MOBILE SECURITY REPORT 2021

INSIGHTS ON EMERGING MOBILE THREATS

Check Point SOFTWARE TECHNOLOGIES LTD | cp<r> CHECK POINT RESEARCH

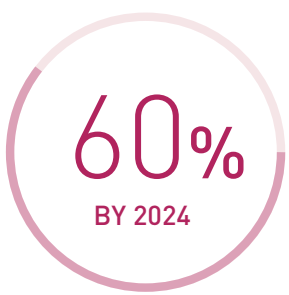
CONTENTS

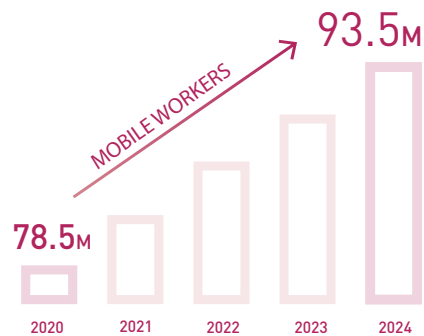
INTRODUCTION

The sudden and swift transition of the global workforce to the home, as spurred on by the outbreak of the coronavirus pandemic, has forced organizations worldwide to make significant changes to their infrastructures so their employees can be productive and comfortable as they work almost exclusively from home.

US MOBILE WORKER POPULATION FORCAST

IDC





And this move to remote work will not go away any time soon, even after the mass distribution of a vaccine. According to a new forecast by IDC, the US mobile worker population will continue grow at a steady rate over the next four years, increasing from 78.5 million mobile workers in 2020 to 93.5 million in 2024. Furthermore, by the end of the forecast period, IDC projects that mobile workers will account for nearly 60% of the total US workforce.

In this new paradigm, the mobile device is used more than ever to access corporate systems, both for routine as well as for critical tasks. This has greatly extended the attack surface and made the mobile device more susceptible than ever to cyber threats, such as phishing scams, malicious apps, man-in-the-middle attacks, rootkit, and more.

Indeed, Check Point researchers have been observing a continuous rise in the number of attacks and data breaches that are coming in through the mobile endpoint. As such, it has become all too clear that the new normal means more numerous and more sophisticated mobile security threats, making robust mobile security a key business imperative.

To help organizations understand where the potential vulnerabilities are, how they are being exploited by threat actors, and how to protect against attacks, Check Point presents this Mobile Security Report.

In this paper we provide insights into the mobile threat landscape that dominated in 2020, including the attacks and campaigns, as well as why enterprise-grade mobile security is the only way to reduce the attack surface and stay ahead of cybercriminals as we move ahead in the new normal.

Neatsun Ziv
Vice President of Threat Prevention
Check Point Software Technologies

METHODOLOGY

The insights contained in this report are based on data that was collected from January 1st, 2020 through December 31st, 2020, from 1,800 organizations that have deployed Harmony Mobile, Check Point's mobile threat defense solution, formerly known as SandBlast Mobile. The information contained herein is also based on comprehensive research that was performed by Check Point Research, the intelligence and research arm of Check Point, as well as that which has been made available by various mobile security vendors and security focused publications.

KEY FINDINGS:
AN EXECUTIVE SUMMARY

> *In 2020 we saw the attack surface continuously expanding, with 97% of organizations facing mobile threats that originated in multiple vectors including applications, networks, devices, and OS vulnerabilities.*
>
> (Check Point Research)

Over the past year, researchers at Check Point have been observing a rise in the number of attacks and data breaches that have come in through the mobile endpoint.

With 97% of organizations having faced mobile threats and with 46% having had at least one employee download a malicious mobile application that threatened networks and data, we can see that the threat to the mobile endpoint has become greater than ever and must be well accounted for by every organization.

AMONG THE KEY FINDINGS OF THE RESEARCH ARE:

1. **COVID-19 is the new app attack premise**, with skilled threat actors exploiting the public's concerns with the pandemic via malicious apps that are masquerading as providers of legitimate help in times of crisis.

2. **Ransomware has gone mobile** as in the case of Lucy, a Malware-as-a-Service (MaaS) botnet and dropper for Android devices.

3. **Mobile devices are inherently vulnerable** as was uncovered in Achilles, a Check Point research, where it was noted that over 400 vulnerable pieces of code were found within a Qualcomm DSP chip. The significance of this cannot be understated with Qualcomm providing chips for over 40% of the mobile phone market.

