Understanding the mobile threat landscape in 2018

2017 was a huge year for mobile security. Malicious actors returned with a vengeance and cyber attacks grew rapidly in sophistication. Ransomware outbreaks like WannaCry and Petya hit enterprises globally causing unparalleled disruption, new vulnerabilities like BlueBorne were discovered and malware variants grew more aggressive and prevalent by the day. This report will summarise the key mobile security trends that emerged in 2017, and summarise thoughts for the mobile threat landscape for the year ahead.

TABLE OF CONTENTS

Introduction 3

The mobile threat landscape 4
- Increased sophistication 4
- A global concern 4
- More vectiors for attack 5
- Organisations left vulnerable 5

Key threat for 2018 6
- Phishing 7
- Malware 11
- Cryptocrime 14
- Network threats 17

Not just threats, but risks 19
- Mobile vulnerabilities 19
- Risky configuations 20
- Data leaks 20
- Protecting customer data 20
- GDPR 21

Protecting your business 23

Introduction

2017 was a remarkable year for mobile security. Attacks aided by AI, sophisticated social engineering techniques and the exponential growth of connected devices, are just a few of the factors that the pathed way to a year of unprecedented threat to the enterprise.

As organizations fight to secure their valuable data against an ever-growing range of threats, the fear of a breach is keeping CISOs up at night. The events of last year proved that organizations have every right to be concerned. Figures show that cyber incidents targeting businesses nearly doubled from 82,000 in 2016, to 159,700 in 2017[1]. Ransomware attacks like WannaCry and SLocker wreaked havoc worldwide and barely a day went by without a data leak or exploit dominating the global headlines.

The threat landscape continues to be asymmetrical, and despite continued investment, enterprises struggle to outsmart cybercriminals. What is it that makes the current mobile security climate that is so volatile? Why do malicious actors seek to infiltrate corporate devices? This report aims to provide answers to these questions by reflecting on recent breaches, giving visibility in the current threat landscape, whilst making forecasts for the year ahead.

It will examine some of the most notable threats to mobile devices over the past twelve months, and predict what the biggest challenges will be to secure the enterprise in 2018.

95%

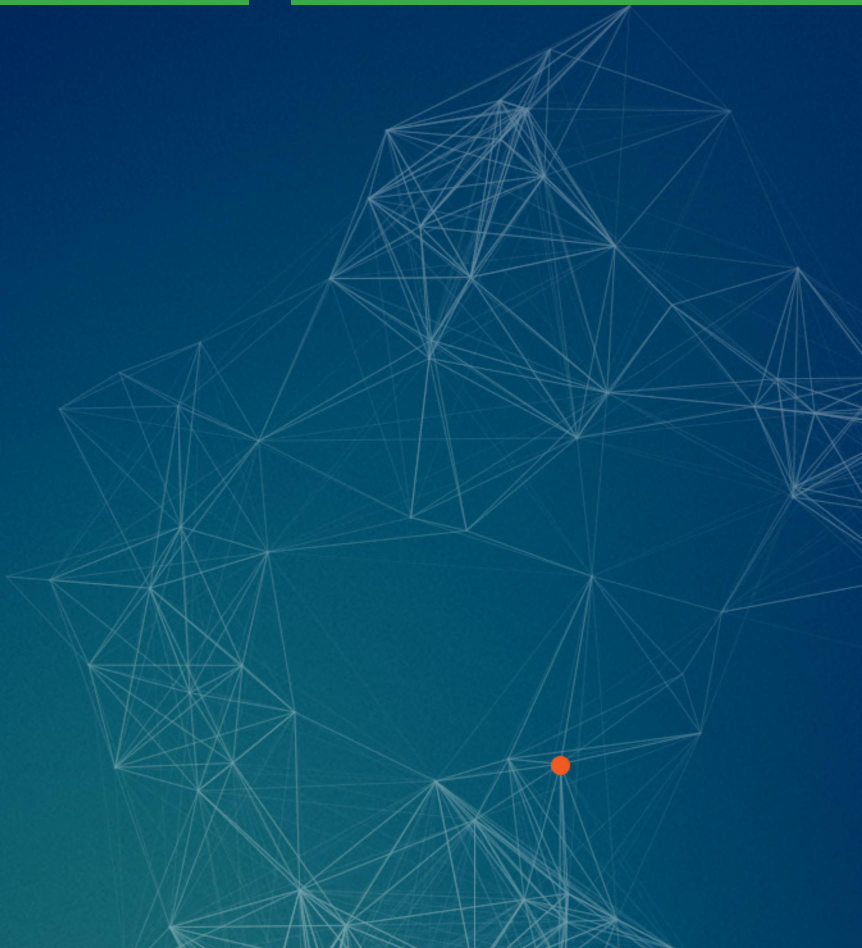
GROWTH MOBILE SECURITY BREACHES IN 2017

88%

RISE IN BUSINESSES TARGETED BY MOBILE RANSOMWARE

#1

MOBILE IS NUMBER 1 CHALLENGE FOR SECURITY TEAMS



[1] *OTA, Cyber Incident & Breach Trends Report*

The mobile threat landscape

It seems like the second the security industry collectively comes to grips with the latest publicly disclosed data breach, a more sophisticated threat gets thrown into the mix. However it's not all doom and gloom - by exploring the key themes and patterns of recent attacks, organizations can find insights to help them avoid becoming the next target.

Increased sophistication

State sponsored actors and well resourced criminal groups were a focal point of attacks throughout 2017. It became abundantly clear that malicious actors are taking their time to research their targets, and play up to their weaknesses. With most web traffic now taking place on mobile devices, scammers are taking note by hitting you with regular device-centric scams. Instead of casting their nets wide with rudimentary techniques in the hope someone will take their bait, attackers focused on creating the perfect malware, or fine-tuning the most effective social engineering technique to bolster their success rates.

The rise of nation state cyber attacks is perhaps one of the most worrying areas of cybersecurity at the moment. When a malicious actor is working for more than financial gain, there is little you can do to deter them. Politically motivated attacks grabbed the headlines throughout 2017, and if they continue to take hold with the same ferocity this year then we could see an escalation from economically driven mobile breaches to politically driven destruction.

> *If 2018 becomes the year of massive data destruction, look for this to have a big impact on the stock value of some companies and sectors. The private sector will certainly respond, but individuals would be wise to decentralise their personal data, especially financial data, and organizations should think through this worst-case scenario.*
>
> - TODD RUBACK, CHIEF PRIVACY OFFICER AT EVIDON

A global concern

The World Economic Forum recently released a report, grouping cybercrime with environmental disasters, large-scale involuntary migration and illicit trade as one of the largest global threats this year.

> *Due to the cumulative impact of powerful spending and attack trends, we should expect to see at least one act of nation-state sponsored cyber warfare that directly impacts citizens this year.*
>
> - JING XIE, SENIOR THREAT INTELLIGENCE ANALYST AT VENAFI

[2] *http://www.telegraph.co.uk/technology/2016/11/01/mobile-web-usage-overtakes-desktop-for-first-time/*

More vectors for attack

Technological advancements, paired with a deeper understanding of how to manipulate a victim, broadened the attacker's repertoire in 2017. We welcomed a range of new technology into our lives that drastically changed the way we interact with the world. We embraced BYOD (bring your own device) policies with opens arms, and as a result, internal IT teams lost sovereignty of how we use our mobile corporate devices. Attackers found new ways to trick us into doing exactly what they want us to do, to infiltrate organizations and retrieve highly confidential data.

Cybercriminals have developed a worryingly deep understanding of human nature and know exactly how to use this new technology against us - driverless cars are a perfect example of this. Although the principal is groundbreaking and welcomed by most technophiles, the penetrable nature of the technology has raised concern amongst the security experts and customers alike. As proved in several demonstrations throughout 2017, hackers can infiltrate a vehicle through a minor device, such as an infotainment system, then cause chaos by taking control of the vehicle's door locks, brakes or even semi-autonomous driving features. A huge concern for consumers and organizations eager to adopt the exciting new tech. The number of mobile phone users in the world is expected to pass the five billion mark by 2019, so it comes as no surprise that mobile is the focal point of attacks.

