GLOBAL MOBILE SECURITY REPORT

2021

pradeo

INTRODUCTION

2020's events have precipitated the transition to remote working, strongly increasing workforces' reliance on mobile devices.

As organizations' routines and security perimeters crumbled, cybercriminals saw in the chaos an opportunity to seize. In the last 12 months, cyberattacks have flourished all over the world, and targeting mobile devices to reach organizations' most sensitive data is now more commonplace than ever.

Mobile applications are at the center of mobile usages, and unsurprisingly they have been keeping for years the position of favored vector to compromise smartphones and tablets, **counting as the source of 76% of mobile attacks in 2020**. However, their tricks are constantly changing to bypass organizations' security gates, making it complex to detect and neutralize them before they do harm.

By being part of a mobile security company that analyzes each year billions of security events collected through mobile devices and apps protected globally, Pradeo's researchers have the best spot to observe the mobile threat landscape. This report features their analysis of the currently most used attack techniques and latest trends.

These statistics are based upon the analysis of billions of security events, and samples of 4 million mobile applications and 1 million mobile devices.

INDEX

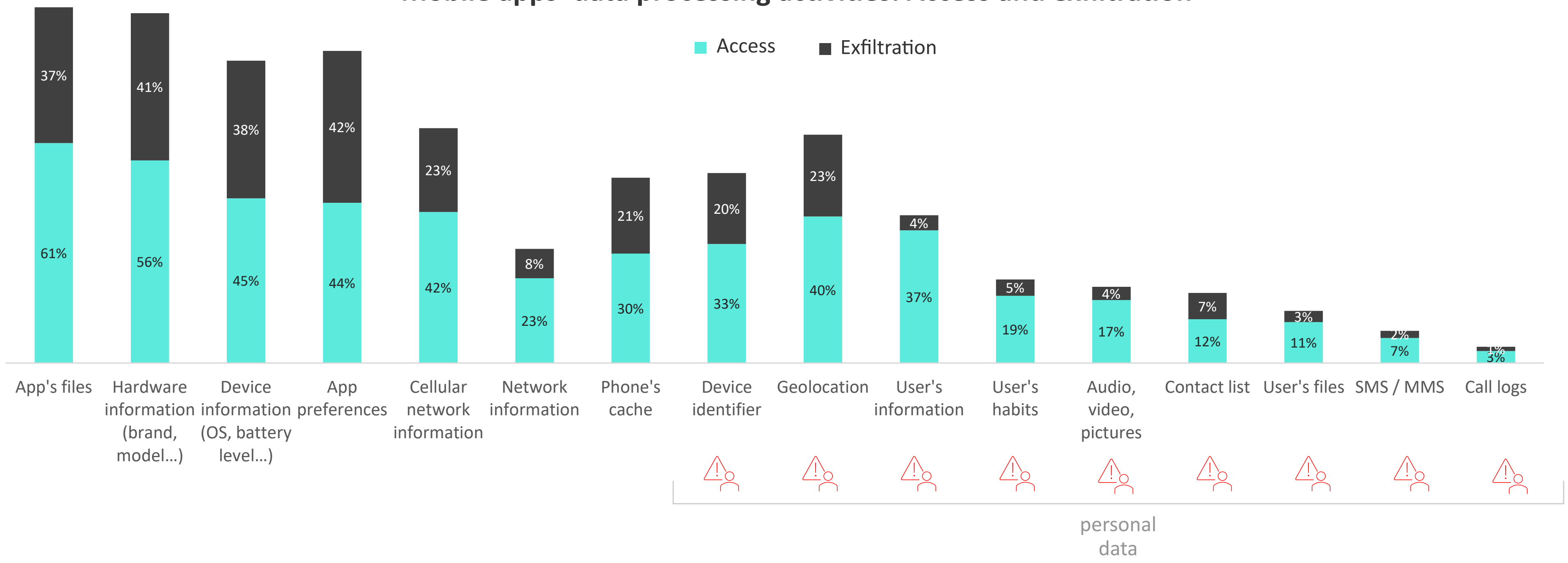
CHANCES YOUR SMARTPHONE HOSTS A SPYWARE ARE HIGH

To run its services, a mobile application requires to access some information on the device hosting it, including some about its user. While most apps could properly work by only accessing and using these data locally, **65% of them are actually programmed to send the collected information to a remote location**.

This silent data exfiltration is often performed to monetize applications, and in this case, details are sold to marketing companies that profile users. By cross-checking information, we observe that 43% of all mobile apps communicate data to servers belonging to one unique global company. On the other hand, this data collection is also sometimes the result of theft and spying, pure and simple.

