Skycure

Mobile Threat Defense

Mobile Threat Intelligence Report

Q2 2016

EXECUTIVE SUMMARY

Given the continuing evolution in the sophistication of cyber attacks, from a broad spam-type strategy to more targeted and financially motivated exploits, it makes sense to shift the focus of this quarter's report to the same group that malicious hackers are increasingly targeting - executives. Executives tend to carry more devices than other employees, and typically have greater access to critical corporate or government information that would be valuable for a hacker to steal, making them ideal targets. At the same time, some executives are more wary of security issues, so may be more likely to take sensible precautions. This is the landscape for the current mobile cyber war.

This report focuses on the executive mobile devices that are outfitted with all of the apps and communication methods to support busy executives that need to be able to respond to the demands of their jobs at any time and from anywhere. These devices either contain or have access to a tremendous amount of sensitive data, including personal, corporate and customer information, making executive mobile devices very appealing targets for malicious hackers.

Note: This investigation is based on tens of millions of security tests from April through June 2016 and includes devices being used by both executives and non-executives.

EXPLOITING EXECUTIVE ACCESS

Mobile devices have become ubiquitous and indispensable gadgets among organizational workers, as well as the population as a whole. However, the group of users who literally rely on their devices as an essential tool around the clock are executives. Forbes has reported that 90 percent of executives use a smartphone every day, and are using tablets more often for business as well. Smartphones are the primary communication device, for both work and personal use, and are used at all hours of the day, at home and on the road. This means that a hacker that is able to compromise an executive device may gain access to any privileged information that the executive has access to, including data found on the device, any corporate resources that may be accessed using the executive's credentials, or voice and data communications.

The same Forbes report showed that the percentage of executives using tablets rose 19 percent in three years, contributing to the increase in number of devices used. Earlier studies have shown that senior executives, on average, utilize more than three devices each, with CEOs and CFOs relying on more than four devices, and that number grows every year. Each device is an additional opportunity for malicious hackers to penetrate existing security measures and increases the likelihood of a security breach. Breaches may come in the form of malware, network-based attacks, device vulnerability exploits, or even physical attacks on the phone directly.

32.5 PERCENT
OF EXECUTIVE DEVICES WERE EXPOSED TO NETWORK ATTACK
in April through June 2016 timeframe

The most frequent threats to mobile devices come from the networks they connect to, exposing communications, and potentially compromising the device beyond the period it is connected to the malicious network. This study found that 32.5 percent of executive devices were exposed to network attacks in the April through June 2016 timeframe. Over the same period, 22.5 percent were infected with malware that rated at least medium severity risk, and 6.3 percent that were determined to be high severity risk. While malware is occasionally identified and removed, this study determined that at any point in time, 1 in 50 executive devices is infected with high severity malware, providing malicious hackers with continuous access to sensitive data and conversations.

