Mobile Threat Report

What’s on the Horizon for 2016

This Threat Report was written by:

Bruce Snell
Cybersecurity and
Privacy Director
Intel Security

Table of Contents

Introduction 3
Stagefright: Setting the Stage for Increased Security 4
Is Your Phone Monitoring What You Watch on TV? 6
SMiShing Continues to Evolve 7
Dangers on the App Stores 8
Mobile Malware Grows Up 10
Looking Ahead: IoT and Wearables 12
Play It Safe 12

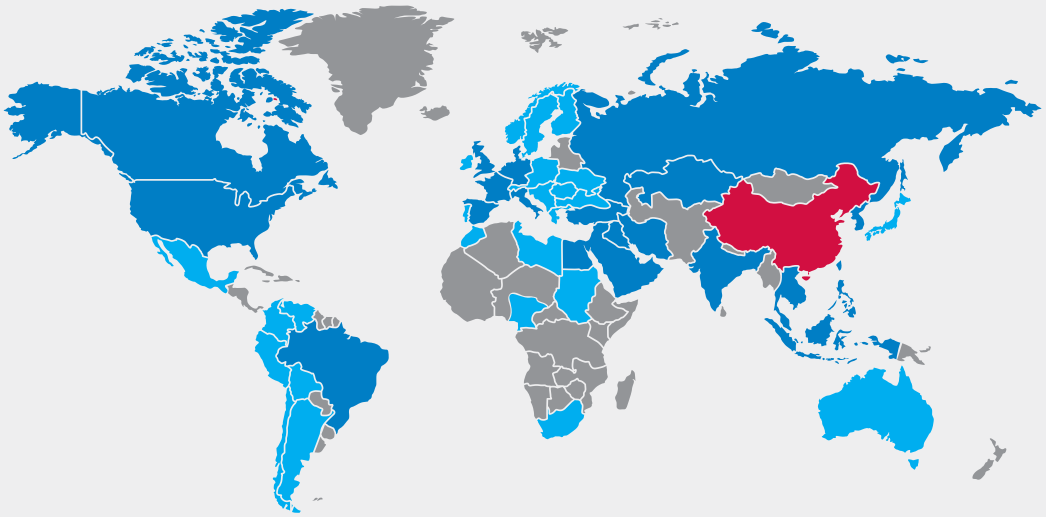
We find the mobile threat landscape continues to grow and evolve with several factors contributing. The increasing speed, power and storage space on mobile devices has led to more people using their devices in more places for online shopping, managing their finances and paying their bills. This leads to mobile becoming a much more valuable target for cybercriminals. This past year, we've seen how major vulnerabilities in the Android OS changed how Google looks at security updates. We also saw aggressive adware spying on your TV and radio habits. Additionally, we saw an increase in more advanced malware that brings threats we've been dealing with for years on PC's into the mobile world. Ransomware, bank fraud and remote access tools (RATs) all have an increased presence on mobile devices.

How are these new threats getting to your mobile devices? In our last report, we detailed the ways in which apps overshare your information; now we take a look at the large numbers of infected apps that make it past the screening process and show up in trusted app stores. Let's dig into some of the major issues of 2015 that are impacting the mobile space in 2016 and beyond.

Rule of three—top three threats facing mobile users:

1. Android moved to monthly security updates, but each manufacturer is responsible for rolling out the updates, often leading to delays
2. Malware continues to slip on to app stores
3. Cybercriminals are expanding their efforts to the mobile space

2016 Mobile Malware: What Happens in 1 Hour?



Intel Security: Malware detected from over 190 countries per hour.

🟥 > 6000 🟦 100 – 1000 🟦 10 – 100

Source: McAfee Labs 2016

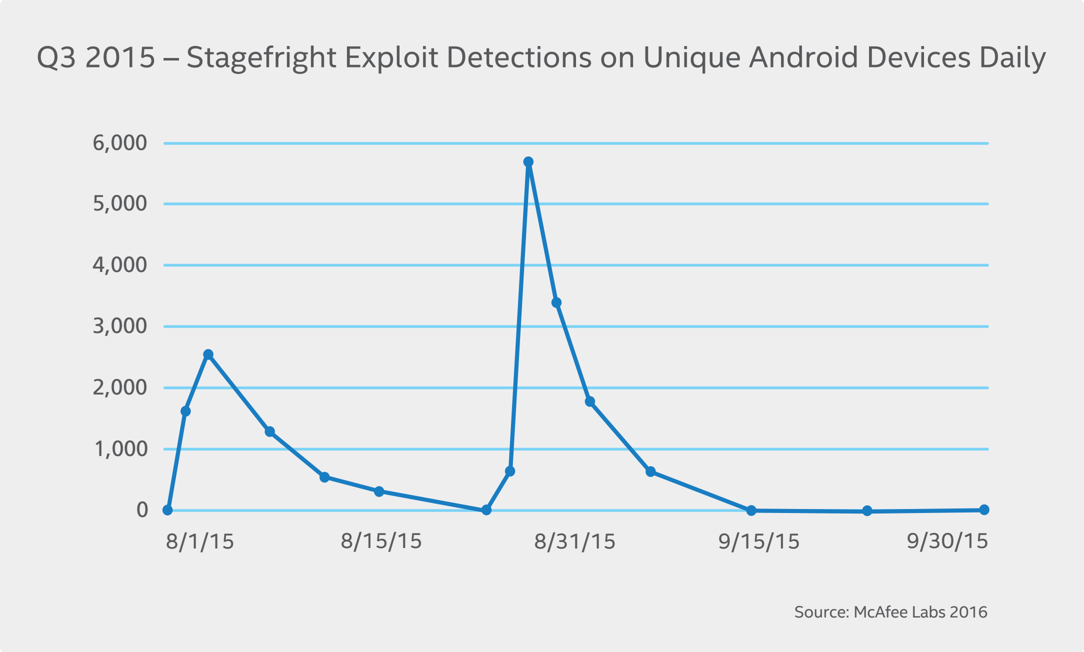
Stagefright: Setting the Stage for Increased Security

