

Mobile Threat Intelligence Report

Q4 2016

MOBILE THREATS – THE YEAR IN REVIEW





GROWING THREATS, SHIFTING TACTICS

Instead of taking a single slice in time, this report attempts to step back a bit to identify and analyze some of the larger trends in mobile threats across the entire year of 2016. The increased focus on the mobile platforms by malicious hackers is undeniable, yet it is useful to try to gain an understanding of where those efforts are concentrated. Taking time to understand the methods and motivations of the attackers, we can gain insight into the methods that must be taken to more effectively defeat them.

The majority of malicious exploits depend on the existence of unpatched vulnerabilities in the mobile operating systems to be successful. Given that, this report analyzed the propagation and adoption of Android security patches through the top five US mobile carriers. The disturbing finding is that **71% of mobile devices are running on security patches that are at least 2 months old**, leaving millions unnecessarily susceptible to breach. Read on to learn about this dangerous “window of vulnerability”.

This report is an analysis of many millions of data points taken from Skycure's global sensors, across the year from January 1 through December 31, 2016, taken in quarters. The three primary mobile threat vectors are presented – Malware, Network Threats and Vulnerabilities – each in its own section. 2016 seems to have been a pivotal year for mobile hackers as much of the data indicates exponential growth in certain types of attacks.

SHIFTING MALWARE TRENDS

Malware (a malicious or risky application), is often the first thing people think about when discussing endpoint security. Once referred to as viruses on traditional computers, malicious apps are deliberate creations with malicious intent that must be installed on the target device to function, and can range from merely annoying, like adware, to truly insidious, like spyware and ransomware. Mobile malware is an increasingly popular attack vector for a variety of reasons. One of the main reasons is that these hacking tools, which used to be the sole domain of super geeks who spent years learning the skills necessary to develop and execute an attack, are becoming somewhat commoditized.

Exaspy, exposed publicly near the end of 2016, is a great example of “off-the-shelf” malware that someone can leverage against a target, even if they themselves do not have a high degree of technical sophistication. Exaspy falls into the category of Spyware, but there are many varieties. Different organizations and security solution providers may use different terms, different definitions, and perhaps even different criteria for the same names. Here are some of the more common types and their generally accepted definitions.

Adware – This may display unwanted ads, collect unauthorized marketing information about you, and redirect search requests to advertising websites, in hopes of getting the user to buy a product.

Hidden App – This has slightly different implications on iOS vs Android, but in general an app that doesn’t display a standard icon to indicate its presence, in effect hiding from the user.

Potentially Unwanted – This may accompany a legitimate app or be installed as part of the process of another app, but is malicious. As this primarily describes the delivery method, other types of malware may also fall into this category.

Riskware – This is not malicious itself, but contains identified security holes that may be leveraged by other exploits with relative ease.

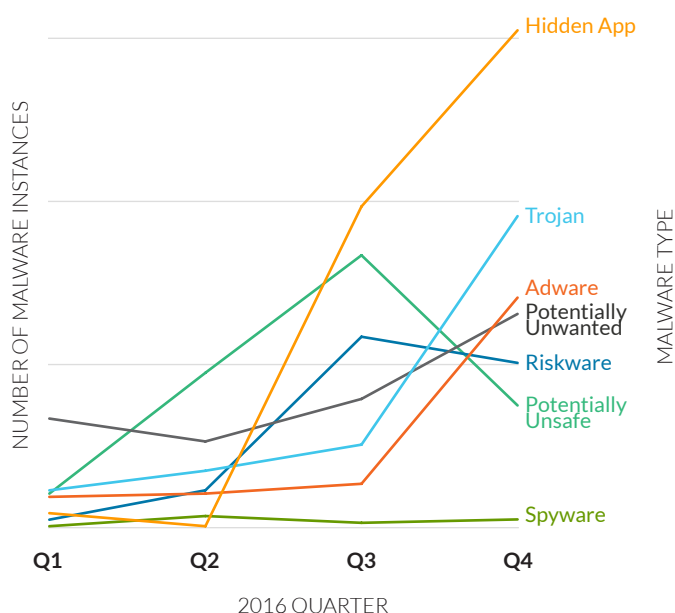
Spyware – This mostly runs in the background with no indication of its presence, often as additional code hidden in a legitimate-looking app, with the objective of stealing information and staying hidden.