Organizations left vulnerable

In the same vein, last September we learned that a series of critical Bluetooth flaws that affect billions of Android, iOS, Windows and Linux devices had been infiltrating popular gadgets - including voice activated personal assistants - like Google Home and Amazon Echo. Researchers also discovered that mobile devices running older operating systems were susceptible to the vulnerability dubbed 'Blueborne'.

The sophisticated attack exploited a total of eight Bluetooth implementation vulnerabilities that allow attackers within the range of the targeted devices to run malicious code, steal sensitive information, take control of the device and launch Man-in-the-Middle Attacks. Unlike traditional malware and common attack methods, the user does not even have to click on a link or download a questionable file, so it is possible that the attack can go unnoticed if this occurs within an organization.

To add fuel to the fire, enterprises were left unprotected against a wide range of mobile vulnerabilities and exploits that could have highly destructive powers within their business. Take the widely talked about Meltdown and Spectre chip exploit. The critical security flaw, that is said to have been around since the early '90s, is a CPU vulnerability that allows malicious actors to access any confidential information being run on the same central processing unit. The research team at Graz University revealed that this two decade old security flaw could have been dormant in billions of global devices.

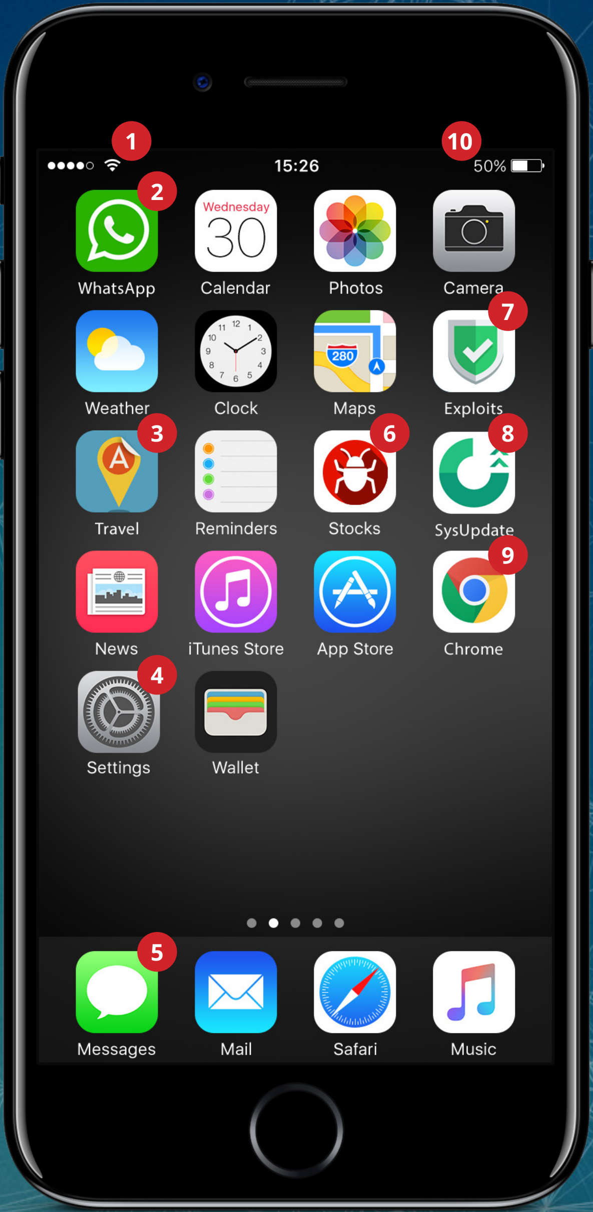
Vendors scrambled and fought to provide quick resolutions to the vulnerability, however, all the while sensitive corporate data was at risk. In fact, research shows 14% of mobile devices are said to unpatchable from the Meltdown and Spectre fixes, further outlining the need for a robust on-device mobile protection. Corporate data is powerful and cybercriminals will stop at almost nothing to get their hands on it.

"In many ways, data is now more valuable than currency"

JAMIE WOODRUFF, ETHICAL HACKER

Mobile security considerations for 2018

1. NETWORK ATTACKS
2. APP-BASED PHISHING ATTACKS
3. LEAKY APPS
4. RISKY CONFIGURATIONS
5. SMS PHISHING
6. MALWARE
7. KNOWN EXPLOITS
8. OUT OF DATE OS
9. RISKY WEB CONTENT
10. CRYPTOJACKING



> *There have been so many prolific hacks like Equifax, that customers have low confidence in large companies or institutions guarding their personal data. The general sentiment is becoming 'if it's online it's at risk'.*

MATT BROOKS, SENIOR PRODUCT MARKETING MANAGER AT CITRIX

1 | Phishing is the number one mobile threat

When people think about phishing, they conjure up thoughts of poorly worded emails offering 'unclaimed lottery winnings', or 'hassle free' payouts from ominous third parties. Fast forward to 2018 and things are very different. In today's threat climate even the most reputable CISOs are finding it difficult to spot a phish.

This was apparent when when one of the Big Four accounting firms email network was infiltrated in 2017. Hackers compromised the consultancy firm through a mobile attack that started within a popular social media app. An employee was sent to a fake Gmail login page and subsequently parted with their login credentials, giving the perpetrators full access to their account. Through this they were granted unrestricted access to the firm's data, and consequently were able to wreak havoc with vast amounts of sensitive corporate data.

Why are phishing attacks so dangerous? Well, they exploit the most vulnerable part of an organization: its employees. Employees are arguably a corporation's best asset, but when it comes to keeping data safe they double up as their biggest security threat. Even the most vigilant team members respond to cleverly targeted phishing campaigns, click on convincing looking files riddled with malware and open attachments from colleagues without giving it a second thought.

18x

***A mobile user is 18x more likely to be exposed to a phishing attempt on mobile than malware.** Less scrutinized channels like SMS, Skype, WhatsApp, games and social media are being employed at scale to distribute phishing links in places employees do not expect*

The fast-paced nature of a corporate environment plays into the attackers favour. People work quickly, act instinctively and for the most part that's encouraged. However when it comes to cybersecurity, this leaves enterprises vulnerable to attack. Human error is expected every now and again and cybercriminals use this to their advantage.

63%

OF PHISHING ATTACKS OCCUR ON IOS

83%

OF SUCCESSFUL PHISHING ATTACKS ON MOBILE TAKE PLACE OUTSIDE EMAIL

26%

OF THESE ATTACKS ARE DISTRIBUTED USING GAMING APPS

Why mobile?

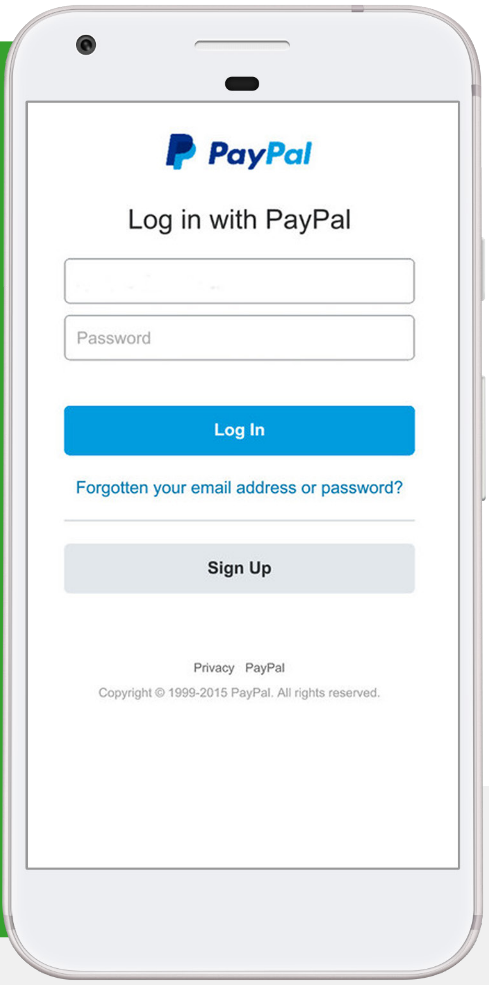
Mobile is a fertile arena for phishing attacks for a number of reasons. The smaller screen size means it's harder to inspect suspicious looking URLs, the on-the-go nature of the device results in users being more distracted, and for a number of reasons users are more trusting towards their inherently personal mobile devices. Data shows that in 2017 92% of organizations fell victim to a phishing attack, and it's expected to become even more prevalent throughout the year ahead. Phishing is not only regular, but it's also the most damaging and high-profile cybersecurity threat facing organizations today - supported by research from Google, Black Hat and US Homeland Security.

