REPORT

McAfee
Together is power.

McAfee Mobile Threat Report

Mobile Malware Continues to Increase in Complexity and Scope

McAfee Mobile Threat Report Q1, 2019

Mobile Malware Continues to Increase in Complexity and Scope

The mobile platform is an increasing target for nation states to observe key individuals. Threat actors against mobile platforms are broader groups than those simply looking to boost ad revenues.

As we analyze the key findings from 2018 our attention turns to the wider ecosystem. The **mobile ecosystem is a feature rich environment**. Apps offer the ability to control everything from home heating and lighting to real-time remote SCADA and process control capabilities for plant operators. Today's statistics are reporting the average person having between 60-90 apps[1] installed on their phone.

What does this mean for the mobile threat landscape?

In 2018 we saw a rapid growth in threats against mobile devices and other connected things, in particular during the second half of 2018. The **number one threat category was hidden apps** which accounted for almost one third of all mobile attacks.

Actions to remove hidden apps from the stores have been timely and effective, but adversaries are innovating and adapting threats just as quickly. In our first detailed article we look at the TimpDoor malware family bypass the Google Play store by contacting potential victims via SMS. This approach **avoids the threat of being removed from the store**, and has proven incredibly effective, impacting more victims than the older Android malware families of Guerrilla and Rootnik combined.

Authors

This report was researched and written by:

- **Raj Samani**
- **Gary Davis**
- **Contributions from the McAfee Advanced Threat Research and Mobile Malware Research team**

Connect With Us

We have to consider the richness of data available to threat actors from a compromised phone. Last year we discussed the rise of nation states targeting individuals via the mobile platform and the past year has seen a continuation of this approach. In 2018 we saw what we believe is the second campaign from a threat group known as the Sun Team. This operation targets North Korean refugees living in South Korea with **spyware that attempts to exfiltrate photos, contacts, SMS messages**, and other sensitive information. While the number of infections appear low, the impact to victims will likely be significant.

As we continue our march toward an average of over 100 apps on our smartphones the platform remains a key target for ransomware developers, identity thieves, and nation states. It is imperative to **maintain diligence before installing any app or following any link**. It is also important that we cascade those behaviors to the devices we bring into our businesses and homes.

We hope you find the content insightful and look forward to your feedback.

Raj Samani
McAfee Fellow,
Chief Scientist
(**Twitter@Raj_Samani**)

Gary Davis
Chief Consumer
Security Evangelist
(**Twitter@GaryJDavis**)

Going in the Backdoor

With smartphones connected to and controlling multiple items in people's homes, it was only a matter of time before criminals looked for ways to trick users into letting them inside. Enter TimpDoor, an Android-based malware family that does just that. TimpDoor first appeared in March 2018, and experienced explosive growth in September, becoming the leading mobile backdoor family by more than 2x.

Mobile backdoor threats are not new. DressCode, MilkyDoor, Guerrilla, and Rootnik are all previously detected Android-based malware families that date back to at least 2016. These were typically distributed through the Google Play store as Trojanized apps, **hidden inside games or customization tools**. Most of these have since been removed from the store, and Google continues its efforts to quickly identify and remove malicious apps.

Bypassing the Store

TimpDoor gets around this by **directly communicating with users via SMS and trying to get them to download an app outside of Google Play**. Currently targeting North America, the threat begins with text messages informing users that they have voice messages to review. The included link to a voice-player app provides detailed instructions to enable apps from unknown sources. Clicking on the link installs a fake voice-messaging application that displays two messages. None of the buttons or icons work except the ones which play the included audio files.

TIMPDOOR

What is it?
Android-based malware that communicates with users via SMS to get them to download an app outside of Google Play

Current threats
- Runs as a background service after user closes app
- Uses devices as an entry-point to internal networks
- No need for root exploits to gain access to the device

Future threats
- Expect attacks to become stealthier and more targeted
- May evolve to ad click fraud, distributed denial of service attacks, and sending spam and phishing emails

