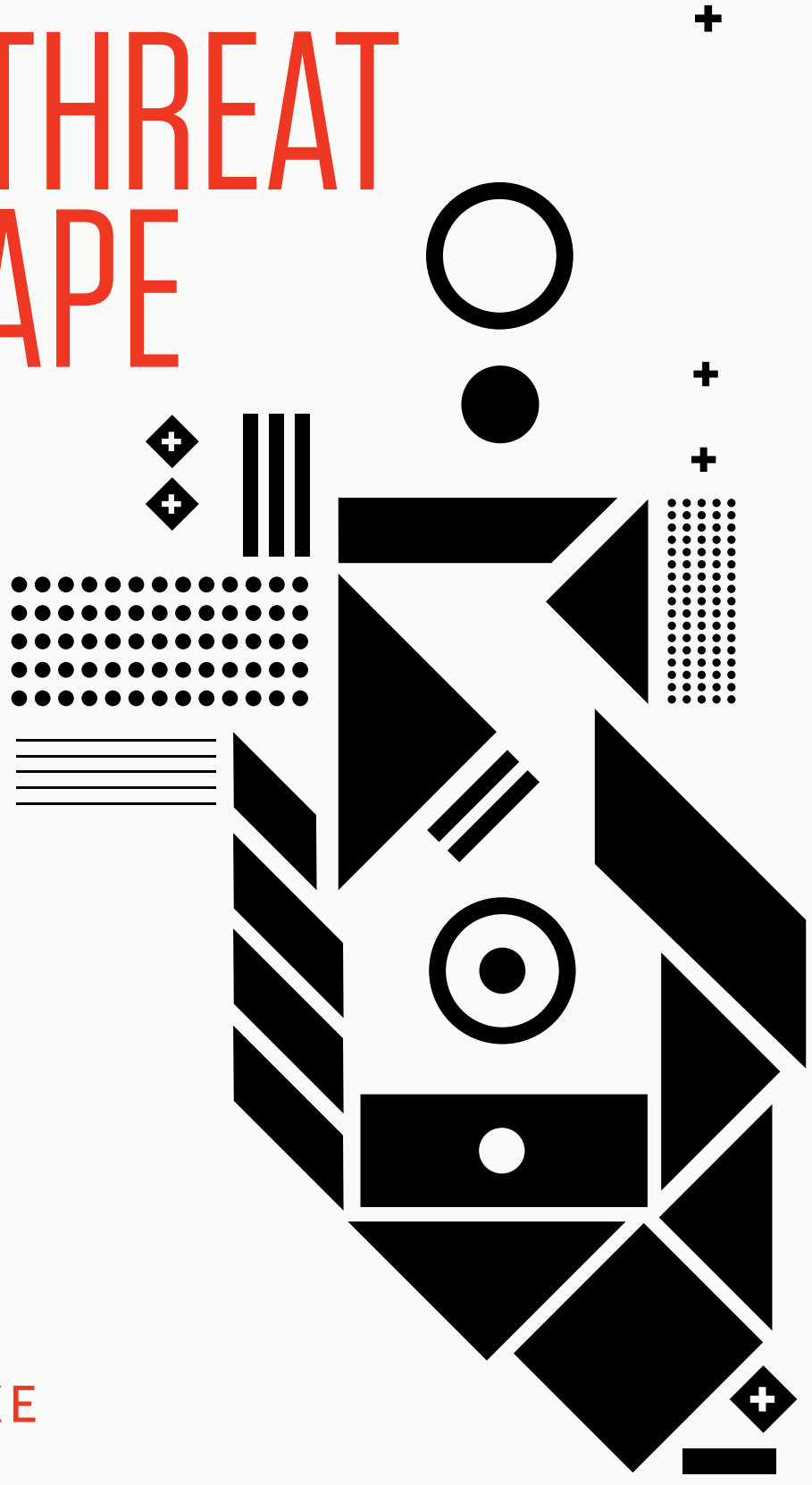
2019

MOBILE THREAT LANDSCAPE REPORT



A COMPREHENSIVE REVIEW OF MOBILE MALWARE TRENDS

CROWDSTRIKE

TABLE OF CONTENTS

INTRODUCTION

As a result of changes in the way people use and protect their devices, malicious actors have increasingly sought to diversify the way they attempt to compromise their targets and achieve their objectives.

In recent years, computing has become commoditized to the extent that mobile devices are increasingly prevalent and have become a key part of their owner's daily lives, supporting both business and personal activities — including email access, banking and authentication. The adoption of these devices is particularly high in geographic regions such as Latin America, where they provide a more convenient and cost-effective route to obtaining this functionality versus desktop computing. The traditional computing landscape has also changed during this time; significant adoption of cloud-based services has decentralized data storage, and a drive towards securing mobile devices against misuse has resulted in a marked increase in the deployment of traditional and next-generation antivirus solutions to combat malware-based threats. This approach to defensive security has also been augmented by the introduction of endpoint solutions that provide granular insight into malicious activity through the generation and investigation of high-resolution device telemetry.

As a result of changes in the way people use and protect their devices, malicious actors have increasingly sought to diversify the way they attempt to compromise their targets and achieve their objectives. This diversification includes the development of malware for mobile devices, which often do not have access to the same level of security monitoring as desktop computers and servers. In fact, the successful compromise of mobile devices provides more extensive access to large amounts of personal data, as they often aggregate multiple data sources (such as email accounts) along with mechanisms for authenticating with other services as part of two-factor authentication (2FA) capability. Furthermore, many devices can also provide the geographic location of their owners through access to global positioning service (GPS) hardware and cell tower information. This density of personal information offers an attractive target to a range of adversaries, leading to an uptick in both targeted and commercial mobile malware families.

This report provides an overview of the key types of mobile malware observed so far in 2019, along with their typical deployment mechanisms. It also identifies how and why certain adversary groups and unaffiliated criminal actors are targeting mobile devices for intelligence and financial gain, and assesses the potential for future changes in this threat landscape.

KEY FINDINGS IN THIS REPORT

1 **The targeting of mobile platforms is increasingly being adopted by a range of criminal and targeted intrusion adversaries.**

2 **Malware targeting mobile banking is likely to remain prolific, supported by an active underground industry of developers operating mobile "malware-as-a-service" subscription models to complement their desktop offerings.**

3 **Targeted adversary groups continue to develop mobile malware variants, typically as ports of established malware families. Development capability has proliferated to less-skilled groups due to the accessibility of proof-of-concept mobile malware variants.**

