Mobile Threat Landscape

Threats in the mobile space continue to grow year on year. In 2017, there was a 54 percent increase in the number of new malware variants alone and it's not just the volume that's increasing. Attackers have developed new methods of infection and tricks to remain on compromised devices as long as possible. They've also come up with a variety of means of generating revenue from devices, from ransomware to cryptocurrency mining.

But while the attacks continue to evolve and mature, the same can't always be said of the device user. Many users continue to make life easy for attackers by continuing to use older operating systems. In particular, on Android, only 20 percent of devices are running the newest major version.

Mobile threats continue to rise

The number of new mobile malware variants grew by 54 percent in 2017, compared to 2016.

Mobile malware variants by year

The number of new mobile malware variants grew by 54 percent in 2017, compared to 2016.

	2016	2017	Change
Mobile Malware Variants	17,214	26,579	54%

Number of malware blocked per day on mobile devices

An average of 23,795 malicious mobile applications blocked on mobile devices each day.

	2016	2017
Total Mobile Malware Blocked	7,193,927	8,684,993
Average per Day	19,709	23,795

Average number of ransomware blocked per month.

An average of 3,510 mobile ransomware were blocked per month in 2017.

	2017
Mobile Ransomware Blocked	42,118
Average per Month	3,510

Number of new mobile malware families identified

The number of new mobile malware families grew by 12 percent in 2017, compared to 2016.

	2016	2017	Change
New Mobile Malware Families	361	405	12%

> **"Many users continue to make life easy for attackers by continuing to use older operating systems. In particular, on Android, only 20 percent of devices are running the newest major version."**

Top 10 app categories for malware

In 2017, 27 percent of malicious apps were found in the Lifestyle category, followed by Music & Audio with 20 percent.

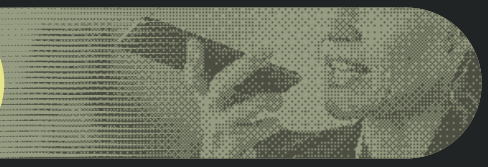
Category	% Malware
Lifestyle	27%
Music & Audio	20%
Books & Reference	10%
Entertainment	6%
Tools	6%
House & Home	5%
Education	4%
Art & Design	4%
Photography	3%
Casual Games	2%

2017 Notable events in the mobile threat landscape

JAN

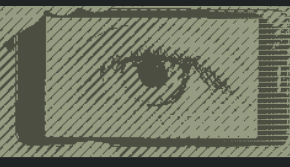
- Ransomware adopted banking malware's social engineering tactics to circumvent new permission model introduced in Android Marshmallow (6.0).

FEB



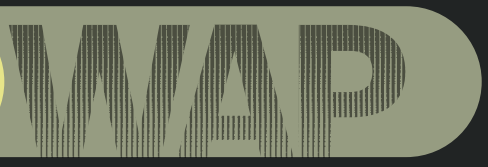
- Ransomware using voice recognition, forcing victims to speak the unlock code instead of typing the key.
- Ransomware using social messenger apps with integrated payment SDKs to facilitate barcoded payments.

MAR



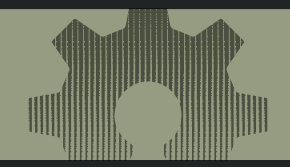
- MobileSpy family of threats using reactive tools to hook into events, such as SMS text received, to trigger other actions and commands remotely.
- Wide availability of mobile malware toolkits help to automate the creation of new variants of malicious mobile apps in large volumes.

APR



- Rise of WAP billing Trojans spawn the next generation in Premium Service Subscription scams by silently visiting WAP service subscription pages and automating the sign-up process, subscribing the victim to the paid-for services without consent.

JUL

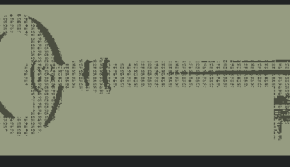


- Rootnik family begins using open-source VirtualApp engine to create a virtual space within the Android device that is used to install and run APKs without any contstraints.

AUG

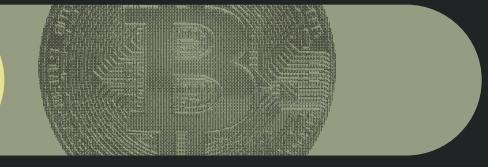
- Devices infected with Adclicker were turned into distributed denial of service (DDoS) bots that were commanded to repeatedly visit specific target URLs.

SEP



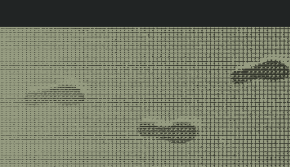
- Banking malware variants found to be using StackTraceElements API to derive decryption keys at runtime.

OCT



- Rise of fake mobile apps with embedded JavaScript-based cryptocurrency miners.

NOV



- Android.Fakeapp variant stealing credentials of online aggregate service providers, covering up the trail by launching legitimate apps using mobile deep-linking URIs.

Notably, with 99.9 percent, the clear majority of discovered mobile malware was hosted on third-party app stores.