This past summer in the days leading up to the annual Black Hat security conference in Las Vegas, a number of vulnerabilities were found in the Android operating systems. This collection of bugs was referred to as “Stagefright” in reference to the stagefright libraries (underlying code in the OS that is shared by many applications) contained in the Android OS. These vulnerabilities are particularly nasty due to the fact that they allow an attacker to remotely execute code on someone’s phone by sending a specially crafted MMS message. Typically, a cybercriminal will try to trick the user into clicking on a malicious Web link or installing an infected application. None of those steps are necessary with Stagefright. If someone knows the intended target’s phone number, that’s all they need to launch an attack. Scarier still, due to the nature of the bugs, it would be possible for an attacker to hack a phone, implant a remote access tool, and cover any trace that the attack had occurred; all while the phone was charging overnight on the victim’s nightstand.

Looking at the results from our McAfee Labs mobile team, we can see the number of devices reporting a Stagefright attack, peaking at a little more than 5000 individual devices attacked toward the end of August, which happened about two weeks after an additional Stagefright vulnerability was found.

Steps to reduce Stagefright vulnerabilities:

1. Turn off MMS messages
2. Update your phone software
3. Don’t open messages from strangers
4. Use comprehensive security software


Q3 2015 – Stagefright Exploit Detections on Unique Android Devices Daily

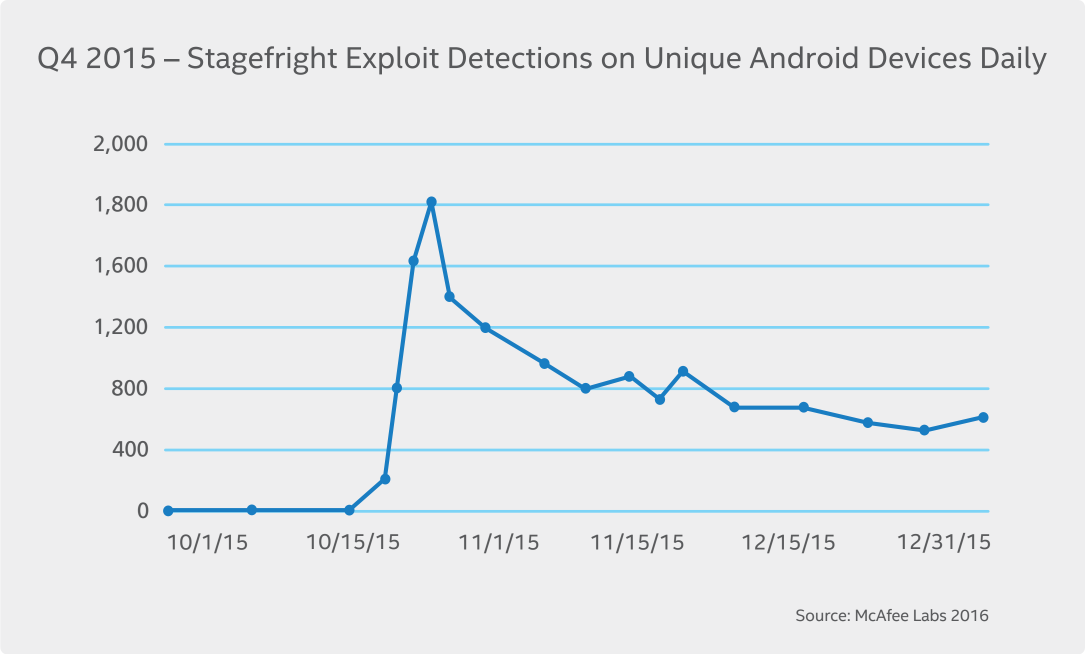
Source: McAfee Labs 2016

Detections of the first version of Stagefright spiked soon after the proof of concept code was released at the Black Hat security conference.

In October, another round of Stagefright vulnerabilities was released (dubbed Stagefright 2), this time using specially crafted mp3 and mp4 files to exploit a vulnerability in a core Android library (libutils) that has existed since Android was first released. This means devices running Android 1.5 to 5.1 are vulnerable to this attack, which is close to 1 billion devices.

