Threats Report* but, more importantly, remember that the age of the mobile phone ended years ago. The devices we use to make calls today are much, much more.

– **Gary Davis**

Chief Consumer Security Evangelist

– **Raj Samani**

McAfee Fellow, Chief Scientist

The Next 10 Years

This year marks 10 years that both the Apple App Store and the Google Play store have been in business. Even though the app store concept dates to the early days of the Symbian operating system—think Nokia and Ericsson phones—the advent of the application market from Apple and Google is what most smartphone users associate with the concept of app distribution.

A decade has now passed, and both outlets have seen their fair share of security-related incidents, as they continue to struggle with post-release issues.

Malware campaigns having targeted users on the Google Play stores almost since its inception. From the very first banking Trojan on Google Play, dubbed Droid09, to the latest ad-click fraud/Bitcoin-mining latent apps that plague the store week after week today. The Google Play store is under siege. What has changed over the years is the growth in the number of infected devices, which now typically can reach into the millions as we discover new aggressive campaigns.

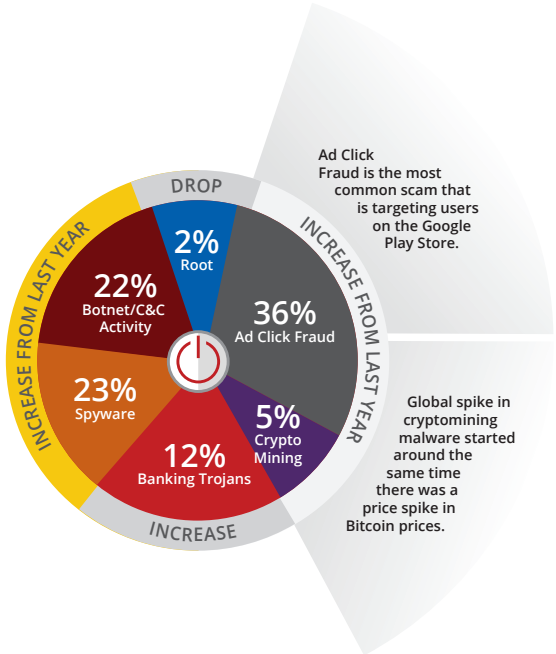

Figure 1. Chart: A breakdown of last year's campaigns vs. threats targeting Google Play in 2016. We have seen growth in several threat vector categories.

The Google Play store is under siege. What has changed over the years is the growth in the number of infected devices, which now typically can reach into the millions as we discover new aggressive campaigns.

Connect With Us

One of the most significant campaigns discovered by McAfee in late 2017 and in early in 2018 was Android Grabos. Grabos, a campaign that pushes unwanted apps on unsuspecting users is commonly known as pay-per-download scam. In total, 144 apps on Google Play were identified and taken down. An estimated that 17.5 million global smart phone devices downloaded apps from the campaign before they were taken down.

Apple is not free of threats, including the ongoing issue with "dead apps." In this practice Apple silently removes apps from the App Store after a security- or privacy-related discovery, without any public disclosure or recall attempt. This practice leaves millions of users at risk of malware incidents targeting development workflow, as well as to source code leaks that give hackers the ability to better understand how to create exploits. Another example of an issue passing through vetting is the simple act of sending a single character in the Telgu language, which can render any device running iOS 11 useless.

"One of the most significant campaigns discovered by McAfee in late 2017 and in early in 2018 was Android Grabos."