> *"Unsuspecting victims are encouraged to click links, or run files to launch malicious code to start the attack. Mobile phishing is relentless within the enterprise and we don't expect this to change any time soon."*

- SACHIN SHARMA, PRODUCT MARKETING AT VMWARE

The most frequently used impersonated organizations in phishing attacks

1. APPLE
2. PAYPAL
3. FACEBOOK
4. GOOGLE
5. AMAZON



PayPal

Log in with PayPal

Password

Log In

Forgotten your email address or password?

Sign Up

Privacy PayPal

Copyright © 1999-2015 PayPal. All rights reserved.

> *"Phishing is one of the top attack vectors within the enterprise at the moment. The explosion of mobile and the on-the-go nature of these devices mean they're attractive targets for attackers"*

- MATT BROOKS, SENIOR PRODUCT MARKETING MANAGER AT CITRIX

Rise of ’secure’ phishing

Social engineering techniques have long been part of the cybercriminal’s playbook. The earliest incidents of phishing transpired over twenty years ago when email was the preferred vehicle of attack. ‘Phishers’ would cast their nets far and wide with rudimentary techniques to encourage victims to part ways with their personal information. Realizing that email was a breeding ground for cyber threats, organizations responded by enlisting email-focused security solutions to protect data, revenue and reputation.

Fast forward a couple of decades and the proliferation of mobile technology has dramatically changed the phishing landscape. Wandera’s 2018 research revealed that 83% of mobile phishing attacks occur outside of email with apps, messaging services, and websites being the most attractive targets.

More sophisticated attack methods

Wandera’s recent phishing research shows an influx of phishing sites utilising HTTPS verification to conceal their deceitful nature. How does this work? Well, SSL certificates are a way of digitally certifying the identity of a website. They inform the user that their personal information has been encrypted into an undecipherable format that can only be returned with the proper decryption key. Countless cybersecurity campaigns advocate encryption and tell people that HTTPS sites are the ones to trust, so what’s the problem? Well, exactly that.

Users perceive HTTPS sites to be secure, so they’re less likely to suspect a ‘phish’. Realising this, hackers use sites like letsencrypt.org to gain SSL certification for their insecure phishing sites. Throughout 2017, the number of phishing sites operating from a secure HTTPS domain skyrocketed, and it’s a trend we expect to continue as attackers continue to advance their techniques.

1 SECURE ‘HTTPS’ PHISHING SITE IS CREATED ONCE EVERY TWO MINUTES

Shift in motivation

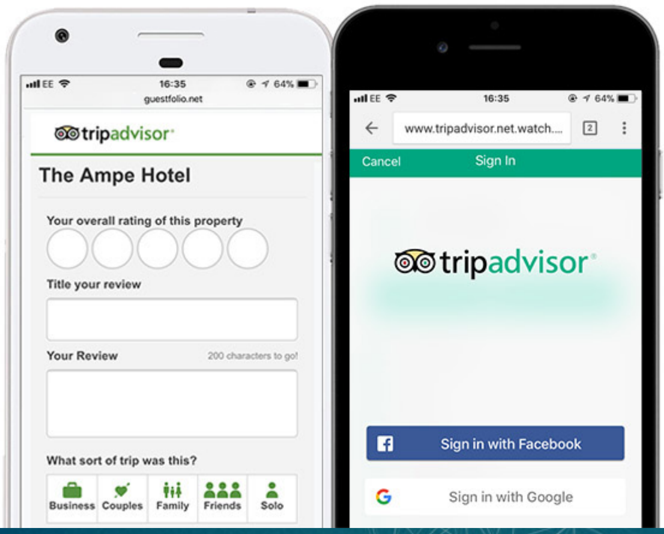
Historically, attackers set out to retrieve information which they could instantly use against the victim - like account credentials and basic personal data. This meant that in most cases, an attacker would infiltrate an organization not longer after successfully harvesting sensitive employee data. This allowed enterprises and individuals to prepare themselves if they suspected a malicious attack. However, the mobile phishing landscape is rapidly changing and attackers are leaning towards a more thought-out approach.

Malicious actors are playing the "long game" when it comes to plotting out campaigns and attack trends show they're taking their time to intimately research their targets. They're profiling victims by gaining generalised personal, financial and employment data prior to orchestrating a spear-phishing attack. Why is this concerning for organizations? Well, it means that they could be taking every step plausible to protect their systems at the current moment in time, but if employee credentials are circulating online, a high-profile breach could be imminent.

Once an attacker has your email address, it only takes a quick search on Twitter or Facebook to retrieve information that they can use against you. We recently discovered a phishing attempt in which the director of a high profile company was targeted. The attack centered on a tweet revealing the target was staying in a particular hotel and consequently received an email impersonating TripAdvisor, encouraging them to enter their details and leave a review.

This multi-pronged approach means that malicious actors are working together, trading credentials and organizational information on places like the Dark web. It's near impossible for an enterprise to outsmart an attacker who already has complete access to their sensitive employee data.

As data becomes more powerful than ever across almost every industry, everyone wants a slice of the action. As a result of this underground markets sell full identities of individuals, and organizations for as little as $10 a piece. They're referred to by the community as 'fullz' - details that provide enough financial, geographic and biographical information on a victim to facilitate identity theft or other impersonation-based fraud. Therefore, it's important that organizations invest in robust mobile threat protection that blocks and prevents data from being exfiltrated by malicious sites and applications in the first place.



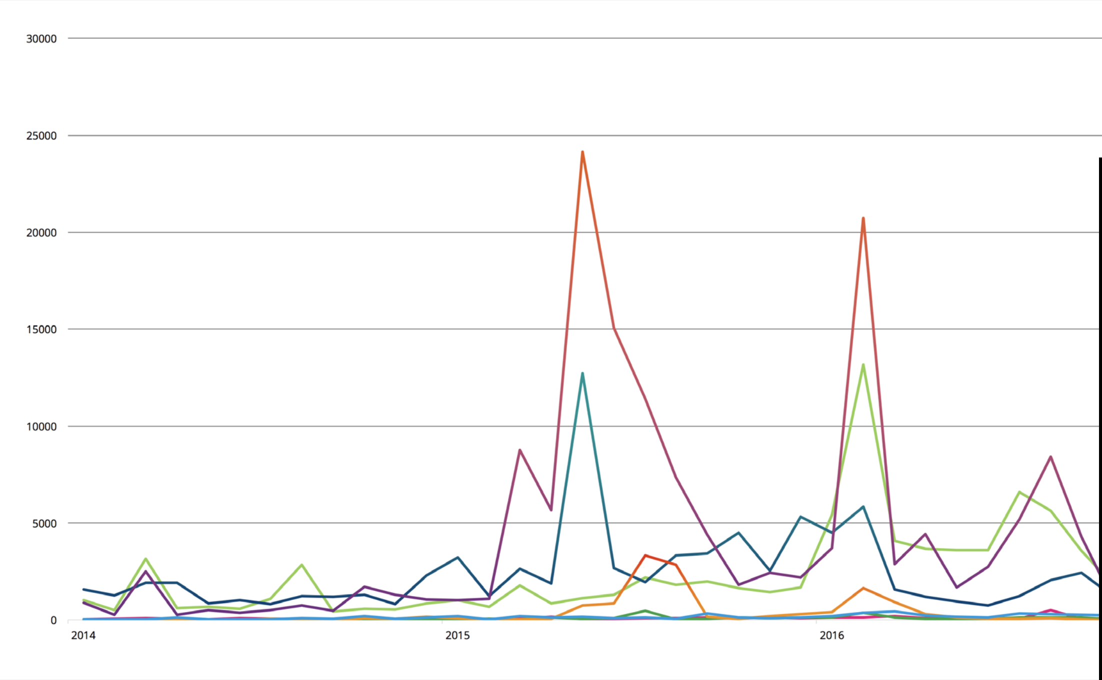
> *"When you get the offer of a one-click login for loads of different services it's incredibly enticing. We're seduced by convenience. We detach ourselves from the reality of the information we're putting out to the world. The lack of mental effort means that we often don't think about the implications it has for our personal data if it gets into the wrong hands, because it's just so easy."*
>
> - NATHALIE NAHAI, AUTHOR OF WEBS OF INFLUENCE