Grayware is made up of programs that do not contain malware and are not obviously malicious, but can be annoying or harmful for users. Examples include hack tools, accessware, spyware, adware, dialers, and joke programs. Like malware, grayware has also continued to increase in volume in 2017.

Number of mobile grayware variants identified

	2016	2017	Change
New Mobile Grayware Variants	3,055	3,655	20%

Number of mobile grayware families identified

The number of new mobile grayware families grew by 5 percent from 188 in 2016 to 198 in 2017.

	2016	2017	Change
New Mobile Grayware Families	188	198	5%

Percentage of apps that leak sensitive information

While not considered malicious, grayware nevertheless presents potential privacy issues for users. We found that 63 percent of the grayware apps in 2017 leaked the phone number and 37 percent revealed the phone's physical location.

Type of Information Leaked	Percentage
Phone Number	63%
Location Info	37%
Installed App Info	35%

Cryptocurrencies and other new vectors for monetization

The goal of the vast majority of mobile malware is revenue generation. Traditional means of revenue generation have included premium rate SMS attacks, where attackers co-opt victims' mobile devices to send paid text messages and collect the revenue, or adware, where attackers collect attribution for ad impressions and app downloads, either by forcing the user to view web pages or download content. Infostealers allowed attackers to harvest personal data from mobile phones which could then be traded in underground markets.

In recent years, attackers have turned to ransomware on mobile phones where profits are made by locking devices or by encrypting personal data and extorting a ransom payment from the victim to allow them to regain access. In 2017, a number of mobile apps emerged that allowed attackers to generate their own ransomware in an automated fashion, lowering the barrier to entry for cyber criminals. Another innovation was the use of voice-enabled ransomware. Rather than having the user key in an unlock code, this ransomware contains a speech recognition module which allows the victim to say the unlock code. The payment methods have also evolved, with some ransomware variants accepting payment from barcodes from social media apps.

> **"Notably, with 99.9 percent, the clear majority of discovered mobile malware was hosted on third-party app stores."**

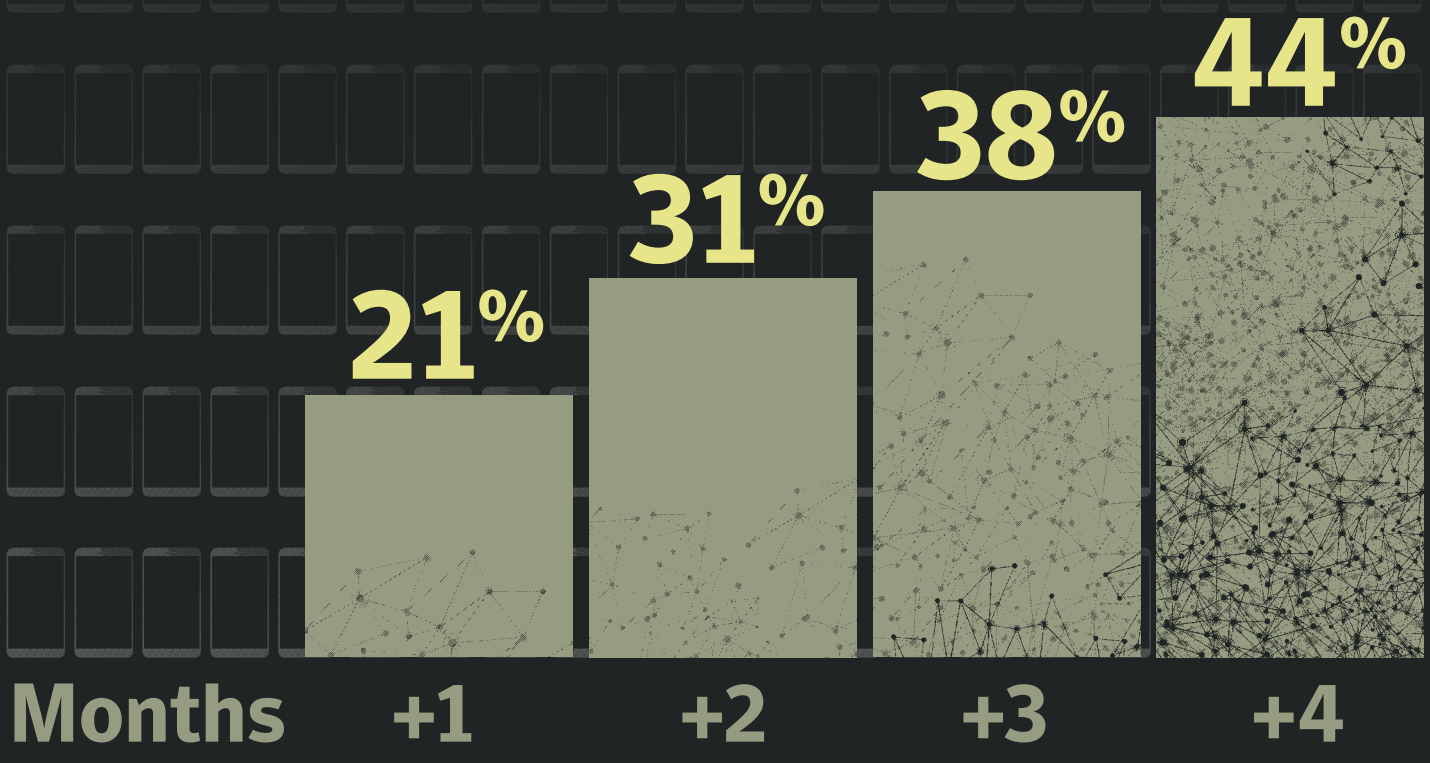
Mobile devices also weren't immune from the cryptocurrency coin-mining explosion of 2017. While mining Bitcoin isn't profitable on mobile devices, Monero provides a lighter alternative means of coin mining and we identified a number of fake apps in 2017 packaged with functionality for mining Monero.

