Skycure

Mobile Threat Defense

Mobile Threat Intelligence Report

Q1 2016

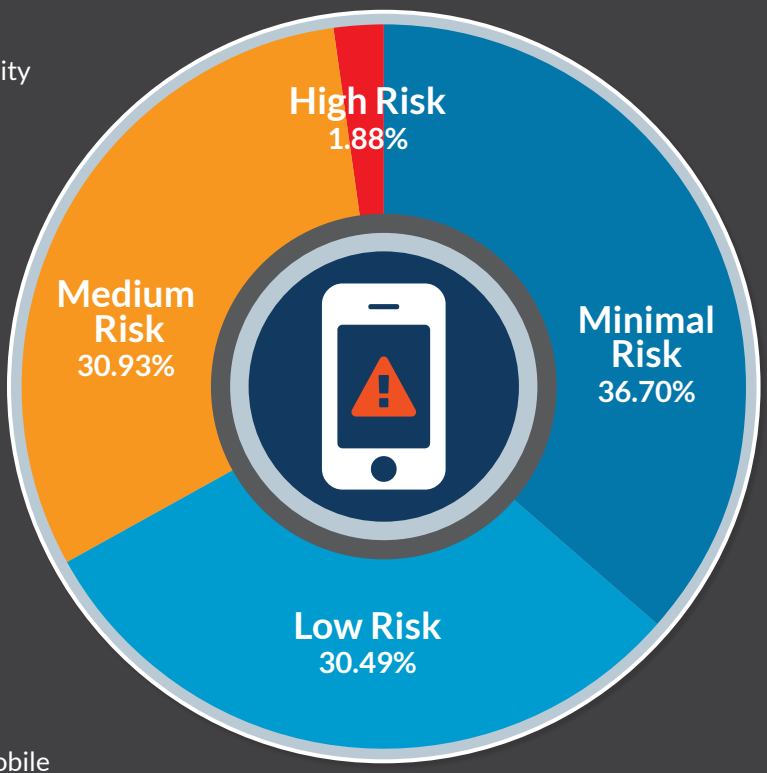
Overview

Mobile malware has been around almost as long as mobile apps, but the worst malware of today is no longer just an annoying inconvenience to the user. Malicious hackers are targeting big enterprises for spying, data theft, defamation and extortion, and they have figured out many creative ways to silently take control of the best surveillance and infiltration tool ever created - your smart phone. This study found that 4% of all mobile devices have malware.
Note: This investigation is based on millions of monthly security tests from January through March 2016 and includes both unmanaged devices and those under security management in enterprise organizations.

One-third of devices have medium to high risk of data exposure

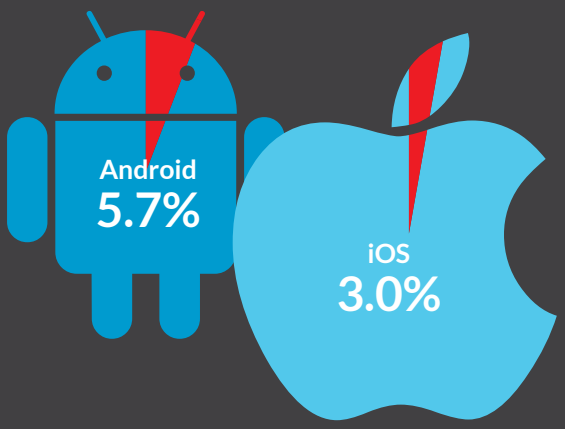
The most valuable information any enterprise security IT professional can know is how much risk their organization is exposed to and where the highest risks exists. Unfortunately, when it comes to mobility, most could not even tell you if they have had a mobile breach, let alone what the steps are to remove the threat and protect the enterprise. Without this essential visibility, security admins are truly flying blind, with no way to identify, quantify or mitigate the risks in their mobile ecosystems.