4. **Mobile Device Management (MDM) is a powerful new attack vector** as was seen, for example, with a new Cerberus malware variant that infected over 75% of one company's devices via corporate-owned MDM.

5. **Major threat groups are focusing on mobile**, conducting elaborate and sophisticated targeted attacks, improving their mobile arsenal with capabilities that have yet to been seen on mobile.

THE NETWORK:
AT THE HEART OF MOBILE ATTACKS

Almost every organization in our research sample experienced at least one mobile malware attack in 2020. And 93% of these attacks originated in a device network.

Most of these attack campaigns aim to gain a better foothold in the device by attempting to dupe the targeted user into installing a malicious payload through infected websites or URLs.

In addition, almost all of the network-based attacks either constitute a phishing attack that is attempting to steal the victim's credentials and impersonate the victim in a later attack, or a command-and-control communication of a malware that is already on the device.

BEWARE OF THE MAN IN THE MIDDLE

Networks that are not well protected pose a serious threat to mobile devices. For example, when the network is not sufficiently secured, attackers can intercept traffic through man-in-the-middle (MitM) attacks, or lure employees into using rogue Wi-Fi hotspots or access points.

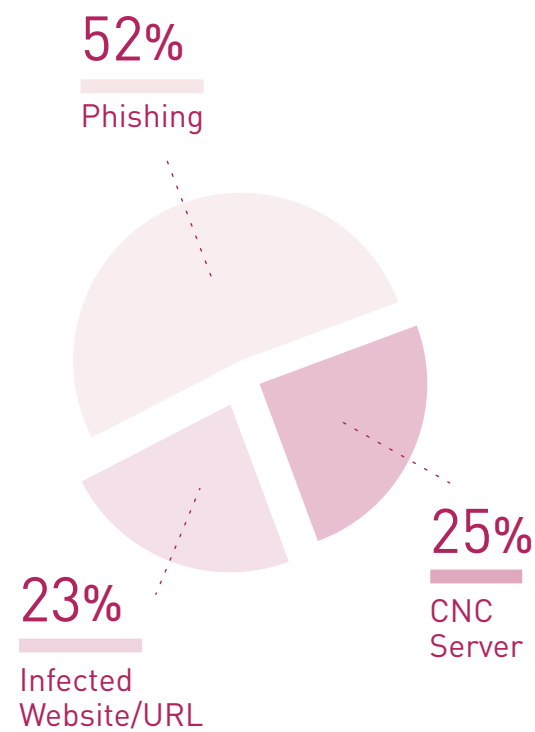
One of the most dangerous threats in this context is traffic interception, otherwise known as MitM. This is often executed through rogue access points, which take advantage of familiar and trusted public Wi-Fi names (SSIDs).

Users may see the name of a legitimate company or brand and connect to it without a second thought. While some of these hotspot names are obviously misspelled (e.g., Starbuckz), many do look perfectly legitimate, and users might even have the access point already stored in their device, causing it to connect automatically.

DEVICE NETWORK ATTACKS

PER TYPE

Check Point Research, 2020



THE MOBILE APP:
EVERYONE IS AT RISK

According to research published in the 2021 Check Point Cyber Security Report, 46% of organizations have had at least one employee download a malicious mobile application that threatened networks and data, making this a prominent threat that must be on every organization's radar.

Below are provided some of the most damaging threats associated with app downloads in 2020.

BANKERS, MRATS, AND DROPPERS

Banking Trojan malware families are used to steal personal or corporate data by obtaining fraudulent access to funds and installing additional malware on the device after gaining an initial foothold.

The increased use of mobile devices during lockdown and social distancing may also be responsible for the substantial growth in bankers.

The Guildma threat actor introduced Ghimob, which is capable of performing transactions on accounts with financial institutions in Brazil, Paraguay, Peru, Portugal, Germany, Angola and Mozambique.

The newly discovered Eventbot focuses on targets in the U.S. and Europe while Thiefbot aims at Turkish users. The list continues with Blackrock, Wroba, TrickMO and others, all of which show the increase in baking Trojans' activity.

CORONAVIRUS-RELATED

Pandemic-driven attacks contain a range of malware that is focused on stealing a user's sensitive information or generating fraudulent revenues from premium-rate services, and include Mobile Remote Access Trojans (MRATs), banker Trojans, and premium dialers.

To learn more from the Check Point research, click here.