The most leaked personal data are **location details, contact lists, usages statistics and pictures, audio and video files.**

Mobile apps' data processing activities: Access and exfiltration

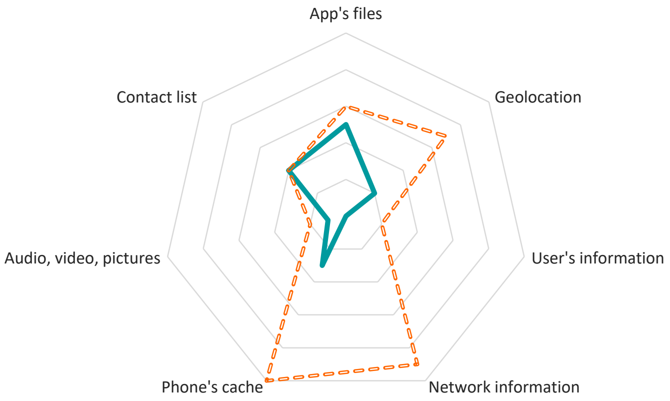


EVEN TOP-RANKING APPS HAVE HIDDEN MOTIVES

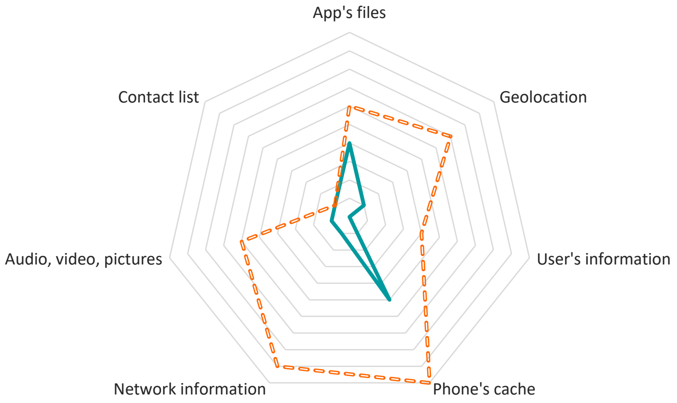
On corporate devices, some categories of applications are more popular than others. News, Productivity, Business and Music apps are the most encountered ones. Like others, they access users' data, hence potentially endangering organizations' privacy in the process. Among the top 10 mobile apps in each of the categories above-mentioned, none embeds a malware, yet many exfiltrate data they should not. Moreover, it is interesting to compare actual data exfiltration to the permissions requested by the apps, since both results are utterly different.

The comparison clearly shows that basing an app's security status upon its permissions induces mostly false-positive alerts.

Top 10 apps in the News category

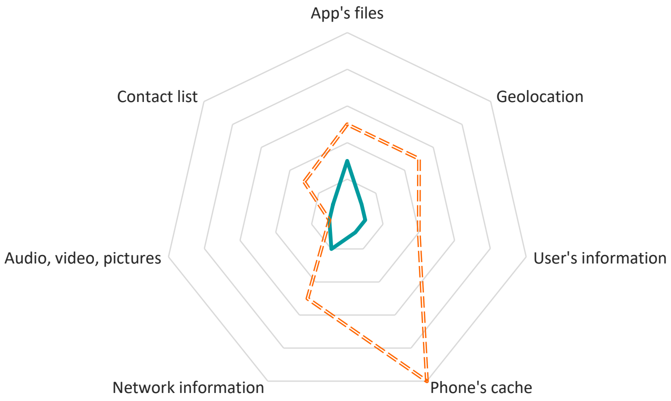


Top 10 apps in the Business category

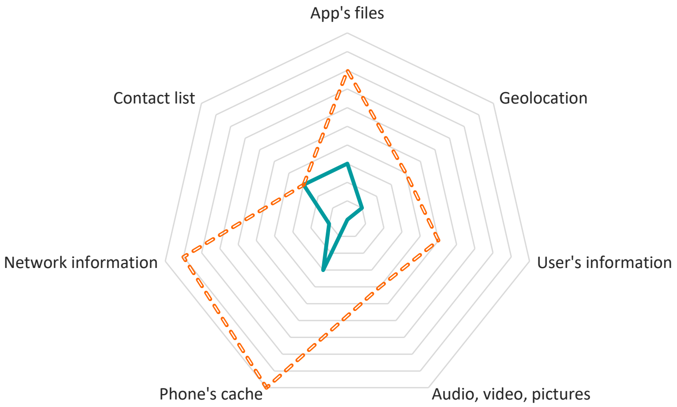


Each corporate mobile device has 10 applications that do not comply with its organization's security policy.

Top 10 apps in the Productivity category



Top 10 apps in the Music & Audio category



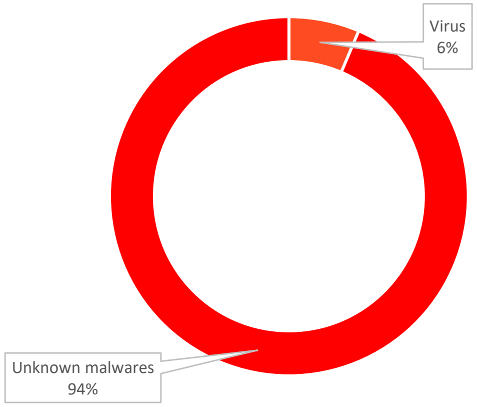
━ data sending

- - - permissions

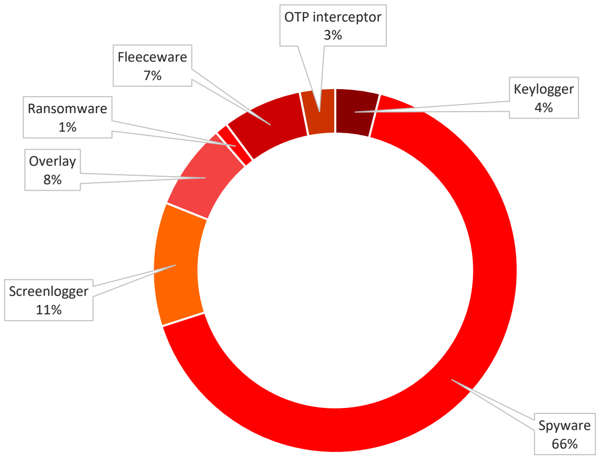
MALWARE IS AN EVER-RENEWING SECURITY CHALLENGE