Trojan – There are many varieties of Trojans (backdoor, downloader, infostealer, remote access, attack), separate programs that sneak into the device as payload of a legitimate-looking app. Each is designed to give the attacker deep access and control over the device.

There are other, less common types of malware not listed here, and there are different opinions on how to classify them. Potentially Unwanted, for example could manifest as a few different types, but for categorization purposes, we will place malware in this category when it meets the criteria for Potentially Unwanted, yet does not fit into any of the other categories. At the beginning of 2016, Potentially Unwanted appeared to be the most prevalent type of malware, and although its frequency grew to almost double by Q4, other types had faster growth across the year. Hidden Apps, which started the year as fifth most common, ended the year with a significant lead.

Total instances of these common malware types grew from Q1 to Q4 by over five times. The trend seems to indicate that the broader the appeal to the attacker, and the easier to deploy, the more often it will be utilized. The least popular of our sample was Spyware. This makes sense, as spyware must be more sophisticated to succeed in both stealth and effectiveness, and to make use of it, the attacker must pay attention to each installation to gain value from it.

Trending Malware Types



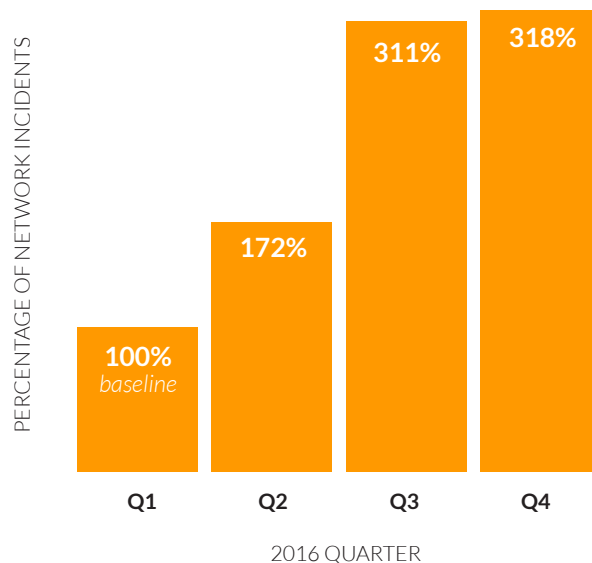
MASSIVE INCREASE IN NETWORK INCIDENTS

We tracked the trends in network incidents in the major technology centers of the US during 2016, observing both the frequency of incidents and the methods used to perpetrate network exploits. It is important to understand that not all network incidents are deliberately malicious attacks. A large number of incidents are simply misconfigured routers or access points that end up removing the secure communication protections implemented by the mobile device and/or the apps being used for the communication. While a large number of security solutions might consider flagging such “misconfigurations” as false positives, not a single CISO would ever advocate or approve connecting to any network that does not fully support secure communications for business interactions.