TOP-5 2020 MOBILE MALWARE

1. Hiddad
2. xHelper
3. Necro
4. PreAMo
5. Guerrilla

THE MOBILE APP:
EVERYONE IS AT RISK

POPULAR APP VULNERABILITIES

Among the applications that had major vulnerabilities in 2020 are the world's most popular social apps, including Facebook, Instagram, WhatsApp:

FACEBOOK

In November 2020, a Facebook Messenger vulnerability was discovered through the company's bug bounty program. Had it not been patched it could have allowed a hacker to call the user and listen to them on their device end even if the call wasn't answered.

INSTAGRAM

In September 2020, Check Point announced that it had discovered a critical vulnerability in Instagram that could have been used to perform remote code execution on a victim's phone.

WHATSAPP

Check Point also uncovered a vulnerability in WhatsApp, which if exploited would cause the app to crash and lose data. In addition, in a late 2020 update, WhatsApp published 15 new CVEs.

GOOGLE PLAY CORE

But it's not just the social networks that were rife with vulnerabilities. The **Google Play Core Library**, an app's runtime interface with the Google Play Store also suffered from a persistent code execution vulnerability. If a malicious application exploits this vulnerability, it can gain code execution inside popular applications and have the same access as the vulnerable application.

It is estimated that 8% of all Google Play Applications had been compromised by this vulnerability since September 2019.

THE MOBILE APP:
EVERYONE IS AT RISK

NEW AND EMERGING THREATS

MALICIOUS APPS

The new and emerging threats that have come to the fore in 2020 and which are expected to continue to wreak havoc in 2021 include the malicious COVID-19 related apps, as mentioned earlier.

In addition, there is the Tekya Clicker which was found hidden in 24 children's games and 32 utility apps on Google Play, highlighting once again that the Google Play Store can still host malicious apps.

DIALERS

Premium dialers are another threat to be aware of. These include, WAPDropper, an Android malware that subscribes victims to telco-provided premium services, and the Joker malware, whose proliferation
Check Point has found to have experienced a 100% increase in its infiltration of Google Play, including three new variants in 2020.

CLICKERS

In this group, an impactful threat in 2020 was the campaign of the clicker family Haken, which Check Point researchers discovered during the early part of the year.

This campaign was launched on Google Play with eight malicious applications that garnered over 50,000 downloads. The capabilities of this clicker include getting a hold of as many devices as possible to generate illegitimate profit.

AD-FRAUD

The two most prevalent types of app-generated ad-fraud include rough ad networks that display ads outside of the application's scope, and auto-clickers that mimic the target victim's interactions with ads.

In addition to the damage they cause publishers, they also impact the user experience by draining the device's battery and by compromising the device owner with data theft and by enabling financial fraud via subscription to services.

TOP-5 MITRE ATT&CK® TECHNIQUES

Among the top techniques identified by Check Point to have been used by mobile threat actors in 2020, are those that are related to data gathering and location tracking:

1. File and directory discovery (MITRE T1420, DISCOVERY)
2. Data from local system (MITRE T1533, COLLECTION)
3. Location tracking (MITRE T1430, COLLECTION)
4. Location_tracking (MITRE T1430, DISCOVERY)
5. Application_discovery (MITRE T1418, DISCOVERY)

THE DEVICE:
VULNERABLE BY NATURE

In the Check Point Achilles research discussed earlier, we presented the fact that at least 40% of the world's mobile devices are inherently vulnerable to cyberattacks.

As we can see, vulnerabilities are not exclusive to the operating systems of mobile devices but can also be inherent to the actual hardware. This means that when the threat is deeply ingrained in the device, it is often hidden and typically attacks by surprise, leaving users and organizations unprepared.

THE IMPACT OF HARDWARE VULNERABILITIES

When the vulnerability is hardware based, such as with the Qualcomm DSP chip mentioned earlier, the damage can bring the following impact on users:

- Attackers can leak information
  including photos, videos, call-recordings, real-time microphone data, GPS and location data, and more, and without any user interaction required.

- Attackers can render the mobile phone unresponsive
  where the owner would have to factory reset the device, causing its entire contents to be permanently deleted.

- Malware and other malicious code
  can completely hide their activities and render them un-removable.

THE DEVICE:
VULNERABLE BY NATURE

THE IMPACT OF OS VULNERABILITIES

ANDROID

In 2020 multiple vulnerabilities were discovered in Android, the most severe of which can enable remote code execution within the context of a privileged process.