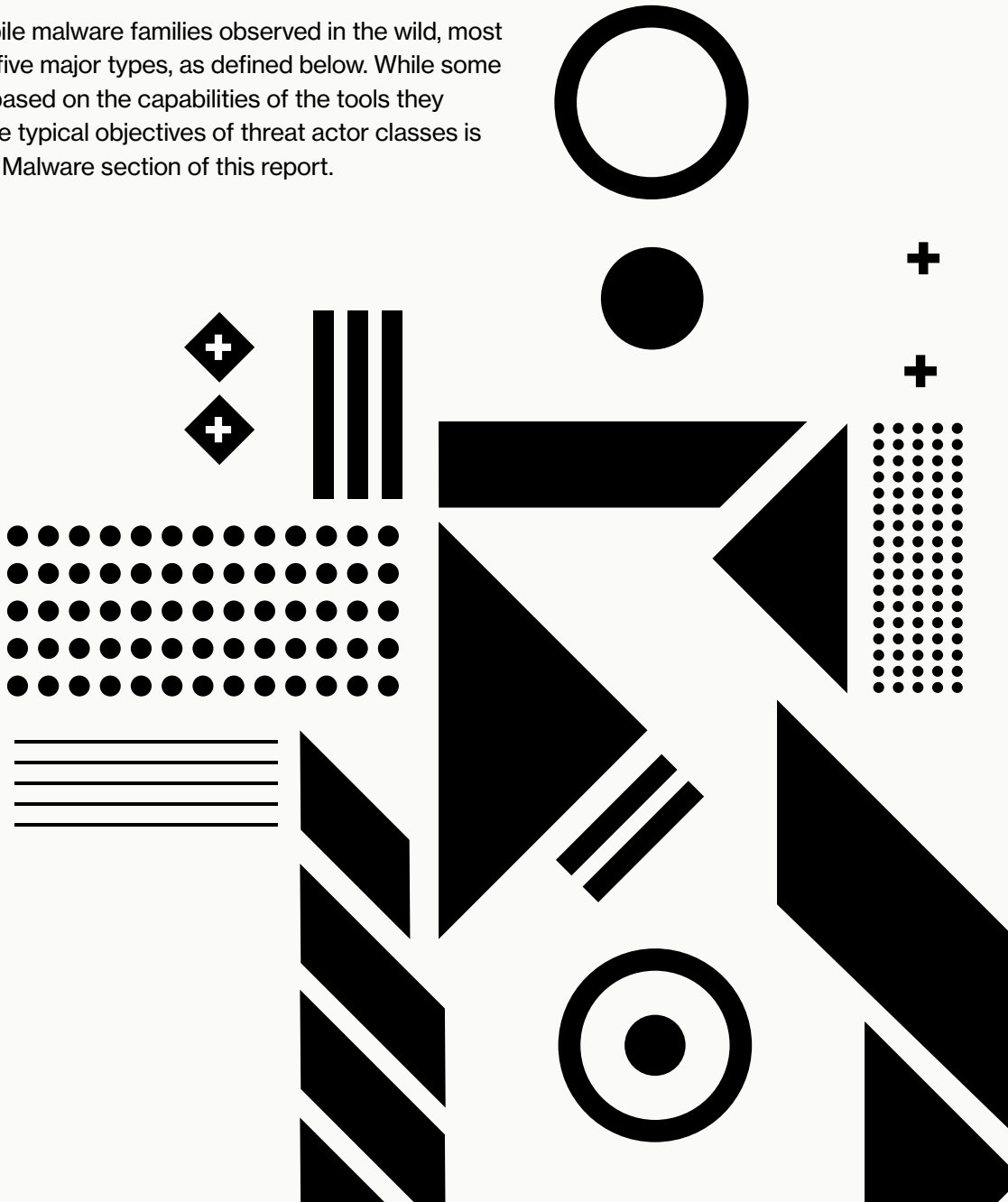
4 **Mobile malware running on the Android operating system is the most prevalent at this time, driven by the ease of installing new applications from third-party sources.**

5 **The current maturity level of mobile security solutions lags behind that of traditional platforms, leading to longer potential attacker dwell times on compromised mobile devices.**

MOBILE MALWARE OVERVIEW

Much like malware families developed for traditional desktop computing platforms, mobile malware can take a variety of forms depending on the capabilities and motivations of the developer and those deploying the malware. While some state-aligned actors may seek to establish long-term persistence on a device to gather intelligence on a target over a period of time, criminally-minded groups develop malware to intercept banking credentials in order to provide a quick route to financial gain. Meanwhile, less sophisticated criminal actors may seek to repurpose existing revenue generation models such as ransomware and cryptomining, although often with limited results.

Despite the wide variety of mobile malware families observed in the wild, most can be categorized into one of five major types, as defined below. While some actor motivations are obvious, based on the capabilities of the tools they deploy, further discussion on the typical objectives of threat actor classes is provided in the Users of Mobile Malware section of this report.



TYPES OF MOBILE MALWARE

Despite the wide variety of mobile malware families observed in the wild, most can be categorized into one of five major types.

REMOTE ACCESS TOOLS

Remote Access Tools (RATs) represent the most comprehensive threat to mobile devices due to their broad functionality and extensibility. They typically enable extensive access to data from infected victim devices and are often used for intelligence collection. The data that is retrievable using mobile RATs often far exceeds the fidelity that could be obtained using traditional RATs targeting desktop computers, primarily due to the easy access to hardware that is standard on most modern mobile devices, such as microphones, cameras, and GPS chipsets. Typical features provided by mobile RATs include:

- Listing of device information such as manufacturer, model, operating system version, and International Mobile Equipment Identity (IMEI)/International Mobile Subscriber Identity (IMSI) numbers, which can be used to uniquely identify the device and associated user
- Listing of installed applications
- Retrieval of device call history
- Retrieval of contact information from the device address book
- Retrieval of web browsing history and bookmarks
- Collection of short messaging service (SMS) data
- Sending SMS messages for command and control (C2) exfiltration or propagation
- Enabling GPS logging and the transmission of device location according to GPS values
- Capture of an active screen via a screenshot
- Enabling front and rear facing cameras to capture images and videos
- Enabling the microphone to capture ambient sound using device

Some of this functionality can have multiple uses. For example, the interception of SMS messages can be used either for general information gathering, or as a way to intercept 2FA tokens sent using this service in order to compromise external services.

The majority of mobile RATs used by targeted adversary groups for intelligence collection purposes are custom-developed, and are often a variant of malware families deployed against desktop computers. However, there is also an active market for commercial RAT offerings that provide a similar range of capabilities aimed at a wider group of paying customers. Some of these tools are offered on criminal forums for a recurring fee, often with support contracts, although this class of malware is typically used to enable financially motivated information collection. In these cases, the RAT may also provide plugins that create web page "overlays" to intercept user credentials, usually for online banking services. This functionality is detailed further in the Banking Trojans section of this report.

SPOUSEWARE / STALKERWARE

In addition to the proliferation of mobile malware for sale on criminal forums, "legal" commercial spyware puts RAT functionality into the hands of the public, to be used wherever someone has physical access to the mobile device. This surveillance software is also referred to as "spouseware" or "stalkerware," due to its frequent use against personal contacts. It significantly lowers the barrier to entry for deploying malicious software and should be considered part of any mobile device threat model.

On the opposite end of the market, several commercial entities have created sophisticated mobile RATs that are supported by professional device exploitation operations and C2 infrastructure administration services. Apart from the full operational management chain, what distinguishes these companies from other mobile RAT developers is their continual maintenance and patching of their malware, as well as producing variants written for non-Android operating systems such as Apple iOS. While the Apple mobile ecosystem is not immune to malicious software, there are barriers to the development and deployment of potentially malicious software that complicate the typical deployment techniques (detailed further in Distribution Mechanisms) often employed to install Android-based RATs. However, remote software exploits or physical access to the devices is often required to install these RATs, which in turn significantly increases the cost of deployment.