2 | Mobile malware is growing more aggressive by the day

As the previous section explains, mobile phishing is a problem that refuses to shy away. However, no discussion about the mobile threat landscape is complete without assessing the prevalence and aggression of the malicious software within the enterprise, that is often distributed by hackers through phishing campaigns and other attack vectors.

Over the last few years mobile malware has become a widely known, fear-inducing security concern for enterprises globally. Ransomware attacks dominated the headlines throughout 2017 with outbreaks like NotPetya, WannaCry and SLocker causing unprecedented destruction. Which variants of mobile malware are most destructive, and what trends should enterprises expect to see over the next twelve months?

MALWARE TYPES



MOST PREVALENT

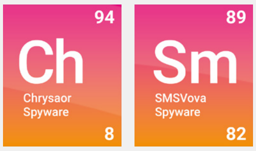
1. 🟪 SMS
2. 🟩 TROJAN
3. 🟦 ADWARE
4. 🟧 RANSOMWARE
5. 🟦 BANKER
6. 🟥 SPYWARE
7. 🟩 ROOTING

LEAST PREVALENT

Ransomware

Ransomware is definitely one of more dramatised enterprise threats. Essentially it refers to a piece of malware that demands money from users and, in exchange, promises to release either the files or the functionality of the devices being held hostage.

SLOCKER - THE DESTRUCTIVE RANSOMWARE THAT CAME BACK ON THE SCENE IN 2017



Spyware

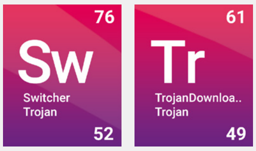
Spyware, like the name suggests, spys on the infected user. From recording audio, to capturing photos - apps riddled with Spyware are usually those with the most invasive permissions.

XAGENT - IOS MALWARE USED TO GATHER PICTURES, CONTACTS AND GEO-LOCATIONS

Adware

Adware or advertising software is designed to show frequent ads to a user in the form of pop-ups, sometimes leading to the unintended redirection of users to web pages or applications. Adware is probably the best-known type of malware, and an estimated 6% of apps within the Google Play Store contain some sort of adware.

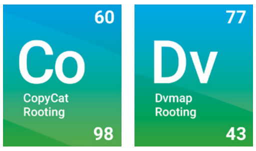
FALSEGUIDE - THE GAMING APP INSTALLED OVER TWO MILLION TIMES



Trojan

Trojan is type of malware that hides itself within a piece of seemingly innocent, legitimate software, and gets it name from the infamous tale of Troy. Rooting a device enables the hacker or the user to install unapproved apps, change the OS, serve the phone malware, and really customize any aspect of the device.

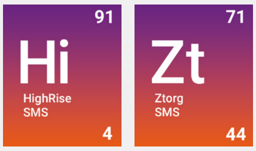
ACEDECEIVER - EXPLOITS DESIGN FLAWS IN APPLE'S DIGITAL RIGHTS MANAGEMENT



Rooting Malware

Rooting is the Android equivalent of jailbreaking a device. This category includes any malware that roots the device, essentially unlocking the operating system and obtaining escalated privileges.

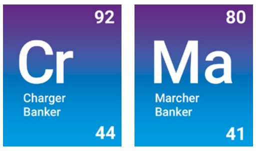
COPYCAT - THIS ROOTING MALWARE AFFECTED NEARLY 14 MILLION ANDROID DEVICES



SMS Fraud

Banker malware takes the form of any malicious software attempting to steal users' banking credentials without their knowledge. With financial credentials at risk, banking malware is one of the most lucrative types of malware for the attacker.

ZTORG - IS A FAMILY OF SMS-FRAUD FOUND IN THE PLAY STORE



Banker Malware

Banker malware takes the form of any malicious software attempting to steal users' banking credentials without their knowledge. With financial credentials at risk, banking malware is one of the most lucrative types of malware for the attacker.

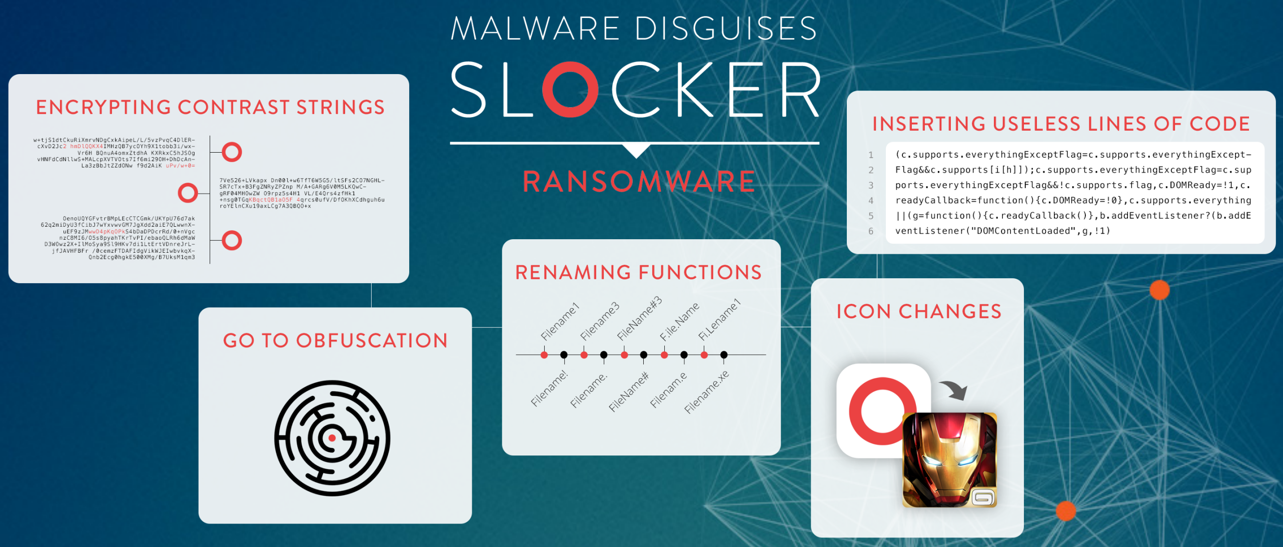
CHARGER - THE BANKING MALWARE SPOTTED IN THE PLAY STORE LAST YEAR

SLocker: the ransomware that came back

An example of how persistent and damaging mobile malware can be comes in the form of SLocker. The ransomware variant, that first caused chaos on mobile devices back in 2016, returned to the scene last year and it came back with a vengeance. SLocker is malware that encrypts images, documents and videos on your mobile device to later ask for ransom to decrypt the files. Once the ransomware is executed, it starts a service that runs in the background of your device without your knowledge or consent.

While initially operating stealthily, once the file encryption process is complete, the service will hijack your phone, blocking your access, locking your screen and constantly showing you an intimidating message. This message usually threatens to expose or destroy the information on your device. Some versions of SLocker have been known to accuse you of having 'perversions' on your device in order to frighten you into compliance. The only way to take back full control of your phone is to pay the ransom demanded, or risk destruction or exposure of your personal data.

