Skycure
Mobile Threat Defense

Mobile Threat Intelligence Report

Q1 2017

10 YEARS OF (HACKING) IOS

THE IPHONE LAUNCHED A REVOLUTION IN ENTERPRISE IT

This report seeks to expose the security impact of iOS in the enterprise at this 10-year anniversary of the iPhone. The original iPhone was not designed or intended to upend the world of Enterprise IT. And yet, here we are. Although Android is by far the more popular platform globally, iOS is still favored by US corporate and government executives, incentivizing hackers to spend a disproportionate effort to identify and exploit iOS vulnerabilities for theft and espionage. Consequently, security is still the primary resistance to mainstream adoption of enterprise mobility.

Apple has always been primarily focused on the end-user experience, historically the domain of the consumer market. Previously, enterprise IT did not have to worry too much about how happy their users were with the devices they were given for work purposes. IT priorities started with standardization and security - keeping costs under control and protecting all of the data inside the company was paramount, and user experience was probably somewhere on page 2. Enterprise users didn't expect anything different, until the iPhone and the App Store started to give them more of the tools they needed to be productive at work as well. Enterprise IT has been playing catch up ever since.

There are two types of data represented and analyzed in this report. First is public historical data covering the ten years since the Apple iPhone was introduced, to provide education and a context of trends leading to today. Second is a study of threats and incidents captured directly by Skycure sensors distributed around the globe during the first quarter, from January 1 through March 31, 2017.

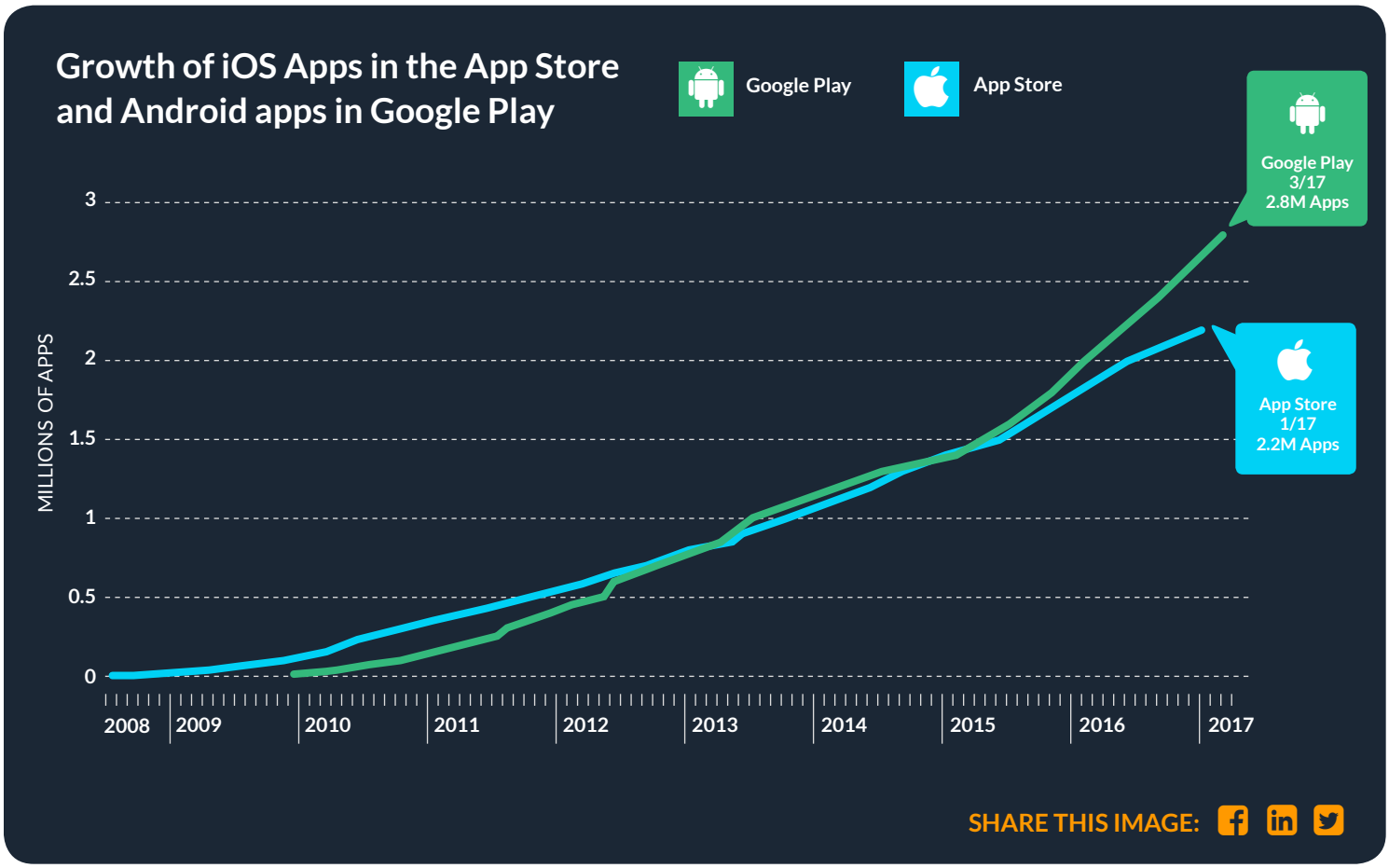
Skycure

THERE'S A (MALICIOUS) APP FOR THAT

Some may be tempted to suggest that Blackberry was the mobile change agent for business work flexibility — but it wasn't. Having access to email and messaging while in the bathroom certainly started a change in work habits, but it wasn't until the iPhone made mobile apps popular that the BIG IDEA started hitting people. "I can be incredibly productive on my mobile device in my personal life — why can't work be the same?" And so it began — the end user revolt and the mainstreaming of shadow IT — long before the term BYOD was invented.

Apple's App Store opened on July 10, 2008 with 500 apps, and today there are over 2.2 million. Initially, this public App Store was the only way to install apps on an iPhone. However, the popularity of the devices in business environments soon prompted Apple to institute the enterprise app concept and the "provisioning profile", which allowed approved organizations (those with a DUNS number and who pay a fee to join the developer program) to manage iPhones and install custom apps that were not made generally available on the App Store. In September of 2010, Apple expanded this offering to approved organizations with less than 500 employees.

This chart shows the growth in the number of iOS apps offered in the App Store, overlaid with the growth of Android Apps in Google Play. Note that although Android started a year later, Android apps surpassed the number of iOS apps in 2013. Unlike iOS apps, Android apps can also be found on other stores, although the Google Play store is the "official" store and has the most apps by far.



Skycure

By allowing businesses to "sideload" apps, installed directly without going through the App Store, Apple created two effects. First, businesses could more easily use the devices for business, leveraging custom apps that were not for public consumption — good. Second, malicious hackers could more easily trick users into installing malware — bad.