The first priority when tackling mobile security in the enterprise is to identify the highest risk devices and either remove the threat on the device or remove that device's ability to access critical corporate resources. The devices with the highest risk almost always have high-severity malware installed, so this special report will focus on the nature and prevalence of mobile malware in the enterprise. The enterprises studied in this report show almost 2 percent of devices rated at high risk of exposing sensitive corporate data. Although that seems like a small number, note that a single breach may be sufficient to destroy a company's reputation or competitive advantage.



Data Exposure Risk

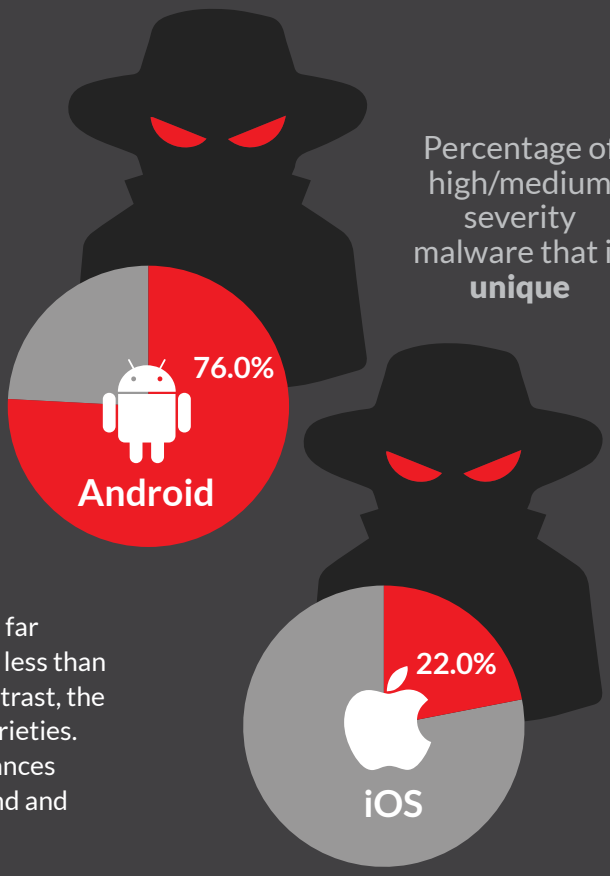
Android devices nearly twice as likely to have malware



Percentage of devices in organizations that have **high/medium severity malware**

This study shows that Android malware is still more prevalent than iOS malware in enterprise, even though U.S. enterprise users are still more than twice as likely to carry an Apple device than one running Android. In fact, in large organizations (those with more than 200 devices) existence of mobile malware is almost assured. BYOD continues to be a driving force in enterprise mobility strategies, which means that locked down and fully controlled mobile devices are limited to only specific business use cases, while the majority of devices are purchased and managed by the employees. This means that many organizations have no control over what apps get installed on the device. Users are very likely to install malware that gets carried into the workplace, and enterprises must find non-intrusive ways to manage mobile security, without hindering productivity or violating the privacy of the users.

Android Malware comes in many varieties

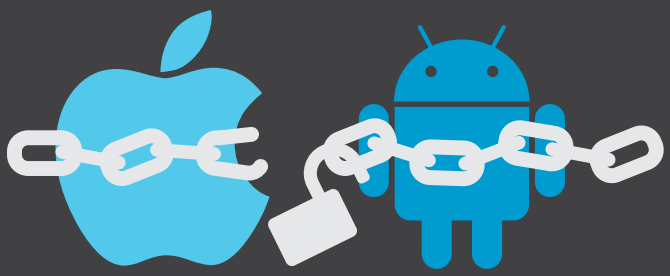


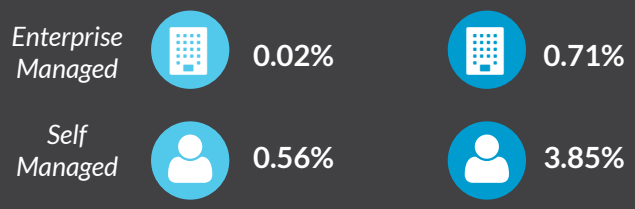
Percentage of high/medium severity malware that is **unique**