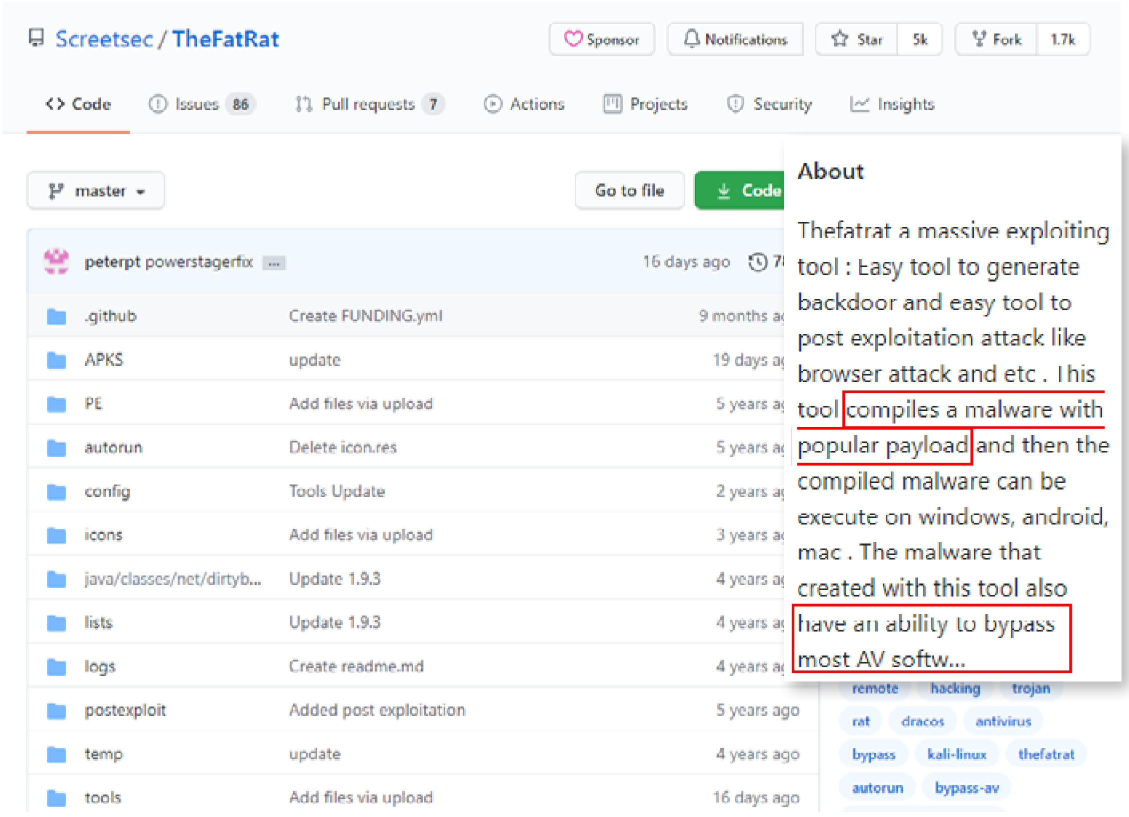
A malware's lifecycle has different stages: At first, its combination of features is new and not classified in any antivirus database. Then, it starts getting recognition and is attributed with a name and a viral signature. To stay under the radar, cybercriminals keep renewing the code and functionalities of their malwares. Unknown malwares are only detected by solutions performing behavioral analysis, and standard mobile security services only relying on virus databases cannot cover them.

Viral signatures VS Unknown malwares



Most encountered malwares





Screetsec / TheFatRat

peterpt powerstagerfix ... 16 days ago

.github	Create FUNDING.yml	9 months a
APKS	update	19 days a
PE	Add files via upload	5 years a
autorun	Delete icon.res	5 years a
config	Tools Update	2 years a
icons	Add files via upload	3 years a
java/classes/net/dirtyb...	Update 1.9.3	4 years a
lists	Update 1.9.3	4 years a
logs	Create readme.md	4 years a
postexploit	Added post exploitation	5 years ago
temp	update	4 years ago
tools	Add files via upload	16 days ago

About

Thefatrat a massive exploiting tool : Easy tool to generate backdoor and easy tool to post exploitation attack like browser attack and etc . This tool compiles a malware with popular payload and then the compiled malware can be execute on windows, android, mac . The malware that created with this tool also have an ability to bypass most AV softw...

remote hacking trojan rat dracos antivirus bypass kali-linux thefatrat autorun bypass-av

Open source malware available on Github

94% of the malwares detected by Pradeo Security in 2020 are unknown to antivirus databases.