The other phenomenon that made it simpler for the bad guys to get malware on devices was "jailbreaking", removing the restrictions imposed by Apple to allow installation of unauthorized software and customization of the interface. Although users intentionally jailbreak their iPhones to give them this flexibility, it also removes the security mechanisms Apple put in place to protect the device and its contents, increasing their exposure to malicious attacks. Forced jailbreaking is now one of the primary objectives of a malicious hack, as it can give unlimited access and control to the hacker. Advanced jailbreak exploits are also getting very good at hiding the fact that the device is jailbroken, increasing the exposure and danger. Enterprises recognized this hazard and started adding policies that prohibited jailbroken devices. Although not always enforceable by EMM alone, in the last quarter, enterprise-managed iOS devices were jailbroken only 0.01% of the time, while self-managed devices were jailbroken 0.32% of the time.

VULNERABILITIES GROW WITH TECHNOLOGY AND FOCUS

With the introduction of iOS (initially called iPhone OS), Apple brought us a new security model for operating systems, an app-centric design with boundaries between apps and limited, controlled access to the kernel. This sandbox approach offers inherent advantages in both security and data privacy over the traditional OS approach found in the PC market. However, software is never perfect, and persistent efforts will uncover flaws that may be used to compromise the system and the data it holds.

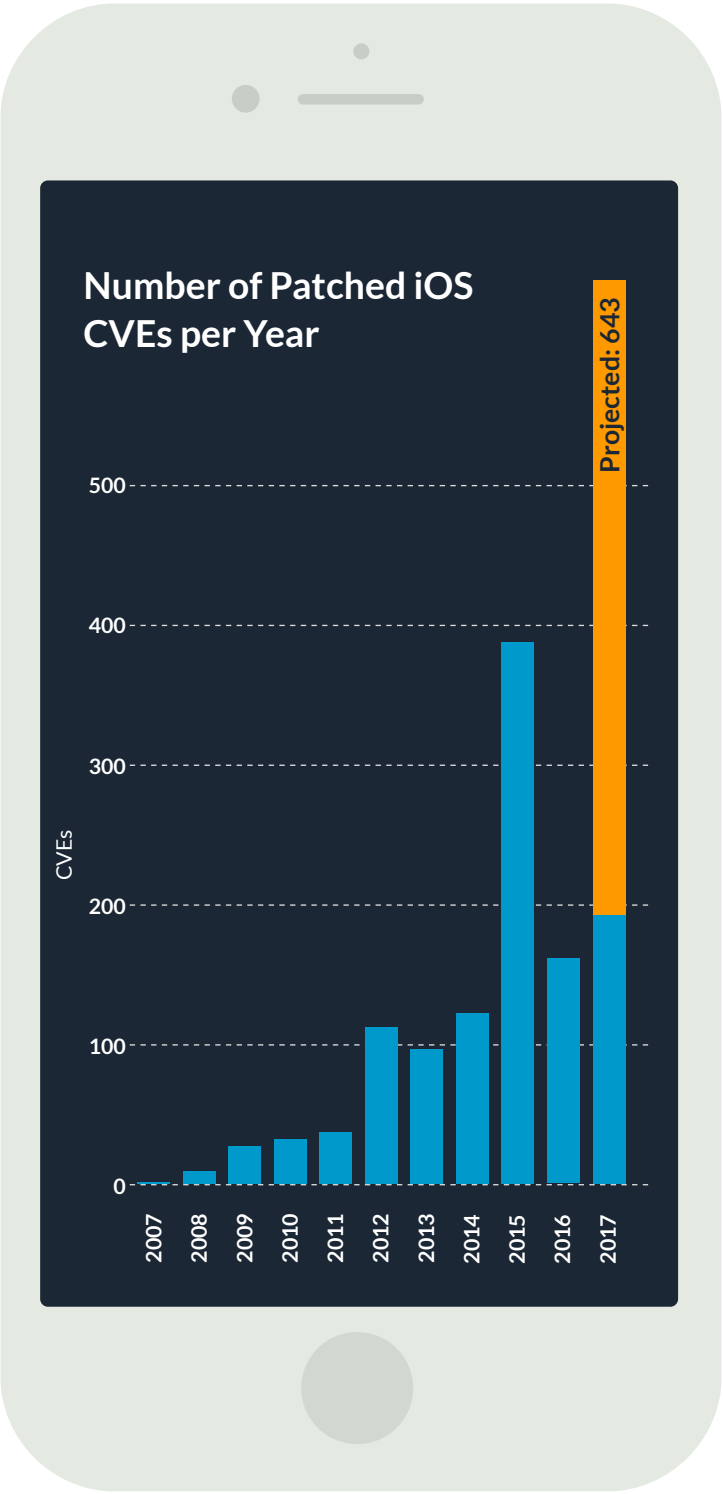
Vulnerabilities are uncovered and patched regularly. As Apple patches each vulnerability, they announce it publicly so that everyone knows what the flaw was in the past versions of the operating system, and has the opportunity to upgrade their device to the newer and safer version. Apple publishes the details of each patched vulnerability in the Common Vulnerabilities and Exposures (CVE) database, hosted by The MITRE Corporation here - **https://cve.mitre.org/cve/cve.html**. Apple publishes the complete set of security updates for each update on their support site here — **https://support.apple.com/en-us/HT201222**, and another site, CVE Details, offers a friendly interface to easily find CVEs by date, platform and other criteria here — **https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html**

Predicting the future, 2017 will be a very big year for iOS vulnerabilities! The number of disclosed vulnerabilities in the first quarter of 2017 was greater than all of 2016.

Note that the number of patched vulnerabilities is NOT an indication of how insecure a platform is, but rather how intensely people attempt to break into the platform. While it seems that eventually all of the vulnerabilities would be identified and patched, that is certainly not the case. The code for an operating system is constantly evolving, with new features, so expect an endless supply of vulnerabilities to find and fix. Note that each CVE also gets a score from 0 to 10 indicating its potential impact on the security of the system, with lower numbers representing less risk and higher numbers representing higher risk. Although the average doesn't seem to change much from year to year (consistently in the 6-7 range), do note that there are a lot more 10s today than there used to be.

The spike in CVEs in 2015 is interesting and also corresponds with a record number of four minor release updates for iOS 8 (ending with 8.4.1), released in October of 2014. Among the patches was a fix for the **No iOS Zone** vulnerability identified by Skycure and released in April of 2015. Here is a list of the highest update released for each major version, a loose indication of the volume of patches required for that version. Note that iOS 10 may still match or surpass this number before iOS 11 comes out later this year.

- iPhone OS 1: 1.1.5
- iPhone OS 2: 2.2.1
- iPhone OS 3: 3.1.3
  (additional iPad releases up to 3.2.2)
- iOS 4: 4.3.5
- iOS 5: 5.1.1
- iOS 6: 6.1.6
- iOS 7: 7.1.2
- iOS 8: 8.4.1← corresponds with CVE spike in 2015
- iOS 9: 9.3.5
- iOS 10: 10.3.1 (as of April 3, 2017)



SHARE THIS IMAGE:

Skycure

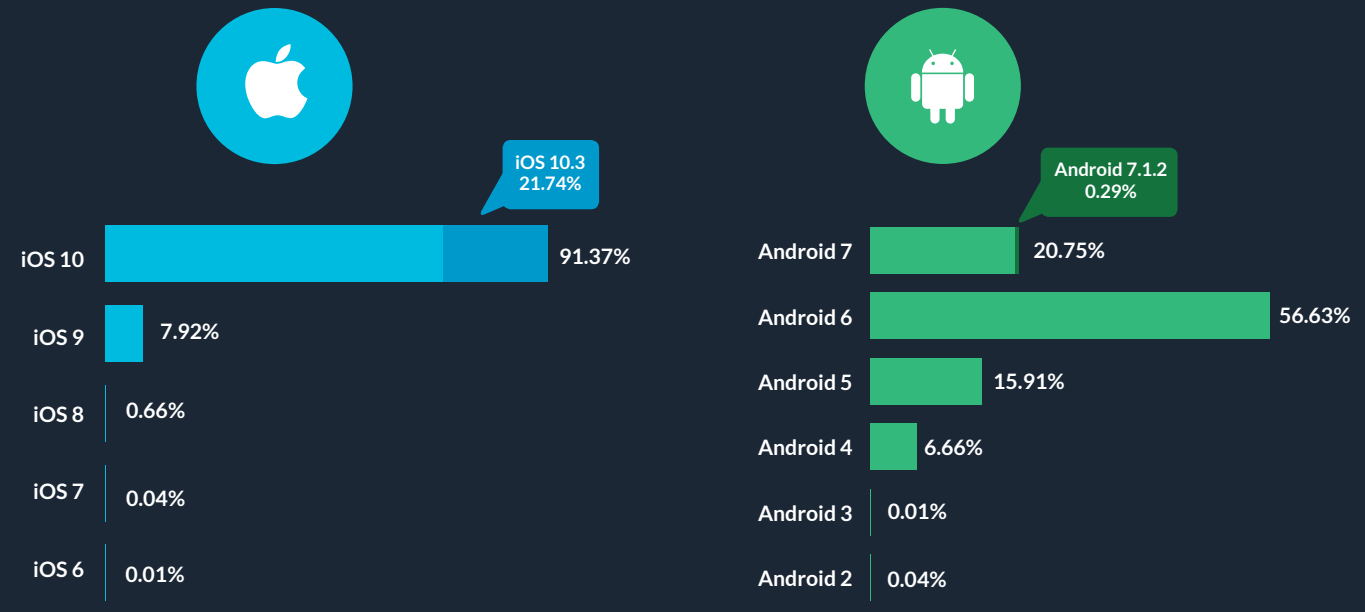
APPLE MAKES SECURITY UPDATES EASY

One of the most important things that can be done to secure a mobile device is to be sure it is on the latest security patch. This eliminates the threat from all exploits relying on previously unpatched vulnerabilities. There is a critical window of vulnerability between the time a patch is released and the time it is installed on the mobile device, during which an attacker can successfully attack these unpatched devices. Because Apple controls the complete vertical chain, from the device hardware and operating system to the app and update distribution channel, Apple does a very good job of making this happen quickly. Impressively, 91% of active devices were on the latest major version (iOS 10), and 22% were already on the latest minor release (iOS 10.3) by the end of Q1.

The window of vulnerability for Android is typically far greater because, although Google releases monthly security updates, it is up to each hardware vendor and each cell phone carrier to create and distribute their own unique versions of each patch, which can extend the window of vulnerability to 6 months or longer.

91% of Active (Apple) Devices are on the Latest Major iOS Version

Percentage of Devices on Each Major OS Version



Reported April 1, 2017

SHARE THIS IMAGE:

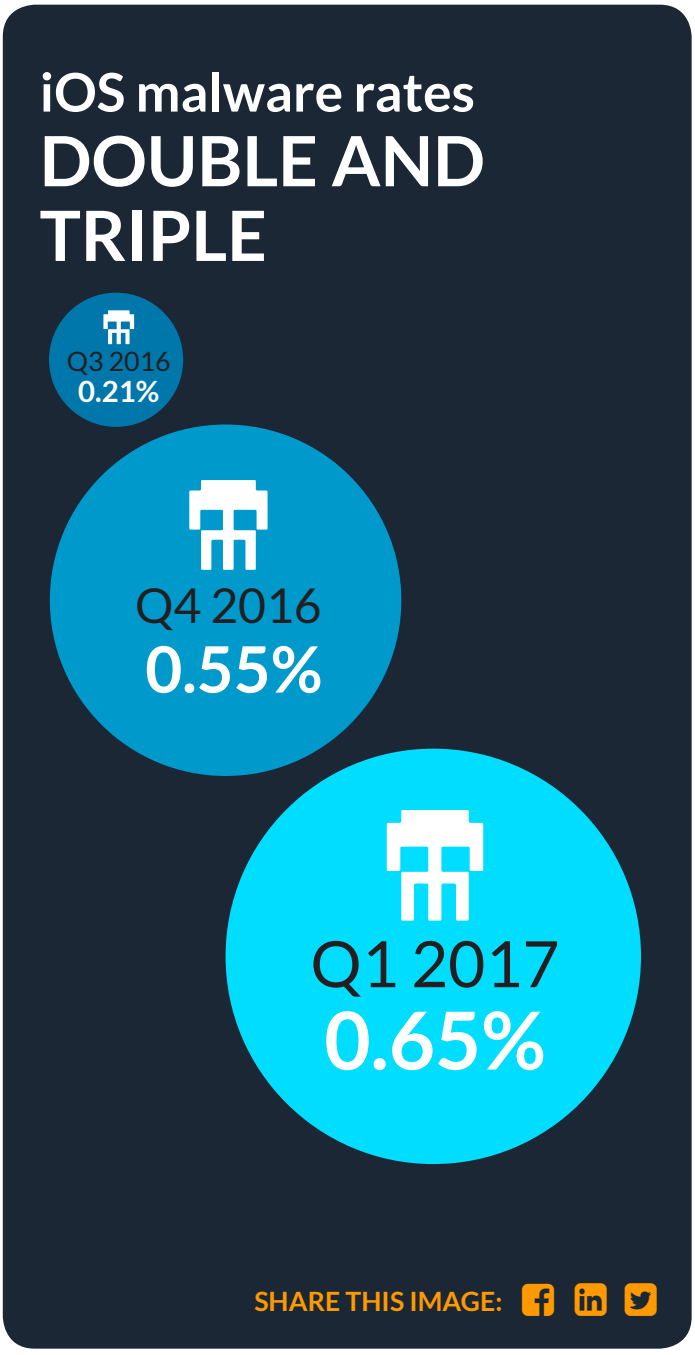
Skycure

iOS MALWARE EXISTS - LOTS OF IT

A common misconception is that iOS devices can't get malware because apps must come from the Apple App Store. In truth, there are many ways to infect an iOS device, including creative ways to get malware into the App Store, as happened with XcodeGhost, where app developers acquired a malicious version of the iOS development environment Xcode through alternate sources, and that development environment inserted malware into the apps without the developer even being aware of it.

Malware on iOS devices is becoming more prevalent as the sophistication of exploits continues to increase. Skycure data from Q1 2017 shows that 0.65% of enterprise iOS devices today have high severity malicious apps installed. This represents a significant increase over the last couple of quarters, increasing threefold compared to Q3 2016. This makes sense, given a marked increase in focus by attackers on high level executives and individuals with access to company finances and financial transactions over the last year. Note that Q4 has historically proven to be a high activity period for malicious hackers, so the growth in infections is far from linear, and even small growth from Q4 to Q1 is notable.