Last year Wandera's mobile intelligence engine, MI:RIAM, identified that nearly 400 unique samples of the SLocker malware were back in distribution. These 400 variants of the so called 'polymorphic' exploit were not only designed to evade detection by signature-based scanners, but they also contained more malicious functionality.



```
(c.supports.everythingExceptFlag=c.supports.everythingExcept-
Flag&&c.supports[i[h]]);c.supports.everythingExceptFlag=c.sup
ports.everythingExceptFlag&&!c.supports.flag,c.DOMReady=!1,c.
readyCallback=function(){c.DOMReady=!0},c.supports.everything
||(g=function(){c.readyCallback()},b.addEventListener?(b.addE
ventListener("DOMContentLoaded",g,!1)
```

3 | Mobile cryptocrime is rife

A developing trend that emerged in 2017 was the explosion of digital currency. Last year it was impossible to flick through a news feed, open a paper or go online without coming across a mention of cryptocurrency, cryptotrading or a crypto-related crime. That's why it's predicted that attackers will target vulnerabilities in systems that implement blockchain technology associated with digital currencies throughout this year.

> *"We'll see a progressive shift in 2018 towards criminal use of cryptocurrencies other than Bitcoin, making it generally more challenging for law enforcement to counter"*
>
> - EXECUTIVE DIRECTOR OF EUROPOL, ROB WAINWRIGHT

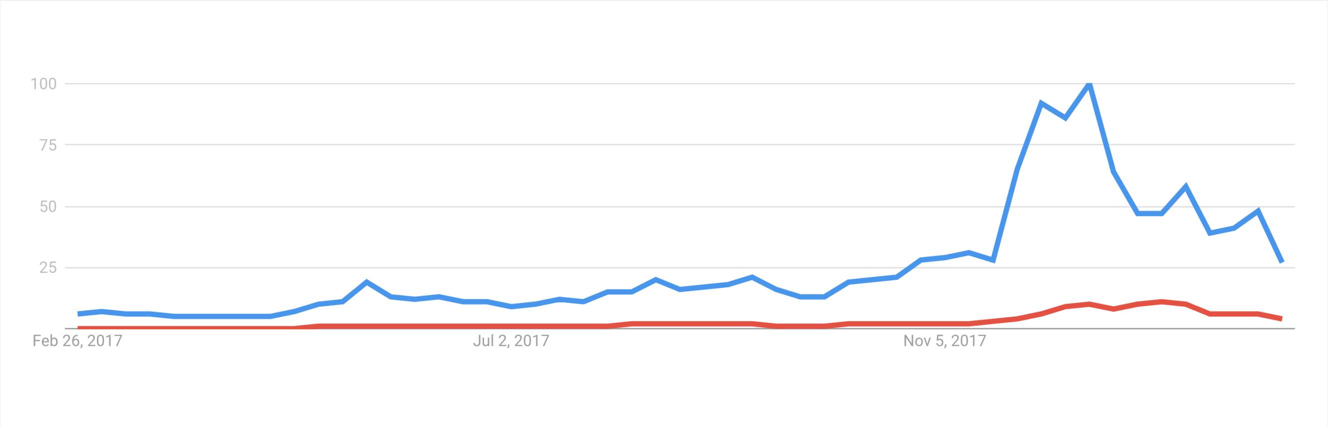
The cryptocurrency boom

In December popular cryptocurrency Bitcoin achieved a monumental milestone. It hit $20,000 dollars a coin after an intense period of growth. The popularity and resultant price boom of Bitcoin and its ilk became a magnet for cybercrime in 2017 and it's a trend expected to continue.

For those who avoided contact with the outside world in 2017, cryptocurrencies, or virtual currencies, are digital means of exchange created and used by private individuals or groups. Many refer to them as "alt currencies" as they're viewed as alternative mediums of financial exchange that exist outside of government controls. Instead, digital currencies rely on a technology called blockchain that makes its transactions so secure that experts consider them to be almost unhackable.

Each time a person purchases an item using cryptocurrency, the transaction is stored in a digital ledger. To keep these transactions secure digital currencies use cryptographic protocols, or complex systems of encryption, rendering them virtually impossible to hack. If digital currency is so secure, what's the issue? The widespread adoption of cryptocurrency means that digital trading apps and services have become a hotbed for cybercrime. As more people invest in the currency, the opportunity to deceive users increases too.

GOOGLE TRENDS: SEARCH TERM "CRYPTOCURRENCY" 2017 - PRESENT



The rise of cryptocrime

While hackers are unlikely to succeed at attacking the complex encryption in the immediate future, cybercriminals have already conceived and distributed malware to exploit weaknesses, mine cryptocurrency and steal digital currency from users' wallets. This presents huge concern for enterprises who accept cryptocurrency, or allow their employees to use crypto related sites and services. If an attackers can infiltrate a device to clear a wallet, then it's not inconceivable that they could exfiltrate highly confidential corporate data at the same time.

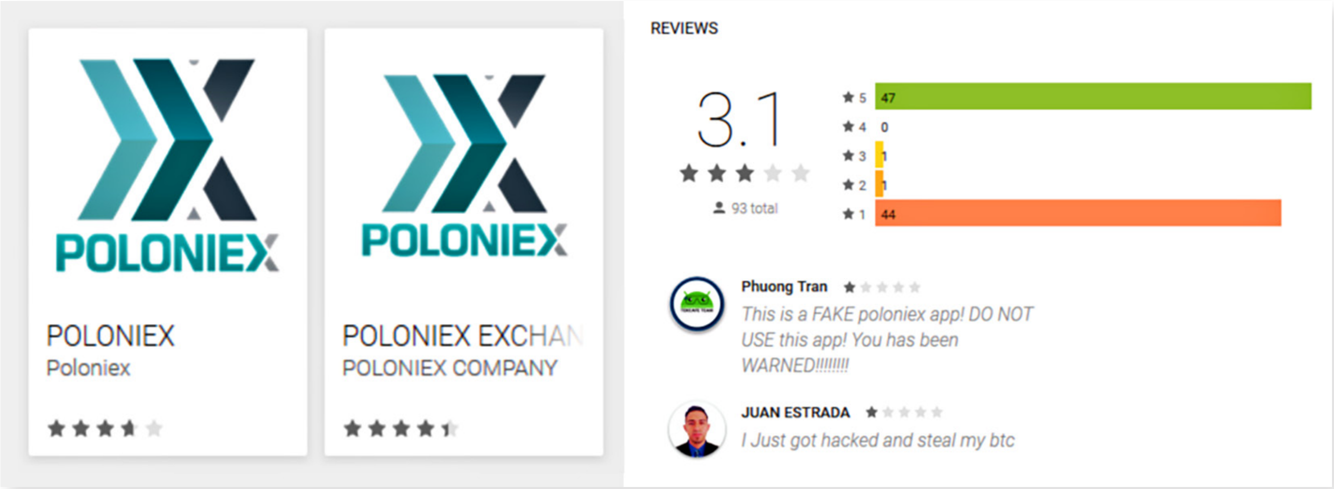
The ¥46.3 billion heist

An example of this emerged at the start of this year, when Tokyo-based cryptocurrency exchange 'Coincheck' said it would return around $425 of the digital money it lost to hackers in one of the largest ever thefts of digital funds. Around 10,000 organizations in Japan accept cryptocurrency, displaying the potential impact of this breach to the wider community.

Coincheck Inc Chief Operating Officer Yusuke Otsuka speaks to the media in Tokyo, Japan

This was also apparent when towards the end of last year, users of the popular cryptocurrency exchange, Poloniex, fell target of two credential thieving attacks. The website – that doesn't yet have an official mobile app – was used as inspiration for attackers, and nine apps surfaced in the Play Store under the guise 'Poloniex'. We Live Security reported how two of these apps, named "Poloniex" and "Poloniex Exchange", were put onto the Android app service and downloaded more than 5,500 times before being removed.

The convincing apps, shown below, were used to mimic the official website, collect user credentials and send back the information to the attacker. The logins were then stored and used to gain access to wallets via the official Poloniex.com website.