The high cost of developing and running such operations make these capabilities best suited for nation-state customers. This comes at an obvious financial benefit to the companies offering the services, as well as providing a level of state-sanctioned acceptance that allows them to operate with relative freedom outside of certain legal constraints. Examples of mobile RATs offered by such companies include:

Table 1.
Example of Commercial Mobile RAT Offerings

Company	RAT Name	OS Compatibility	Assessed Release Date
Hacking Team	Remote Control System (RCS)	Android, iOS, Windows Mobile, BlackBerry, Symbian	2009
Gamma Group	FinFisher	Android, iOS, Windows Mobile, BlackBerry	2011
NSO Group	Pegasus	iPhone*	2016
DarkMatter	Karma	iPhone*	2016

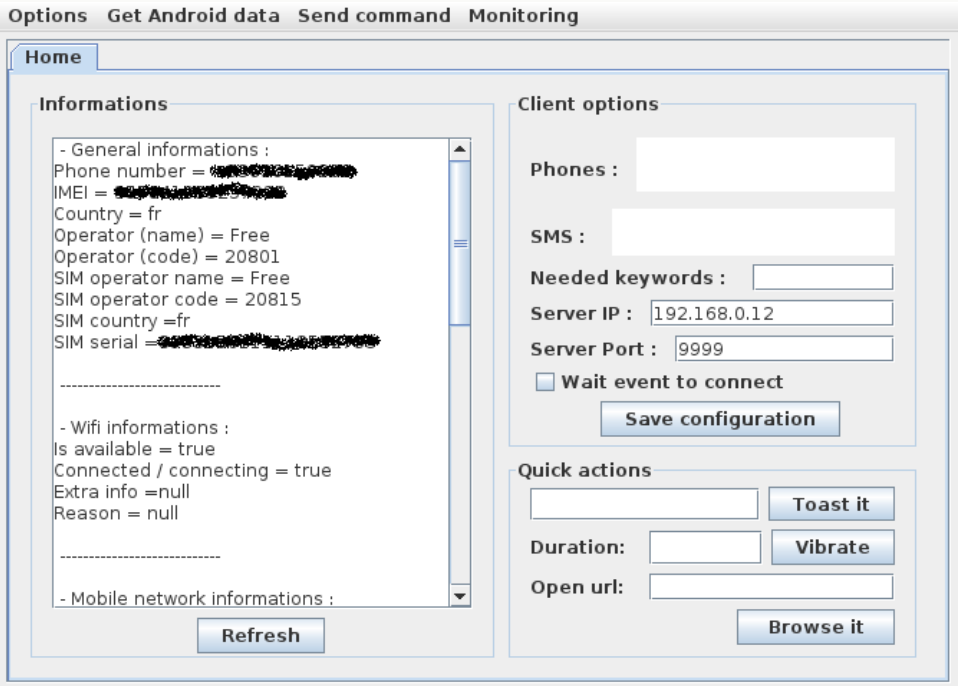
(* publicly identified capability, may not be exhaustive)

Although some deployment operations of this type may involve using zero-day exploits to silently install their malware on target devices, some groups also take the more traditional route of packaging their malware to make it seem legitimate. For example, the group responsible for the Exodus malware took extensive steps to register with Apple as an enterprise developer, using the identity of a possible cover company called Connexxa S.R.L., allowing them to distribute a version of their malware for iOS devices.

While these high-end commercial RATs are likely to be deployed only in limited circumstances against targets that their customers consider high value, the sophisticated nature of such operations is worth considering as part of an overall threat model.

Finally, there are mobile RATs that are offered free-of-charge to the public at large. Many of these have been published allegedly for educational purposes or to enable "adversary simulation," but as they are often provided with a full suite of tools to assist in "Trojanizing" existing mobile applications and controlling infected machines, they are also an attractive proposition for low-skilled attackers to use in active campaigns. For example, AndroRAT provides a "binder" that automatically includes malicious code in user-provided, legitimate Android Package (APK) files such as WhatsApp, which can then be sent to targets in a variety of ways.

Figure 1.
AndroRAT Client GUI



These RATs also assist malicious actors in the development of their own capabilities, as the source code is either freely offered or easily recovered using decompilation processes. The recovered code base can then be adapted or extended to suit a malware developer's requirements, as well as modified to evade antivirus detection — for instance, the STATIC KITTEN adversary has used AndroRAT as a basis for early versions of their mobile malware capability. These freely available mobile RATs have been able to jump-start an industry of campaigns against a broad spectrum of targets and spurred by a variety of motivations.

BANKING TROJANS

Banking Trojans are a popular subset of mobile malware that specifically target mobile banking services for financial gain. In recent years, the enthusiastic adoption of mobile devices and their ability to deliver banking services has made them attractive targets for criminal groups.

The Trojans are often distributed disguised as a legitimate application, while also embedding additional functionality that enables the interception of user credentials and 2FA tokens sent to the device. Many of the banking Trojans available on criminal forums offer a range of features as plugins, which are available depending on the package purchased. Most of them function effectively as standalone RATs.

The primary use of most banking Trojans is to deploy "overlays" that are shown on the user's screen when they attempt to access mobile banking services on their devices. These overlays place invisible input boxes over legitimate logon panels in order to intercept, log and then pass on user credentials to the real banking service to maintain expected functionality. The developers of these Trojans will often add compatibility for additional banking services or provide updates to existing overlays if the targeted applications change their layout; this in itself is a revenue-generating process, as the developers charge a recurring fee for access to updated overlays, motivating them to continue supporting their tools over extended periods of time.

In order to subvert additional security measures such as the implementation of 2FA as part of banking service authentication processes, banking Trojans were developed with the ability to intercept tokens sent by the bank as SMS messages, ultimately relaying them to a C2 server. This process is supported by an automated backend system that immediately authenticates with the bank using the stolen credentials and token, thereby giving the attacker access to the account. While this functionality can be performed exclusively on the mobile device, due to the prevalence of mobile banking, variants of malware such as SpyEye were performing SMS interception for this purpose in 2011 and earlier. In these cases, an infected desktop machine could attempt to infect mobile devices owned by the target. This was done by displaying injected web page content with links to a malicious APK that would then work in conjunction with SpyEye to intercept 2FA tokens, even though the majority of the banking activity was occurring on the desktop.

Recent evolutions of the capabilities exhibited by banking Trojans include more sophisticated ways of performing overlays, in an attempt to avoid detection by source code analysis procedures and application sandboxing undertaken by application store owners and security companies. For example, the Gustuff Android banking Trojan attempts to actively coerce victims into entering their banking credentials by sending fake push notifications that display a phishing page when clicked. It then uses Android's accessibility features to intercept credentials input through the virtual keyboard.

MOBILE RANSOMWARE

Ransomware is malicious software that seeks to deny victims the full use of their computing devices and/or data until a ransom has been paid to the attacker, typically using a digital currency. The majority of ransomware strains targeting desktop machines operate by encrypting data files found on the hard drive, and preventing access to a user's documents, photographs, and other media files. As with other classes of criminal malware, the concept of ransomware has been replicated within the mobile environment to take advantage of the wide adoption of mobile devices.

While some mobile ransomware families attempt a file encryption process similar to desktop versions, this strategy often fails. This is due to the prevalence of cloud storage for files on these devices, as well as limitations on the speed of encryption created by mobile CPUs and battery life. Instead, it is far more common for ransomware authors to "lock" the device by using their malware to display a message and not accept any further input until the correct access code has been provided. The access codes are provided when the victim pays a ransom, which is similar to the way traditional ransomware operates.

Mobile ransomware is often distributed through dropper Trojans that can be used to quickly package up a standard ransomware code base in large numbers of malicious application files. These files can then be repeatedly uploaded to app stores in an attempt to infect the maximum number of victims in a single campaign. This makes detection via traditional antivirus mechanisms more challenging, as these files need to be inspected thoroughly to determine their true purpose.

CRYPTOMINING MALWARE

A further adoption of traditional revenue generation schemes applied to mobile devices is the introduction of cryptomining. This involves the covert execution of calculations that generate digital money (cryptocurrency) for the malicious actor. Cryptomining can be performed either directly through Trojan code hidden in otherwise legitimate-looking applications, or via JavaScript code executed using the device's web browser. In both cases, Trojanized applications have been observed on the Google Play store that embed cross-platform mining frameworks, such as CoinMiner and Coinhive, to generate Monero currency without the knowledge of the user. It's worth noting that cryptomining via mobile devices is inefficient due to the reliance on battery power, which is rapidly consumed by the calculations performed by the device, as well as the lack of algorithm optimization for mobile central processing units (CPUs). However, the vast number of potential victim devices available may still represent an attractive target to less skilled malware developers.