Connect With Us

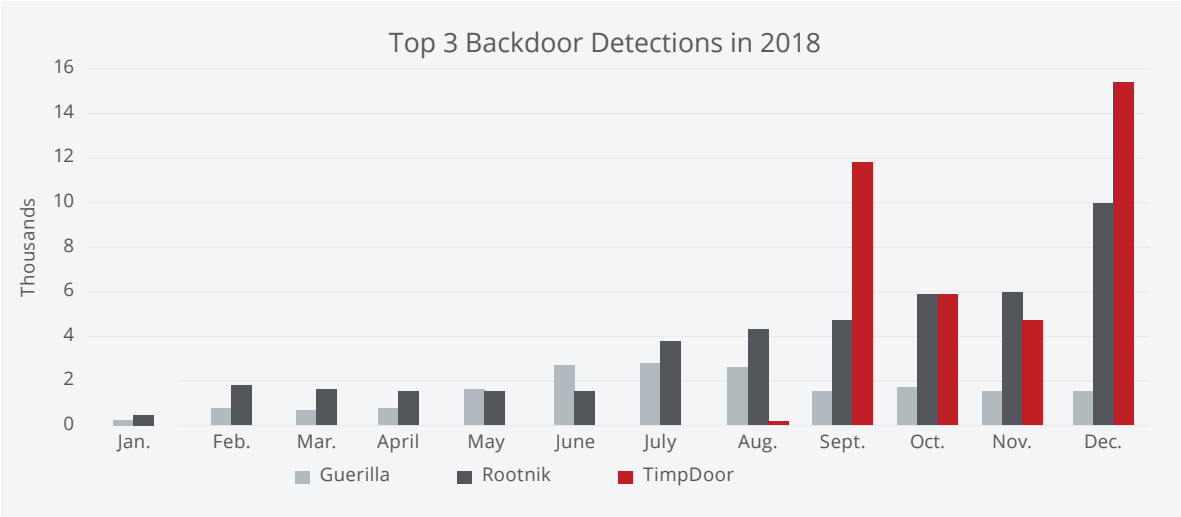


Figure 1. Mobile backdoor detections in 2018

Hiding in the Background

Since most people will not remember to disable unknown sources after installation, the phone remains vulnerable to other malicious apps. When the user closes the app, it **hides the icon but continues running as a background service**, making it more difficult to detect and delete. Redirecting all network traffic through an encrypted tunnel to a third-party server hides from most firewalls and other security protections and opens up the home or business network to infiltration and infection.

Evolving Functionality

Earlier versions of TimpDoor use an HTTP proxy to forward web traffic, while the newer version uses a SOCKS proxy that can reroute any network traffic. Establishing the tunnel and keeping it open are currently the only included functions in TimpDoor. The evolving but still basic functionality implies that this attack is still under development. Since cybercriminals are mostly interested in money, the most likely additions to this attack are ad click fraud, distributed denial of service attacks, and sending spam and phishing emails. As they evolve, **we expect attacks like this to become stealthier** and increasingly targeted at specific devices, companies, or demographics.

"TimpDoor shows how cybercriminals are constantly turning Android devices into mobile backdoors potentially allowing covert access to internal home and corporate networks"

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

Connect With Us

Gaining Root Access with the User's Permission

TimpDoor demonstrates that proxy-based mobile backdoors are becoming more relevant, taking advantage of the always-connected nature of mobile phones. Increased processing power in phones is enabling more sophisticated functionality, such as the socks proxy and network payload encryption. Devices infected with TimpDoor can be used for reconnaissance, as **an entry-point to internal networks**, to access servers and devices that are air-gapped or otherwise shielded from the open Internet.

The shift away from Google Play as the distribution mechanism is also a significant concern. Tricking users into installing fake apps to listen to fake voice messages is a novel approach. Leveraging popular websites and a convincing social-engineering attack to trick users into enabling unknown sources **removes the need for root exploits to gain access to the device**.