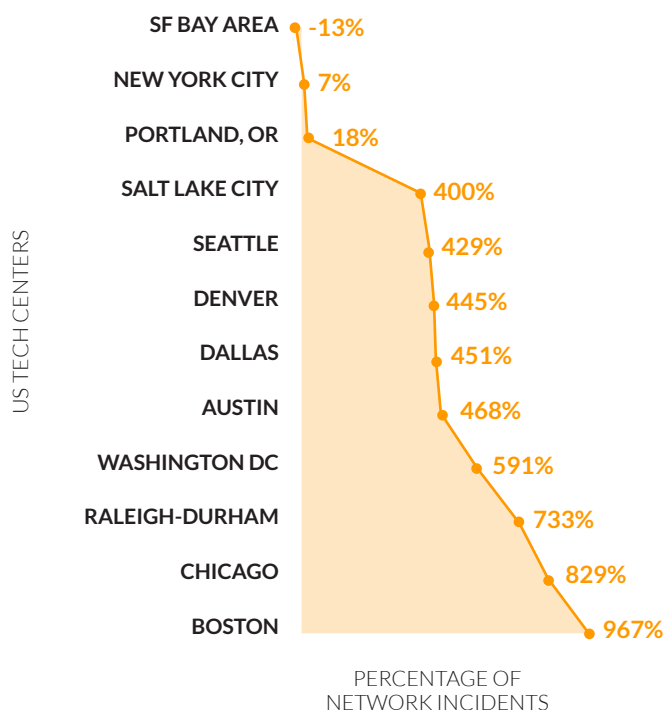
With that in mind, the nature of network incidents (which specific types of attacks were performed in which proportions) did not significantly evolve over the course of the year. However, the volume increase in the tech centers was staggering. Q2 2016 showed a 72% increase in incidents compared to Q1, and Q4 grew to more than three times the first quarter of the year. An interesting note on the trend is that the incident numbers rose dramatically across the first three quarters, then slowed in Q4 overall, with drops observed in a few of the tech centers, from Q3 to Q4 – Seattle, Salt Lake City and Boston the most notable. The slowing in network incidents is likely related to the changing behavior of people over the holidays, with less business travel and more focus on family-oriented activities in known safe locations. Boston also demonstrated the greatest increase in incidents throughout the year, reaching about eleven times the number of incidents across the year.

Although most tech centers increased significantly in the quantity of incidents from the beginning of the year, there were three areas that remained relatively flat – San Francisco Bay Area, New York City and Portland, Oregon. Interestingly, there may be different reasons why each of these three saw small growth. The San Francisco Bay Area uniquely ended the year with fewer network incidents than at the beginning (down 13%), although Q3 was up 37%. Perhaps they are already ahead of their time in growth of malicious activity and have reached a temporary plateau.

Total Growth Across All Tech Centers



4-Quarter Growth for Each Tech Center



THE WINDOW OF VULNERABILITY

Although there are many different strategies and methods to attack mobile devices and use them for some advantage against an individual or organization, there are two principle factors that allow these attacks to be successful – user behavior and device vulnerabilities. User behavior is almost always a factor, as attackers often require the user to perform some action, like installing an app or clicking on a link, in order for their exploit to work. The attacker may promise something, like free movies, or perhaps the victim is enticed to install and play a game that is also spyware or ransomware. In the end, the user has unwittingly helped the attacker to gain access to and control over the device and often any organizational information the device has access to.

The other principle factor in allowing attacks to be successful is the vulnerabilities in the device itself, primarily in the operating system and its core apps. All operating systems are designed with security measures in place to protect the data, the communications, and the device resources against unauthorized access. But no system is perfect, and diligent efforts by both good and bad actors will discover these vulnerabilities.

When a good actor, like a security company or a white hat hacker, identifies a vulnerability, they bring it to the attention of the vendor and help them to patch it prior to a public disclosure of the patched vulnerability. This process ultimately makes the devices more secure. When a bad actor identifies a vulnerability, they keep it to themselves, develop and sell exploits that take advantage of it. The method of exploit against a vulnerability may be to use a malicious app, a network attack, a malicious link or webpage, or other mechanism. In fact, the majority of mobile threats across all vectors of attack rely on some vulnerability of the device.

Protecting against vulnerabilities requires multiple steps, leaving the individual exposed until all steps have been completed.