Due to its wider range of vulnerable devices, this new version resulted in another uptick of Stagefright based malware that continued steadily through the end of 2015.

Ramifications of Stagefright: Google shifted to monthly security updates.



Source: McAfee Labs 2016

Soon after the announcement of “Stagefright 2.0” on 10/1/15, the number of unique Android devices detecting Stagefright based exploits has remained steady.

What Does This Mean for the Consumer?

Stagefright caused a dramatic shift in how Google handles security patches. Historically, there was no set schedule for updates, but following the events of the summer of 2015, Google has committed to rolling out updates on a monthly basis. However, it is important to note that these security patches are distributed to other manufacturers and wireless carriers, and it is up to those companies to provide these updates to their customers. On the upside, there are now monthly updates, but on the downside, those updates may take time to reach all Android devices. As you can see from the previous chart, the Stagefright attacks have steadily continued since the release of the vulnerability. If your device has not yet been patched for these vulnerabilities, you can follow these steps below to reduce the danger of infection:

- **Turn off MMS auto retrieval.** This isn’t necessarily convenient, but you should turn off your phone’s ability to automatically retrieve MMS (Multimedia Message Service) messages so long as Stagefright poses a threat. Tap the “message” icon on your Android home screen. Then tap the three dots (or lines) in the upper right corner and scroll down to settings. Scroll until you see “MMS” and flip that switch to “off.” You can also go into certain apps themselves to adjust settings that might auto-load MMS attachments.
- **Update your phone regularly.** Many updates contain security fixes to previously unknown vulnerabilities on your devices. When you learn of a new software upgrade, or get an update notice, update your device. Implementing updates as they become available is one of the best ways to protect your device from attacks like Stagefright.
- **Don’t open messages from strangers.** Don’t open or accept text messages from people you don’t know. Texts from unfamiliar numbers may be attempts to infect your device with Stagefright or another unknown vulnerability.
- **Use comprehensive security software.** Regardless of whether you’re on a mobile, laptop or desktop device, you’ll need to protect yourself from cybercriminals.

Is Your Phone Monitoring What You Watch on TV?

In our previous threat report, we talked about apps that were grabbing data from your phone without your knowledge. Now, a company from India has released an advertising software developer kit (SDK) called SilverPush that uses your phone's microphone to listen for near-ultrasonic sounds placed in TV, radio and Web advertisements. Once SilverPush detects the signal, it collects data from your device and sends information about your device back to the advertiser. While this is not a piece of malware, it is a huge concern from a privacy perspective. It collects personal information from your device, including, but not limited to:

- IMEI number (a unique number that identifies your phone)
- Operating system version
- Location
- Potentially the identity of the owner
- The user's television, radio and Web behavior

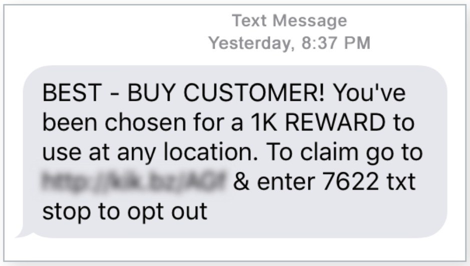
SilverPush is not a standalone app, but is embedded as part of another application and typically runs without the user's consent. If an application on your mobile device is detected as containing SilverPush, the best solution is to remove that application from your device.

The SilverPush Problem

Your phone could be monitoring what you watch on TV without your knowledge or permission.

SMiShing Continues to Evolve

SMiShing (SMS phishing) has continued to grow in popularity as a social engineering tool for cybercriminals. The aim of SMiShing is to trick the user into clicking on a link in a text message; that link goes to a page prompting you to enter personal data. The objective is to gain access to sensitive information like usernames and passwords. Additionally, many SMiShing messages will include links with malware waiting on the other side for anyone who clicks on them.



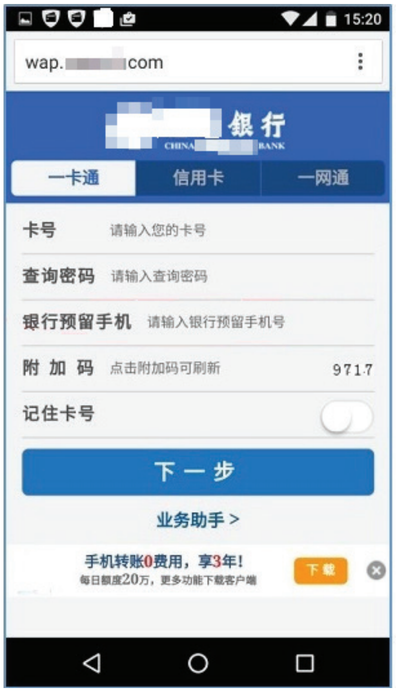
Text Message
Yesterday, 8:37 PM

BEST - BUY CUSTOMER! You've been chosen for a 1K REWARD to use at any location. To claim go to [redacted] & enter 7622 txt stop to opt out

Often the SMiShing attempt is easy to spot, with claims that you have won a contest you never entered or an “unclaimed refund” waiting for you. Many of the same techniques used in phishing email have made their way over to the SMiShing world.