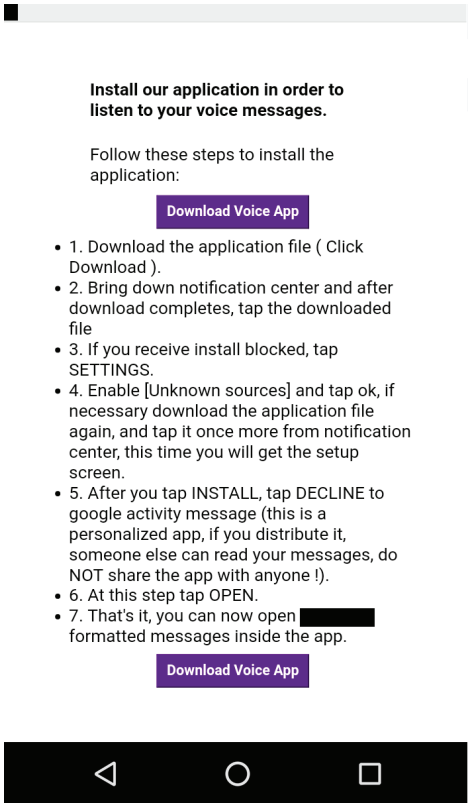


Figure 2. Website prompting user to download fake voice app

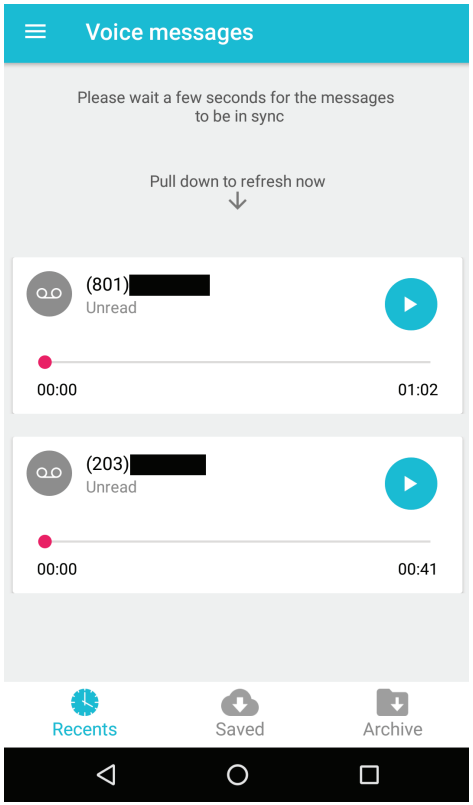


Figure 3. Main screen of the fake voice message app

Faking it on Fortnite

Sixty-million downloads is a target-rich environment for malware. The incredible popularity of the multi-player game Fortnite has led to several fake apps pretending to be various versions of the game, enticing downloads that do not require an invitation code, promised beta releases, and tutorials.

An invitation-only beta version of Fortnite was initially distributed during August 2018 to Samsung devices via the Samsung store. This resulted in a **wave of eager users** trying to get invitations and others trying to help them. It also encouraged criminals to target these gamers with YouTube ads explaining how to get the app and links to fake apps. Because the game is not available from Google Play, users may not be surprised that they have to enable apps from unknown sources, allow admin access, or give the app other privileges.

Very Convincing Fakes

These fake apps are very convincing, with the **same images, music, and loading screens** as the legitimate app. After prompting for a log in, the user is asked for mobile verification and then directed to a link with instructions on how to unlock their phone and get the game. However, the install button simply takes them back to the install screen or Google Play store. Thinking that something may have gone wrong during install, many probably try again, driving up the number of downloads and generating revenue for the criminals.

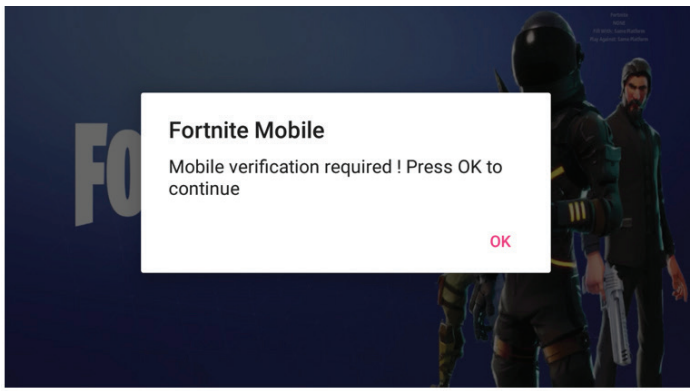


Figure 4. Fake Fortnite App verification screen

FAKEAPP

What is it?
General-purpose malware family that mimics popular apps

Current threats
- App from unknown sources is enabled, allowing admin access or other privileges
- Generates revenue through ads and redirects to download other apps
- Sends SMS messages, downloads hidden apps, or displays annoying ads

Future threats
- Other organizations might deliver outside GooglePlay
- Users may not re-reset their settings to block apps from unknown sources, leaving their devices vulnerable

Connect With Us

Multi-purpose Malware

When the Fortnite beta was announced in August there was a 3-4x spike in detections of FakeApp, a general-purpose malware family that can be used for multiple purposes. Most of the deployments of this app seems to be relatively benign to the user, generating revenue through ads and redirects to download other apps. However, some variants have been captured **sending SMS messages, downloading apps that hide upon execution, or displaying annoying ads**. Other malicious versions act as spyware or cyptocurrency miners.

Popularity Will Encourage Others

The popularity of Fortnite and the decision by Epic Games to distribute outside of Google Play normalizes this distribution method. Even users installing genuine versions of Fortnite will probably not re-reset their settings to block apps from unknown sources, **leaving their devices open to other attacks**. It is likely that other legitimate organizations will follow Fortnite's example and partner with manufacturers or other ecosystems to deliver exclusive versions of their app, in the hopes of generating additional buzz. We **expect to see continued growth of this attack vector** as cybercriminals take advantage of the public's acceptance of installing Android apps from unknown sources. Since revenue is the current object of most of these criminals, we anticipate increasingly malicious threats and aggressive attacks, including ad click fraud, ad overlays, mobile billing fraud, banking Trojans, and downloading of other malicious apps.