There is a greater variety of Android malware compared to iOS in organizations. Hackers still seem to find many more different ways to infect Android devices with malware than iOS devices. For Android, it is much simpler to create and distribute malware, so there are naturally a large variety of malware instances. iOS, on the other hand, tends to be more difficult, so once a method is found, it is more likely to be used repeatedly, resulting in less variety. Although the study indicates total instances of malware are dramatically on the rise for both operating systems, the variety of malware is far greater for Android, with the number of unique iOS malware less than one quarter of the total amount of installed malware. By contrast, the total quantity of Android malware consists of 76% unique varieties. In fact, enterprises have on average more than 3 unique instances of malware, so don't expect to be safe from malware if you find and remove only one variety.

Jailbroken/Rooted

Rooting an Android device, or Jailbreaking an iOS device, is a way for the user to gain greater control over the device, allowing better access to system files and enabling greater personalization and functionality of the device that wouldn't otherwise be allowed by the operating system as designed. Users will do this to their own phones to improve their productivity or enjoyment of the device, but this has become less common than it once was, as newer operating systems naturally allow some of the functionality that could previously only be achieved through rooting or jailbreaking.



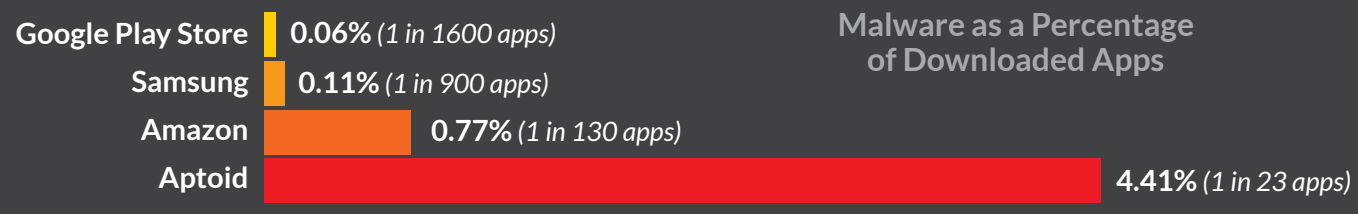


Percentage of **Jailbroken or Rooted Devices**

Because of the greater control over the device that this affords, it is a common goal of hackers to figure out ways to root or jailbreak devices, and malware is a common way to do that. A user that roots or jailbreaks their own device should be aware that they may be simply making it easier for hackers to exploit, so it is not generally recommended.

One in five (19.3%) Android devices in enterprises allow app installation from third party stores

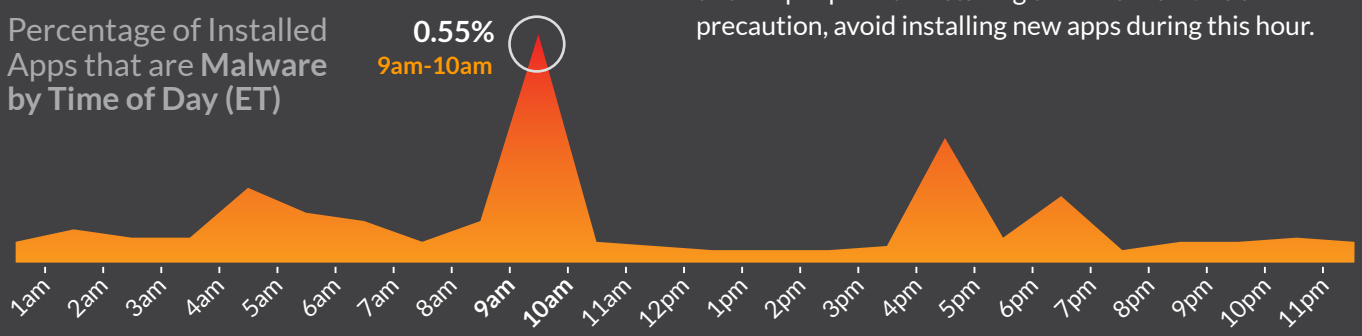
More than 19 percent of enterprise Android devices in the study still allow app installation from third-party stores, despite a system-level setting to turn off this feature. According to the study, this could be a big problem for organizations because third-party app stores are much more likely to deliver malware. The Google Play store is by far the safest place to get Android apps, with only one in approximately 1600 apps being malware. Users are nearly twice as likely to download malware from the Samsung store and more than 12 times more likely to find malware at the Amazon store. Other Android stores may be far riskier, such as Aptoid stores, which are 72 times more likely to deliver malware, representing one out of every 23 apps!