The very first iOS malware found in the wild was called the Ikee-virus, also called Eeki. It was a worm transmitted between jailbroken devices with OpenSSH installed, but still using the default root password. When infected, the lockscreen background changes to a photo of Rick Astley. This is where it all started, a spam-type malware that spread broadly, with an impact that most would put in the annoying category (depending on how you feel about Rick Astley).



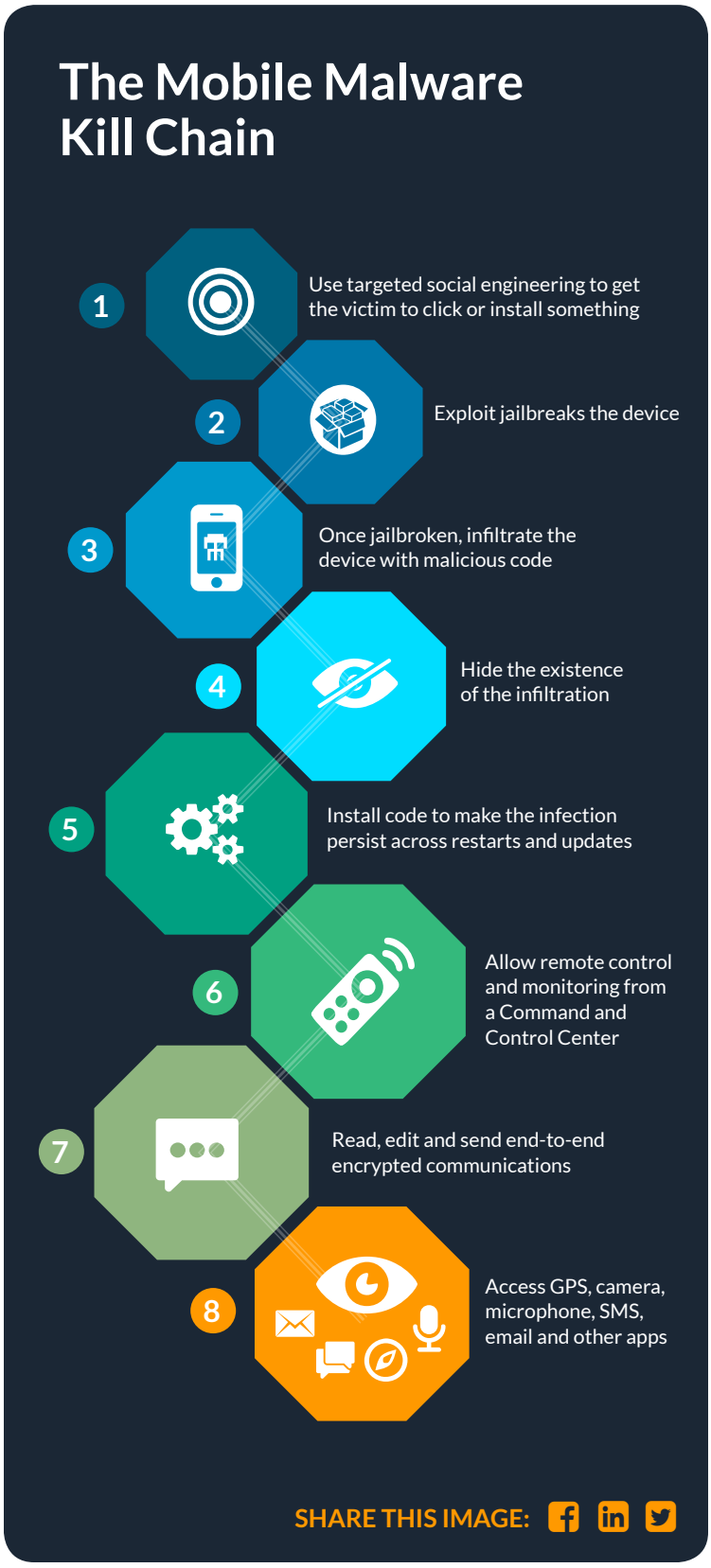
Skycure

Ways to Infiltrate an iOS Device

Here are a few ways to get malware onto an iOS device, along with examples of real exploits that used that method.

SHARE THIS IMAGE:

Skycure



iOS malware started getting more sophisticated, eventually able to infect non-jailbroken devices, like YiSpecter, which abused private/enterprise APIs mentioned earlier in the report to implement malicious functions. The next level was to be able to view and steal data from the device, then control the device remotely as attackers implemented callback functions to their Command and Control centers.

Today, the most sophisticated exploits may leverage multiple vulnerabilities, like Pegasus which uses the three iOS vulnerabilities called Trident, target specific individuals or company executives, and are very good at hiding their presence to extend the period of control or spying access. The motivation is often financial gain or corporate or state-sponsored espionage. Here is a kill-chain process flow of the most dangerous iOS malware today.

With a successful infiltration, the user will not know he has been compromised, and all but the most sophisticated mobile security software will also be unaware of the malware's existence.