★ 5	47
★ 4	0
★ 3	1
★ 2	1
★ 1	44

Phuong Tran ★
This is a FAKE poloniex app! DO NOT USE this app! You has been WARNED!!!!!!!

JUAN ESTRADA ★
I Just got hacked and steal my btc

MOBILE CRYPTOJACKING GREW BY 287% BETWEEN OCTOBER AND NOVEMBER LAST YEAR

Cryptojacking will steal the show

It's not just fake crypto apps and services that we'll see distributing malware this year, cryptojacking has become one of the most worrying new threats for enterprises and security teams. For a long time now, the Dark web has been utilizing cryptocurrencies for its transactions. The untraceable nature of the currency, along with how simple it is to transfer funds, made it prefered by criminal groups. A recent trend has emerged where malicious actors who have turned to mining these currencies using stolen compute power from organizations and individuals. The threat has since turned mobile, as devices powerful CPUs and always-on nature, make them an attractive target for covert mining operations.

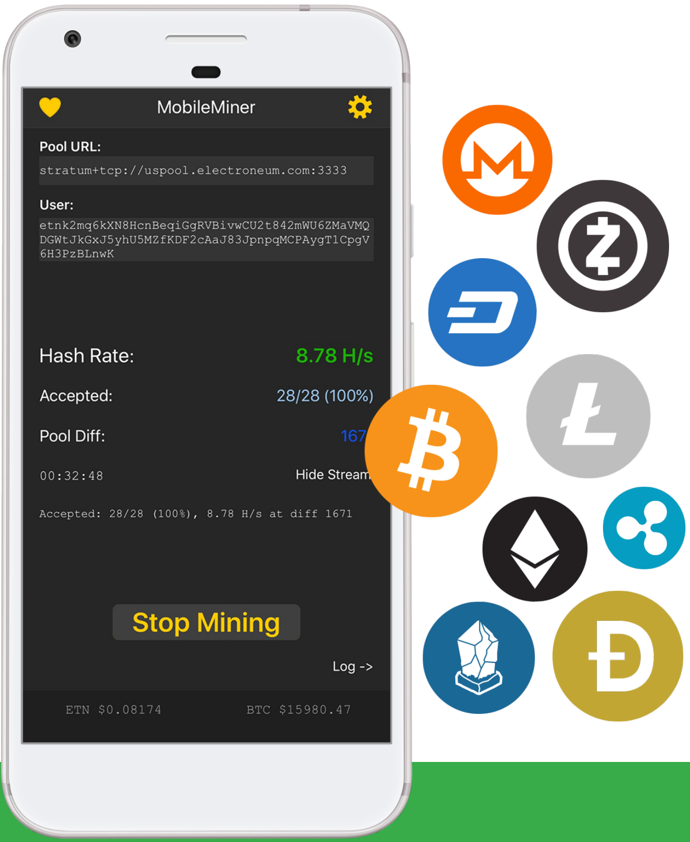
The technique involves the use of scripts that run on web pages or in mobile apps. These scripts are designed to harvest the processing power (CPU) of the user's device to mine for cryptocurrency. Currencies such as Bitcoin, Ethereum and Monero are all continually 'mined' using distributed computing resources to work out problems that generate 'hashes'.

Anyone can use their machines to process new coins in this way, but with cryptojacking, website owners and app developers are able to harness the CPU of their audience instead, earning them cryptocurrency in the process. Individually, the amount earned from each device is small, but when running on thousands of devices cryptojacking can prove to be quite lucrative. Furthermore, when this is done without the users consent it can be extremely disruptive. The device can overheat, slowing down the processor can slow down, making it impossible for the user to complete simple functions.

Mobile cryptojacking is an enterprise threat

Towards the end of last year, Wandera conducted an analysis of 100,000 sampled devices in its network of corporate-assigned smartphones and tablets. These devices are protected by Wandera's mobile security solution, and therefore does not include connections to cryptojacking services that were blocked by security administrators.The data reveals a number of interesting findings.

Firstly, the number of mobile devices connecting to cryptojacking sites and apps grew by 287% month-on-month, and almost all of the exposed users are unaware that the script is running on their device. Furthermore, more than a quarter of organizations had at least one mobile device running a cryptojacking script in their fleet.



Pool URL:

```
stratum+tcp://uspool.electroneum.com:3333
```

User:

```
etnk2mq6kXN8HcnBeqiGgRVBivwCU2t842mWU6ZMaVMQ
DGWtJkGxJ5yhU5MZfKDF2cAaJ83JpnpqMCPAygT1CpgV
6H3PzBLnwK
```

Hash Rate: 8.78 H/s

Accepted: 28/28 (100%)

Pool Diff: 167

```
00:32:48
```

```
Accepted: 28/28 (100%), 8.78 H/s at diff 1671
```

```
ETN $0.08174          BTC $15980.47
```

The plugin crytpojack hack

In February this year, thousands of websites around the world from the UK's NHS to the US government's court system were found to be secretly mining cryptocoins when a popular plugin was hacked.

The affected sites all use a fairly popular plugin called 'Browsealoud', made by British business Texthelp, which reads out webpages for the visually impaired. The technology was compromised in some way, either by hackers or rogue insiders altering Browsealoud's original source code in the app, to silently inject Coinhive's Monero miner into every webpage using the Browsealoud plugin.

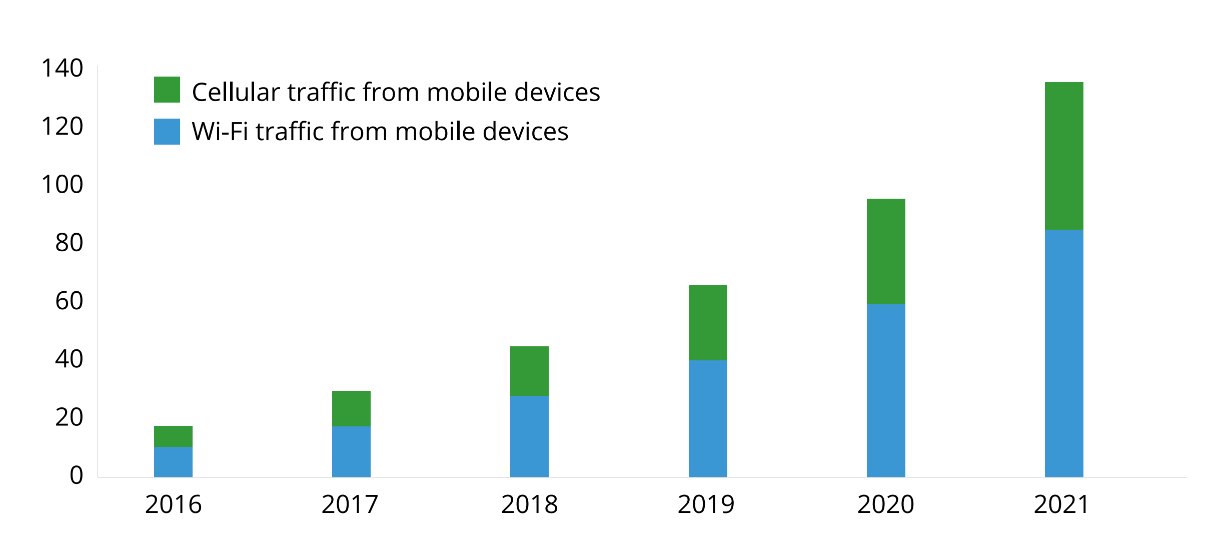
MORE THAN A ¼ OF ORGANIZATIONS HAVE A LEAST ONE MOBILE DEVICE RUNNING A CRYPTOJACKING SCRIPT

4 | Wi-Fi threats are giving hackers access to your information

People tend to prefer Wi-Fi over cellular connections for a number of reasons. They're usually faster, don't drain your data plan and are widely available across the globe. With trains, buses, coffee shops, restaurant, bars and even gyms offering Wi-Fi, it's not difficult to see why connecting to new hotspots has become part of everyday life.