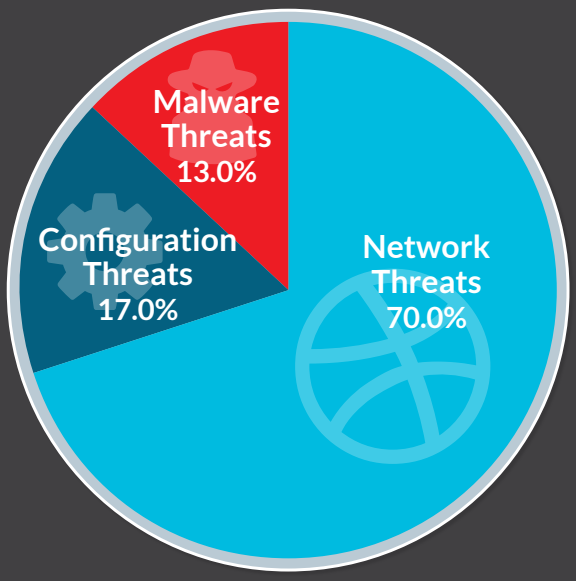
Average number of apps installed on an Android device: 213

Worst hour of the day to install apps: 9-10 am EST

Although app installation rates around the world remain relatively flat across the day, with slightly more during working hours in the US, the ratio of malware installations during the 9:00-10:00am (Eastern Time) hour is as much as 10 times the rate of other hours during the day. Malware incidents are best identified at the time of installation, before they can do any real harm, using traditional or advanced detection methods. This seems to be a common time for hackers to deploy social engineering methods to trick people into installing their malware. As a precaution, avoid installing new apps during this hour.



Network incidents 5X more likely than malware incidents



Type of **Threat Incidents**

Many mobile security solutions focus entirely on identifying and protecting devices from malware. With so much focus in the industry on mobile malware, it is easy to forget that this is only one source of attack that malicious hackers use. In fact, data from this study shows that network incidents are 5 times more frequent than malware incidents. Diving deeper into the network threats, the study found the largest number of threats from SSL Man in the Middle attacks, which intercept and decrypt communication between two systems. The second largest threat came from content manipulation attacks, in which hackers may alter part of a website to lure victims to perform desired actions through a manipulated interface or in a third-party system. This study also evaluated configuration vulnerability incidents, such as not having a lock screen passcode or allowing installation of apps from third party app stores. Of these three types of incidents, 70 percent in the study were network-based incidents, 17 percent came from configuration vulnerabilities, and only 13 percent of incidents came from malware.

Consider, however, that while network incidents may represent a mixture of malicious intent and unintentional exposure of sensitive information, **malware is almost always malicious and deliberate.**

Ransomware

Ransomware, primarily of the screen-lock variety, has been prevalent on PCs for some time, and started migrating to the Android operating system starting in late 2014, continuing to increase in frequency through the current quarter. In addition to screen-lock ransomware, crypto-ransomware is becoming far more popular, where content is encrypted and unrecoverable even if the victims are able to access the files. With more data, including corporate data like emails and documents, and personal data like photos, stored on mobile devices than ever before, this is becoming a lucrative and more common exploit to be aware of.