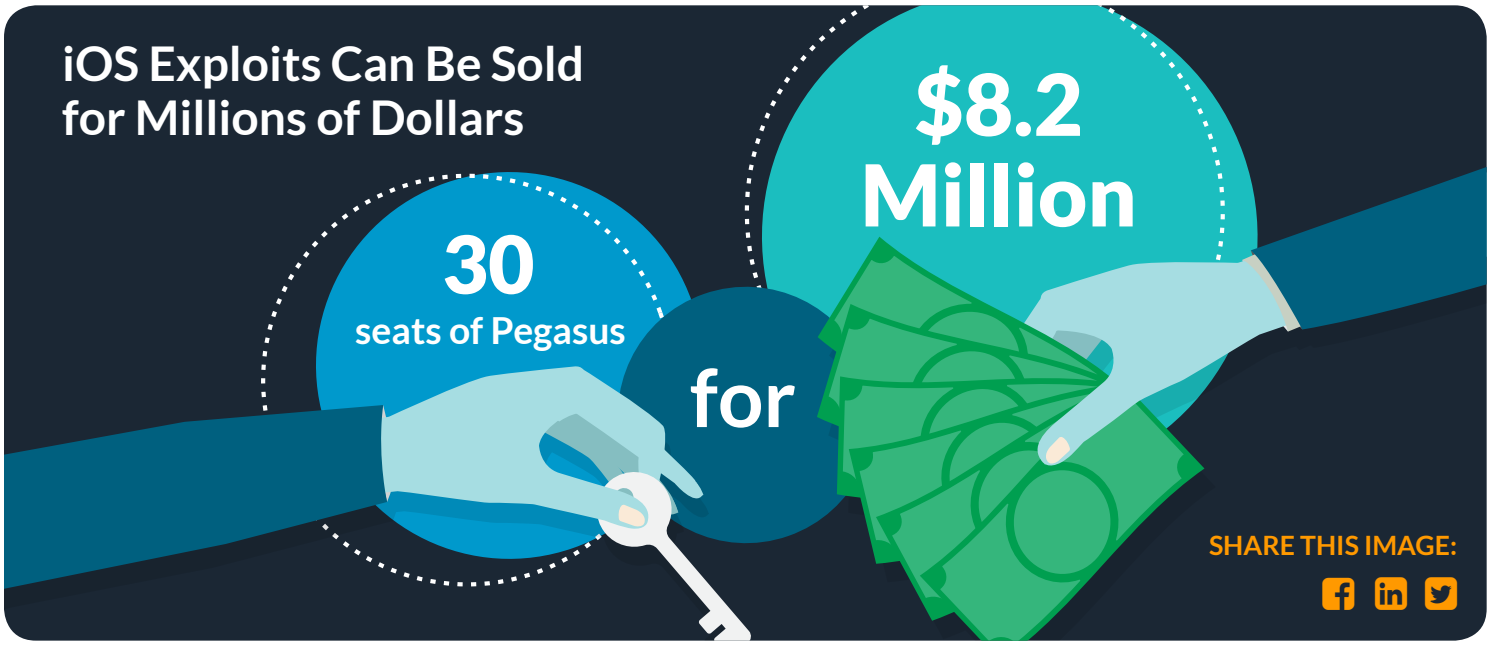
Skycure

THE IMPORTANCE OF AGGRESSIVE 'WHITE HAT' RESEARCH

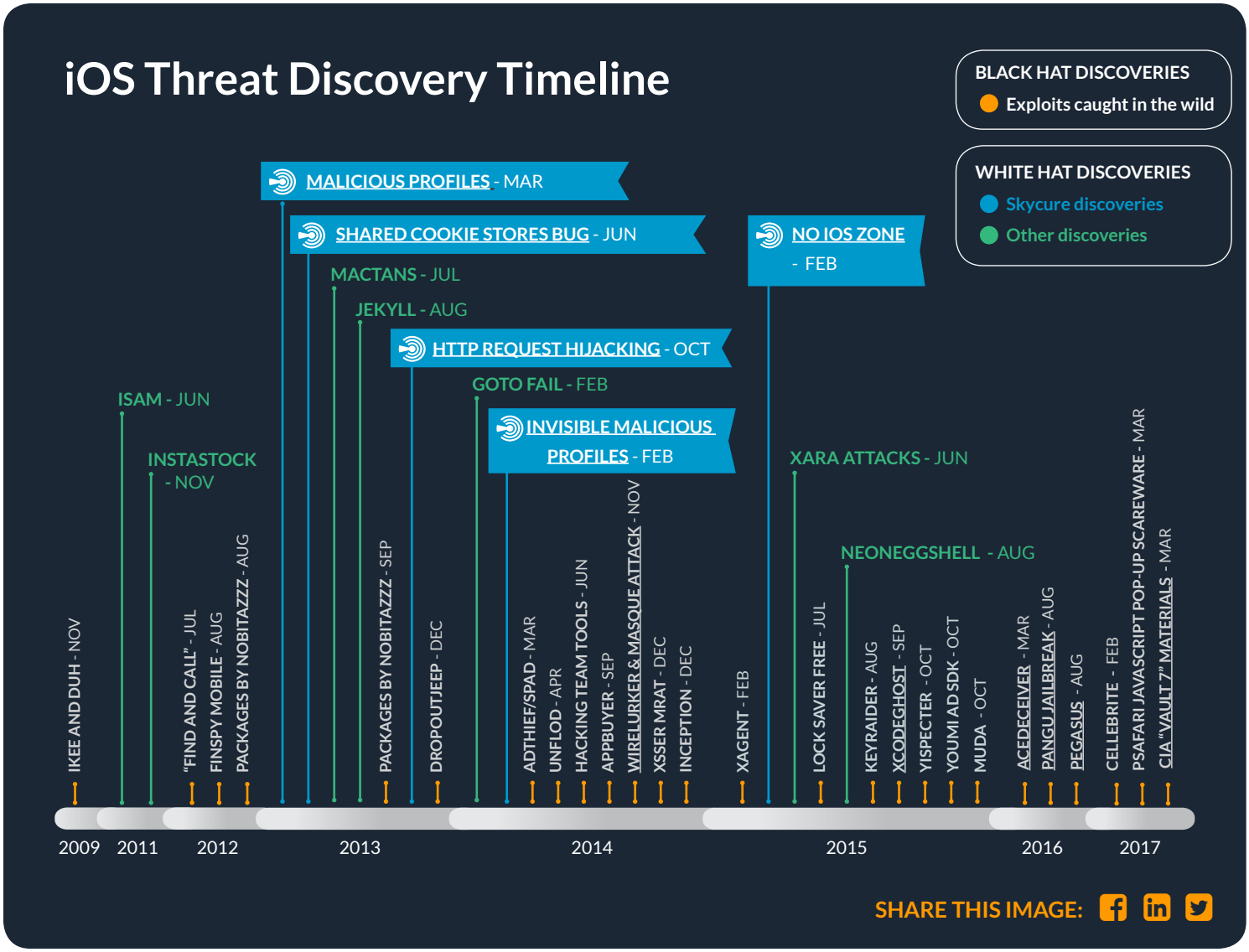
Vulnerabilities exist, whether they have been identified and reported or not, and each one presents a risk to the security of the devices they are running on. If a vulnerability is discovered by someone with good intentions, like a security provider or independent 'white hat' researcher, there is generally a responsible disclosure process that may be followed, where Apple is notified of the discovery and they have an opportunity to patch it before disclosing its existence. By doing this, users and organizations are informed and have the opportunity to upgrade their devices to protect themselves from anyone with bad intentions that may want to exploit that vulnerability. This also presents a hazard, in that a malicious 'black hat' researcher now knows about the vulnerability and may be able to create an exploit that will be successful on OS versions prior to the one with the update. This is why keeping devices on the latest updates is critical to maximize security.

When a black hat researcher, also referred to as a 'malicious hacker' or 'attacker', finds a vulnerability, it is an opportunity to create an exploit and use it to infiltrate susceptible devices. In these cases, Apple is unaware of the vulnerability until after the attacker has successfully deployed the attack. Some exploits are discovered very quickly, after only a small number of devices are impacted, while others may impact thousands or millions of devices first. One of the most advanced attacks on iOS to date is the **Pegasus spyware**, exploiting three separate vulnerabilities to track and spy on the victim and everything that takes place on the device. Three hundred exploit seats were sold for 8.2 million dollars. Apple was only able to patch the Trident vulnerabilities after Pegasus was discovered and reported by an alert victim.

For the most part, vulnerabilities discovered first by white hat researchers are able to be patched before attackers learn about them, and very few of these are successfully exploited in the wild. There may be rare exceptions, where white hats and black hats identify a vulnerability in parallel. Black hat discoveries, on the other hand, are generally identified in the wild after some damage is already done. For this reason, we should be rooting for the white hats to find as many vulnerabilities as they can, as fast as possible, because that reduces the opportunities for attackers.



Skycure



Here is a list of sample iOS malware and the approximate discovery dates, showing both exploits caught in the wild after infecting devices, and research results from white hats that were discovered and fixed before falling into the wrong hands. These are only the most notable exploits and is NOT an exhaustive list. Exploit types include virus/worm, adware, scareware, trojan, ransomware, spyware and others, many of which do not require the device to be jailbroken.

While many of these vulnerabilities are able to be patched in a matter of weeks after disclosing them to Apple, there have been notable exceptions. A vulnerability may be technically very difficult to remedy, or there may simply not be a good way to fix it without adversely affecting some important feature or user experience. The Shared Cookie Stores bug, first reported to Apple by Skycure on June 3, 2013, turned out to be incredibly complicated and took two-and-a-half years to issue a fix.