User behavior and security profiling

Keeping up-to-date

Analysis of Android mobile devices that are on the latest major version, e.g. 7.x or 8.x for 2017, reveals that 20 percent of devices are on the latest major release, and only 2.3 percent are on the latest minor release. Although only 1 in 5 Android mobile devices are kept up-to-date with the latest major release, this is an increase compared with only 15 percent (1 in 7) for 2016. It is a difficult gap to close however, since many older devices will never be powerful enough to run the latest version and currently 80 percent of Android devices are lagging the latest major release.

Cumulative exposure to network threats



Percentage of Android devices running newest version of OS

	2016	2017
Android Devices on Newest Major Version	15.0%	20.0%
Android Devices on Newest Minor Version	11.8%	2.3%

Percentage of iOS devices running newest version of OS

	2016	2017
iOS Devices on Newest Major Version	79.4%	77.3%
iOS Devices on Newest Minor Version	24.0%	26.5%

The story is a little different for iOS™, as we see approximately 77.3 percent of iOS devices using the latest version, and 26.5 percent using the latest minor version. iOS updates are rolled out much more quickly as they are not dependent on a carrier making the updates available for their devices on their network, often with bespoke changes required before doing so. Interestingly, although this figure is higher on iOS than for Android, the number is in decline since 2016, when 79.4 percent of iOS devices were patched to the latest major version, and 24 percent were at the latest minor release.

Cumulative exposure to network threats over time

We analyzed the scale of the potential threat from devices being exposed to insecure networks over a longer period. As can be seen, the effect becomes cumulative over a longer period. For example, typically 21.2 percent of new devices were exposed to network threats in their first month of use. This figure rises to 43.7 percent after four months. In this model, a network threat may be something such as a malicious man-in-the-middle (MitM) style attack.

Such an attack may be used to intercept and decrypt SSL traffic, or to manipulate content in transit to or from the device. Sometimes this can be down to a misconfigured router that can expose certain data. Regardless of intent, individuals and organizations would be wise to avoid any network that does not accurately and securely perform the connection services originally requested by the user and the device.

Jailbroken and rooted devices

The act of "rooting" an Android device, or "jailbreaking" an iOS device, is a means by which the user can gain greater control over the device and bypass certain security controls enabling access to more personalization options and functions which are otherwise blocked by the operating system. This activity has decreased in recent years as newer versions of operating systems now provide increased functionality. However, because of the power it can offer an attacker, jailbreaking or rooting a compromised device is still a goal, and monitoring for such activity can often reveal it as an indicator of compromise.

"Regardless of intent, individuals and organizations would be wise to avoid any network that does not accurately and securely perform the connection services originally requested by the user and the device."

Ratio of devices that are jailbroken or rooted, by year and by operating system

	2016		2017	
	iOS	Android	iOS	Android
Enterprise	1 in 10,839	1 in 254	1 in 14,351	1 in 1,589
Individual or Consumer	1 in 694	1 in 92	1 in 1,658	1 in 281

Additionally, in 2017, 1 in 107 devices were identified as high-risk, including rooted or jailbroken devices and devices considered to have high certainty of malware apps installed, compared with 1 in 65 for 2016.

Percentage of devices that have passcode protection enabled by operating system

In 2017, approximately 1 in 20 enterprise devices were not protected with a passcode, and this number rises to 1 in 10 for consumers.

	2016	2017
Enterprise	84.1%	95.2%
Individual or Consumer	70.0%	90.5%

Percentage of devices that have encryption enabled by operating system

In relation to encryption, we can see the proportion of Android devices not being encrypted is falling, but it is still at a considerably high level.

Android Only	2016	2017
Enterprise	57.8%	43.1%
Individual or Consumer	57.7%	45.5%

iOS provides encryption by default, as has Android in recent years. However, it is still a potential risk for older versions of operating systems, if they are still in use and remain unencrypted. Encryption is key to ensuring data on a device is not exposed if it becomes lost or stolen.

Recommendations

Since user behavior is such a huge factor in mobile security, user education is one of the most important things an organization can do to minimize the threat posed by mobile devices. Users should know to only install apps from the primary app stores, and don't click on untrusted links or approve device permissions and accesses without good reason.