22.5 PERCENT

OF EXECUTIVE DEVICES HAVE BEEN INFECTED WITH **HIGH OR MEDIUM SEVERITY MALWARE**

6.3 PERCENT

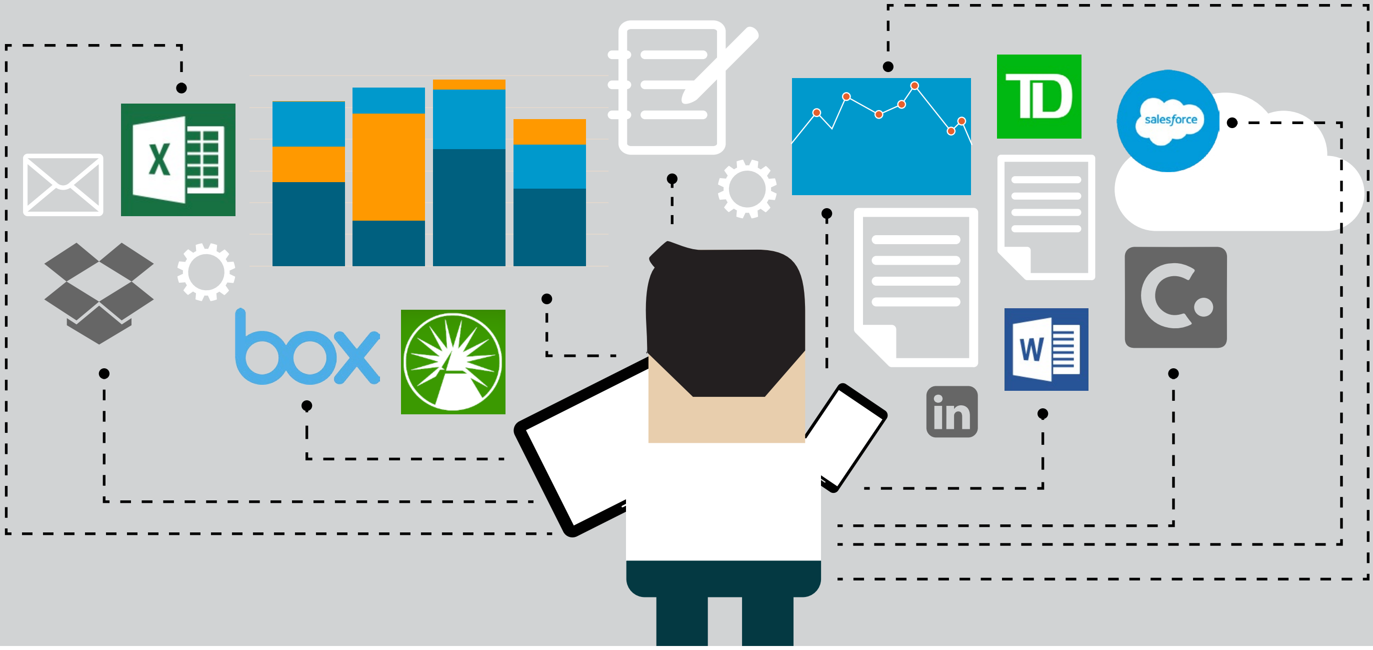
DEVICES HAVE BEEN INFECTED WITH **HIGH SEVERITY MALWARE**

EXECUTIVE APPS CONNECT TO EVERYTHING

Since executives are relied upon to make fast decisions, they need easy access to all of the information they will need to make those decision, and it is the apps on their mobile devices that deliver the vast majority of that data, for both their business and personal lives. For business, commonly used apps include customer relationship management (CRM), document storage and editing, expense tracking, and other mission critical apps that may be designed specifically for their business. Personal apps, like those used for banking and investing, also hold or access sensitive data that may be tempting for hackers to try to view or steal.

With virtually unlimited access to all critical corporate information, executives are understandably desirable and popular targets for hackers. This also explains the trend of malware toward more spear phishing and ransomware that is designed to target specific individuals, as opposed to the broad-based dragnet approaches that were more popular in the past. These new methods of corporate espionage, combined with executive access, exposes not just corporate information, but potentially that of their customers and partners as well.