"Fake Apps are and will be one of the most effective methods to trick users into installing suspicious and malicious applications in Android"

Alan LeFort, Vice President & General Manager, Mobile and ISP Solutions, McAfee

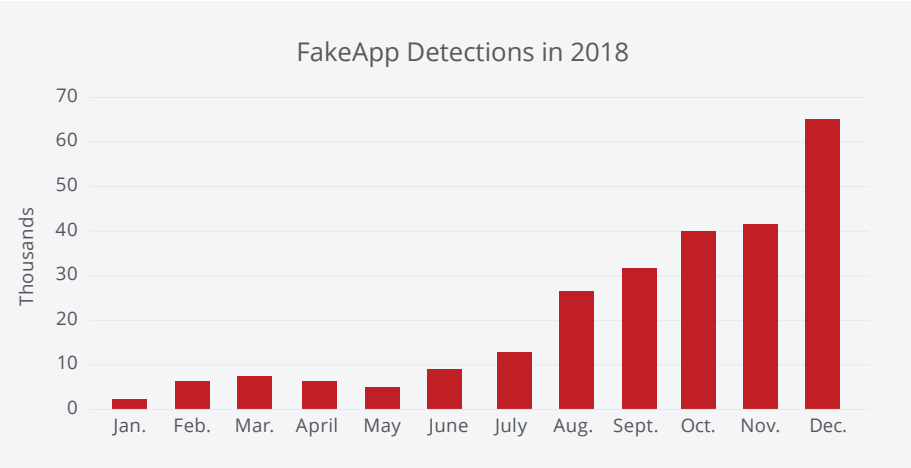


Figure 5. Growth of FakeApp detections in 2018

Connect With Us

Banking on Trojans

Stealing banking or other financial credentials from mobile devices is also on the rise, as more and more people embrace the convenience of mobile banking and payments. In last year's **2018 Mobile Threat Report**, we noted a 77 percent increase in banking Trojans and predicted that this type of exploitation would continue to grow. Unfortunately, that prediction has come true.

From June to September 2018 we detected a 2x increase in banking Trojans, with the Banker family of malware showing the strongest growth, followed by a further 75 percent spike in December. Often **disguised as a legitimate banking application**, the malware uses an overlay window to prompt for the user's credentials.

Bypassing the Store, Part 2

At least part of this growth is due to cybercriminals adapting to security restrictions and **finding new ways to bypass Google security**. Popups or overlays had been blocked in previous versions of Android but malware authors have found a way to get them working again.

Dynamic Deception

Another technique used to bypass the security checks has the app on Google Play functions as advertised. However, this mock app then **dynamically downloads and decrypts the malicious code** either after a specified period of time or after the base app has been installed and confirmed to be running on a real device and not in a sandbox. These Trojans could then be distributed via more trusted sources in the ecosystem, making them more difficult to catch. Banking Trojans are also evolving and adding new functionality, such as keylogging and other spyware jobs, expanding their risk profile.

BANKING TROJANS

What is it?
Disguised mobile malware used to steal banking or other financial credentials

Current threats
- Dynamically downloads and decrypts malicious code after a time period
- Can add keylogging and other spyware jobs

Future threats
- Major source of revenue for cybercriminals
- May move into ransomware, ad click fraud, and other types of malware

Connect With Us

Banking on Extra Security

Banks worldwide are being put in a tough position with these apps. Continued warnings to customers about unexpected popups and overlays asking for sensitive information are essential, as are supplementary authentication techniques. Banks also need to warn their customers about providing apps with additional privileges and service access, as these help the malicious apps further infect the device. Banks may also want to **encourage customers to install an additional layer of security software on their devices** to aid in detecting fraudulent software and protecting their credentials.

Banks Are Where the Money Is

Android banking trojans will continue to evolve and adapt to bypass security measures inside and outside Google Play. They are a **major source of revenue for cybercriminals** and they will continue to evolve into more sophisticated threats with broader functionality. Their success in getting onto mobile devices means they will also explore adding additional forms of revenue like ransomware, ad click fraud, and acting as a download conduit for other types of malware.