Pravat Lall
Vice President of Engineering,
Mobile & ISP Solutions, McAfee

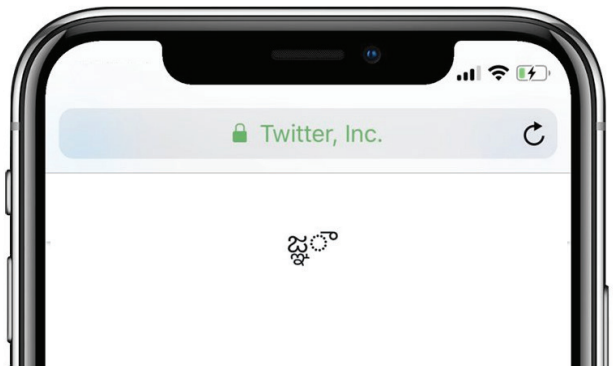

Figure 2. Sending just a single character in the Telgu language, as pictured above, can render any device running iOS 11 useless.

```
1   # Copyright (C) 2007-2014 Apple Inc. All rights reserved.
2   # Copyright (C) 2006 Apple Computer, Inc. All rights reserved.
3   #
4   # This document is the property of Apple Inc.
5   # It is considered confidential and proprietary.
6   #
7   # This document may not be reproduced or transmitted in any form,
8   # in whole or in part, without the express written permission of
9   # Apple Inc.
```

Figure 3. iOS source code leak.

Connect With Us

A Booming Industry Ripe for Fraud

Security is of paramount concern to both Google and Apple, as shown by the investment they have made to fortify the platforms from the component level to the app stores. Yet a lot more work needs to be done.

In 2017 we saw more threats campaigns targeting mobile devices on Google Play than in previous years. Thus it should come as no surprise that independent tests of the detection capabilities of Google Play Protect show that the built-in security measures failed to detect or protect against the most common malware threats campaigns. In fact, when tested in an independent test against threats discovered in the past 90 days, Google Play Protect failed to pass.

Given that mobile ad spending is a billion-dollar industry and relatively a new field, the business is a target ripe for fraud. A clear majority of malware campaigns discovered by McAfee in 2017 were ad clicker Trojans, which while appearing to provide some service, were fraudulently manipulating mobile ads in the background to generate revenue for the author of the app.

"Although security is of paramount concern to both Google and Apple—evident by the investment they have made into resources to fortify the platform all the way from the component level to the App store—a lot more work still needs to be done."

Shailaja Shankar
Vice President & General Manager
Mobile and ISP Solutions

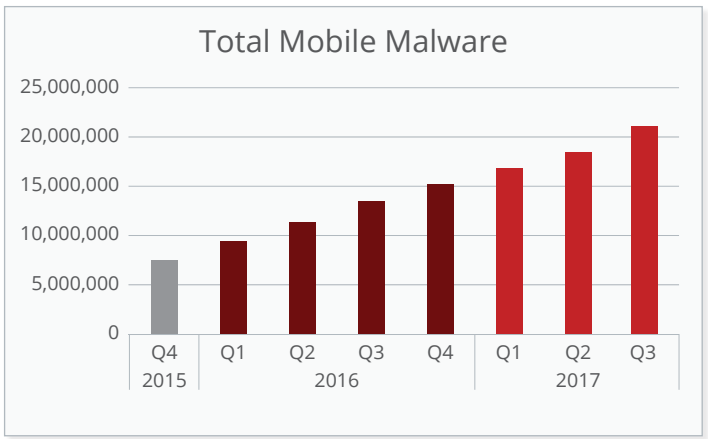

Figure 4. Total malware samples from 2015 – 2017.

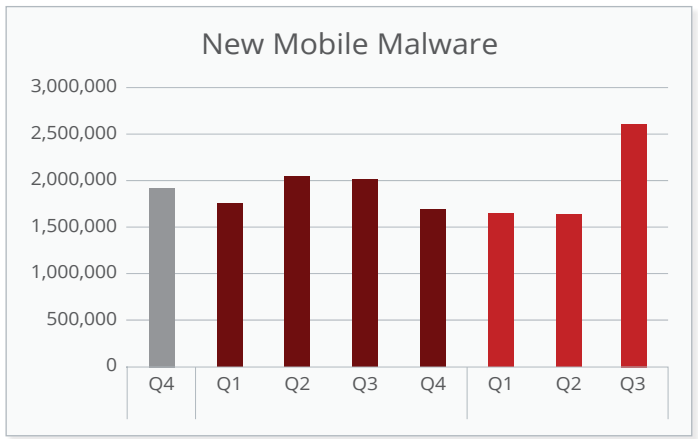

Figure 5. New malware samples from 2015 – 2017.

Connect With Us

A Billion-Dollar Industry Beyond 2020

In its infancy, mobile malware took its initial steps toward monetization using toll fraud (fraudulent long-distance calls) and premium SMS scams. Two tactics emerged.