While most SMiShing attempts will show up as an unfamiliar number, making them appear suspicious to attentive users, mobile banking users in China have recently started receiving SMiShing texts that appear to come from their bank’s official phone number. Mobile phones are designed to hop from network to network in order to maintain a connection while traveling. Cybercriminals can use this design to set up a fake base station with a mass SMS sending tool to send out text messages that appear to be completely legitimate. As long as the fake base station is producing a signal that is more powerful than the real base station, then anyone traveling through the area will receive the text. The hardware required for this setup is relatively inexpensive and could be operated from the back of a vehicle. Then it’s a simple matter of driving to a populated area, sending some mass texts and then moving on to your next area.

A recent campaign in China sent out messages saying the customer’s bank account will soon become unavailable, followed by instructions to log in and validate their account information. Clicking on the link would take the user to a mobile site that mimicked the official bank website and required the user to input bank account, password and mobile number. Looking at the images below, you can see how closely the fake interface on the left matches the legitimate interface on the right.



15:20

wap.[redacted]com

[redacted]银行
CHINA [redacted] BANK

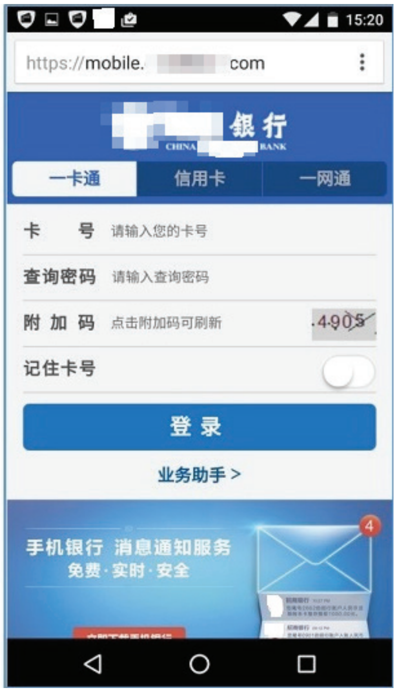
卡号 请输入您的卡号

查询密码 请输入查询密码

银行预留手机 请输入银行预留手机号

附 加 码 点击附加码可刷新 9717

记住卡号



15:20

https://mobile.[redacted]com

[redacted]银行
CHINA [redacted] BANK

卡　　号 请输入您的卡号

查询密码 请输入查询密码

附 加 码 点击附加码可刷新 4905

记住卡号

What can you do to stay safe?

The best defense against SMiShing is to learn to recognize suspicious text messages. If you don’t click on the link, the danger of SMiShing decreases dramatically. On our consumer blog, we show some examples of things to look for to spot phishing emails and most of the rules of spotting phishing emails do apply to SMiShing.

Get the scoop here.

Dangers on the App Stores

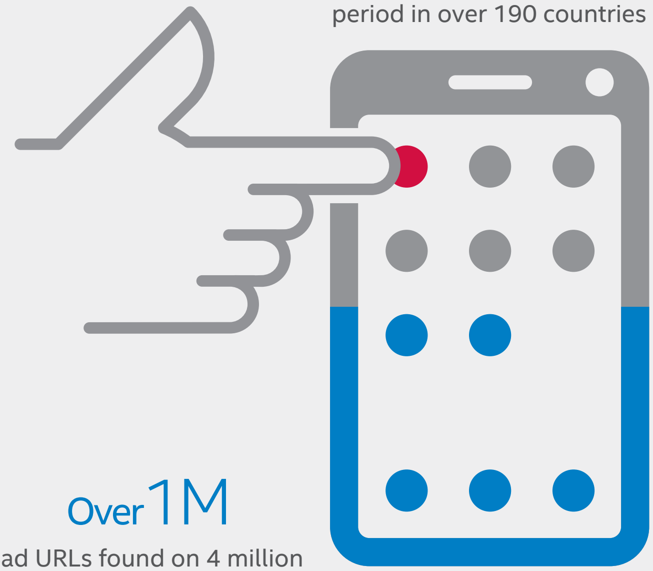
During the past year, there have been hundreds of apps pulled from both Google Play and the Apple App Store for security reasons. For iOS, the biggest threat this year came from apps with overly aggressive adware, whereas Google Play saw a fair number of apps infected with malware. Both Google and Apple have been very quick to remove malicious apps from their associated app stores, however it's inevitable that some infected apps will still slip through the screening process.

Over the past six months, McAfee Labs has crawled through the app stores checking for security issues and returned a number of interesting results:

There's always something new:
During the writing of this report, over 60 Android games hosted on Google Play were discovered to be infected with "Android.Xiny.19.origin" which hides Android executables (APKs) inside images to avoid detection.