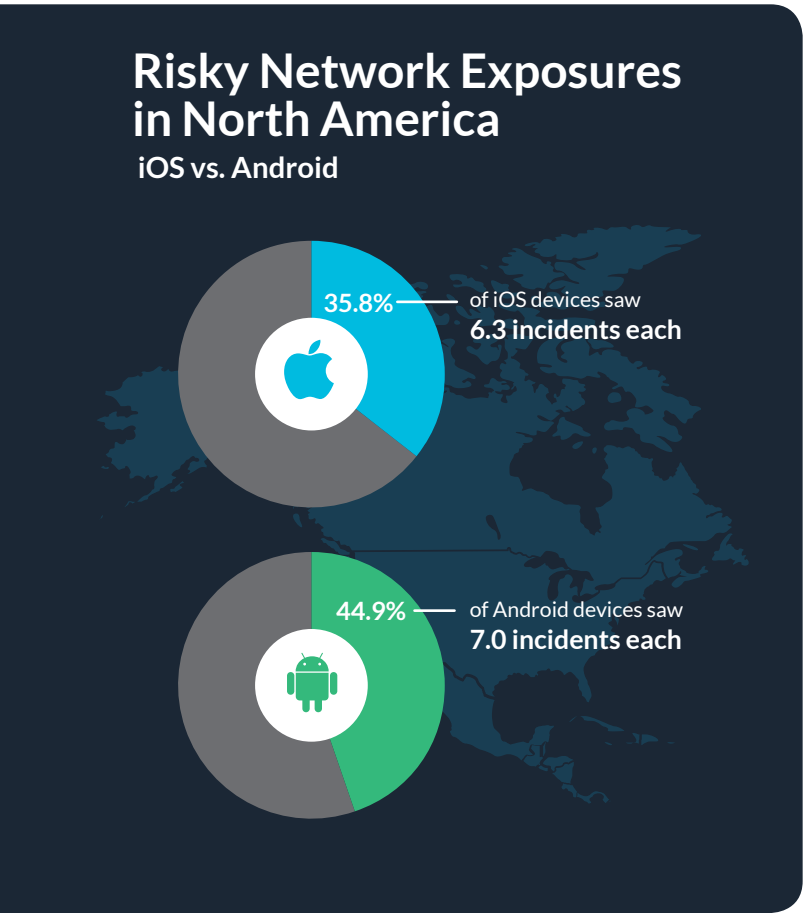
Malicious Profiles falls into the other category - more of a vulnerability by design. Skycure first identified the malicious profiles vulnerability on March 12, 2013. Over the next few years, Apple made several attempts to change the user experience of installing profiles to reduce the likelihood of successful social engineering attacks. With the release of iOS 10.3, Apple made the most significant effort yet to reduce this threat. It is only a partial fix, but requires users to manually enable installation of root certificates in a more cumbersome process, raising the bar for how good a social engineering exploit must be to succeed. This should have a good impact toward reducing the likelihood of such attacks.

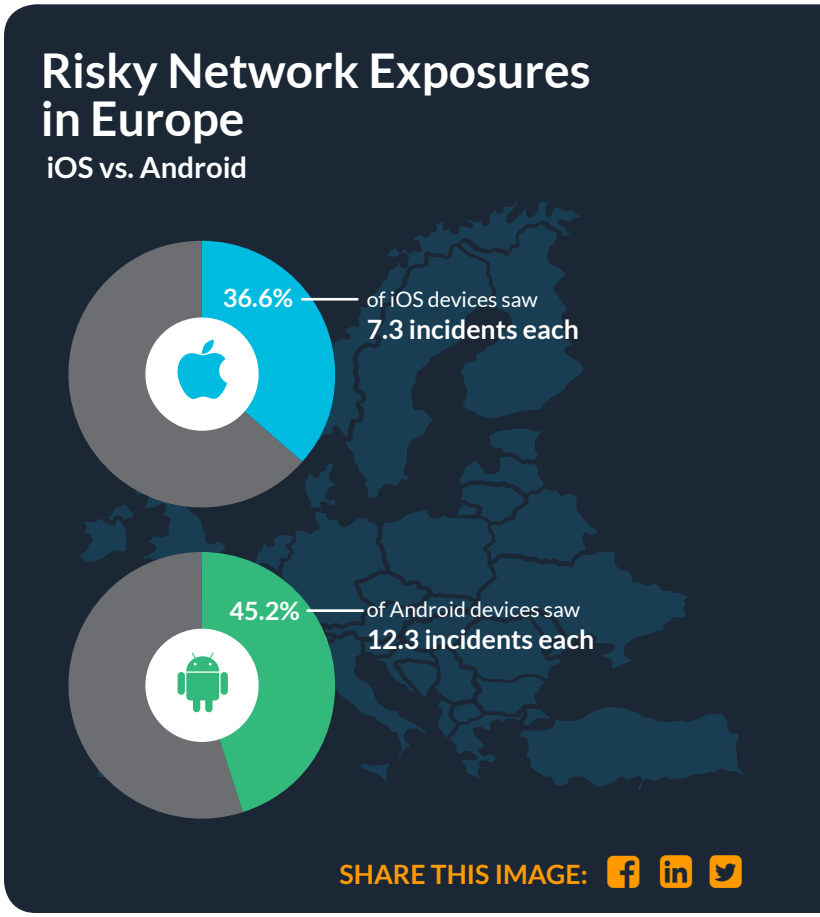
REGIONAL VARIATIONS IN RISKY NETWORK EXPOSURE

At the end of 2016, iOS represented 17.9% of the global mobile device market share, while Android commands 81.7%. Yet in the US, iOS sold 43.5% of the mobile devices compared to Android's 55.3%. This represents a 6.4% increase over 2015 for iOS, stealing most of that from Android. Clearly the US is Apple's strongest and biggest market for iOS devices. So how do Americans' love of Apple devices affect their behavior compared to their counterparts in Europe?

Data collected for this analysis includes both personal and enterprise devices and focuses on connecting to risky networks. It appears that iOS users tend to be more careful about the networks they connect to, or are more willing to use cellular data than Android users, regardless of what continent they are on. In Europe, mobile users either take more risks than those in North America, or there is simply a higher rate of risky Wi-Fi networks there.

In North America, 35.8% of iOS devices connected to risky networks, averaging 6.3 incidences per device during the reporting period. At the same time, 44.9% of Android users connected to risky networks, averaging 6.5 incidences per device. In Europe, 36.6% of iOS devices connected to risky networks, averaging 7.3 incidences per device during the reporting period. At the same time, 45.2% of Android users connected to risky networks, averaging a remarkable 12.3 incidences per device.





Skycure

ARE IPHONES OR IPADS MORE RISKY?