The result of being compromised by cryptomining malware is likely to be most acutely observed through the slower performance of a mobile device as it conducts the required calculations, and it may also cause devices to fail due to extended periods of high CPU use. A secondary effect may also be observed through the increase in device battery usage, which reduces the life of a single charge and the overall lifespan of the device through more frequent discharge/charge cycles.

Early attempts at performing cryptomining on mobile devices were first seen around 2014 in the LepriCon malware family, although activity has

appeared to have peaked between 2017 and 2018, correlating with record highs in the valuation of digital currencies. While the profit generated by this class of malware is likely to have been reduced due to an overall downturn in the current trading rate of the major digital currency such as Monero, CrowdStrike® Intelligence assesses that Trojanized mobile applications will continue to embed cryptomining code due to the relatively low development requirements and risk incurred by the malware authors.

ADVERTISING CLICK FRAUD

Another class of mobile malware is observed through the distribution of tools designed to accomplish advertising click fraud, in which devices are hijacked to perform fake clicks on ads in order to generate income for the criminal actor. This activity represents a potentially lucrative stream of income; in 2016, the World Federation of Advertisers estimated that this type of fraud could total up to $50 billion by 2025.

The click fraud process is enabled through the creation of hidden HTTP requests to specific advertising resources associated with the actor. Although this technique is a reimplementation of activity seen on desktop devices for many years, the large potential installed base and geographic distribution of mobile devices can provide extra challenges for companies looking to detect this type of fraud using statistical analysis methods.

While malware designed to perform click fraud may not represent an obvious or direct threat to the owner of the device, the procedure can cause financial loss because of the use of mobile data required to load the link and the subsequent landing pages required to register the advertising impression for payment. A second-order effect may be the increase in device battery usage similar to that which occurs with cryptomining malware.

As with the other classes of mobile malware discussed in this section, click fraud malware also represents a potential future threat as it can be repurposed easily to perform other functions. For example, click fraud malware for the Android OS was observed being repurposed to conduct distributed denial of service (DDoS) attacks through the modification of target URLs and the frequency of the requests. The power of such DDoS botnets may be limited by mobile device bandwidth and battery life, although the malware is likely to infect devices for longer periods of time due to the limited range of available antivirus tools.

DISTRIBUTION MECHANISMS

More sophisticated malicious actors may seek to develop and deploy exploits against mobile software that allow them to install malware without user interaction or awareness.

Mobile malware can be installed on target devices using a number of different mechanisms, although most variants ultimately take the form of some kind of Trojan application that the user is persuaded to install. This can be passive, such as appearing like an attractive application such as a game or utility, or it can be a more active approach triggered by a phishing attack that leads the victim to install the malware.

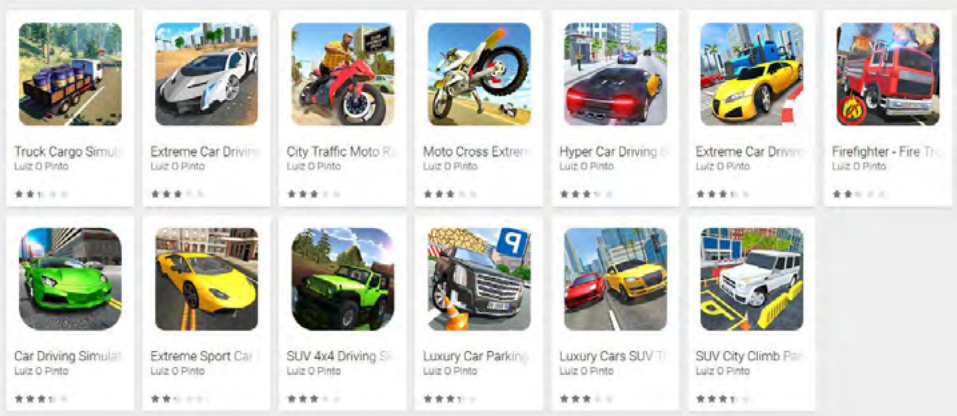
However, there are exceptions to this rule: More sophisticated malicious actors may seek to develop and deploy exploits against mobile software that allow them to install malware without user interaction or awareness. This approach subverts typical security advice, which would normally minimize the risk of infection by ensuring that users only install applications from trusted sources.

TROJAN APPLICATIONS

APP STORE DISTRIBUTION

The simplest Trojan distribution technique uses the offer of free tools or popular, legitimate applications as carriers for the malware. These Trojans are uploaded to app stores in large numbers to take advantage of volume distribution in much the same way that spammers rely on a small percentage of respondents from the millions of emails they send in each run. Some of these campaigns can result in vast numbers of installs, which is further amplified by applications that are prominently featured in stores. Often this is due to algorithms that select popular or trending software for wider user consideration. In one example disclosed by a security researcher, 13 applications created by a developer called “Luiz O Pinto” were downloaded over 560,000 times after they were added to the Google Play store. While they purported to be driving simulation games, when opened, they instead downloaded an additional APK (Android package) to display advertisements to the user each time the device was unlocked.

Figure 2.
Luiz O Pinto Malware Featured in Google Play Store



(Source: Lukas Stefanko)

While the previous example contained no legitimate functionality, malware authors are able to easily decompile legitimate applications and add code to perform malicious actions alongside the normal functionality. To the casual user, the recompiled apps are often indistinguishable from the originals. Typically, they are added to app stores using slight variations of the legitimate developer's name to further establish some credibility with users. When this occurs with enough frequency, inadvertent installations of these Trojan apps on mobile devices are inevitable.

Official app stores for the two most popular mobile operating systems — Google Android and Apple iOS — take slightly different approaches to their developer verification and application submission processes, leading to different levels of risk that a user might download a Trojan app. While Apple requires developers to register in order to submit their applications to the App Store (including paying a fee), the open source nature of Android is far less restrictive about who can develop for their platform and be featured in the Google Play store. This has prompted a larger volume of submitted apps, increasing the complexity of a detailed verification process in comparison with Apple's offering.