Inside McAfee Labs: The Magic Numbers Behind the App Stores

150M
Apps scanned on client in last three month period in over 190 countries



9M
Malwares

9M
Suspicious apps

3M
Devices were affected over 6 months

Over 1M
Bad URLs found on 4 million devices over 6 months

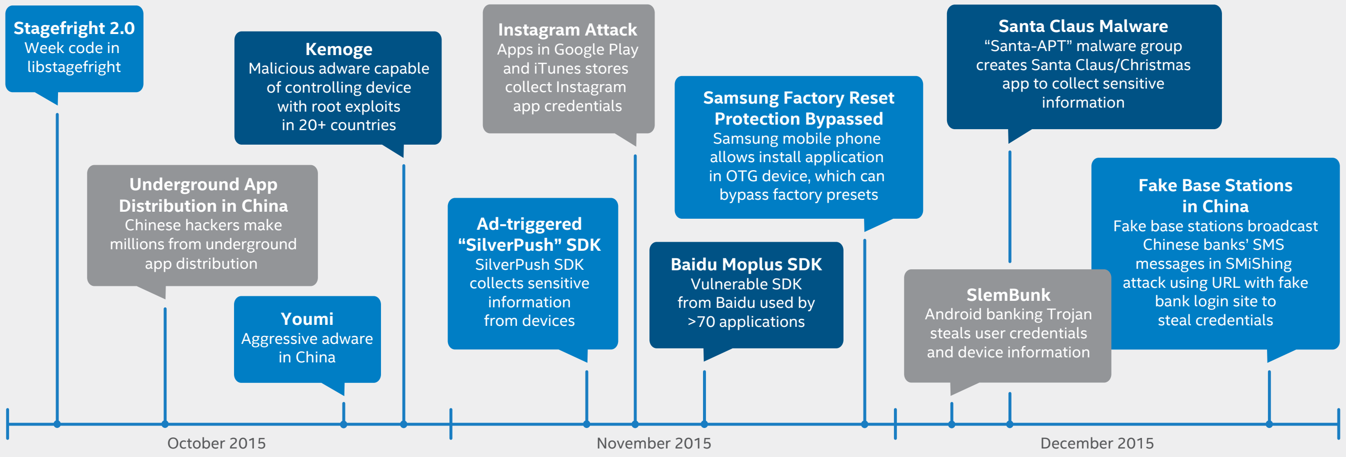
1M
Apps with bad trust score

37M
Total count of malware detected over 6 months

Source: McAfee Labs 2016

McAfee Labs routinely scans major app stores for infected systems as well as apps with suspicious behavior.

Noteworthy Mobile Threats: October – December 2015



Stagefright 2.0
Week code in libstagefright

Underground App Distribution in China
Chinese hackers make millions from underground app distribution

Youmi
Aggressive adware in China

Kemoge
Malicious adware capable of controlling device with root exploits in 20+ countries

Ad-triggered “SilverPush" SDK
SilverPush SDK collects sensitive information from devices

Instagram Attack
Apps in Google Play and iTunes stores collect Instagram app credentials

Baidu Moplus SDK
Vulnerable SDK from Baidu used by >70 applications

Samsung Factory Reset Protection Bypassed
Samsung mobile phone allows install application in OTG device, which can bypass factory presets

SlemBunk
Android banking Trojan steals user credentials and device information

Santa Claus Malware
“Santa-APT” malware group creates Santa Claus/Christmas app to collect sensitive information

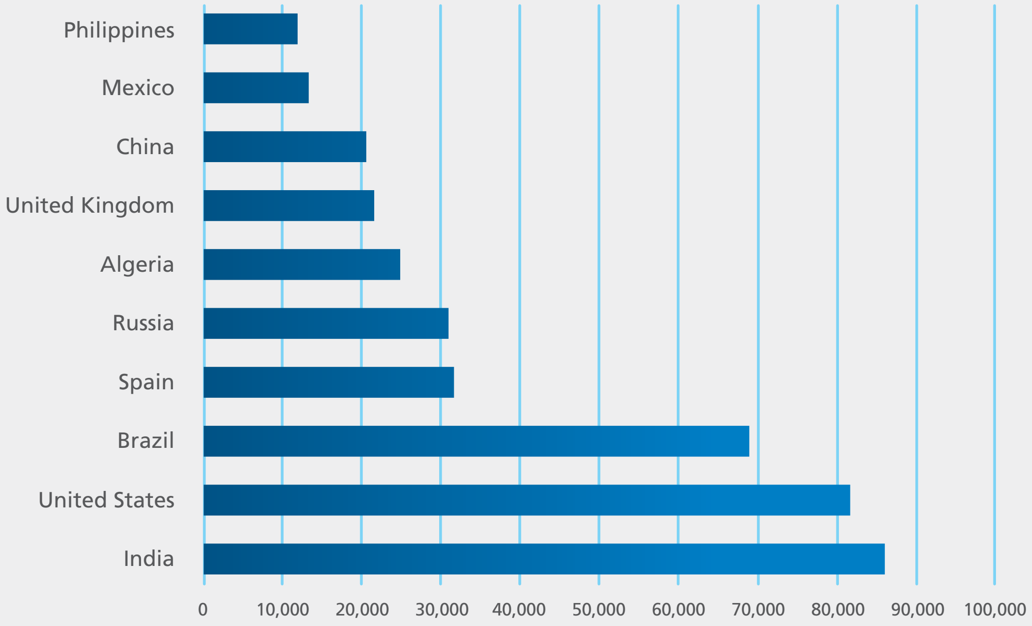
Fake Base Stations in China
Fake base stations broadcast Chinese banks' SMS messages in SMiShing attack using URL with fake bank login site to steal credentials

Source: McAfee Labs 2016

McAfee Labs

McAfee Labs is the threat research division of Intel® Security and one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. McAfee Labs threat researchers correlate real-world data collected from millions of sensors across key threat vectors—file, web, message, and network—and deliver threat intelligence in real-time to increase protection and reduce risk.