1. Discovery of the vulnerability
2. Notification to the developer
3. Development of a successful patch
4. Availability of each carrier-specific patch
5. Distribution of the patch
6. Installation of the patch

In the case of a bad actor, this process stops after step 1, and all relevant devices are vulnerable until the vulnerability is discovered by a good actor, either independently, or as a result of catching an attack of the bad actor. In the case of a good actor, relevant devices are vulnerable starting at step 4, and the faster the user learns of the patch and installs it, the smaller the window of vulnerability is for him. Note that the progression from step 2 to step 3 can be very fast or extraordinarily long.

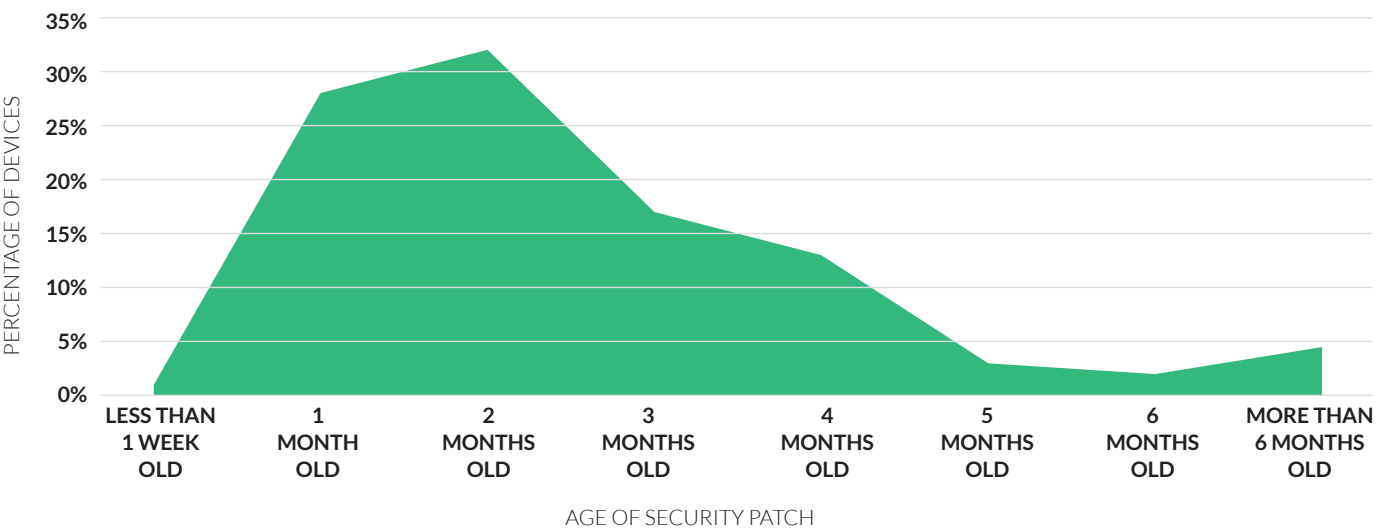
The [Shared Cookie iOS vulnerability](#), for example, was one of the first vulnerabilities patched in 2016, yet was first identified by Skycure in June of 2013, two-and-a-half years earlier. For Apple iOS devices, once the patch is available, the last few steps proceed quickly, as there is tight integration with the software, hardware and distribution.

This is not the case with Android. As an open source operating system, there are many varieties of Android, each particular to the specific device manufacturer, integrated hardware, carrier, and other factors. This often makes the progression from step 4 to step 6 excessively long, extending the window of vulnerability. We took a snapshot of security patch installations across the year to see how effective the various carriers are in distributing and implementing patches. This process is a combination of how long it takes to create the patch variation (after Android developers release the base patch), distribution through the independent carriers, communication to the individual users and/or organizations, and installation at the device.

The leading carriers are ultimately responsible for how quickly their users update their Android devices, so we analyzed devices to determine the age distribution of security patches. We took a snapshot in the first week of January 2017 and looked for patches that were released across 2016. The most recent security patch was only adopted by a very small percentage of the population, having just been released, but AT&T users were up to 10 times more likely to have this latest patch already installed. Other carriers evaluated were Verizon, Sprint, T-Mobile and MetroPCS.