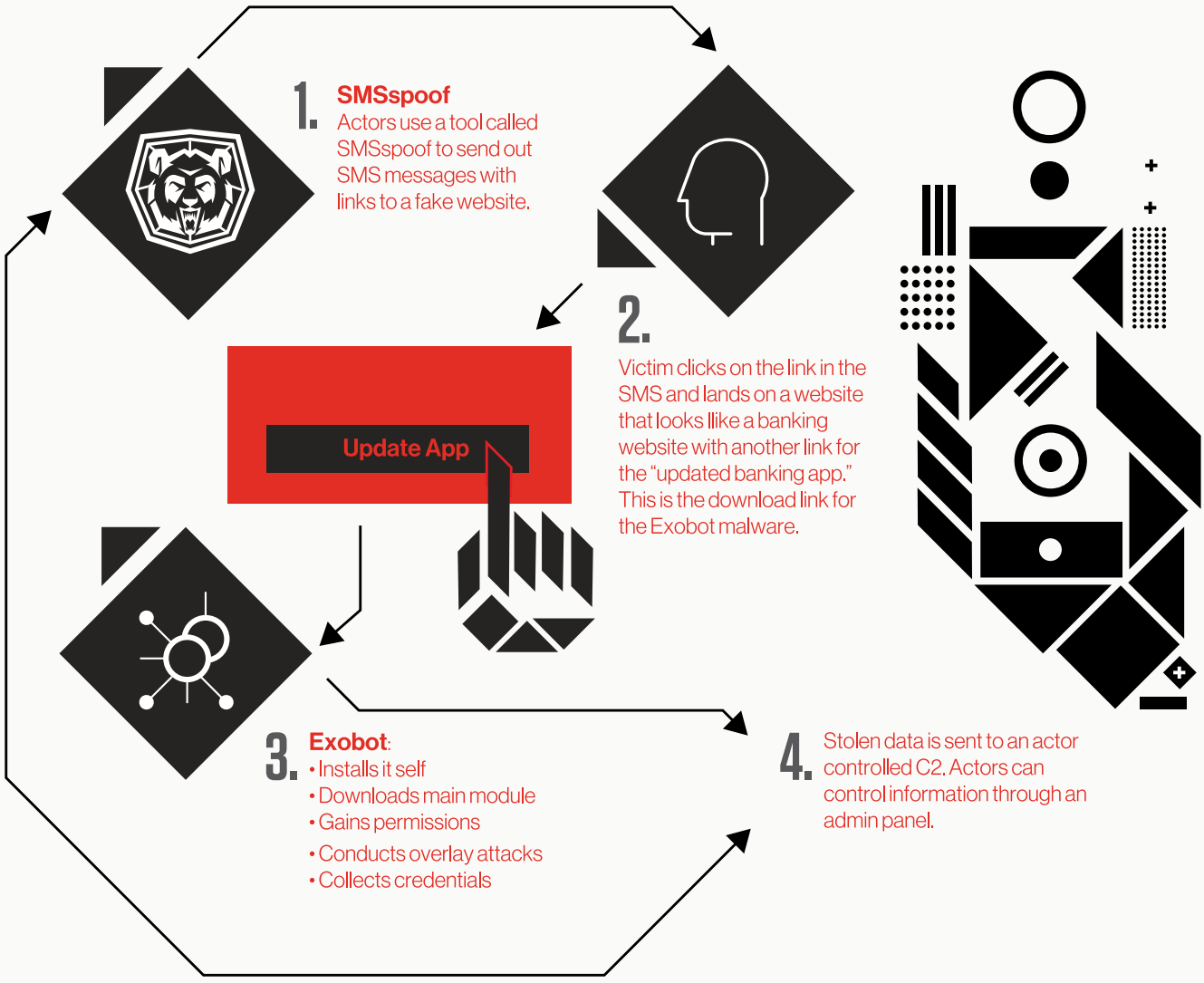
Although Apple appears to employ a more stringent approach to investigating apps for malicious intent, occasionally, malware gets submitted successfully and made available for download via the company's app store, at least for a period of time. For example, a Mac OSX Trojan, in the form of a paid-for app on the Mac App Store called Adware Doctor, was discovered in July 2018 by a security researcher. It was also determined that the app collected and exfiltrated the web browsing history on infected machines. While this particular malware targeted desktop machines, the approval process for mobile apps is largely the same and therefore demonstrates that apps that could be considered malware still have the potential to be downloaded by the public.

A further risk posed to Android users is the availability of third-party app stores that primarily rely on user reviews — which can be easily manipulated — as the primary mechanism for verifying whether an app is trustworthy. In addition, users may take advantage of the ability to load APK files directly on a mobile device without having to use an app store at all. This paves the way for malicious actors to distribute their Trojan software outside the Google Play app store ecosystem.

PHISHING-ENABLED DISTRIBUTION

A popular method for coercing users into installing malicious applications is to send them links to APK files hosted on attacker-controlled websites, normally achieved through either SMS or email spam messages sent to large groups of targets. Figure 3 shows how operators of the banking Trojan Exobot have distributed links to the fake mobile banking app that enables website overlays and credential stealing on infected devices.

Figure 3.
Exobot SMS Phishing Infection Chain



Recently, a new version of the MoqHao malware was distributed using SMS spam messages primarily targeting Japanese and South Korean users. Android users were prompted to install a malicious APK from an actor-controlled website. The malware would act as an information stealer to collect SMS messages and audio from an enabled microphone. The adversary approached the targeting of iOS devices in a different way because the devices only allow applications to be installed from the official Apple App Store. Instead of deploying malware to the device, the users were shown a phishing page that profiled their devices and attempted to obtain Apple ID credentials.

DISTRIBUTION VIA COMPROMISED WEBSITES

In more targeted operations, the dissemination of mobile malware may be facilitated through the compromise of a legitimate website that is then used to host a malicious app. This approach lends an additional layer of legitimacy to the campaign, as potential victims are unlikely to assume that a known website is attempting to compromise their mobile devices. For example, CrowdStrike Intelligence analysis of a mobile malware family, likely developed by the threat actor STATIC KITTEN, suggests that the Turkish NGO website setav.org was used to propagate mobile malware as part of a spreading mechanism delivered to additional targets via SMS.

Although this methodology still relies on installation of an application without using an app store (therefore excluding iOS devices), it may still be successful in campaigns where the actor may already know the device usage patterns of their targets.

DISTRIBUTION VIA COMPROMISED OPERATING SYSTEM IMAGES

An alternative to app store deployment of mobile malware is the distribution of Trojan applications through their inclusion in custom operating system (OS) images. On platforms that allow device manufacturers to load their own OS version images at the point of distribution, there is a risk that Trojan apps may be included as part of standard distributions that are installed by default on new phones.

COMPROMISED SOURCE CODE

Legitimate applications can also be Trojanized by a malicious actor without the knowledge of the original developer. A malware strain dubbed SimBad was estimated to have been installed 150 million times during 2018 in an operation that involved the compromise of the RXDrioder Software Development Kit (SDK) used by a number of legitimate developers to create applications that with each build include malicious code in the app package.

Sometimes this approach can be even more subtle. CrowdStrike Intelligence has previously reported on a FANCY BEAR operation to compromise users of an application designed to facilitate secure communications between groups of people on military service in Ukraine. Given that the application was only distributed to a limited number of individuals, it is likely that the adversary gained access to the developer's computer in order to retrieve source code, so that it could be modified prior to redistribution. The act of redistribution was performed using emails spoofed to look like they came from the original developer, which instructed the recipients to install a new version of the app from an attached file.

SOFTWARE EXPLOITATION

While the distribution of Trojan applications is the most common form of deployment mechanism for mobile malware, there are limited circumstances where a malicious actor may develop or procure remote exploits for typical software installed on target devices, and then use them to install their payloads without user interaction. An example uncovered in May 2019 was the disclosure of a vulnerability in the WhatsApp chat application (designated identifier CVE-2019-3568) that enabled attackers to gain remote code execution on target devices through a specially crafted series of secure real-time transport protocol (SRTCP) packets. When successfully executed, this could facilitate the download and installation of malware without the user's awareness or consent. Although exploits of this class are relatively rare compared to the larger attack surface seen on desktop machines and servers, their existence demonstrates that even strict adherence to not downloading untrusted applications may not be sufficient to avoid compromise for certain classes of targets.

Software exploits are also frequently used by malware in a post-installation phase to escalate privileges to a level that allows actors to collect information from the target device and perform other malicious actions. Even though malicious actors may seek to develop privilege escalation exploits themselves, they may also take advantage of a significant community of researchers who identify and publish these techniques to enable individuals to "root" their own devices so that they can load custom OS images. While details of privilege escalation exploits and techniques are too numerous to list in this report, their existence underscores the importance of keeping mobile software, and the operating systems it runs on, up to date with security patches at all times.

LOSS OF PHYSICAL CONTROL

Most of the deployment mechanisms described above involve compromise that occurs while the device is in the possession of the user, whether this is through user interaction or remote exploitation. However, there may be situations where a malicious actor seeks to leverage a period of time when the device is not in the possession of the user. Scenarios such as monitoring software installed by authorities during a border transit, or a device left unattended in a hotel (a so-called "evil maid" attack), are likely to occur only in very specific situations, but could still arise depending on the value of the target.

While device compromise through a lack of physical control of the device is an unlikely scenario in many cases, it may still be applicable to individuals or organizations travelling to hostile areas. This class of threat may potentially be avoided through the use of PINs or passwords (unless these are obtained through coercion or through passive monitoring via video surveillance or traditional "shoulder surfing" techniques) in some situations, or through the use of completely clean devices that only carry the minimum of data and are completely reset to their original settings once the user has returned.