Top 10 Countries Ranked by Infections in Q4



Source: McAfee Labs 2016

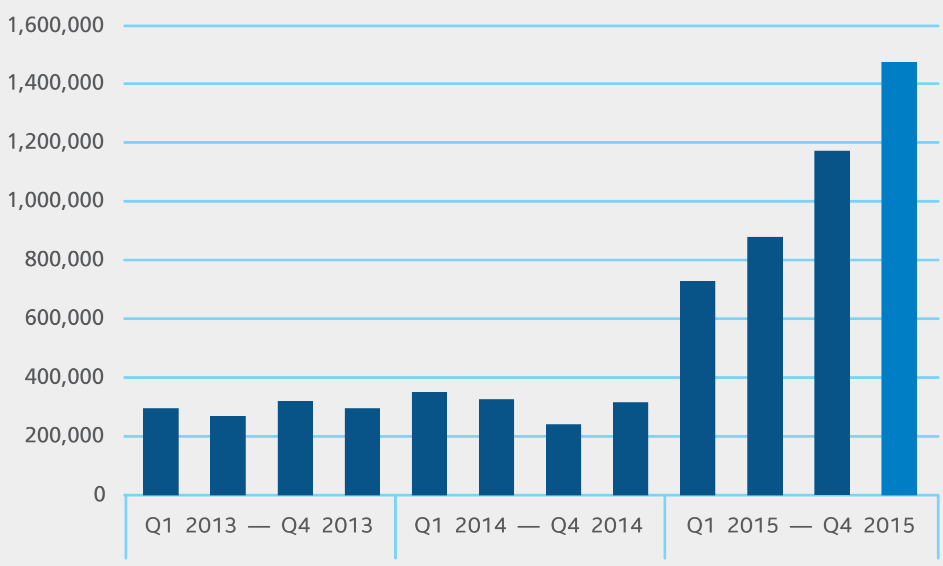
These numbers represent the total unique infections with repeated infections discarded.

Mobile Malware Grows Up

Over the last year we have seen a dramatic increase in not only the number of new malware, but also an increase in sophistication and complexity. There is also something of a vicious cycle with malware. Security patches are released which make most of the current malware obsolete. Then malware writers search for new vulnerabilities and release new malware or variants of old malware to get around the new protections. To compound the problem, enterprising malware authors will package their malware as an exploit kit for sale to other cybercriminals. Then new patches are released to fix the newly discovered vulnerabilities and the cycle starts over once again.

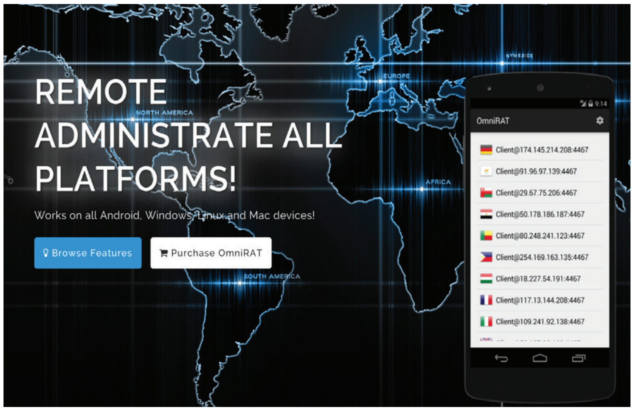
Unique mobile malware samples collected by McAfee Labs—24% increase from Q3
Historically, mobile malware has been something of an afterthought for cybercriminals with most of their efforts focused on PC. However, over the last year we have seen a dramatic increase in not only the number of new malware, but the sophistication and complexity of mobile malware.

Mobile Malware: Threat Statistics



Source: McAfee Labs 2016

A Trojan named “SlemBunk” was discovered in mid-December that behaves very much like an advanced persistent threat (APT) one would find attacking a PC. It is installed by a drive-by download (meaning a user simply has to visit an infected site to become infected), installs a downloader in the background and communicates to a backend command and control server and pulls down the latest update code for the malware. This setup has all the earmarks of a sophisticated cybercrime campaign and could become a serious issue in 2016.



REMOTE ADMINISTRATE ALL PLATFORMS!