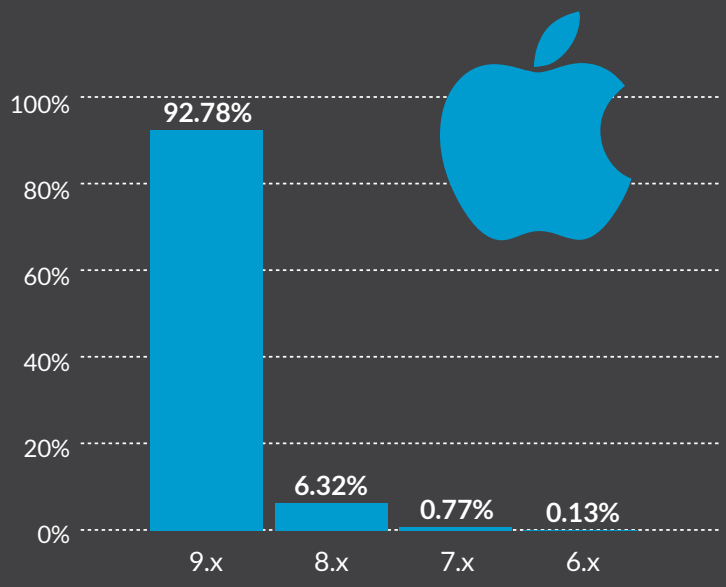
Accessibility Clickjacking, an Android vulnerability identified by Skycure Research Labs during the period of this study, may be leveraged in a ransomware attack. A simple malware app is created to take advantage of the Accessibility Clickjacking vulnerability, which in turn grants the hacker almost unlimited visibility and access into the device, including the ability to acquire administrative rights and proceed with data encryption and/or device lockout.

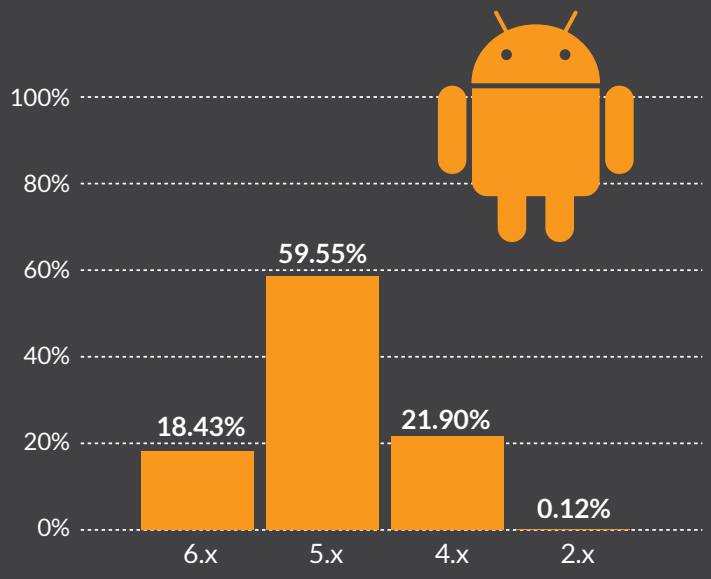
Broad, spam-based attacks of ransomware are also giving way to a greater number of precision spear phishing attacks that are well researched to target specific executives and other individuals in positions of power that are more likely to pay large sums of money to protect valuable corporate or personal information that may be devastating if exposed. In the case of enterprise executives, it may be the company itself that is willing to hand over the money to recover its proprietary information or keep it from public exposure.

OS versions

There are multiple security patches added into every new release of iOS and Android to fix vulnerabilities that have been discovered in the operation system or system apps, so newer versions of each operating system are generally more secure than the previous ones. iOS users will generally move to newer operating systems very quickly because the hardware is standardized and inherently compatible with each new version (excepting very old hardware). Android, on the other hand, is more fragmented and hardware dependent, so variations of each new operating system must be created for each platform, delaying and staggering the availability of each new version according to the destination hardware platform, leading to slower and less consistent adoption.

When vulnerabilities are discovered by malicious hackers, they may be pathways into the device that allow data theft, spying, or even complete takeover of the device. Depending on the vulnerability, there are a number of ways a hacker might exploit it, ranging from sending a simple text sequence to the device to take advantage of an SMS vulnerability, to creating elaborate malware that provides a continuous stream of audio, visual and textual information from the device and allows the hacker to remotely control the device and communicate with others on the user's behalf. Upgrading to newer operating systems as soon as possible is a good way to increase security and limit the hacker's options.