USERS OF MOBILE MALWARE

So far, this report has focused on typical types of mobile malware and how they may be placed on a victim's device — describing the "what" of the current threat landscape. The following section addresses some of the aspects of "why" mobile malware is used and "who" are some of the notable users of these capabilities. Of course, while it is not possible to fully define every possible use case and threat actor currently operating within this attack class or seeking to develop similar capabilities, this section examines some notable cases that demonstrate the threat to mobile devices and their users.

DEPLOYMENT MOTIVATIONS

FINANCIAL GAIN

Arguably the most prevalent use case for the development and deployment of mobile malware is to facilitate financial gain on the part of the criminal actor. At the lowest end, passive revenue generation via cryptomining or ad fraud may have only a minor impact on infected devices through increased mobile data usage and battery power consumption. However, the adoption and growth of mobile banking has made these devices an attractive and valuable target for criminals, who have built whole operational frameworks to automate accessing victims' online bank accounts and transferring funds to other accounts under their control.

BANKING TROJANS

There is a wide range of mobile malware designed to capture banking credentials to facilitate theft, with additional families being offered for sale on criminal forums on a regular basis. In late March 2019, a new malware family called Gustuff began being distributed to targets in Australia via an SMS spam campaign. Gustuff gets victims to enter their credentials by triggering push notifications sent by the fake banking app, and using a mechanism called automatic transfer system (ATS) to pass captured credentials on to the legitimate applications afterwards. At the time of this writing, overlays for over 100 financial institutions in the U.S., Australia, Poland, India and Germany are provided by the malware.

The profitability of this style of campaign has triggered a security "arms race" in much the same manner as has been observed in the traditional computing sector, where each feature added by the banks is systematically evaluated by malware authors in order to build work-arounds. For example, simple credential phishing pages became less effective as dedicated mobile applications were introduced, leading to the development of malware that can display custom overlays to intercept credentials whenever the targeted apps are opened.

Mobile devices have also been adopted as part of the security landscape by acting as the second factor in 2FA schemes used to secure services such as banking and email accounts. This approach causes additional challenges for credential interception malware installed on desktop machines. Therefore malware authors have begun targeting the mobile devices to collect 2FA tokens produced as part of challenge-response authentication protocols.

Of all the technical implementations of 2FA token transmission, the interception of tokens sent using SMS appears to be the most prevalent, where mobile malware monitors for incoming messages and forwards them to the attacker. Online services have now begun to adopt other 2FA mechanisms due to insecurities in SMS, such as the ease with which inbound challenge messages can be spoofed and message interception attacks against the Signalling System 7 (SS7) telecommunications standard. As a response, mobile malware has also adapted to collect these tokens in different ways. An example of this is demonstrated by the Bankosy Android banking malware, which overcame interception challenges caused by 2FA tokens being sent in voice calls by configuring target devices to set up call-forwarding to an attacker-controlled number so that they could be monitored and used without the user's awareness. In the future, it is likely that attackers will implement further mechanisms for gaining account access, such as automatically clicking one-tap authentication challenges generated by recent 2FA implementations.

The highly-centralized nature of user communications on one device — such as email account data — also provides criminals with further opportunities for account takeovers, which can be monetized in a number of ways.

INTELLIGENCE GATHERING

As previously discussed, the installation of RAT malware on mobile devices provides access to a large amount of high-resolution victim data, including but not limited to:

- Device information
- Contact information
- Email/message contents

- Arbitrary file contents
- Image data from on-board cameras and screen displays
- Audio data from on-board microphones
- Geographic location via GPS and cell tower telemetry

In its totality, this range of information could be of significant value to a number of classes of malicious actors who seek to collect information on a target over a period of time. While the exact data to be extracted will vary depending on the origin of the threat actor (e.g., nation-state or state-aligned, law enforcement, private investigators, or even users of so-called "spouseware"), it is likely that many of these sources of information will be exploited during mobile malware campaigns.

Such tools may also be used to facilitate further monitoring of victims using external collection capabilities. For example, 2FA tokens may be intercepted to provide remote access to cloud-based services such as email accounts, while access to IMEI and IMSI numbers could potentially allow for alternative target correlation and data collection using indigenous signals intelligence (SIGINT) programs operated by sophisticated state actors.

DISRUPTION

Another use case for mobile malware could be to support an operation that seeks to disrupt business operations as part of a wider attack against a company or sector. During targeted ransomware attacks against traditional computing assets, for example, companies may fall back to using mobile devices with email and document data stored on cloud services in order to maintain a level of business continuity. While the scenario is hypothetical at the time of this writing, it is possible that adversaries may seek to incorporate pseudo-ransomware that implements PIN-lock techniques alongside ransomware targeting traditional computing devices, to amplify the effect of the attack, whether it is financially or politically motivated.

It is worth noting that successful disruption attacks typically benefit from maximum coverage of infected hosts along with a short period of time to encrypt or otherwise disable the devices. Spreading mobile pseudo-ransomware may be possible using targeted phishing attacks for deployment, with a waiting period before the payload is triggered. It is also conceivable that adversary access to corporate mobile device management (MDM) or mobile application management (MAM) systems could allow them to push out over-the-air (OTA) updates that install the malware on each corporate device at the same time. An example of the use of this deployment methodology was identified in July 2018 as part of a highly targeted attack against a small number of targets in India. In this case, the targeted iPhone devices were enrolled to use an attacker-controlled MDM server, which was then used to push malware-infected versions of legitimate apps, such as WhatsApp and Telegram.

TARGETED ADVERSARY GROUPS

CrowdStrike Intelligence tracks a number of targeted intrusion adversaries that have begun developing mobile malware as part of their overall operational tool kit. Often these implementations are mobile ports of malware originally developed for desktop computers, and therefore share commonalities including general capabilities and C2 protocols. This adoption of such variants is indicative of the recognition that the shift in user computing towards mobile devices provides a number of benefits to intelligence collection, and is likely to continue as a trend. Table 2 summarizes some of the known targeted mobile malware variants tracked in recent years.

Table 2.
Examples of Targeted Adversary Mobile Malware

Actor	Malware	Earliest Observed Date	Targeting Motivation
FANCY BEAR	X-Agent variant	2013	Targeting of military forces in regional conflict areas
BERSERK BEAR	BARBARIAN variant	2014	Targeting of individuals in CIS countries for counter-terrorism purposes
Unknown PANDA with possible connections to Ministry of State Security (MSS)	Unnamed Android and iOS malware	2014	Targeting of protestors associated with the Umbrella Revolution/Occupy Central movements in Hong Kong
RICOCHET CHOLLIMA	Cumulonimbus	2017	Targeting of North Korean defectors and journalists in Republic of Korea
LABYRINTH CHOLLIMA	Manup	2018	Targeting of individuals in the Republic of Korea, possibly relating to government or military sectors
LABYRINTH CHOLLIMA	Hawup variant	2016	Targeting of individuals in Republic of Korea
STATIC KITTEN	TitanRAT	2018	Targeting in Middle East region
VICEROY TIGER	KnSpy	2018	Targeting of individuals in the disputed Kashmir region
MYTHIC LEOPARD	Unnamed Android malware	2016	Likely targeting of India-based individuals
DEADEYE JACKAL	ChatSecureRAT	2016	Targeting of Syrian opposition forces
EXTREME JACKAL	Unnamed Android malware	2016	Targeting of Israeli citizens

THREAT OUTLOOK

MOBILE DEVICE SECURITY

The initial development and increased distribution of mobile malware in recent years appears as a tacit acknowledgement by a range of malicious actors of not only the general shift in user computing, but also the utility of mobile devices as a source of intelligence or financial gain. As with malware designed to target desktop machines, there is a continual battle between defenders and attackers seeking to maintain or subvert the security of these devices. This has resulted in an ever-increasing set of malware capabilities that have been developed to ensure that malicious actors can continue to achieve their objectives.