EXECUTIVE APPS PROVIDE ACCESS

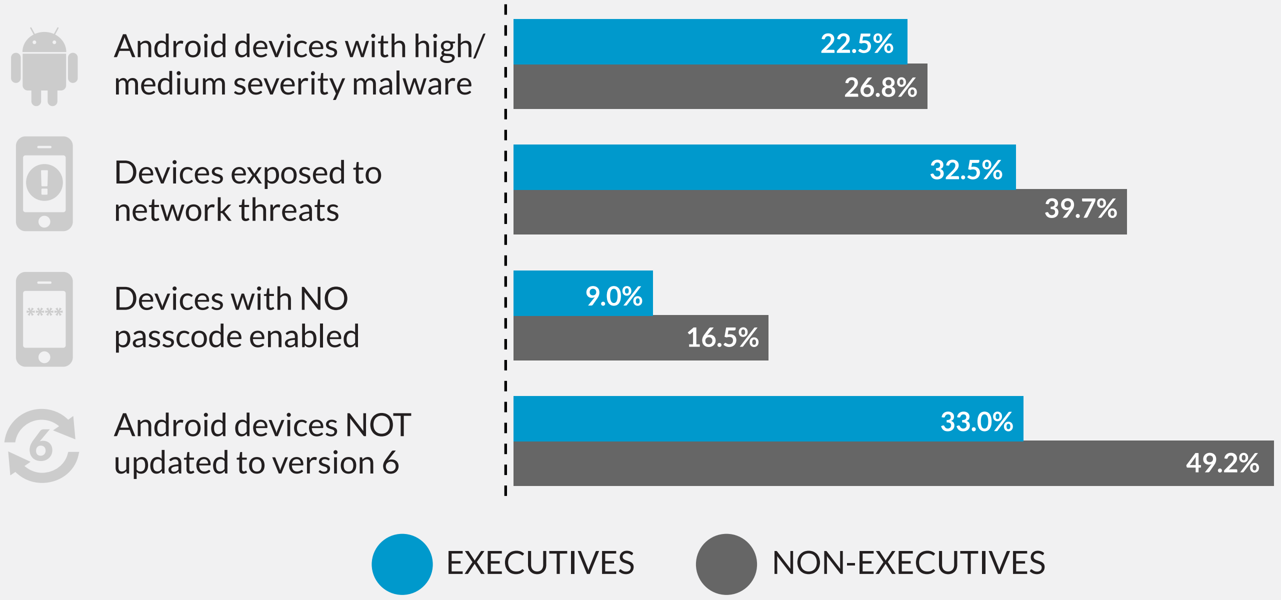


MORE SECURITY AWARE, BUT STILL EXPOSED

In light of the increasing aggressiveness of malicious hackers, it is good to see new evidence that mobile users are learning to take more security precautions, like locking their devices with passcodes. There is even evidence that mobile users are updating the operating systems on their mobile devices more quickly than they used to. Considering the vast majority of operating system patches address security issues, quickly updating to the latest OS version is an important step to minimize the risk of exposure to device vulnerability exploits.

This study reveals that executives may be slightly ahead of the curve when it comes to awareness about mobile security issues. They may be aware of the added risk they pose to their businesses by using more devices and having greater access to more critical data, or perhaps they are more sensitive to security issues in general, and that carries over to their mobile lives. Note that the increase in security awareness of executives over the general population is relatively small. So, as encouraging as this trend may be, it is unlikely to even come close to offsetting the added risk factors that executives introduce.

EXECUTIVES VS NON-EXECUTIVES

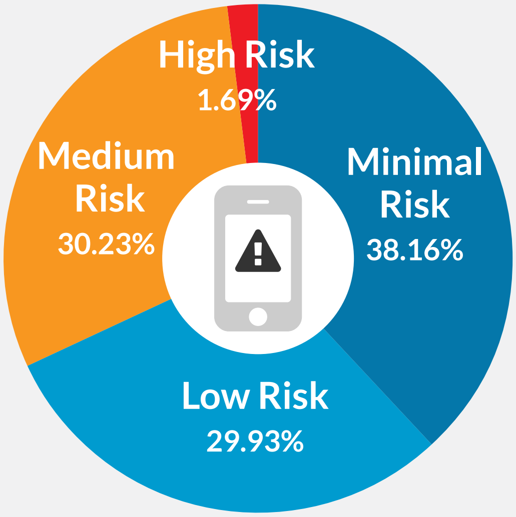


** April through June 2016 timeframe*

AND THE ESSENTIALS....

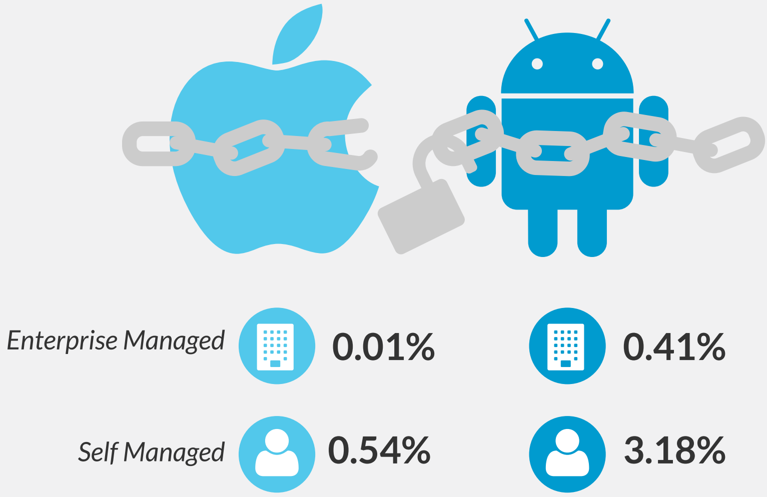
Almost a third of all devices are risk

About 32 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 Q2 2016 to 1.7 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.