EXPECT TO ENCOUNTER RANSOMWARES AND FLEECEWARES

Ransomware attacks

Several European national cybersecurity agencies recently warned organizations about ransomwares. In the recent months, two new trends have emerged. On the one hand, ransomwares are now **often used as part of large-scale attacks**, sometimes prepared months in advance and targeting carefully selected organizations. Qualified as Big Game Hunting, these onslaughts are often carried out by teams of hackers who have more financial and/or human resources than the average.

The second trend is the opposite of the first. It is the widespread of **Ransomware-as-a-Service** offers on the dark web, aimed at people with little IT knowledge and looking for a simple and fast way to launch attacks. The Jigsaw ransomware, for example, is sold for about 3,000 dollars on cybercriminal forums. Much less powerful than Big Game Hunting, RaaS usually targets individuals or small businesses, randomly.

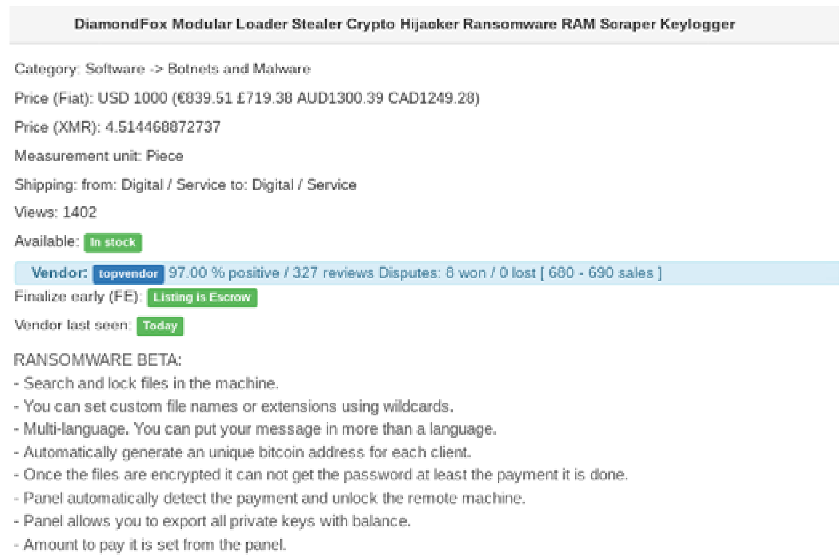
Ransomwares are now found in 1.1% of mobile apps, against 0.01% a year ago (+10900%).

They increasingly leverage mobile devices to compromise organizations' systems.

Fleeceware fraud

The most infamous fleeceware is **Joker,** a malware repeatedly found in a very large number of mobile apps on Play Store. Its main activity is to simulate clicks and intercept SMS to subscribe to unwanted paid premium services unbeknownst to users. By using as little code as possible and thoroughly hiding it, Joker generates a **very discreet footprint** that can be tricky to detect.

7% of mobile apps hide a fleeceware.



DiamondFox Modular Loader Stealer Crypto Hijacker Ransomware RAM Scraper Keylogger

Category: Software -> Botnets and Malware

Price (Fiat): USD 1000 (€839.51 £719.38 AUD1300.39 CAD1249.28)

Price (XMR): 4.514468872737

Measurement unit: Piece

Shipping: from: Digital / Service to: Digital / Service

Views: 1402

Available: In stock

Vendor: topvendor 97.00 % positive / 327 reviews Disputes: 8 won / 0 lost [680 - 690 sales]

Finalize early (FE): Listing is Escrow

Vendor last seen: Today

RANSOMWARE BETA:
- Search and lock files in the machine.
- You can set custom file names or extensions using wildcards.
- Multi-language. You can put your message in more than a language.
- Automatically generate an unique bitcoin address for each client.
- Once the files are encrypted it can not get the password at least the payment it is done.
- Panel automatically detect the payment and unlock the remote machine.
- Panel allows you to export all private keys with balance.
- Amount to pay it is set from the panel.

Ransomware-as-a-Service for sale on the dark web

MITRE ATT&CK®: AN OVERVIEW OF SOME TECHNIQUES USED ON MOBILE

Percentage of mobile devices on which these behaviors have been detected

Credential access	2.9%	**Man-in-the-Middle / Network Sniffing**	Adversaries may attempt to position themselves between two or more networked devices using a man-in-the-middle (MiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.
	0.8%	**2FA Interception**	Adversaries may target two-factor authentication mechanisms, such as smart cards, to gain access to credentials that can be used to access systems, services, and network resources.
Collection	65%	**Automated Exfiltration**	Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.
Impact	0.2%	**Data Destruction**	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources.
	1.2%	**Data Encrypted for Impact**	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key.
	0.2%	**Data Wipe**	Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources. With direct write access to a disk, adversaries may overwrite portions of disk data.
	0.8%	**System Shutdown / Reboot**	Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems.

MOST APPS AFFECTED BY COMMON CODE MALPRACTICES

Mobile applications can be vulnerable because of some errors in their source code or in the libraries they embed. These vulnerabilities expose them to attacks. Hundreds of vulnerabilities are referenced by the US National Vulnerability Database, the OWASP mobile security project, USCERT, etc. to help developers building and maintaining secure mobile applications. **Pradeo's security testing tool has detected at least one vulnerability in 57% of the apps it analyzed.**

SQLite
The app uses SQLite Database and execute raw SQL query. An untrusted user input in raw SQL queries can cause SQL Injection.