Despite some similarities between the implementation and goals of desktop and mobile malware, the security landscapes they operate in are very different. While desktop computing has benefited from years of development in commercial and open-source malware research and detection, the current state of defensive technology in the mobile space is less mature; although mobile malware is researched by the security community, detection methodologies that can be employed by the user — such as antivirus monitoring — are currently more limited in comparison. This factor is particularly acute in the Apple ecosystem, where software access to operating system internals is extremely limited, thereby preventing comparable introspection in ways that could identify malware running on these devices. As such, most security vendors focus on creating apps that attempt to prevent access to malicious web content via hooks provided by the operating system, although these tools will fail to detect malware installed using remote exploits, for example.

Furthermore, the increase in the adoption of filesystem encryption on mobile devices has made post-exploitation forensic analysis more challenging. In addition, the nature of mobile communications often means that centralized network monitoring strategies are likely to miss C2 messages sent by mobile malware, unless the host devices are connected to corporate networks. Therefore, mobile devices infected with malware are likely to remain undetected for longer periods of time, increasing the window of opportunity for attackers.

INFECTION VECTORS

While the loading of malicious applications from untrusted sources is likely to remain the most prevalent source of infection in the mobile threat space, this mechanism typically relies on targeting devices that allow this type of installation process. Mobile operating systems that do not allow installation from outside their application store ecosystems need to be “jailbroken” by their users before they are able to accept third-party apps. This severely limits the availability of targets susceptible to such attacks.

CrowdStrike Intelligence assesses that they are likely to see further porting of traditional targeted malware families to mobile platforms in order to aid the intelligence gathering process, particularly by actors who require tracking their victim's physical location via GPS telemetry, or who focus on specific geographic regions.

As a solution to this challenge, adversary use of malicious MDM servers to install malware payloads is likely to become a more popular infection vector over time, particularly as these facilities can command significant control over the mobile devices. While there are still hurdles to overcome regarding the registration of target devices with the malicious server, a combination of social engineering techniques may be used to achieve this goal.

It is unlikely that there will be a significant increase in the use of fully remote, non-interactive software exploits to install mobile malware in the near future, primarily due to their relative rarity and corresponding value in the exploit broker community. This vector will therefore continue to be used selectively as part of targeted operations instead of across a broader range of campaigns.

EVOLVING THREAT CLASSES

In this report, several mobile malware threat classes have been defined and their deployment motivations discussed within the context of their capabilities. While many of these threats are simply variants of traditional security threats that have been extended into the mobile computing space, the opportunities they present to malicious actors are likely to have an impact on the way they evolve in future.

REMOTE ACCESS TOOLS

An ever-increasing scrutiny of desktop machines by security products is likely to lead to further investment in the development of mobile RATs, particularly by targeted threat actors who seek to maintain access to their victims for extended periods of time. To this end, CrowdStrike Intelligence assesses that they are likely to see further porting of traditional targeted malware families to mobile platforms in order to aid the intelligence gathering process, particularly by actors who require tracking their victim's physical location via GPS telemetry, or who focus on specific geographic regions. State actors with SIGINT collection missions are also likely to invest in the creation of mobile malware as a solution to the increased adoption of encrypted network communications across email, web, and messaging services, as access to a mobile endpoint will provide opportunities to subvert this trend. This is likely to be particularly prevalent in Middle Eastern countries where the commonplace deployment of ISP-level traffic monitoring hardware may be defeated through the use of application-level encryption.

Outside of state actor development of mobile malware, sophisticated commercial developers are also likely to continue to develop mobile monitoring solutions as part of their portfolios, due to the lucrative contracts associated with their sale. This development has continued despite the compromise of two vendors of such RATs (Gamma Group and Hacking Team) between 2014 and 2015 by the hacktivist Phineas Fisher, where extensive details of their portfolios and tool capabilities were published publicly.

Criminal actors are also unlikely to reduce their development of mobile RATs in the future, due to the financial opportunities they continue to present. While the facilitation of banking theft is an obvious motivation, data collection provided to an attacker through the interception of email credentials can yield numerous benefits, including the takeover of third-party accounts. In addition, many developers of criminal RATs tend to operate at a lower level of personal risk, as they merely offer malware for rent through subscription processes instead of leveraging the tools themselves.

BANKING TROJANS

The vibrant development community built around the creation and sale of mobile banking Trojans shows no sign of slowing down, as the potential benefit from successful infections can be particularly lucrative. As with many criminal enterprises, most operational complexities and security issues stem from the process of transferring and laundering money so that the identity of the thieves remains unknown. However, the majority of banking Trojan developers offset this risk by selling their capabilities via subscription. These subscriptions are maintained through the continual development and improvement of banking app overlays, ensuring that their customer base continues to invest in capabilities that allow them to maintain access to a wide pool of potential targets. While some Trojans may fall out of favor or be removed from public sale (such as Red Alert Bot), CrowdStrike Intelligence frequently observes new families being introduced in underground criminal forums, and it assesses that this process will continue into the future.

ACCESS FACILITATION

The adoption of mobile devices as a second factor in 2FA schemes has marked them as a new target of opportunity for malicious actors who seek to gain access to accounts and services protected by these mechanisms. Although the ever-present nature of mobile devices offers greater convenience to users when compared to legacy 2FA tokens, built-in network connectivity dramatically increases their attack surface. As more corporate

environments implement 2FA to protect access to services from external connections, it is likely that specific mobile malware designed to subvert these protections for targeted operations will be observed in future.

Malware designed to intercept tokens transmitted via SMS or voice and mobile components of desktop malware are already common. In addition, screenshot capture capabilities implemented by many RATs could easily be leveraged to copy visual output from on-device 2FA authenticators generating time-based one-time passwords (TOTP), and then pass the credentials to an attacker before they expire. A combination of attacks may also be used to trick users into opening their authenticator app to enable this process, such as using installed malware to send fake push notifications claiming to be issued in response to an authentication challenge.

Other 2FA implementations such as Duo Mobile offer a "one-tap authentication" mechanism that triggers in response to an authentication event pushed from an external service, allowing the user to approve or deny requests sent to their mobile devices. While CrowdStrike Intelligence has not yet observed malware targeting such a mechanism, it is possible that auto-click functionality already demonstrated in many mobile malware families may be used to automatically approve malicious connections to a service without the user's knowledge.

RANSOMWARE

Mobile ransomware is relatively easy to implement and therefore provides malicious actors with opportunities for financial gain with a minimal outlay of resources. The majority of mobile ransomware strains are likely to be PIN-lock variants that prevent access to the device without payment, as opposed to crypto-ransomware that encrypts files on a device.

Although many ransomware variants target single users, there are indications that the model may also be adopted by organized criminal actors, possibly in response to customer or affiliate requirements. For example, PINCHY SPIDER's recruitment of an APK reverse engineer, along with individuals skilled in lateral propagation techniques, suggest that they may be seeking to adapt their services to target corporate environments, possibly including mobile platforms.

Previous observations of ransomware being used as a cover for disruption campaigns in the traditional computing sector indicate that malicious actors may attempt to apply this approach to mobile devices, as well. While there are several hurdles to overcome in this style of operation, such as the ability

to self-spread easily among connected devices, an effort to achieve total business disruption may be considered by particularly motivated actors in some circumstances.