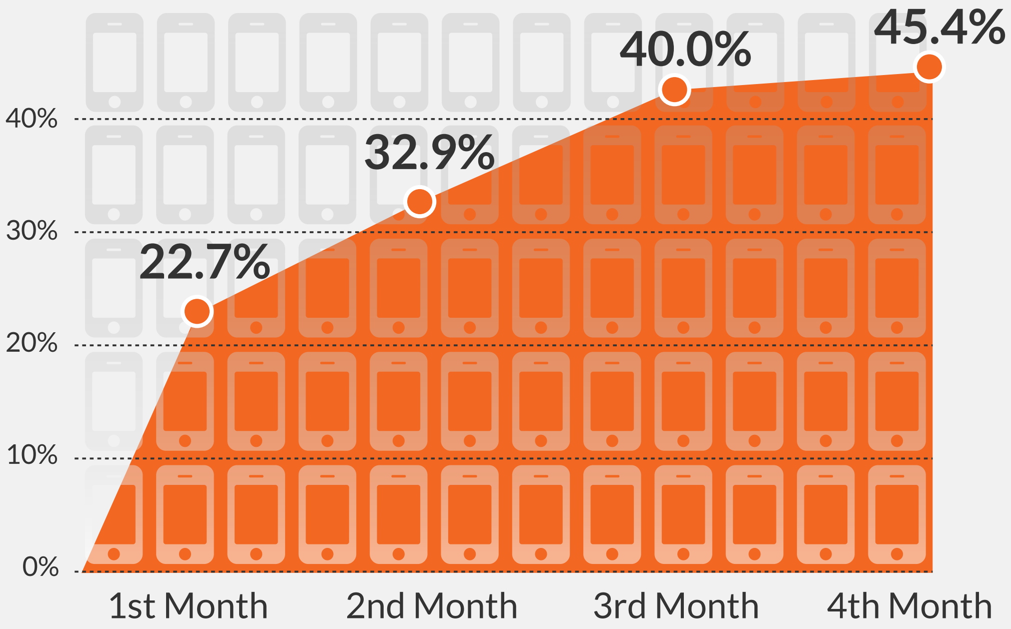
Because of the greater control over the device that this affords, it is a common goal of hackers to figure out ways to root or jailbreak devices, and malware is a common way to do that. A user that roots or jailbreaks their own device should be aware that they may be simply making it easier for hackers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

AND THE ESSENTIALS....

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.

CUMULATIVE EXPOSURE TO NETWORK THREATS



TOP 10 RECOMMENDATIONS FOR EXECUTIVES

1. Use a numeric or biometric passcode on your device, in case the device is stolen.
2. Avoid connecting to Public WiFi networks, especially networks with "Free" in their name.
3. Avoid accessing highly sensitive information when connected to public WiFi.
4. Be sure WiFi name is sensible for the location - no Heathrow WiFi in New York.
5. Only download apps from reputable app stores like Google Play and Apple's App Store.
6. Update your device to the most current operating system to have all security patches.
7. Disconnect from the network if your phone behaves strangely (crashes or warnings).
8. Read security warnings and don't click "Continue" if you don't understand the exposure.
9. Check for top mobile threats in any destination by visiting https://maps.skycure.com
10. Protect your device with a free mobile security app like Skycure - https://apps.skycure.com/

Threats to mobile devices affect all mobile workers, but malicious hackers are increasingly targeting executives due to the high value information that can be accessed and used for personal gain or competitive advantage. Organizations looking to defend their executive devices, and the rest of their mobile ecosystems, from the various threats should follow advice from the major EMM vendors, which all recommend adding a Mobile Threat Defense solution to protect valuable corporate data. Traditional approaches that leverage standard static and dynamic methods alone are good, but not enough to protect from the malware, network-based threats and vulnerability exploits 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.

THE SKYCURE EXECUTIVE PACKAGE

Given the focus by hackers on executive devices, we have decided to make it easy for organizations worldwide to protect these most targeted devices. For that reasons we have launched the

Skycure Executive Package:

- 20 Free Skycure licenses for company executives
- Free licenses valid for 6 months
- Must have 100 or more employees to qualify
- Open availability through 12/31/2016, limited availability after

GET THE FREE EXECUTIVE PACKAGE

About the Mobile Threat Intelligence Report

The Skycure Mobile Threat Intelligence Report reviews worldwide threat intelligence data. Today's report is based on tens of millions of monthly security tests from April through July 2016 and includes both unmanaged devices and those under security management in enterprise organizations. Executive devices were determined based on the apps installed on their devices. 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. 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 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.