This vulnerability enables an attacker to install programs, view, change, or delete data, and create new accounts with full user rights.

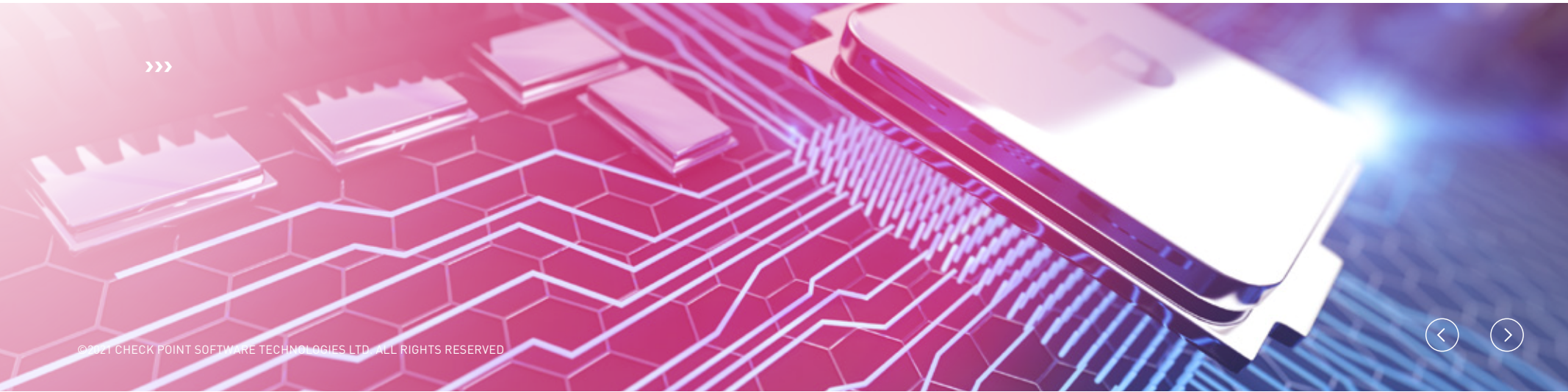
StrandHogg, is another new privilege vulnerability that allows hackers to gain access to almost any app.

As for the good news, Samsung patched a zero-click vulnerability that had been impacting all of its smartphones since 2014, as well as a vulnerability that causes crashes in devices that are eligible for receiving security updates.

iOS

The major vulnerabilities discovered in iOS in 2020, include:

- A 'sign in with Apple' bug that left any account exposed to a hijack attack;
- A zero-click vulnerability that enables threat actors with remote code execution and infection capabilities via sending emails that consume a lot of memory;
- A zero-click radio proximity exploit that can cause any iOS device in radio-proximity to reboot, with no user interaction;
- CheckRa1n and ROM, jailbreak vulnerabilities; and
- LightSpy, a modular malware that exploits a remote code execution vulnerability in the Safari browser. This malware grabs data from the iOS Keychain, which is responsible for handling credentials that are stored on the device.



MDM:
A POWERFUL NEW ATTACK VECTOR

During 2020, Check Point observed an event with significance that is far-reaching. Namely, for the first time, corporate MDM was used as an attack vector.

Regrettably, the MDM's most notable feature, and arguably the reason for its existence – a single, central control for the entire mobile network, is also its major weakness.

And the reason is that when it is breached, so is the entire mobile network. To illustrate, a new Cerberus malware variant infected over 75% of one company's devices via corporate-owned Mobile Device Manager (MDM).

This malware is very damaging, for once installed, it can collect large amounts of sensitive data, including user credentials, and send it to a remote command and control (C&C) server.

MAJOR ACTORS ON THE PROWL

The mobile endpoint has become a very attractive target for various APT groups, such as APT-C-35 (DoNot), APT-C-50 (DomesticKitten), RoamingMantis, and APT-C-23 (Hamas), who are conducting elaborate and sophisticated targeted attacks with a mobile arsenal with new and advanced capabilities.

For example:

- Machine learning tools are being used to bypass human verification mechanisms such as captcha;
- They are stealing encryption keys for popular applications; and
- They are exploiting OS and popular applications vulnerabilities, among others.

A noteworthy campaign is the newly discovered Firestarter campaign of DoNot, which uses the legitimate Google service – Firebase Cloud Messaging, to notify its authors of the final payload location, and is therefore very difficult to detect.