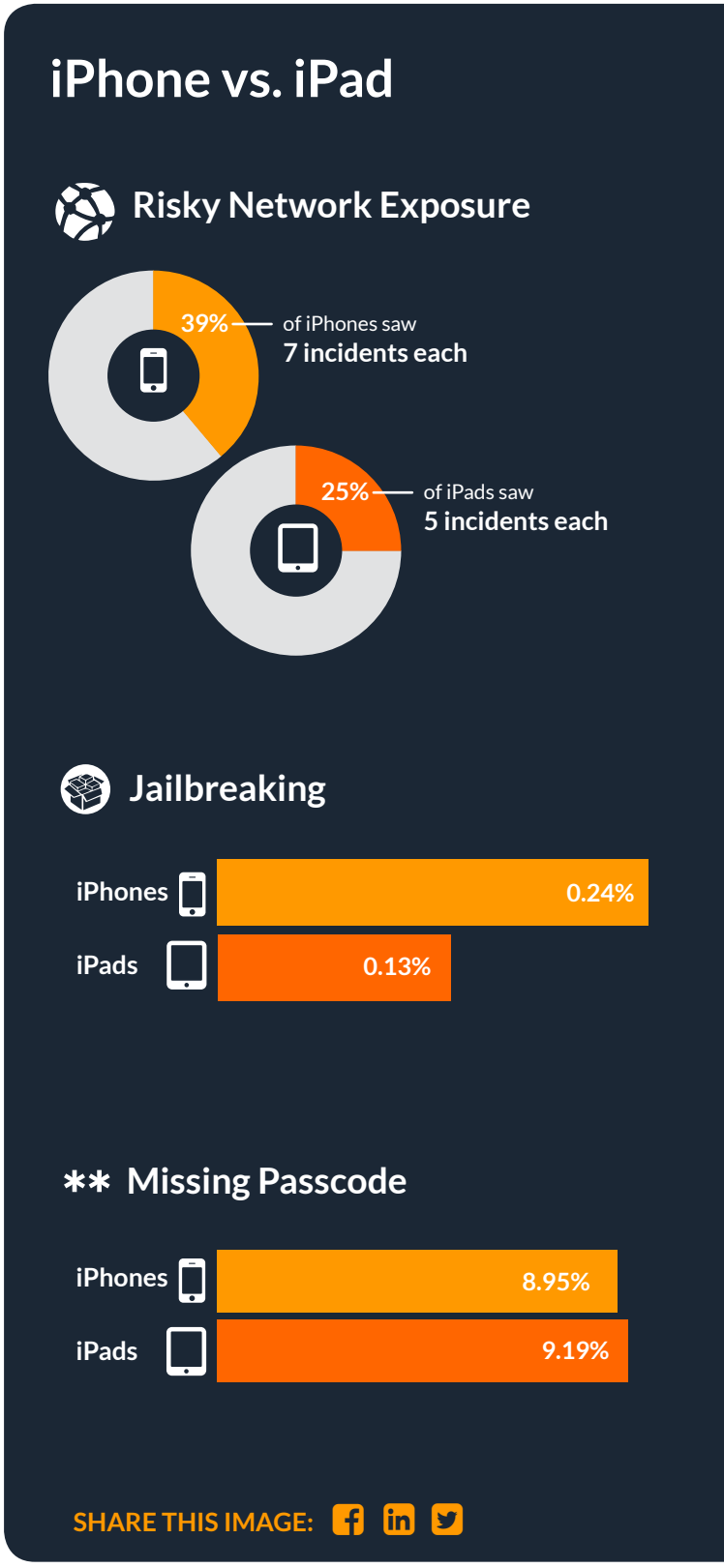
Apple's iOS devices come in two basic flavors, iPhones and iPads, both of which are heavily used in enterprises today, for user productivity and flexibility, as well as customer engagement and timely delivery of value. Looking at incident statistics from the reporting period, it is interesting to note how the usage and risk exposure varies between the two form factors.

In our sample of enterprise devices, iPhones outnumbered iPads by a factor of three, yet some patterns emerged. iPads are less likely to connect to a suspicious or malicious network by a significant margin. About 39% of iPhones experienced risky network incidents, averaging over 7 incidents per affected device, while only 25% of iPads were exposed, averaging only 5 incidences each.

iPhones are more commonly the primary device for an enterprise user, and most are on 24/7 and travel with the user constantly, so it makes sense that more of them are exposed to network threats. iPads in the enterprise are more likely to be shared devices, and may be used in limited locations, often within corporate-controlled networks, but clearly not all of them.

Jailbreaking is an activity that also varies across the different iOS form factors. We have tracked in recent years that the rate of jailbreaking has been steadily declining, especially in the enterprise where such things may be controlled by policy. In our sample, iPhones were jailbroken at a rate of 0.24%, and iPads at just over half that rate at 0.13%. The primary reasons for jailbreaking — user customization and access to unauthorized apps — seem to be less necessary today than in past years, as Apple has continued to open the interface to more official customizations and enterprise app stores allow a legitimate means to install necessary apps that are not distributed through the App Store.

Interestingly, missing passcodes occur with nearly identical frequency on iPhones and iPads, both coming in at about 9%.

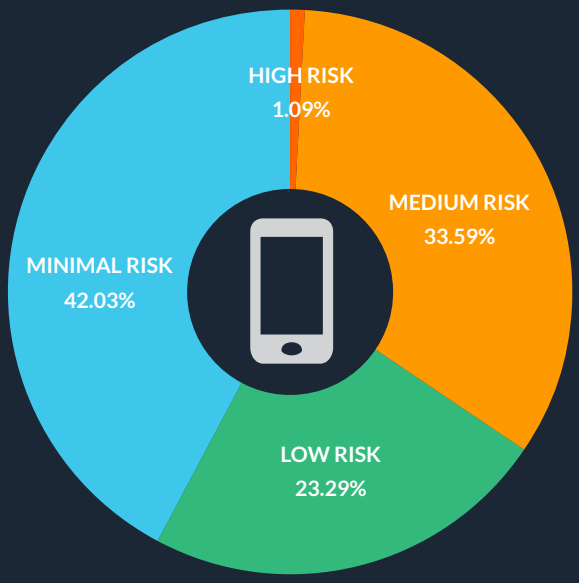


Skycure

AND THE ESSENTIALS...

One Third of All Devices are Risky

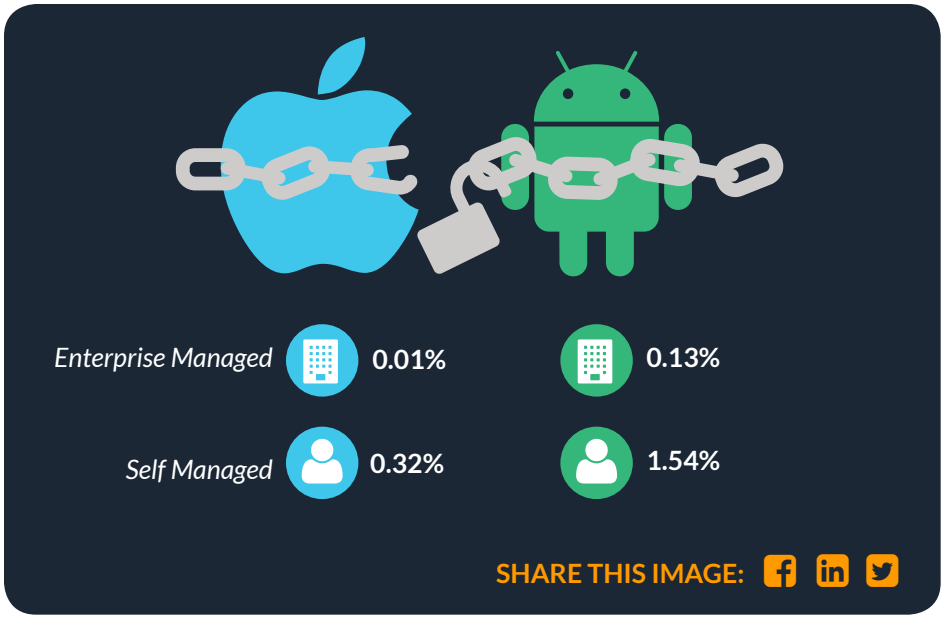
Over 34 percent of all mobile devices are rated as medium-to-high risk according to the Skycure Mobile Threat Risk Score, only slightly higher than Q4 2016. The percentage of high risk devices dropped slightly in Q1 2017 from 1.2 to 1.1 percent. These devices have either already been compromised or are currently under attack. The Skycure risk score takes into account recent threats the device was exposed to, device vulnerabilities, configuration and user behavior.