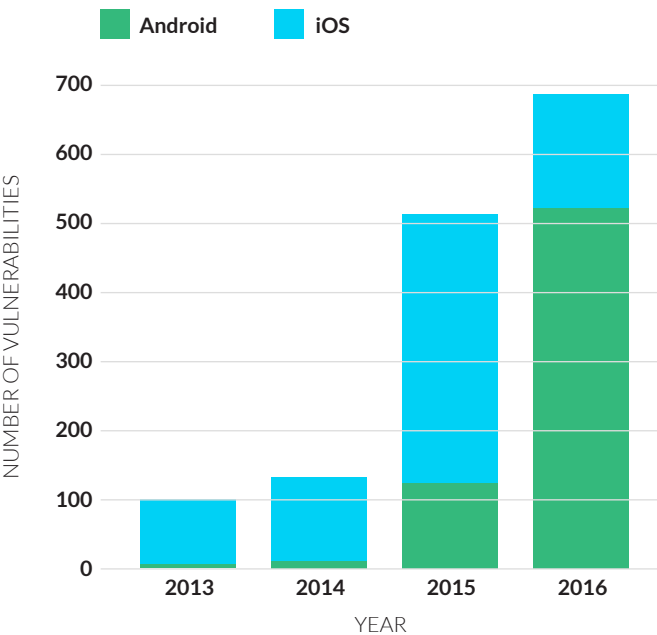
Age of Security Patches

Looking at mobile devices across all of the 5 major US carriers, we found that 60% of all devices were running on security patches that are one or two months old, and 6% of devices are running security patches that are 6 months old or older.



Android saw a massive surge in identified vulnerabilities in 2016, with a greater than four times increase over 2015. Almost half of those vulnerabilities allowed excessive privileges, while others allowed other bad effects, like leaked information, corrupted memory, or arbitrary code execution.

Mobile OS Vulnerabilities



Source: MITRE Corporation CVE Database

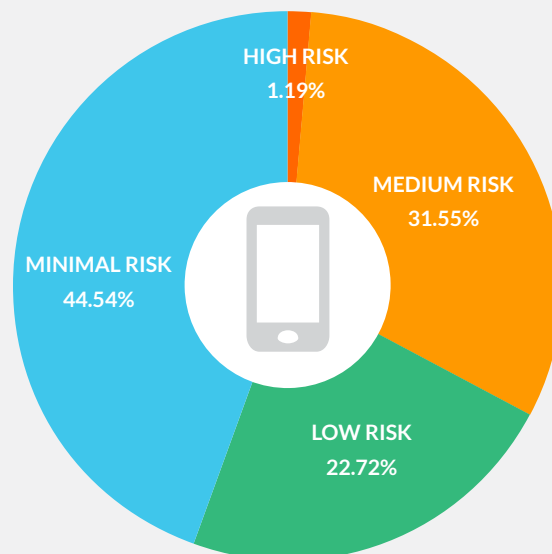
Some of the notable vulnerabilities that were patched, either partially or completely, in 2016 are:

- [Shared Cookie Stores](#)
- [Accessibility Clickjacking](#)
- [Quadrooter](#)
- [Pangu Jailbreak](#)
- [Pegasus/Trident](#)

AND THE ESSENTIALS...

Over Half of All Devices are Risky

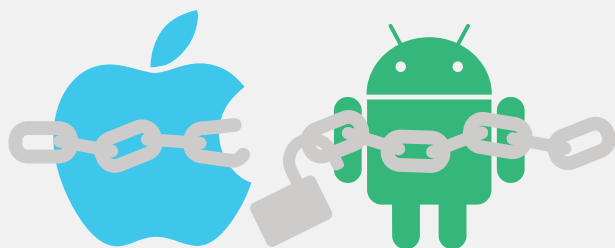
About 33 percent of all mobile devices are rated as medium-to-high risk according to the Skycure Mobile Threat Risk Score. The percentage of high risk devices dropped slightly in Q4 2016 from 1.4 to 1.2 percent. These devices have either already been compromised or are currently under attack. The Skycure risk score takes into account recent threats the device was exposed to, device vulnerabilities, configuration and user behavior.