There is also Rampant Kitten, an ongoing surveillance operation by Iran that targeted expats and dissidents for years, and which was unraveled by Check Point. A 2020 update to the Rana Android malware enables snooping via Whatsapp and Telegram IM. And a Hamas Android espionage malware was also discovered.

In addition, mobile ransomware, which has long been associated with the traditional landscape, has been found by Check Point to have evolved into a major mobile threat as well.

As noted earlier, one of the biggest threats in 2020 came from Lucy, a Malware-as-a-Service (MaaS) botnet and dropper for Android devices. And another comes from MalLocker.B, an advanced malware that is difficult to detect and manages to evade many available protections.

THREATS ON THE HORIZON

As we have seen, the mobile threat landscape presented multiple, new, and great challenges to security in 2020. And when we look ahead to 2021 and beyond, we recommend that every organization take the following into consideration when crafting the security strategy for the year ahead:

COMPLEXITY IS ON THE RISE

Check Point researchers have observed the increasing complexity in malware functionality and infrastructure used by threat actors, as well as the countermeasures that they are using to avoid detection.

Malware will keep evolving and adapting to the new techniques and methods that are employed by security vendors to protect users and their devices against malicious actors who are attempting to gain access.

MALWARE IS GOING NATIVE

More and more malware is implementing malicious behavior by using native-code, making it difficult for security vendors to detect malicious behavior, with Haken, Tekya, and Joker as a few examples.

And due to the fact that malicious behavior is implemented in native code (as opposed to via Java) it also becomes harder to analyze and, therefore, harder to detect.

IT'S ALL ABOUT THE MONEY

Fraudulent ad revenue and banking Trojans should also be on every organization's radar.

It may not be new that malicious actors are financially driven, seeking ever new methods to generate revenue from fraud. What is new is the growth in the number of applications that conducted ad fraud over the past year, with a greater focus than ever on abusing the CPI model.

THE PROLIFERATION OF DROPPERS IS INCREASING

Another prediction for 2021 is the shift away from "direct malware" on official markets towards the use of "droppers," which are used by attackers to control which payload is served, if any, or to bypass security evaluation by official markets.

THIRD-PARTY HOSTS ARE MORE COMMON

Check Point researchers have also observed that more and more malware is shifting away from inserting malicious code into applications. Rather, it is now opting to assume the payload from a third-party party host.

For example, Joker aims at a hybrid approach with a variant that embeds the payload as encoded class-strings, which decode and load the payload upon receiving a command from the command-and-control server.

RainbowMIX, for example, executed a single ad fraud campaign on Google Play, compiling over 240 Android applications, and having been downloaded over 14 million times.

This is estimated to have flooded agencies with over 15 million daily impressions, and to have greatly impacted the user experience, usability, battery performance, and to have made it easier for second stage malware to execute financial fraud and theft of sensitive information.

HARMONY MOBILE:
ADDRESSING MOBILE PROTECTION NEEDS

Check Point is helping organizations all over the world secure the mobile endpoint with Harmony Mobile.

Harmony Mobile is a Mobile Threat Defense solution that keeps corporate data safe by securing the mobile devices of employees across every attack vector, including the network, apps, and operating system.

Designed to reduce admin overhead and increase user adoption, it fits perfectly into the existing mobile environment, deploys and scales quickly, and protects devices without impacting user experience nor privacy.

AMONG ITS UNIQUE CAPABILITIES ARE:

- Preventing malicious app downloads
- Preventing phishing across all apps
- Preventing man-in-the-middle attacks
- Blocking infected devices from accessing corporate apps
- Detecting advanced jailbreaking and rooting techniques and OS exploits

Harmony Mobile's MARS app vetting feature enables security admins to easily analyze new applications and provide internal app vetting during development cycles, enabling comprehensive security and privacy review for app approval within the organization's environments.

Harmony Mobile

To learn more about how Harmony Mobile can help you protect your organization's mobile fleet, we invite you to schedule a personalized demo by clicking **here**.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

To learn more about us, visit: www.checkpoint.com

CONTACT US

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv

67897, Israel

Tel: 972-3-753-4555

Fax: 972-3-624-1100

Email: info@checkpoint.com

U.S. Headquarters

959 Skyway Road, Suite 300,

San Carlos, CA 94070

Tel: 800-429-439 / 650-628-2000

Fax: 650-654-4233

Check Point
SOFTWARE TECHNOLOGIES LTD