Wi-Fi traffic now exceeds cellular traffic overall, and this change in usage isn't something we expect to change anytime soon. Cisco predicts by 2021, 63% of total mobile data will be on Wi-Fi, compared to 60% it was at last year. Furthermore, according to research by Wandera, the ratio of Wi-Fi to cellular data usage for the average employee is 3:1.

BY 2021, 63% OF TOTAL MOBILE DATA TRAFFIC WILL BE ON WI-FI



4%

OF CORPORATE MOBILE DEVICES HAVE COME INTO CONTACT WITH A MAN-IN-THE-MIDDLE ATTACK IN THE PAST MONTH

12

THE AVERAGE NUMBER OF WI-FI CONNECTIONS THE TYPICAL CORPORATE DEVICE MAKES PER DAY

Wi-Fi security

There are a number of things that come to mind when discussing the security of Wi-Fi connections. Firstly, the way in which employees use corporate devices has drastically evolved. Historically, organizations invested in heavily regulated and secure networks within their offices, and when employees traveled, their laptops used strict blocks to stop them from accessing certain content deemed not suitable for corporate devices.

However the proliferation of mobile means employees are connecting to Wi-Fi hotspots all the time, and not always for "work" related reasons. In fact, according to data pulled from Wandera's global network of enterprise mobile devices, the average number of Wi-Fi connections the typical corporate device makes per day is 12.

Wi-Fi hotspots are an enticing attack vector for cybercriminals wanting to exfiltrate data for corporate devices. For minimal cost, an attacker can get their hands on equipment advanced enough to set up your own hotspot. Following a relatively simple process, a hacker can monitor online traffic to capture valuable information, and obtain sensitive corporate data.

> *With the exponential growth in Wi-Fi and the fact that consumers show a strong preference for it, Wi-Fi is emerging as a truly global, roamable network.*
>
> - EVAN KAPLAN, CEO OF IPASS

A rise in higher-layer protocol attacks

There are a number of ways that attackers can tamper with a seemingly secure Wi-Fi connections, and with 1 Wi-Fi hotspot for every twenty people on earth - it's no surprise they've become an attractive target to attackers. Here a few of the techniques we expect to grow in prevalence throughout the next twelve months.

Growth of SSL stripping

In summary, SSL stripping is a technique by which a website is downgraded from a secure HTTPS, to a HTTP connection. The attacker turns their focus to the established connection between a user and the internet in order to tamper with the security protocol. Why should enterprises be concerned about this? Well, HTTPS uses a secure tunnel (known as a SSL) to transfer and receive data which validates its security. In SSL strip, the traffic from the victim's browser is forced to communicate in plain-text over HTTP. Therefore it exposes the user to eavesdropping and data manipulation when the service is downgraded.

To execute an SSL strip attack, there must be three different things apparent – a Wi-Fi connection, a victim's system and an attacker's system. Had there been no attacker in between, the communication would only happen between victim's system and the web server of website. Hackers favor SSL stripping because a successful attack can kill a secure communication, without the user - or the organization they work for - suspecting a thing. If sensitive corporate information is stored on the device in question, then data be exfiltrated without raising any alarms.

More DNS spoofing

Another widely used MitM technique to look out for is DNS spoofing, or cache poisoning as it's known to some, whereby the the attacker supplies an incorrect IP address to the user. How does this work? Well, the user types in a web address like www.Facebook.com and a DNS request with a unique ID number is made to the server. The attacker can then intervene and respond to the DNS request with their own malicious website's IP address using the same identification number so that it is accepted by the victim's computer.

Not just threats, but risks

The previous section summarises the key threats apparent within the current mobile security landscape. However, in order for an organization to fully protect their mobile estate, it's crucial to understand the vulnerabilities and exploits placing corporate data at risk.

> *The more that employees and contractors use mobile devices to access organizational systems, applications and data, the more important it is to protect such access. Furthermore, it's essential to prevent the mobile devices that are supposed to boost productivity and add to the bottom line from opening unauthorized means of access to information and other assets; this turns them into a danger and a possible drain on revenue instead.*
>
> - ED TITTEL, INTERNET CONSULTANT AND FORMER DIRECTOR OF TECHNICAL MARKETING AT NOVELL

Mobile vulnerabilities

DENIAL OF SERVICE

The clue is in the name. A Denial of Service vulnerability within an iOS or Android operating system results in the mobile device becoming more susceptible to a Denial of Service attack. DoS attacks are primarily focused on rendering the device unusable for the purpose for which it was designed. How does this happen? Well, hackers infect mobile devices with large malicious files, overthrowing the central processing unit, CPU, causing the device to shut down and stop working. Mobile devices are particularly vulnerable to this kind of attack as mobile devices have less processing power than your average desktop device.

OVERFLOW

An overflow vulnerability is a flaw in OS code that can lead to hacker exploitation and subsequent overwriting of device executable code and data. The vulnerability usually lies in the stack/heap buffers, which are meant to limit the amount of data written into the memory of the device. When this is exploited by a hacker, the buffer is unable to limit the amount of code generated, and this leads to other code being overridden. The result is erratic device behaviour, crashes and data loss.

BYPASS SOMETHING

A bypass something vulnerability, also known as a 'back door' in an OS, makes a device susceptible to a third party circumventing a layer of protection set up by the user, administrator or OS itself. Bypass attacks usually involve a hacker 'getting around' the security authentication procedure of a device. Within mobile devices the flaw is usually embedded in the OS code.

CODE EXECUTION

An execute code vulnerability is a bug within an operating system that gives an attacker the power execute code on a device. A program that is designed to exploit this vulnerability, resulting in a code execution attack, is called a 'code execution exploit'. An example of this is a command to download a piece of malware, or send arbitrary requests and cause a Denial of Service attack. Code execution is one of the highest severity vulnerabilities, as the results of an attack can mean the 'bricking' of a device as well as any type of malware becoming active on the phone.

MEMORY CORRUPTION

A memory corruption vulnerability is a programming error in the operating system that leaves the memory component of a device open to exploitation by a hacker. The vulnerability lies in the memory location of a device and an attack occurs when the code is modified, violating the safety of the information kept in the memory. This type of attack can lead to a device crashing as well as other odd behaviour.

GAIN INFORMATION/PRIVILEGES

A gain information or gain privilege vulnerability is one that allows a hacker to exploit a flaw in the operating system to gain access to either private information or a heightened permission level on the device. This can be done using a malicious web page, program or application. Attacks of this nature usually result in the exfiltration of personally identifiable information from the device to an external hacker.

Risky configurations

Another factor that may put organizational data at risk is mobile devices that may have unauthorized modifications. The process of altering a mobile device to remove its limitations so users can add features - known as "jailbreaking" or "rooting" - changes how the security for the device is managed and could increase security risks. Jailbreaking allows users to gain access to the operating system of a device to allow the installation of unauthorized software functions and applications. Also popular with users trying to free their device from a certain carrier.

While some users may jailbreak or root their mobile devices purposefully to install security enhancements, others may simply be looking for an easier way to install their favourite applications. Like to customise the look of their OS, or simply to install more games. In the latter case, users face increased security risks, because they are bypassing the application vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. In addition, jailbroken devices may not receive notifications of updates from the manufacturer that may pose as further risks to their security.

Data leaks

Organizations are also increasingly vulnerable to "leaky apps". Data leaks involve the unauthorized or unintentional transfer of sensitive information from an enterprise mobile device to another internet space. By not protecting the data, the app developer is essentially making the data available to anyone who utilizes the same network as the device with the vulnerable app.

A recent example of this came in the form of the Sonic the Hedgehog game series. The apps that have collectively been downloaded over a hundred million times, were found to be leaking users' geolocation and device data to uncertified servers. A huge risk for mobile fleets which have one of these leaking applications installed.

Protecting customer data

Given the cyber atrocities committed against consumer data over the decade or so, it's no shock that legislative changes are being implemented this year to protect the sharing and storing of customer's personal identifiable information (PII).