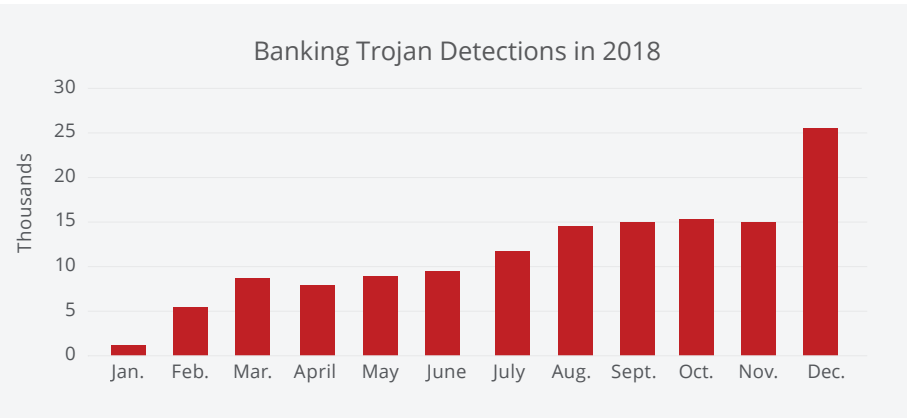
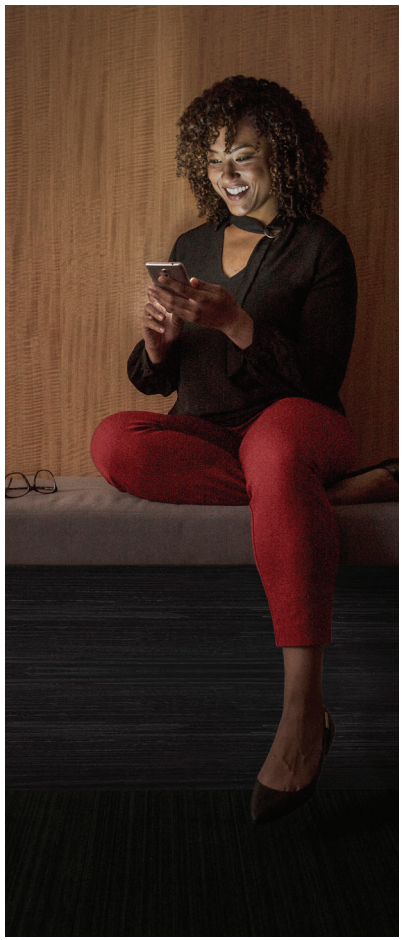