CRYPTOMINING

Due to the low-revenue nature of cryptomining on non-specialized mobile CPU hardware, this threat class was likely to have been a reasonable source of criminal income only during periods where cryptocurrency valuations were at the peaks — observed between 2017 and 2018. The subsequent crash in a number of digital currency markets has reduced the overall value in operating such campaigns; this is evidenced by the discontinuation of the CoinHive mineware service in February 2019 due to profitability issues. Although it is likely that some lower skilled malicious actors will continue to operate in this space by creating margins on the basis of large malware install bases, it is unlikely to represent a significant threat in the overall mobile landscape.

Previous observations of ransomware being used as a cover for disruption campaigns in the traditional computing sector indicate that malicious actors may attempt to apply this approach to mobile devices, as well.

Despite this, cryptomining performed by some legitimate applications as an alternative to including advertisements or requiring an outright purchase may still continue, although this approach is harder to categorize as malware in a traditional sense.

GEOGRAPHIC VARIATIONS IN THE THREAT LANDSCAPE

In the future, different mobile malware threats are likely to disproportionately affect some regions more than others. For example, Latin American countries have a high reliance on mobile devices across the general population, as they are a more cost-effective mechanism for personal computing. As such, a larger proportion of users are likely to conduct some degree of banking using these devices, presenting an attractive developing market for criminal groups. While it could be argued that access to bank accounts on a per-infection basis may be higher in other regions, the prevalence of mobile banking in Latin American countries is favorable for actors who rely on a “numbers game” for profitability.

As previously discussed in this report, the security postures and policies of the major mobile operating systems have implications that define the threats they face, the likelihood and mechanisms of infection, and the capabilities malware can leverage once installed. Regional variations in purchasing habits will therefore have some bearing on the type of mobile malware targeting specific users. For example, although Android is the most prevalent operating system in most markets, the significant majority it holds in the Asian and

South American regions (reflected by Samsung's market penetration) suggests that most malware targeting users in those regions will be authored for the Android platform.

There is near domination of the market between Google Android and Apple iOS platforms, therefore it is likely that almost all malware will be designed to operate on one of these two operating systems, despite some malware supporting Windows Mobile and the defunct RIM/Blackberry OS. While some of these variants are likely to be highly targeted commercial malware designed to cover a portfolio of targets, including those in emerging markets, the economics of software development and return-on-investment for malware authors suggest this approach will stay consistent for some time.

Aside from socioeconomic factors defining the adoption of mobile computing, political and commercial factors may also contribute to an uneven security landscape. The addition of Huawei, the Chinese telecommunications manufacturer, to the May 2019 U.S. executive order barring U.S. firms from conducting business with companies that threaten national security may have future implications for the security of devices produced by that company. This inclusion resulted in Google suspending all business with Huawei requiring the transfer of software and technical services, including their access to updates for Google's version of the Android operating system. Although a Google spokesperson claimed that users of Huawei devices would still have access to Google applications and updates, the hardware manufacturer will currently have to rely on the open-source version of the operating system, which may increase their vulnerability to software flaws and decrease the cadence of critical security updates. This change is likely to disproportionately affect mobile device owners in Europe, where Huawei has significant market penetration, as compared to the North American market where the manufacturer's devices can only be purchased directly from vendors without subsidies offered by U.S. telecommunication providers. As the majority of U.S. consumers procure their mobile phones through carrier plans, the distribution of Huawei devices is much lower in this market. However, it remains to be seen whether this executive order will significantly impact the security of Huawei devices in comparison with Google-supported competitors.

Geopolitical issues could also be exploited by malicious actors to distribute mobile malware, potentially compromising large numbers of victims by leveraging fear to trick individuals into installing the Trojan application. For example, in August 2018 actors suspected to be affiliated with the Palestinian group Hamas released an application containing malicious

functionality that mimicked a genuine application used to alert Israelis of incoming rocket attacks. The release of the malicious application, IsraelAlert, was timed to coincide with escalating tensions between the two countries, thereby increasing the chances that unwitting victims would install the fake application. To see an image of the fake application next to the genuine alert app, go to the Ynet news article, "Hamas launches fake app to hack Israeli cell phones."

INSIDER THREAT / ACCIDENTAL EXPOSURE

In addition to mobile malware, organizations need to be vigilant against any malicious or unintentional transfers of sensitive data. According to a Ponemon study, 50 percent of organizations have had an incident involving an insider threat or accidental exposure of corporate data using a mobile device. The ability to monitor mobile app behavior is critical to not only identifying mobile malware, but also identifying and preventing attempts to exfiltrate sensitive data via potentially risky user interactions — such as cut and paste, taking screenshots and videos, or storing data in an unauthorized network location. Consider implementing tools to enable security teams to proactively hunt for threats on mobile devices and search through telemetry such as mobile network activity, clipboard actions and peripheral connections to identify anomalous and malicious actions.

RECOMMENDATIONS

Flaws in operating system software can be exploited by malicious actors to install mobile malware and escalate operating privileges to obtain greater access to data and capabilities on the device.

The ubiquitous, global use of mobile devices and the amount of corporate data so many of them hold mean that mobile threats will continue to proliferate. Just as certainly, both nation-state and eCrime groups will continue to innovate and refine their mobile attacks to evade your organization's security defenses. CrowdStrike recommends that all organizations consider the following measures to help better secure the mobile devices connecting to sensitive corporate data every day:

1. **Download applications from trusted sources such as official app stores:** The majority of mobile malware is distributed from third-party sources that do not perform comprehensive checks of the applications they provide. This provides opportunities for malicious actors to include unwanted code contained within Trojanized applications. Official sources such as the Apple App Store and Google Play Store provide some level of verification on the apps they provide, limiting the risk of exposure to mobile malware. However, numerous instances of malware have still been distributed via these official channels, even though apps were subjected to checks, and users need to be wary of the applications they download; gaming and mobile banking applications are particularly popular carriers of malicious code.

2. **Be on the lookout for phishing messages:** Users should be wary of messages being delivered by SMS or email that prompt them to install applications from untrusted sources, because this mechanism is often used by attackers to trick their targets into installing mobile malware.

3. **Regularly apply security patches to mobile operating systems and installed applications:** Flaws in operating system software can be exploited by malicious actors to install mobile malware and escalate operating privileges to obtain greater access to data and capabilities on the device. In response, vendors will identify vulnerabilities and develop patches to secure devices from exploitation. These patches should be installed at the earliest opportunity to reduce the risk of exposure.

4. **Establish security around solid MDM processes:** Corporate management of mobile devices can provide protection against mobile malware by restricting which applications can be installed, and allowing for the automatic deployment of security patches. However, this capability can also provide opportunities to an attacker, who may be able to leverage their own MDM servers to deploy malware. That's why organizations should lock down their corporate devices to ensure they are unable to communicate with untrusted MDM servers, and establish user security training to minimize the risk that phishing techniques could be used to trick them into enrolling manually with a rogue server. Servers running MDM software for the organization should also be heavily monitored using endpoint protection, to ensure they are not compromised from within the network and used to push out malicious updates to mobile devices.

5. **Evaluate mobile endpoint detection and response solutions:** Solutions such as CrowdStrike Falcon for Mobile™ take a visibility-first approach to mobile security, eliminating blind spots that lead to breaches. Security teams can see activity generated by Android and iOS enterprise apps, gaining deeper insight into their behavior and enabling threat hunting and rapid incident investigation. Learn more about Falcon for Mobile.

6. **Maintain physical security of physical devices:** Enabling strong passwords, or biometric authentication measures such as fingerprint or facial identification, in addition to ensuring that mobile devices are not left unattended, can reduce the risk that a malicious actor may be able to install malware manually during so-called "evil maid" attacks.

ABOUT CROWDSTRIKE

CrowdStrike® Inc., a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Qualifying organizations can gain full access to Falcon Prevent™ by starting a free trial.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**