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.



Enterprise Managed 0.01%

0.14%

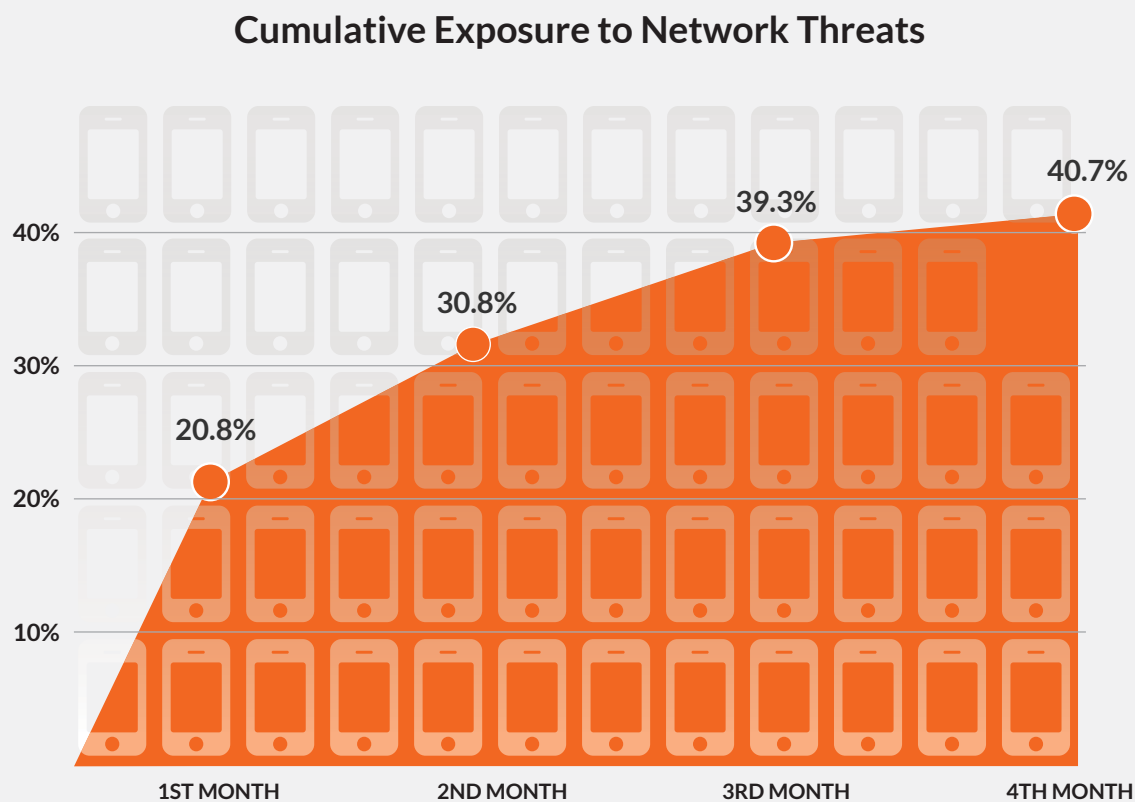
Self Managed 0.18%

1.78%

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.


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.




Top 3 Recommendation to Keep Your Mobile Device Safe

1




Don't click, install or connect to anything that you are not confident is safe.

2



Always update to the latest security patch as soon as it is available for your device.

3



Protect your device with a free mobile security app like Skycure
<https://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 to their organizations through 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.

The other important thing an organization can do is install Skycure, which will proactively protect devices in real-time, 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.



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 October through December 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. Skycure analyzes 1 million apps and more than 1.5 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 is backed by Foundation Capital, Shasta Ventures, Pitango Venture Capital, New York Life, Mike Weider, Peter McKay, Lane Bess, and other strategic investors.