Figure 6. Increase in banking Trojan detections



Connect With Us

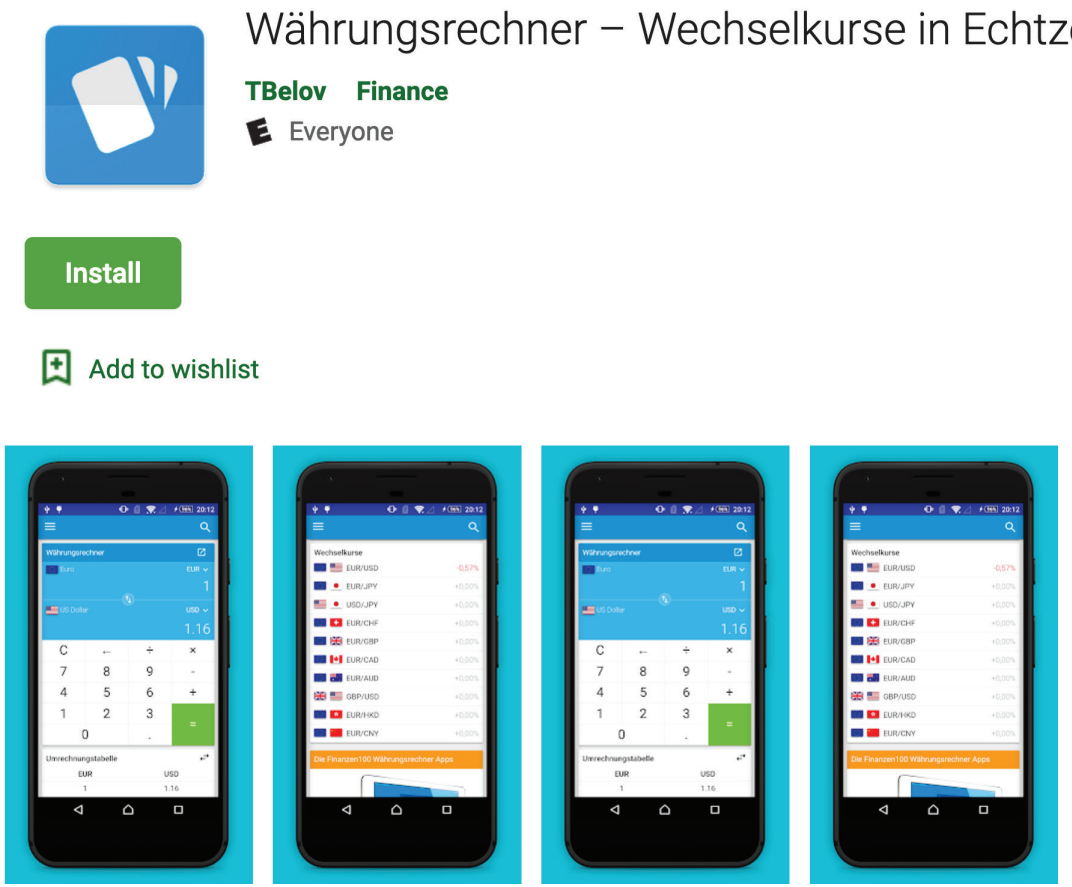


Figure 7. Banking Trojan dropper in Google Play

"As long as Banking Trojans are able to pretend to be legitimate banking and financial apps, cybercriminals will continue to improve its distribution methods to reach its victims and generate as much fraudulent revenue as possible"

Sreenu Pillutla, Sr. Director, Software Engineering, McAfee

Connect With Us

Operations RedDawn and FoulGoal

Last year we predicted that the number of targeted attacks on mobile devices would increase. Two recent examples are Operation RedDawn, targeting North Korean defectors, and FoulGoal, possibly targeting Israeli FIFA World Cup fans.

More than 30,000 North Korean refugees live in SouthKorea, with 1,000 or more defecting each year. The **phones of these refugees are being actively targeted by spyware**, which attempts to copy photos, contacts, SMS messages, and other sensitive information and send it to the attackers. RedDawn is the second operation of 2018 that we have identified and linked to a hacking group called the Sun Team, as they attempt to install spyware on the devices of their Korean victims.

So far, the number of successful infections appears to be quite low, around 100 devices This is partly due to active efforts by Google Play and the security industry to quickly identify and remove these apps from the store.

Fake Accounts from Fake Apps

The probable nationality was identified by tracing an exposed IP address to North Korea and finding some Korean words in the logs that are not in the common vocabulary of South Korea. The code is based on publicly available malware, which suggests that the attackers are not technically skilled. Perhaps the most worrisome aspect of this threat is the **use of stolen photos and other sensitive data to create fake accounts** on various online services, and even steal user's identities.

SPYWARE

What is it?
Targeted attacks on mobile devices

Current threats

- Uses stolen photos and other sensitive data to create fake accounts on online services
- Can steal SMS messages, contacts, GPS details, and audio recordings
- May steal user's identities

Future threats

- Nation state actors may spy on dissidents or other groups of interest

Connect With Us

Red Card for Football App

The FoulGoal campaign used an app called Golden Cup to install spyware on victims' devices. This app promised users streams of games from the Russian 2018 FIFA World Cup, as well as a searchable database of previous World Cup records. In addition to stealing the user's phone number, device details, and installed packages, FoulGoal can download dex .data files from its control server that expands the infection to steal SMS messages, contacts, GPS details, and audio recordings. While this app was downloaded in many countries, the majority of downloads were in the Middle East, after a Twitter post in Hebrew promoted the app.

"The richness of data that can be collected makes mobile devices an attractive target of nation state actors looking to spy on dissidents or other groups of interest"

Gary Davis, Chief Consumer Evangelist, McAfee

Figure 8. Malicious apps targeting North Korean defectors

Connect With Us

Voicing your Concerns

"Hey Robot, will my home be hacked today?"

"I am sorry Dave, it has already been compromised."

Over 25 million voice assistants or smart speakers, are already in use. In addition to simple queries, these devices are often connected to other things in the home, controlling lights, thermostats, and door locks, among others. Many of these Internet of Things (IoT) devices are **failing at even rudimentary security practices**, such as easily guessable passwords, well-known buffer overflow issues, and unpatched vulnerabilities documented on other devices that use the same components. As the voice assistant and smart home market grows rapidly, to as many as 275 million smart speakers over the next 5 years, it will become an increasingly valuable attack vector for cybercrime.

In It for the Money

While a lot of the media coverage on cybersecurity focuses on data theft and privacy breaches, most of the **cybercriminal activity is driven by money**. From building botnets, to stealing banking credentials, perpetrating click fraud, or threatening property or reputation damage unless a ransom is paid, money is the goal. The rapid growth and broad access of voice assistants and their connected IoT networks make them a prime target.