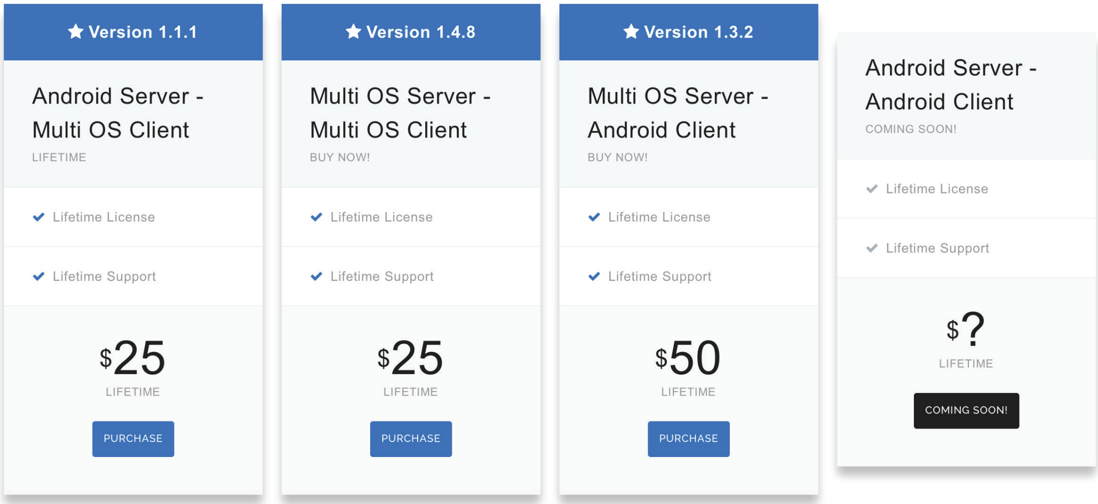
Works on all Android, Windows, Linux and Mac devices!

Client@174.145.214.208:4467
Client@91.96.97.139:4467
Client@29.67.75.206:4467
Client@50.178.186.187:4467
Client@80.248.241.123:4467
Client@254.169.163.135:4467
Client@18.227.54.191:4467
Client@117.13.144.208:4467
Client@109.241.92.138:4467

We’ve also seen remote access tools (RAT) easily available on the Internet for sale. One particular tool even has a well-polished website that puts most commercial software to shame with tutorials, multiple pricing models and easy to use payment systems. Now instead of digging around in the Dark Web, you can use common electronic currency to purchase a client and server package that will allow you to control infected systems (both PC and mobile) from your platform of choice.

Do I smell a RAT?

A remote access tool, commonly referred to as a RAT is used by hackers to give full control to a system. They are typically used by cybercriminals in a server/client model in which a large number of infected systems are controlled by one system to launch attacks against other systems, to send out SPAM, or for any number of nefarious things. Over the past few years, RATs have become more robust and polished with features that rival commercial remote management tools.



★ Version 1.1.1

Android Server - Multi OS Client

LIFETIME

✓ Lifetime License

✓ Lifetime Support

$25

LIFETIME

PURCHASE

★ Version 1.4.8

Multi OS Server - Multi OS Client

BUY NOW!

✓ Lifetime License

✓ Lifetime Support

$25

LIFETIME

PURCHASE

★ Version 1.3.2

Multi OS Server - Android Client

BUY NOW!

✓ Lifetime License

✓ Lifetime Support

$50

LIFETIME

PURCHASE

Android Server - Android Client

COMING SOON!

✓ Lifetime License

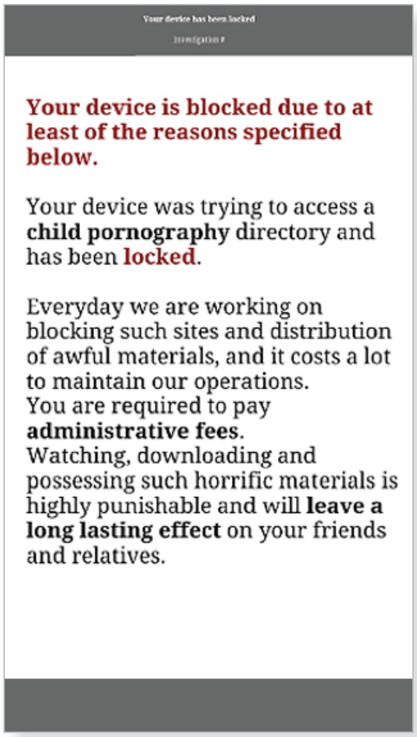
✓ Lifetime Support

$?

LIFETIME

COMING SOON!

Along with APTs and RATs gaining more traction on mobile, we're also seeing an increase in ransomware on Android. Whereas ransomware on the PC tends to encrypt files and demand a ransom for unlocking them, Android ransomware leans more toward locking a user out of their device until a fee is paid. Since a mobile device tends to be backed up more often than a PC, ransomware authors often combine a bogus legal threat to go along with the lock, scaring the victim into paying instead of just wiping the system and restoring from a backup.