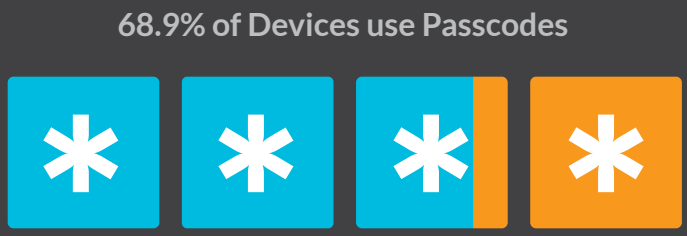




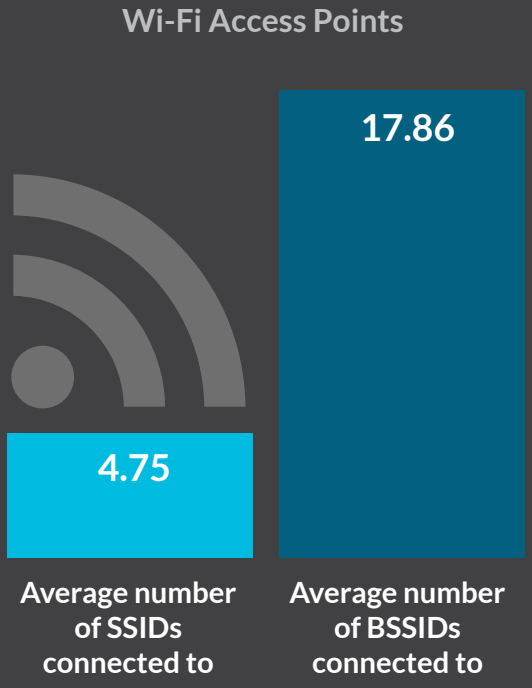
OS Versions in Use

And the Essentials...

31% of devices still do not use a lock screen passcode



The study found 68.9% of devices surveyed do have a passcode set to protect access to content on the device, or content that may be accessed through the device. Many companies using MDM to manage mobile devices will mandate the use of a passcode in order to be compliant with corporate policies. Since BYOD has become the predominant strategy for organizations, this will drive up the use of passcodes for these same personal devices. Plus, it seems more people are choosing to use a passcode on their personal devices even when not required to do so by their company.



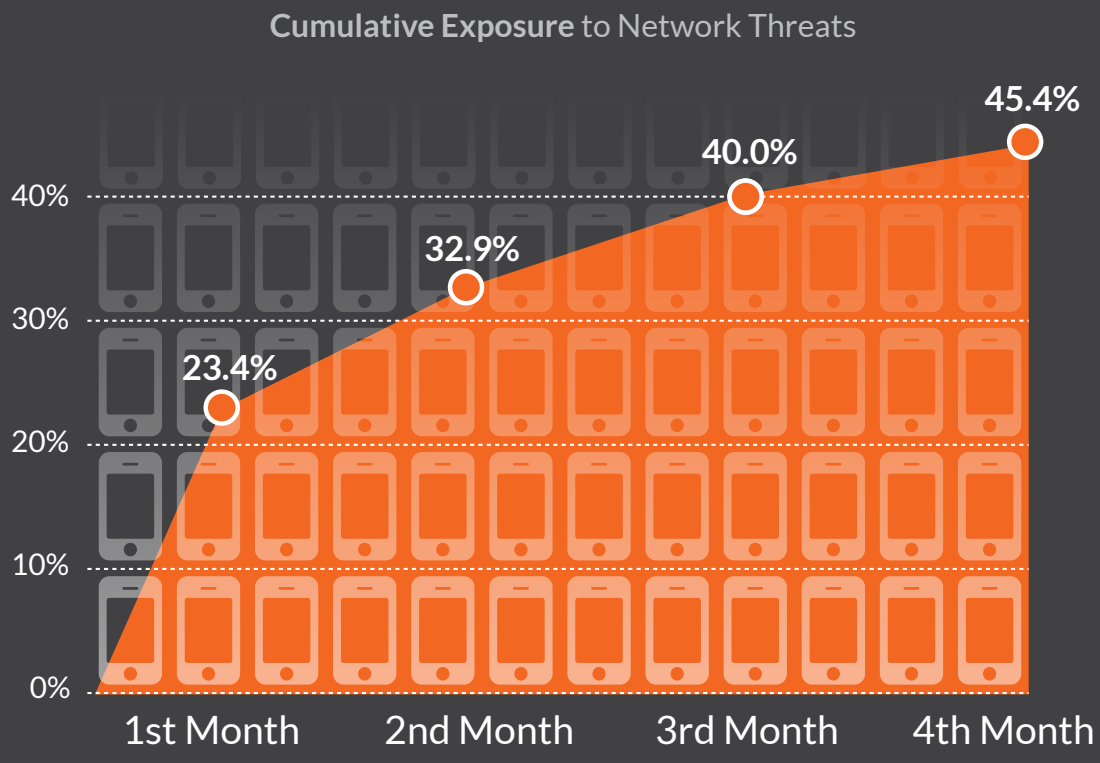
Mobile devices connect to many access points