ECB
The app uses the ECB mode in its encryption algorithm. The ECB mode is known for being weak, because it uses the same encoded text for identical plain texts blocs.

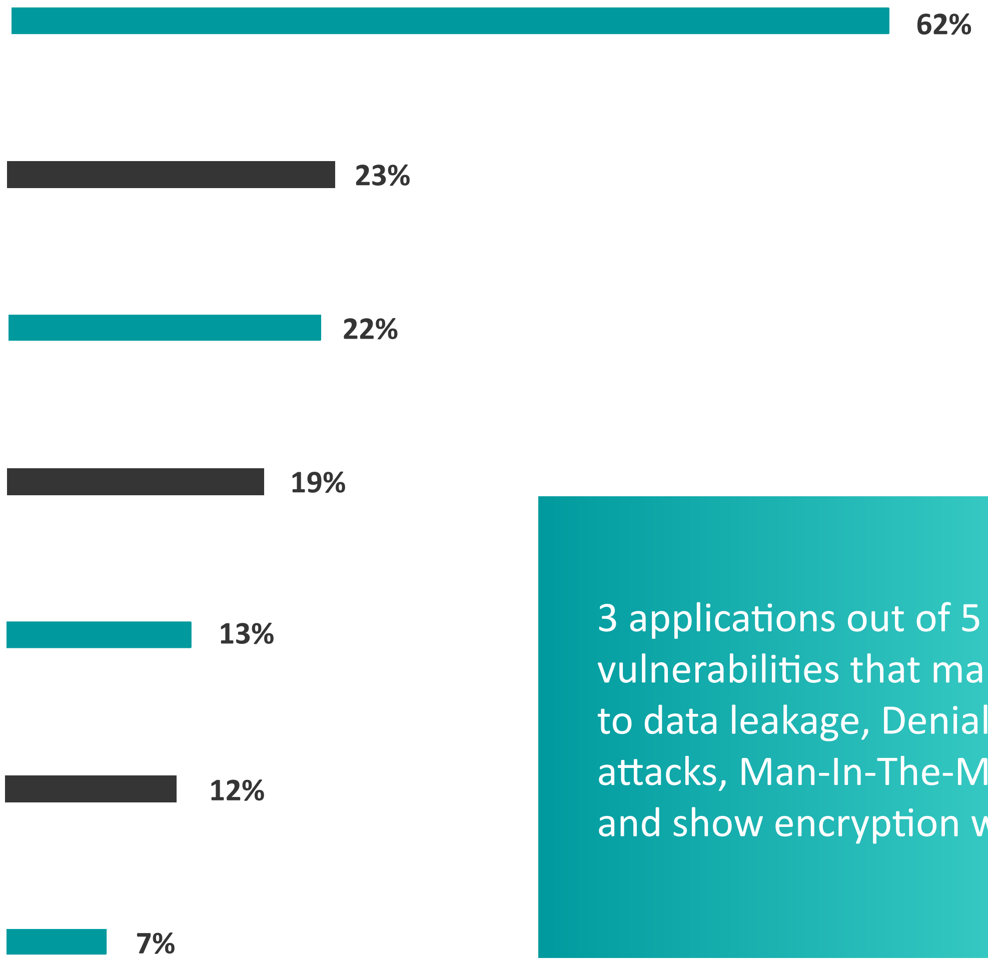
Rootcheck
This app has root detection capabilities.

X.509TrustManager
X.509TrustManager is implemented in an unsafe way in this app. It ignores all SSL certificate validation errors when it connects in HTTPS to a remote host.

Dex debug
This app uses DexGuard Debug Detection code to detect whether other apps are debuggable.

RSA_no_pad
This App uses RSA Crypto without OAEP padding. The purpose of the padding scheme is to prevent attacks that only work when the encryption is performed without padding.

Broadcast-Service
The application's 'Service' component hasn't a high enough protection level. It allows third-party apps to launch or to link itself to the service.