IoT ATTACKS

What is it?
Vulnerabilities in IoT devices being exploited

Current threats
- Accesses the stream or microphone of voice assistants to spy or perform actions
- Uses IoT devices to access to the rest of the network

Future threats
- Weak to non-existent security controls from device manufacturers
- Explosive growth in the market for IoT devices

Connect With Us

> **"The volume of connected things flooding into homes and businesses coupled with weak to non-existent security controls from device manufacturers will make voice assistants and devices in general an attractive target."**
>
> Gary Davis, Chief Consumer Security Evangelist, McAfee

You Never Know Who Might Be Listening

The attack surface of a typical home with a voice assistant is quite broad. Hackers could get access to the listening stream or microphone and **monitor everything said in its vicinity**. Smart speakers could be commanded to perform actions by some other device with a speaker, such as embedding commands in a TV program or Internet video. Customized actions could be modified, altering one of your automated tasks into something that performs additional steps to benefit the criminal.

Another Way In

However, the bigger vulnerability comes from associated IoT devices, such as smart plugs, door locks, cameras, or connected appliances, which have their own set of quirks and vulnerabilities and could provide **unfettered access to the rest of the home network**. Network segmentation, or grouping devices on separate IP subnets, is a common corporate IT practice that is slowly moving into the home network in an effort to reduce the overall vulnerability of the home to these types of attacks. Tools that enable network segmentation in the home are becoming easier to find and use.

The Up and Down of Mobile Cryptomining

The popularity of digital currencies has attracted criminals looking to find ways to add value to their digital wallets without the cost of doing their own mining.

With the cost of cryptomining machines upwards of $5,000, hackers are using malicious code to use your devices to add blockchain entries to cryptocurrencies. The popularity of Android-based devices not only makes them a prime target, but the latest technique can **jump from phone to table to smart TV** to infect your entire environment. Some of these malicious apps, such as ADB Miner, are spreading through a publicly accessible port via the Android Debug Bridge (ADB).

Whole Lot of Mining Going On

The number of cryptomining mobile apps has grown substantially in the last year. Cybersecurity researchers found **more than 600 malicious cryptocurrency apps**, spread across 20 different app stores. While mobile app store companies are actively working to identify and remove these apps, they do not necessarily notify users who downloaded them before they were removed.

CRYPTOMINING

What is it?
Malicious code using devices to add blockchain entries to cryptocurrencies

Current threats
- Can jump from phone to table to smart TV to infect your entire environment
- Some apps like ADB Miner, are spreading via the Android Debug Bridge (ADB)
- Can put excessive strain on the device

Future threats
- Apple and Google have banned apps in stores
- Mobile coin mining is not as profitable

Connect With Us

Cracking the Case (of Your Phone)

Malicious cryptomining apps can do far more harm than just use your processor. Some of them consume so much processing capacity that they are causing batteries to swell enough to crack the back cover, or **making the processor overheat and implode**. In June 2018, Apple took the additional step of changing its developer guidelines to ban mining apps completely on its devices, including apps which drain the battery, generate excessive heat, or otherwise put excessive strain on the device. Google enacted a similar ban for Google Play apps shortly after.

Dropping in Value

As we move into 2019, mobile cryptomining appears to be declining. This could be due to the drop in value of many cryptocurrencies, to the point that **mobile coin mining is no longer as profitable**. As a result, these attackers may switch to various forms of mobile ransomware as a more reliable revenue source.

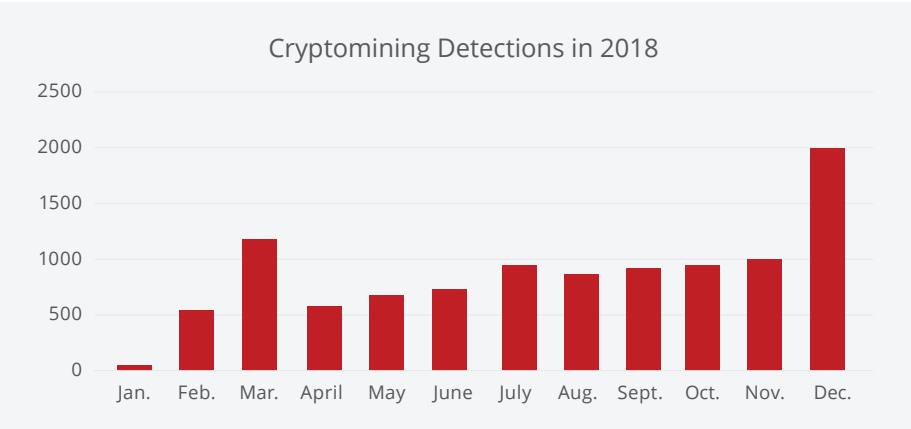


Figure 9. Growth of cryptomining detections

"Recently we have seen the see-saw between ransomware vs crypto-mining tip the balance toward extortion. However, rather than focus on the ups and downs of crypto-mining which will likely show fluctuations in line with the price of various currencies, we need to acknowledge that crypto mining is very much an active threat vector on the mobile platform."