The key aim of the European Union's General Data Protection Regulation - GDPR - which comes into effect in May this year, is to give EU citizens greater control and protection of their personal information. It also aims to provide a common regulatory framework for global businesses operating in the EU.

Perhaps most salient part of the new legislation is the way in which it extends to non-EU companies processing data of EU citizens, meaning its effects will be felt at most global businesses - including many of those i the United Kingdom after Brexit.

> *UK-based businesses cannot afford to ignore GDPR despite the fact the country has voted to leave the EU.*
>
> DR KUAN HON, PRIVACY, SECURITY AND INFORMATION GROUP AT FIELDFISHER

GDPR: the facts

WHEN DOES THE REGULATION START?

MAY 25, 2018

WHO DOES IT APPLY TO?

ANY ORGANIZATION STORING, TRANSMITTING AND SHARING DATA WITHIN THE EU

WHO ENFORCES THE LAW?

THE INFORMATION COMMISSIONER'S OFFICE

WHAT IS CHANGING?

THERE ARE NEW RIGHTS FOR PEOPLE TO ACCESS THE INFORMATION COMPANIES HOLD ABOUT THEM, OBLIGATIONS FOR BETTER DATA MANAGEMENT FOR BUSINESSES, AND A NEW SET OF FINES.

Why now?

The General Data Protection Regulation was developed to protect customer data. You didn't have to think particularly hard to remember a high profile data leak in 2017. Take the well publicised Equifax breach back in September 2017. Equifax originally revealed the breach impacted 145 million US customers and half a million Brits. It was only a month later, when Equifax admitted that a file containing 15.2 million UK records had been exposed as a result of the leak.

Fast forward six months, and Equifax would be facing hefty fines in the post GDPR landscape. Article 33 of the reform requires an organization to report any suspected breaches within 72 hours, in attempt to aid transparency and allow consumers to take the necessary measures to protect their PII from being spread even further.

What are the consequences?

REPUTATIONAL RISK

Companies must disclose data breaches to regulators and in certain circumstances to affected individuals, within 72 hours of their occurrence.This has the potential to be catastrophic in terms of business reputation and shareholder value.

> *Although the top-tier companies are doing a much better job of protecting themselves against mobile threats, most of the companies are falling behind. Hackers are finding mobile apps a great place to attack and these apps in the wild have binary code that's vulnerable and unprotected.*
>
> MANDEEP KHERA, CMO AT ARXAN

FINANCIAL RISK

Non-compliance can lead to very significant fines, potentially rising to 4% of worldwide turnover. In the UK for example, this greatly exceeds the current maximum of £500,000. This means that if data breaches remain consistent, the fines paid to the European regulator could see a 90-fold increase, from £1.4bn in 2015 to £122bn after the legislation comes into effect.To make things worse, security experts at FireEye predict that malicious actors will use these fines against organizations in attempt to get a payout. Our advice, know the facts. Study the legislation and make sure that you have the right security software in place to protect data that is stored and shared within your organization.

> *For organizations the greatest risk is having a data breach when the reforms are fresh. GDPR implements new requirements for giving notice of a breach which will then attract a cascade of investigations into not only the organization's security, but also its compliance with the many other complex features of GDPR.*
>
> *GDPR gives strong incentive to scrutinise all incidents that could be deemed as a breach. It may be wise for enterprises to invoke legal help when analyzing whether something is a breach.*
>
> - BENJAMIN WRIGHT - GDPR EXPERT AND PRIVATE ATTORNEY

How can organizations get ready for GDPR?

Jim Walker, CIO at Wandera

CIOs need to consider the enterprise risks and must plan to take the following steps ahead of May 2018.

Step 1: GDPR Assessment

Familiarize yourself with the regulation and understand your current data protection maturity against the new regulations.

Step 2: Complete a Privacy Impact Assessment (PIA)

Assess your current systems and projects to identify key data protection risks.

Step 3: Establish a Data Inventory

Know what personal data you collect, process and store, where this happens and who has access. Depending on the complexity of your business, you may need to use a discovery tool to help in this process.

Step 4: Establish an Improvement Program

Build a program that addresses your gaps identified in the steps above, but focus on your highest risks and most sensitive data first. Educate your organization on the importance of data privacy. Build new systems and processes with privacy and security incorporated 'by design' from the outset.

In summary, start with knowledge gathering, document your current position and your gaps, then address those gaps prioritizing highest risks first.

> *"As with most legislative changes, part of the battle is getting your head around the detail. The most important thing about the GDPR is that it applies to any company using any kind of personal data on EU citizens. This means that the vast majority of US and UK firms that operate on an international scale must now be compliant with the regulation."*
>
> TECHNOLOGY ADVISOR AND CEO OF EXTRACLOUD, SEB MATTHEWS

Protecting the corporate mobile fleet

When it comes to protecting your mobile estate from the wide range of threats and vulnerabilities, there are many things you can do. Part of the issue is education and part of the issue is infrastructure. As we've seen throughout this report mobile is indisputably the new frontier for cyber threats. Businesses must do more than simply detect when an attack has occurred. For effective risk management and protection against threats, it is imperative that enterprises have full insight and visibility into how devices are being used.

The best way to prevent a breach within your enterprise is to have a security solution monitoring device traffic at all times, ensuring that insecure Wi-Fi connections are flagged, traffic to phishing sites is detected and blocked at the proxy level and vulnerabilities are examined before they can be used against you.

Prevent, detect and contain

Wandera built MI:RIAM - our mobile insights and threat intelligence engine - to solve some of the biggest challenges in security. Billions of data points are generated every single day, and analyzing these to identify threats and achieve this kind of visibility is a huge undertaking. That's why we've turned to machine learning to augment these security features, enhancing our ability to detect and block the growing number of risks posed to businesses.

ZERO-DAY THREAT DETECTION

MI:RIAM uses Wandera's global footprint to identify patterns of risk, enabling Wandera's mobile security solution to identify new leaks and highlight previously unknown vulnerabilities.

ANOMALY IDENTIFICATION

Trained on the standard operating procedure of devices, apps, Wi-Fi access points and user groups, MI:RIAM builds a baseline understanding of behaviour, then seeks out anomalies.

RISKY APP DISCOVERY

MI:RIAM continuously analyzes apps that are installed and the network traffic they generate. This higher-level analysis allows MI:RIAM to identify risky apps before they put the organization at risk.

INFRASTRUCTURE RISK ASSESSMENTS

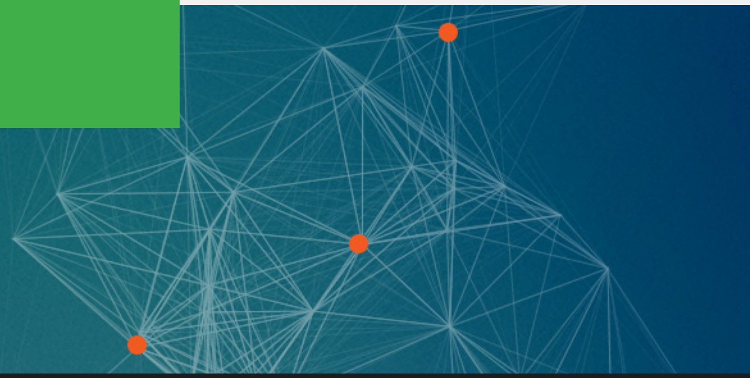
MI:RIAM uncovers malicious infrastructures, as well as conducts analysis of potentially problematic regions or into the extent of breached devices.

RAPID RESPONSES

MI:RIAM makes informed, intelligent decisions about the security events she encounters, enabling Wandera to respond by blocking, filtering and build a profile on the most prevalent mobile risks.

For more information or to request a free demonstration, visit

wandera.com/demo



wandera

Wandera is the global market leader in enterprise mobile security, delivered through its pioneering web gateway. Providing maximum visibility into mobile data, Wandera goes beyond threat detection to prevent attacks and contain data leakage. The solution's threat intelligence is powered by MI:RIAM, a real-time security engine that analyzes the industry's largest mobile dataset to uncover new vulnerabilities and zero-day threats as they emerge.