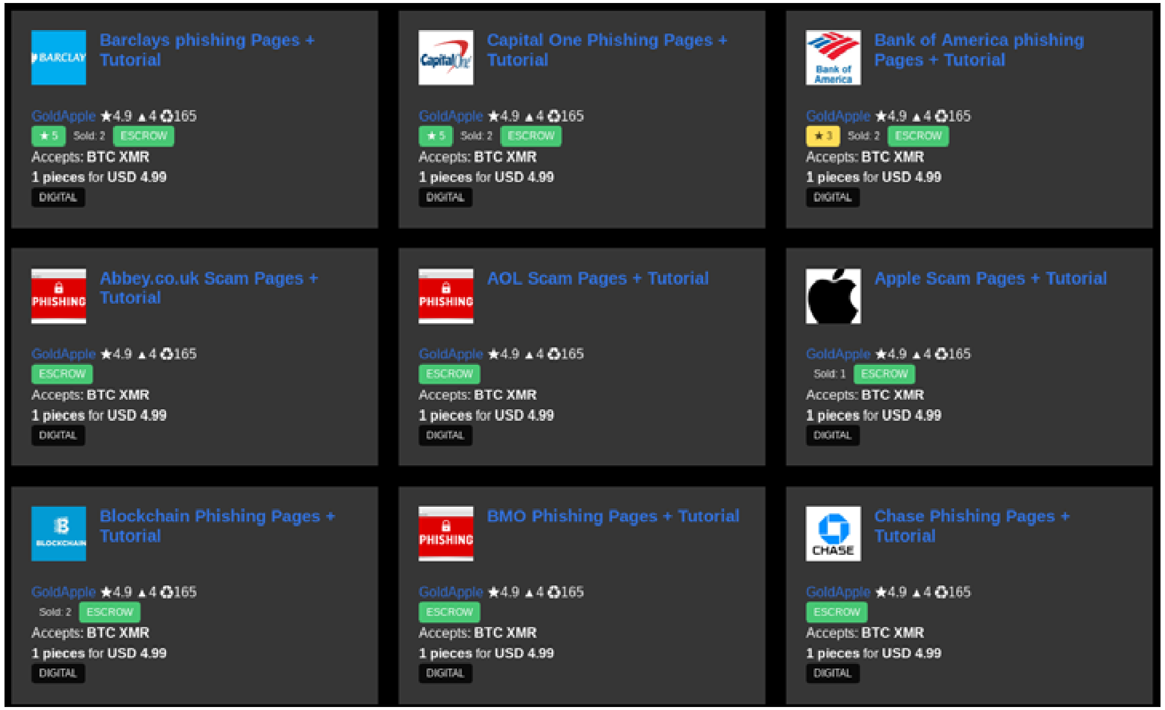


3 applications out of 5 feature vulnerabilities that make them prone to data leakage, Denial of Service (DoS) attacks, Man-In-The-Middle attacks and show encryption weaknesses.

PHISHING KITS ARE FLOURISHING ON THE DARK WEB

As classified in the MITRE ATT&CK® matrix, phishing campaigns can serve two purposes: stealing information or having users install a malicious program. Today, **88% of spear-phishing on mobile devices is carried out through mobile apps**. The campaigns are increasingly sophisticated, and a lot of mobile users are still unaware of their existence, hence easily falling in the trap.

In 2020, 34% of employees clicked on the link showcased in a phishing attempt. A complementary study revealed that 19% of victims go through the process by providing their credentials or downloading the malicious program. As phishing is undeniably effective, the dark web is flourishing with phishing kits and credential databases for sale.



Barclays phishing Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
★5 Sold: 2 ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

Capital One Phishing Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
★5 Sold: 2 ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

Bank of America phishing Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
★3 Sold: 2 ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

Abbey.co.uk Scam Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

AOL Scam Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

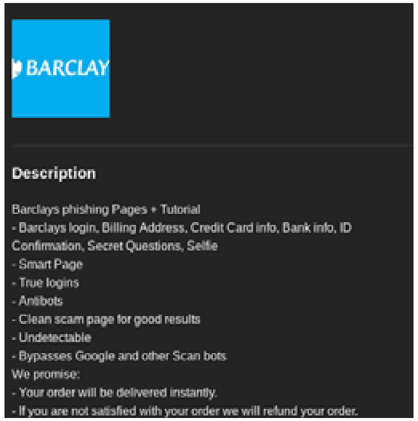
Apple Scam Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
Sold: 1 ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

Blockchain Phishing Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
Sold: 2 ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

BMO Phishing Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

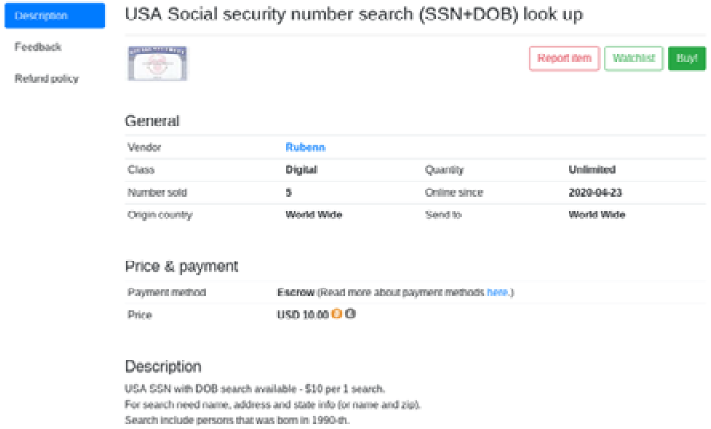
Chase Phishing Pages + Tutorial
GoldApple ★4.9 ▲4 ♻165
ESCROW
Accepts: BTC XMR
1 pieces for USD 4.99
DIGITAL

34% of employees are trapped by phishing attempts.



Description

Barclays phishing Pages + Tutorial
- Barclays login, Billing Address, Credit Card info, Bank info, ID Confirmation, Secret Questions, Selfie
- Smart Page
- True logins
- Antibots
- Clean scam page for good results
- Undetectable
- Bypasses Google and other Scan bots
We promise:
- Your order will be delivered instantly.
- If you are not satisfied with your order we will refund your order.