SHARE THIS IMAGE:

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 continues to decrease in popularity as newer operating systems naturally allow some of the functionality that could previously only be achieved through rooting or jailbreaking.

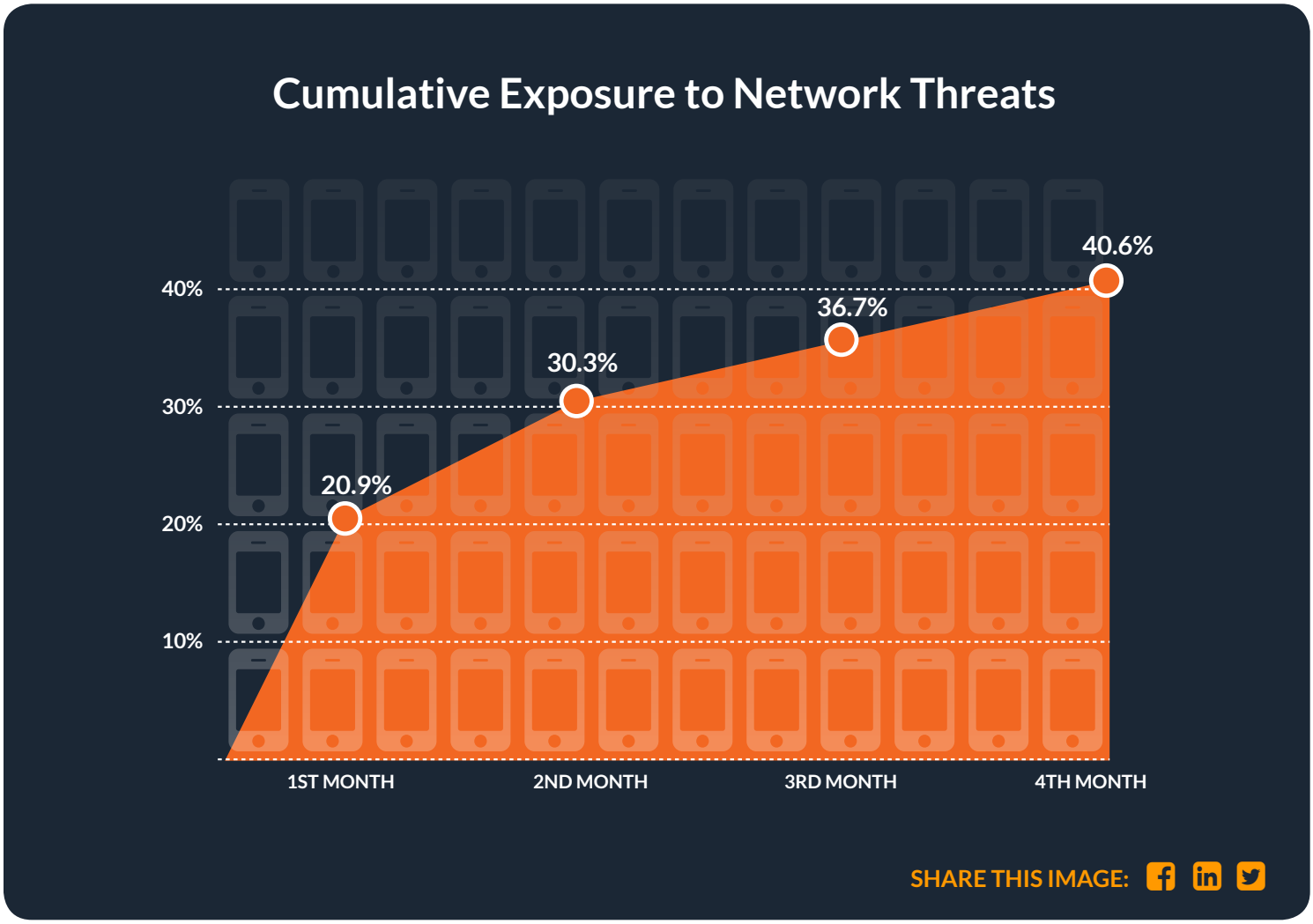


Because of the greater control over the device that this affords, it is a common goal of hackers to figure out ways to root or jailbreak devices, and malware is a common way to do that. A user that roots or jailbreaks their own device should be aware that they may be simply making it easier for hackers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

Skycure

Devices Exposed to Network Threats Over Time

In any typical organization, about 21% of the mobile devices will be exposed to a network threat in the first month of security monitoring. This number goes to 41% 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.



Skycure

Top 5 Recommendations to Keep Your Mobile Device Safe

1. Don't *click, install or connect* to anything that you are not confident is safe.
2. Only install apps from reputable app stores.
3. If you are not confident the Wi-Fi is secure, don't perform sensitive work while connected.
4. Always update the latest security patch as soon a it is available for your device.
5. Protect your device with a free mobile security app like Skycure. apps.skycure.com

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 from mobile devices. Users should know to only install apps from the primary app stores, don't click on untrusted links or approve device permissions and accesses without good reason.

The other important thing an organization can do is install Skycure, which will proactively protect devices in realtime, often even if the user is doing something that is unsafe. Skycure will also inform users and IT admins about the upgradability of both iOS and Android devices so that the window of vulnerability is minimized.

GET A FREE ENTERPRISE TRIAL

Protect your mobile device with the free mobile app from Skycure.

Available on the App Store | Available on Google play

About the Mobile Threat Intelligence Report

The Skycure Mobile Threat Intelligence Report reviews worldwide threat intelligence data. Today's report is based on millions of monthly security tests from January through March 2017 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. Skycure analyzes over 1 million apps and more than 2 million unique networks worldwide every year.

About Skycure

Skycure is the leader in mobile threat defense. Skycure's platform offers unparalleled depth of threat intelligence to predict, detect and protect against the broadest range of existing and unknown threats. 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 App-in-the-Middle, Accessibility Clickjacking, No iOS Zone, Malicious Profiles, Invisible Malicious Profiles, WifiGate and LinkedOut. The company was founded by security industry veterans Adi Sharabani and Yair Amit, and is backed by Foundation Capital, Shasta Ventures, Pitango Venture Capital, New York Life, Mike Weider, Peter McKay, Lane Bess, and other strategic investors.

Skycure