In Asia, malware would subscribe users to small payments as low as a few yuans; the victims would not notice until months later that something was amiss. These were dubbed by the Chinese police as money suck scams. The other tactic, developed by malware authors in Eastern Europe, was the more brazen smash-and-grab strategy, in which a deceptive app would infect a device and make off with a one-time charge of, $45–$100, for example. The latter method laid the foundation for mobile ransomware targeting users in North America, which to this day is still primarily created and operated by malware authors working from Eastern Europe.

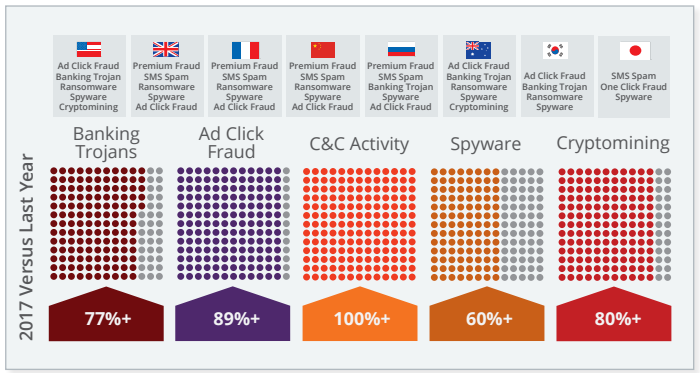

Figure 6. Rise in cybersecurity risks from 2016.

By our estimation, In 2010 the highest-paid malware campaign could potentially earn revenue between $100,000–$300,000. In the current threat landscape, a full-fledged campaign exploiting ad click fraud or pay-per-download scam (a market valued around $40 billion in 2018) or a prevalent banking Trojan could potentially bring in revenue of $1 million–$2 million. If mobile malware continues on its current trajectory, it could create revenues for malware authors touching in the billion-dollar range by 2020.

Last year marked not only an explosion in mobile malware, but also showed dramatic changes in the mobile landscape, setting up 2018 to be one of the riskiest years yet. The estimated five billion mobile subscribers worldwide in 2017 proved to be enticing bait for malware authors, who ramped up the number of attacks and their sophistication.

McAfee Labs detected over 16 million mobile malware infestations in the third quarter of 2017 alone, nearly doubling the number we saw a year earlier.

McAfee Labs detected over 16 million mobile malware infestations in the third quarter of 2017 alone, nearly doubling the number we saw a year earlier.

Connect With Us

Threats emerged from around the globe, from Afghanistan to Cuba. But Russia, China, and South Korea suffered the greatest number of infections, with a common motivation: making money.

We have seen traditional attack vectors, such as premium text messages and toll fraud replaced by botnet ad fraud, pay-per-download distribution scams, and cryptomining malware that can generate millions in revenue.

Further, we have seen a jump in cryptocurrency malware by 70% (including a 5% increase in cryptocurrency activity on Google Play) and a 60% increase in mobile banking Trojans in the last year alone.

The Android platform continues to serve as low-hanging fruit for malware authors, who eye its more than two billion users and relatively open app distribution. The number of threat families we found in the Google Play store increased by a whopping 30% in the last year, making even the official Android app store a risky proposition for users.

In just one example, we encountered pirated versions of legitimate apps that could be used to generate advertising money. The developers may also have intended to sell the developer accounts to criminal organizations so the latter could deliver malware and spyware through the platform.

In both scenarios, monetization continues to drive their actions. In other instances, we encountered malicious messaging apps that contain spyware to snoop on users, fake apps purporting to protect users against ransomware attacks, and Trojanized apps that sign up users for premium services without their consent.

We expect the targeting of mobile devices by cybercriminals to steadily increase in 2018 and beyond as these bad actors hone their exploitation and monetization skills.

"We expect the targeting of mobile devices by cybercriminals to steadily increase in 2018 and beyond as these bad actors hone their exploitation and monetization skills."