USA Social security number search (SSN+DOB) look up

General

Vendor	Rubenn		
Class	Digital	Quantity	Unlimited
Number sold	5	Online since	2020-04-23
Origin country	World Wide	Send to	World Wide

Price & payment

Payment method	Escrow (Read more about payment methods here.)
Price	USD 10.00

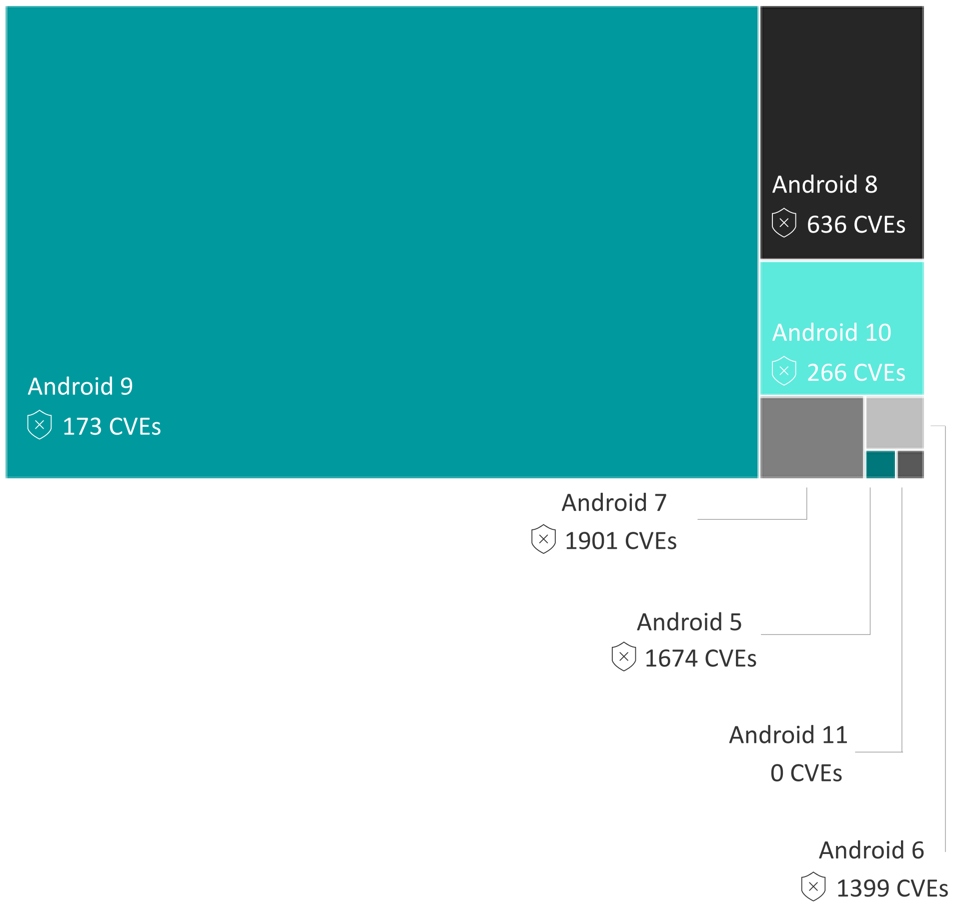
Description
USA SSN with DOB search available - $10 per 1 search.
For search need name, address and state info (or name and zip).
Search include persons that was born in 1990-th.

MANAGED MOBILE DEVICES RUN ON OUTDATED VERSIONS OF THEIR OS

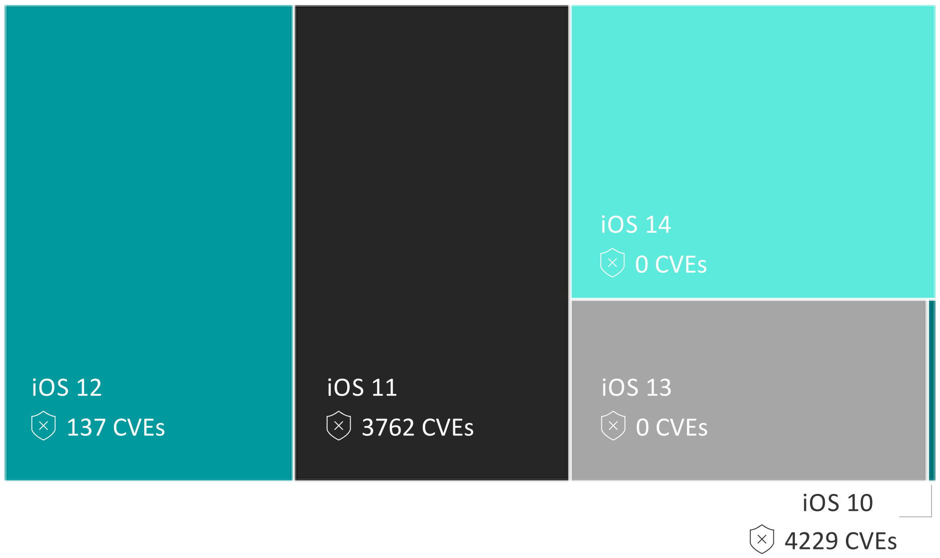
On a regular basis, security holes are discovered in the code of operating systems. Once detected, OS publishers develop patches that they push to users through updates and simultaneously disclose the vulnerabilities (CVEs) existing in the former version. Once made public, cybercriminals can exploit outdated devices' vulnerabilities to gain extended rights and illegally access data or communications.