Over the 3 months of data collection, the average number of network names (SSIDs) connected to for each mobile device was 4.75. Named networks may have multiple access points deployed, each with a unique identifier (BSSID). The average number of unique Wi-Fi access points (BSSIDs) connected to per device during this period was 17.86. A mobile device will automatically authenticate to a new BSSID of the same name without prompting the user. Malicious hackers will use this behavior to their advantage by setting up an access point with the same name and authentication as a legitimate network, such as a common airport or hotel Wi-Fi. A device may join the malicious network, assuming it is one previously authorized, allowing passwords and data to be stolen even if the user does nothing and is unaware of the connection.

The Essentials...continued

Devices exposed to network threats over time

In any typical organization, about 23% of the mobile devices will be exposed to a network threat in the first month of security monitoring. This number goes to 45% over the next 3 months. A network threat may be a malicious Man in the Middle (MitM) attack that decrypts SSL traffic or manipulates content in transit to or from the device. It can also be a simple misconfigured router that exposes otherwise encrypted data for anyone to view. Regardless of how malicious the intent of the network threat is, 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.



Recommendations

Mobile malware is a challenge every enterprise security team faces today. Organizations looking to defend their mobile ecosystems from such threats should follow advice from the major EMM vendors, which all recommend adding a Mobile Threat Defense solution to protect valuable corporate data that may be accessed from mobile devices. Traditional approaches that leverage standard static and dynamic methods alone are good, but not enough to detect malware created with the new methods hackers are devising every day. The SANS Institute suggests a strategy that builds on this traditional approach by adding multiple layers of threat intelligence and advanced analytics. In addition to the local threat information collected and analyzed on the device, organizations can benefit from crowd-sourced threat intelligence from many distributed devices and additional server-side analysis to identify and protect enterprises even from sophisticated malware that bypasses classical detection methods.

About the Mobile Threat Intelligence Report

The Skycure Mobile Threat Intelligence Report reviews worldwide threat intelligence data. This report is based on millions of monthly security tests from January through March 2016 and includes both unmanaged devices and those under security management in enterprise organizations. Data includes Skycure's proprietary Mobile Threat Risk Score, which acts as a credit score to measure the risk of threat exposure for mobile devices. For organizations, Skycure condenses millions of data points to calculate a risk score so that IT can quickly discern the state of the overall system and the risk to each device.

About Skycure

Skycure is the leader in mobile threat defense, detecting and preventing cyber attacks without compromising the user's privacy or mobile experience. Skycure's predictive technology uses a layered approach that leverages massive crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits. Skycure Research Labs have identified some of the most-discussed mobile device vulnerabilities of the past few years, including Accessibility Clickjacking, No iOS Zone, Malicious Profiles, Invisible Malicious Profiles, WifiGate and LinkedOut. The company is backed by Shasta Ventures, Pitango Venture Capital, New York Life, Mike Weider, Peter McKay, and other strategic investors.