Raj Samani
McAfee Fellow, Chief Scientist

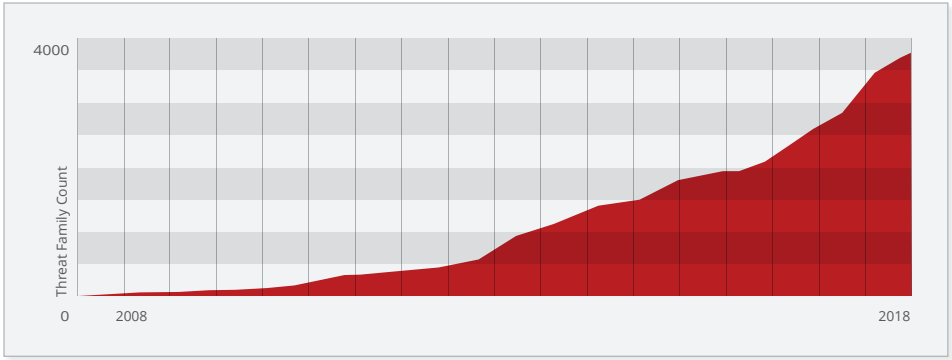

Figure 7. There are more than 4,000 mobile threat families and variants in the McAfee sample database today.

Connect With Us

Attack Trends

In another sign that mobile malware authors have set their sights firmly on monetization, they have taken the traditional PC attack vector of banking Trojans and added ransomware capabilities to create a new threat on the mobile platform. This is no doubt a response to the explosion in mobile banking and financial applications that we have seen during the last couple of years.

In 2017 we saw an increase in malicious banking Trojans, such as the Android/Marcher malware, that take advantage of the auto install vulnerabilities in the Android platform. It victimized millions of Google Play users by impersonating legitimate apps for video players, Flash players, games, and system utilities.

We have also seen mobile banking Trojans delivered as fake updates or through targeted email or SMS phishing. But the most sophisticated so far has been the Android/LokiBot malware, which takes all the functions of Android/Marcher and adds crypto ransomware capabilities, among other malicious activities.

It can encrypt files and lock devices, send phony notifications to trick users to open their online banking apps, and even allow the attacker to impersonate the victim's IP address for use in other fraudulent activities.

Android/LokiBot has targeted more than 100 financial institutions around the world. By our estimate LokiBot has generated close to $2 million in revenue from kit sales on the "dark web."

"Android/LokiBot has targeted more than 100 financial institutions around the world. By our estimate LokiBot has generated close to $2 million in revenue from kit sales on the 'dark web.'"

Sreenu Pillutla
Sr. Director, Software Engineering

Connect With Us

Banking Trojans also target both large multinationals and small regional banks using specially crafted mobile apps or phishing campaigns. Take, for instance, the Android/MoqHao malware aimed at major Korean banks. This threat spreads via SMS using a clever social engineering lure—asking the recipients to verify a picture of themselves.

Once the recipient clicks on the malicious link, it installs a fake banking app and then scans for and deletes legitimate banking apps on the user's phone. But traditional banks are not the only targets.

With the growing interest in cryptocurrencies and escalating prices for Bitcoins, cybercriminals have attempted virtual bank robberies by distributing fake mobile wallets, and have stolen Bitcoins outright by targeting workers in the cryptocurrency industry. In the last year, we have seen a massive 80% increase in malware related to Bitcoin mining.

In an even more brazen example of the cryptocurrency craze, a group of armed robbers in Ottawa, Canada, in January targeted a financial institution related to Bitcoin. But this kind of real-world crime against digital assets is nothing compared with escalating online threats.

Since 2012 the risk of banking Trojans has only grown. Given the crypto craze and malware authors' ability to disguise the true nature of their malware in legitimate applications, we do not expect this threat to diminish soon.

In the last year, we have seen a massive 80% increase in malware related to Bitcoin-mining.

Targeted Attacks

A modern-day plague of (cyber) RATs

One of the most significant concerns we have come across in the last 12 months is the evolution of targeted attacks moving to mobile devices. It took 20 years to reach two million malware samples on the PC. It took just five years to do the same on mobile.

Connect With Us

The McAfee Mobile Research team discovered an Android malware sample that contains a backdoor file which appears to be the first attempt of the Lazarus cybercrime group to move into the mobile space. The Lazarus group, which is believed to be connected to the North Korean government, had previously grabbed headlines with its WannaCry ransomware attack, which crippled the UK's National Health Service and thousands of other organizations in the first half of last year.