In corporate mobile fleets, most devices are outdated because they are either too old to support the newest versions or because administrators are holding back updates. The latest is currently happening in many organizations to **delay the migration to Android Enterprise, which is mandatory from Android 10 onwards**.

Android versions repartition



iOS version repartition



95% of Android devices run on obsolete versions, versus 76% of iOS devices

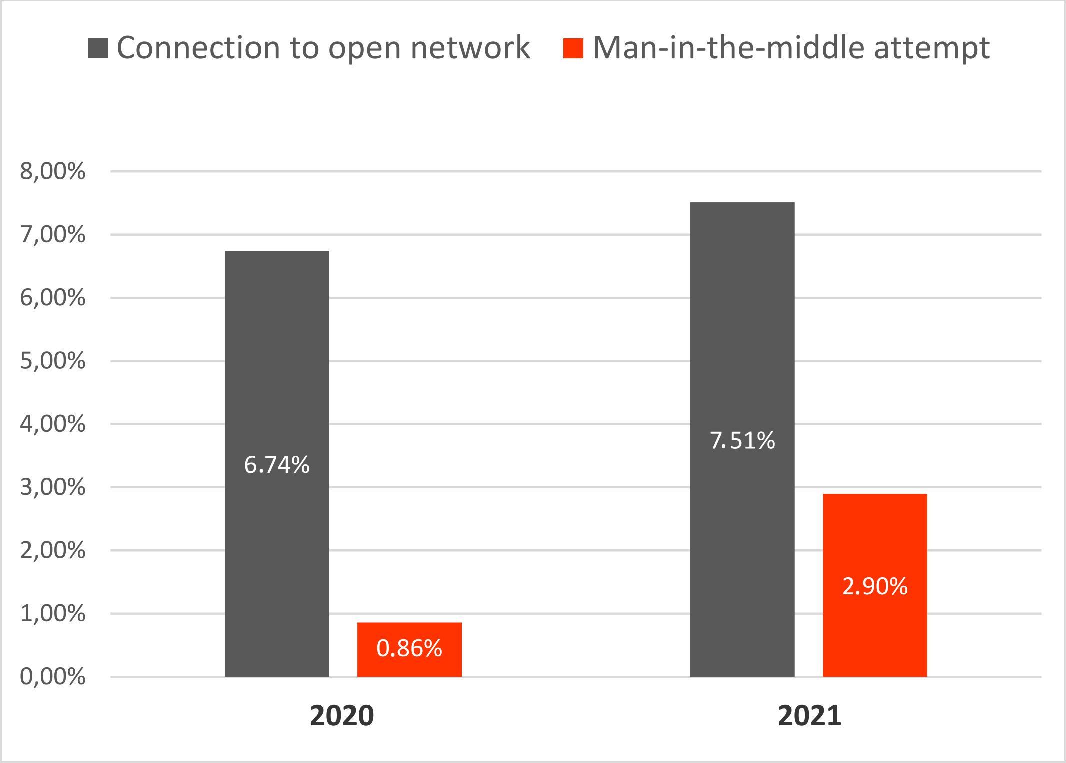
MAN-IN-THE-MIDDLE ATTACKS ARE GROWING ALONG REMOTE WORKING

Nearly all organizations have recently been urged to embrace teleworking. As the workforce more often connects to networks outside its company's perimeter, **hackers have more room to perform man-in-the-middle attacks than ever.**

This type of attack consists in intercepting or altering a communication between two parties. It can lead to data theft or fraud when a transaction is performed by the mobile user while the attack happens.

Man-in-the-middle attacks are correlated with the tendancy to connect to open WiFis. In Asia and in the United States for example, as it is very common to use public networks, mobile fleets are more impacted by this threat.

Globally, MITM attempts have grown by 236% in the last year.



UNIFIED MOBILE SECURITY WITH PRADEO

Pradeo is the European global leader of mobile security.

The company ensures the protection of all mobile usages, by offering services dedicated to securing smartphones, tablets and mobile applications.

Pradeo's cutting-edge AI-based technology, Pradeo Security, is **recognized** as one of the most advanced mobile security technologies **by Gartner, IDC, Frost & Sullivan and Forrester**. It provides a reliable protection from mobile threats to prevent data leakage and reinforce compliance with data privacy regulations.

Pradeo counts Governments, public administrations and Fortune 500 companies from various industries among its clients. Along the years, Pradeo has developed strong relationships with enterprise mobility leaders (Microsoft, BlackBerry, IBM, Samsung, VMware...) through advanced integrations and joint solutions.

For more information,
visit www.pradeo.com
or write to contact@pradeo.com.

Pradeo Security answers the following use cases:

- **Protect collaborators' mobile devices:** A Mobile Threat Defense solution that ensures a multilayer and real-time protection of mobile devices (COPE, BYOD, Android, iOS…).
- **Provide secure mobile services to collaborators using non-managed devices:** A Secure Private Store offer to safely distribute mobile services to BYOD devices, without requiring managing them.
- **Ensure mobile applications' security level:** A Mobile Application Security Testing tool providing visibility on applications' behaviors and vulnerabilities, in one click. Comes as a ready to use web platform or an API to integrate within developers' interface.
- **Protect mobile applications' data and transactions:** A security module (SDK) to integrate within mobile applications to protect them from threats operating on users' device.