Raj Samani, McAfee Fellow, Chief Scientist

Connect With Us

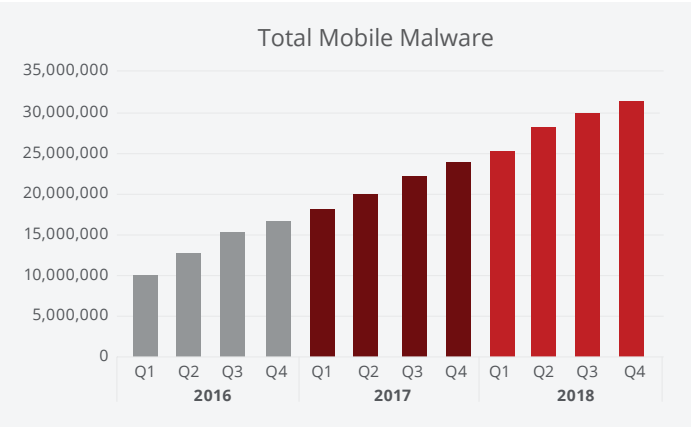
Summary

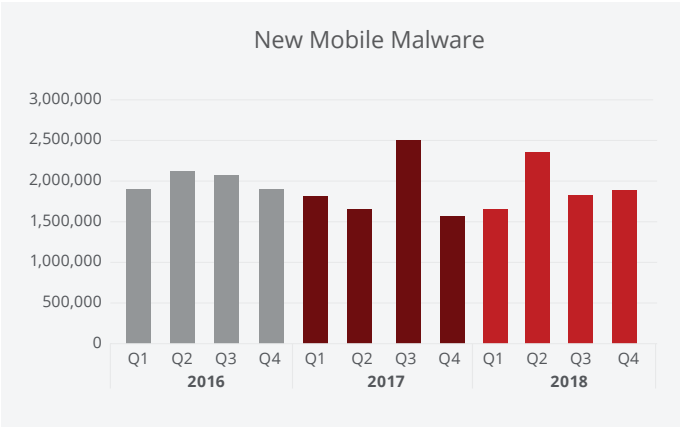
Everything is vulnerable to some type of malicious exploit.

If 2018 was the year of mobile malware, **2019 is the year of everywhere malware**. Detections of backdoors, cryptomining, fake apps, and banking Trojans all increased substantially in the latter half of the year. Attacks on other connected things around the house gained momentum as well. While hidden apps and Adware remain by far the most common form of mobile threats in Android, the others are growing and learning how to infect other types of devices as well.

Criminals Go Where the Money is Easiest

One common thread through much of the mobile attack landscape is the quest for illicit profits. Criminals are looking for ways to maximize their income, and **shift tactics in response to changes in the market**. As the value of cryptocurrencies drops, they shift away from cryptomining. App stores get better at finding and deleting malicious apps, so they bypass the stores and go direct to consumers. Some services have been slower to crack down on fake ad clicks, leaving themselves open to continued click fraud.





Connect With Us

Finding the Weakest Link

Connected things in the home and workplace will continue to be of interest as **weak to non-existent security controls from manufacturers** and lack of implementing even the simplest of evasion techniques such as changing the default user name and password make them particularly interesting targets.

Someone is Always Watching

The other primary thread we identified in our research is the **focus on surveillance**. Whether this is nation states looking to gain valuable national or corporate intelligence, companies looking to collect and monetize behavioral data, or disruptors trying to influence social or political behavior, many apps are gathering data on mobile users beyond their consent. In addition to repeated communications to consumers to be vigilant about what they download to their devices, we expect to see an increase in political discussion about potential regulations aimed at protecting consumer privacy and penalizing corporate offenders.

What to Do

There are a few simple steps that users can take to drastically improve their own security posture and that of the devices that surround them.

Do not install apps from unknown sources.
If you receive a text with a link for you to download something, do your homework. Research the app developer, download statistics, and app reviews. Be on the lookout for typos and grammatical errors in the description. This is usually a sign that the app is fake.

Click with caution.
Only click on links in text messages that are from trusted sources. If you receive a text message from an unknown sender, stay cautious and avoid interacting with the message.

Go directly to the source.
Comment sections are prone to links for fake websites and apps so criminals can make money off of downloads. Only download software straight from a company's home page.

Use mobile security software.
These days your smartphone is just as data rich as your computer. Protect your critical information and your privacy by using **comprehensive mobile security software** that protects you from online threats.

Stay aware.
New mobile threats are emerging all the time. Keep up on the **latest scams** and warning signs, so you know what to look out for.

1. https://9to5mac.com/2017/05/05/average-app-user-per-day/

Connect With Us

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place.

www.mcafee.com.

McAfee™
Together is power.

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