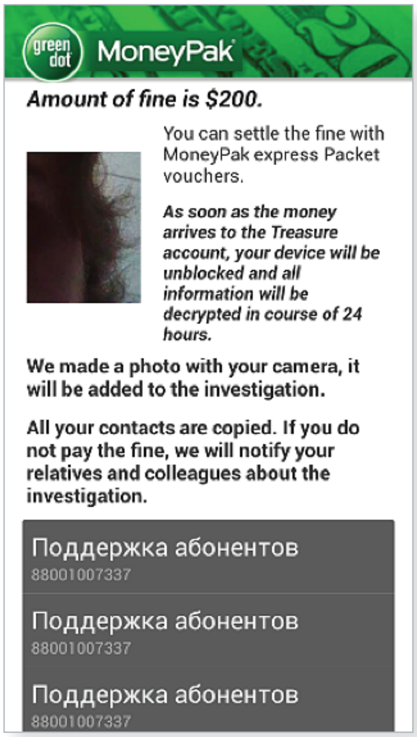
Your device has been locked

Investigation #

Your device is blocked due to at least of the reasons specified below.

Your device was trying to access a **child pornography** directory and has been **locked**.

Everyday we are working on blocking such sites and distribution of awful materials, and it costs a lot to maintain our operations.
You are required to pay **administrative fees**.
Watching, downloading and possessing such horrific materials is highly punishable and will **leave a long lasting effect** on your friends and relatives.



Amount of fine is $200.

You can settle the fine with MoneyPak express Packet vouchers.

As soon as the money arrives to the Treasure account, your device will be unblocked and all information will be decrypted in course of 24 hours.

We made a photo with your camera, it will be added to the investigation.

All your contacts are copied. If you do not pay the fine, we will notify your relatives and colleagues about the investigation.

Поддержка абонентов
88001007337

Поддержка абонентов
88001007337

Поддержка абонентов
88001007337

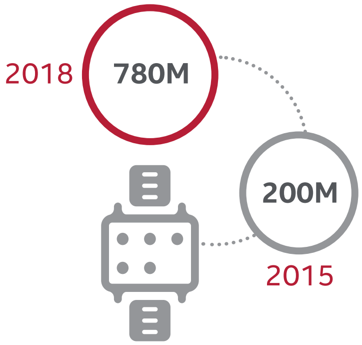
For example, Svpeng tells the user that their system was locked because they were trying to access a website containing child pornography and that to unlock their system they must pay "administrative fees." The ransomware will also use the device's camera to take a picture of the user as an additional "scare tactic."

Looking Ahead: IoT and Wearables

Current industry estimates put the number of Internet-connected wearables around 780 million by 2018, which works out to a wearable device on one of every 10 people on Earth. If we allow for fewer wearables in developing countries, that number is probably closer to one of every four or five people in wealthier countries who will have some sort of wearable device.

From a hacker's perspective, densely populated areas are a target-rich environment for attacking wearables. Although breaking into a wearable device does not necessarily provide immediate value for a hacker, the real value lies in the wearable's connection to a smartphone. Most of these devices use Bluetooth LE (low energy) technology, which has suffered a number of very well-documented security flaws and likely will produce more with each new version. This makes the connection between the wearable and its mobile device easier for hackers to access a lot of sensitive and personal information.

Wearable Devices



Smart security for a smart home?
We are seeing a tremendous growth in Internet of Things (IoT), including a big push towards Internet connected appliances, thermostats and more. As the number of these devices grows, cybercriminals may start looking towards attacking IoT as a way to get a foothold into your home network.

Play It Safe

As we've seen in this report, mobile threats continue to increase in frequency and complexity. As we become more dependent on our mobile devices, we must think more about security as we go about our day-to-day activities. Here are some tips to help keep your digital life safe and secure:

1. Update!

To keep your data secure and private, you have to keep cybercriminals from getting a foothold on your devices. The majority of malware infections could be prevented by simply keeping your system up to date with the latest OS and application updates.

2. Use Only Official App Stores

As Intel Security scans the app stores for malicious apps, app stores are alerted when new malicious apps are found, so even if something slips through, you are still safer going through a trusted app store than going through an unverified source.

3. Review App Reputation Scores

We have found there are many apps that while not technically malicious, do disclose far too much personal information without a legitimate reason. Because of this, it is important to be aware of an app's security and privacy reputation.

4. Be Suspicious

Cybercriminals will try all sorts of methods to get your data, and one of the more successful methods is social engineering. Always be wary of clicking on any link in an email or SMS you weren't expecting to receive. This includes messages from people you know, as they may have been infected and don't realize they are sending malware.

5. Use Comprehensive Security Software

Keeping your mobile device up to date will help you stay safe from older viruses, but you should also install anti-virus software on your devices to protect against new threats or older threats that haven't yet been fixed by OS or application updates. Most have other benefits such as looking for apps that may be suspicious based on the permissions they are asking for and notifying you when you're about to connect to a potentially unsafe Wi-Fi.

Summary

Smartphones and tablets are amazing tools for staying connected with friends and family, for keeping up to the minute with work, for shopping, for paying our bills and managing our free time. Cybercriminals are seeing an opportunity to prey on victims by attacking mobile devices, driving an increase in the number and sophistication of threats. We expect to see this trend continue in the next year, requiring more diligence and awareness by both the security industry and end users. We think this will become even more complex as consumers bring connected devices into their homes and use more wearables.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com