The Android malware poses as a legitimate Korean-language Bible-reading app on Google Play, and targets South Korean users. Once the user's smartphone is infected, it turns the device into a bot. Although we cannot be sure, we believe that the attack was meant to target a group that supports religious organizations in North Korea that have been seen as sympathetic to South Korea.

From People Power to State Power

While the proliferation of mobile devices has brought radical changes to how people communicate, organize, and even protest—as they did during the Arab Spring—we are now starting to see this empowerment shift in the other direction. State-sponsored actors realize how potentially easy and efficient it can be to use the mobile platform to monitor opponents or silence dissent.

For example, McAfee researchers recently discovered that North Korean dissidents and journalists using the popular South Korean chat app KakaoTalk were targeted in a malware campaign. Unknown parties sent shortened links to malware through the chat app or social networks to implant spyware on the victim's device. This was a clever tactic, given that many users have learned the dangers of clicking on links in emails from unknown sources. However, they are not accustomed to using the same caution with their chat friends.

Another discovery from the McAfee Mobile Research team was Android/Grapher, which targeted protesters in Iran. Anti-government demonstrations in Iran made headlines in January. The first protest took place in Mashhad, Iran's second-largest city, and initially focused on economic concerns but expanded in scope to include political aspects as it spread to more cities. Regardless of the motivations behind the protest, one sure thing is the vital role that technology played in organizing and communicating. The critical mass achieved by the protest would not have been possible without technology such as smartphones, social networks, and messaging apps.

With an estimated 40 million users based in Iran, almost half the population of the country, Telegram is a popular messaging service that served as a strategic communication network for the protesters. The Iranian government soon blocked the service, citing its abuse in promoting violence during the protest and leading to riots. "Cyberspace was kindling the fire of the battle" said Ayatollah Ahmad Khatami, during a Friday prayer sermon.

As protesters sought to keep the communication channels alive, they turned to using virtual private networks (VPNs) or hacked versions of messaging services that claimed to subvert the ban.

A McAfee Mobile Research analyst discovered that one of the apps in circulation under the guise of a modified version of a functional Telegraph app was, in fact, a remote access Trojan that was sending information from infected devices to an external site.

Android/Grapher sports dozens of features, including interception of SMS, contacts, call logs, and browser histories along with credential snatching. Although we cannot be sure who were the people behind this campaign, the aim was clearly to gather intelligence around anti-government protesters.

With so many people connected continuously via their mobile devices, we expect some nation-states to actively keep tabs on their citizens.

Figure 8. This picture of an Iranian student protester went viral on social media during the protest.

"Cyberspace was kindling the fire of the battle."

Ayatollah Ahmad Khatami

Connect With Us

The Insecurity of Things

In the era of the Internet of Things (IoT) consumers embrace smart home technologies that make their lives more convenient, or just cooler. Sales of products such as connected speakers that act as digital assistants, smart thermostats, and interactive toys among several categories of devices have skyrocketed.

According to research firm Gartner, 8.4 billion connected "things" were in use last year, up 31% from 2016. By 2050 Gartner expects 50 billion connected devices will populate consumers homes—roughly five times greater than the number of people predicted to inhabit the earth at that time.

But although all these devices certainly bring convenience and ease, they also significantly expand the attack surface. Most of those devices have focused on time to market and convenience with little to no thought about security.

Consumers have yet to realize the full potential of the risks devices pose and typically do very little to secure them in their homes. While reports of hijacked IP cameras have brought the awareness of potential spying on users, we are still discovering what it means to have so many possible points of attack in our homes.

Just look at what an enticing target IoT devices were to the Mirai botnet authors, who used millions of them to create a botnet army. The botnet, using primarily compromised webcams, flooded popular websites with up to 1.2 terabits of data per second in the largest distributed denial of service attack ever recorded. This was an obvious power play against Internet giants, but the massive botnet threat could be targeted against any organization or country.

"IoT attacks took center stage late last year, 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."

Gary Davis
Chief Consumer Security Evangelist

Connect With Us

Cybercriminals are already working out how they can manipulate IoT for their purposes. Last fall researchers hacked a home assistance robot to perform a stabbing motion, just as a proof of concept on how a digital toy could be used to do physical harm. Of course, cybercriminals are usually motivated by money, so a more likely scenario is that an IoT device could be used to steal credit card information, mine cryptocurrency, hop over to other high-value devices such as PCs or mobile devices, or even alert thieves when the owner is away from home.

The Reaper malware, which created as many as two million infections in the second half of 2017, represented a step up from the IoT attacks we saw just a year ago that took advantage of inadequate security on many connected home devices.

Reaper differed from Mirai in that instead of using brute-force techniques with a series of default usernames and passwords, it looked for devices with known vulnerabilities to exploit. It implemented a set of hacking tools that showed greater sophistication. This evolution represents a growing threat to consumers who continue to bring devices into their homes at an unprecedented rate.

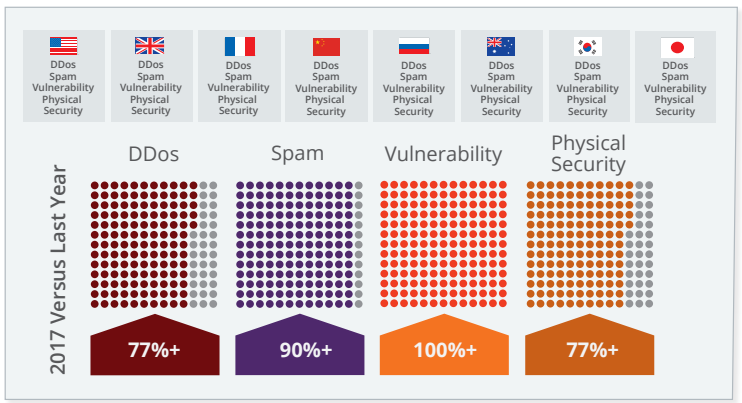

Figure 9. Rise in cybersecurity risks from 2016.

Connect With Us

Network Security Risks

While consumers welcome more technology into their homes and personal lives, many at the same time realize how risky public networks can be, especially in the age of big data.

At McAfee, we have seen network spoofing increase dramatically during the last 18 months, with hackers setting up their networks in public places, waiting for users to connect, and watching the traffic for sensitive information such as banking logins and credit card numbers. Or, cybercriminals simply spy on the traffic flowing over unsecured networks in locations such as airports and hotels.

These tactics are especially dangerous because users tend to lower their security guard while on vacation. According to our 2017 "Unplugging Travel Survey" less than half (49%) of travelers take the time to ensure their connection is safe, even though 58% know how to check if their Wi-Fi is secured.

When you combine these concerning trends with news about the recently discovered KRACK vulnerability in the widely used WPA2 encryption protocol, network safety has become even more complicated. KRACK potentially allows an attacker to see the traffic sent between a device and the router, even if it is encrypted, unless it uses the HTTP protocol to scramble data. Around 41% of Android devices were vulnerable, even if they connected to a secure network. This flaw underscores why it is important to use mobile security in addition to a VPN.

As news continues to make the headlines about the risk of public Wi-Fi and newly discovered vulnerabilities in the connections we rely on, consumers will look to protect their privacy using VPNs.

Summary

Could 2018 be the year of mobile malware?

As global cybercrime is estimated to cost $600 billion in 2018, the preferred choice of access for a majority of the world's population is a mobile device. Mobile malware authors are aiming for, and generating revenues in the millions of dollars with their malicious campaigns. Considering that mobile malware has been around for only 15 years—from the first mobile botnet discovered in 2009 to the targeted attacks from the Lazarus group on smartphones—the pace at which malware has evolved on mobile devices is alarming.

With banking Trojans generating revenues in the millions, as well as ad click fraud, and cryptomining latent apps flooding online stores, we expect to see considerably more exploitation in 2018. Targeted attacks in Iran and South Korea are just the beginning. These elements and the discovery of the Lazarus group bringing the sophistication of persistent PC-based tactics to mobile devices could turn 2018 into the year of mobile malware.

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.

McAfee™
Together is power.

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