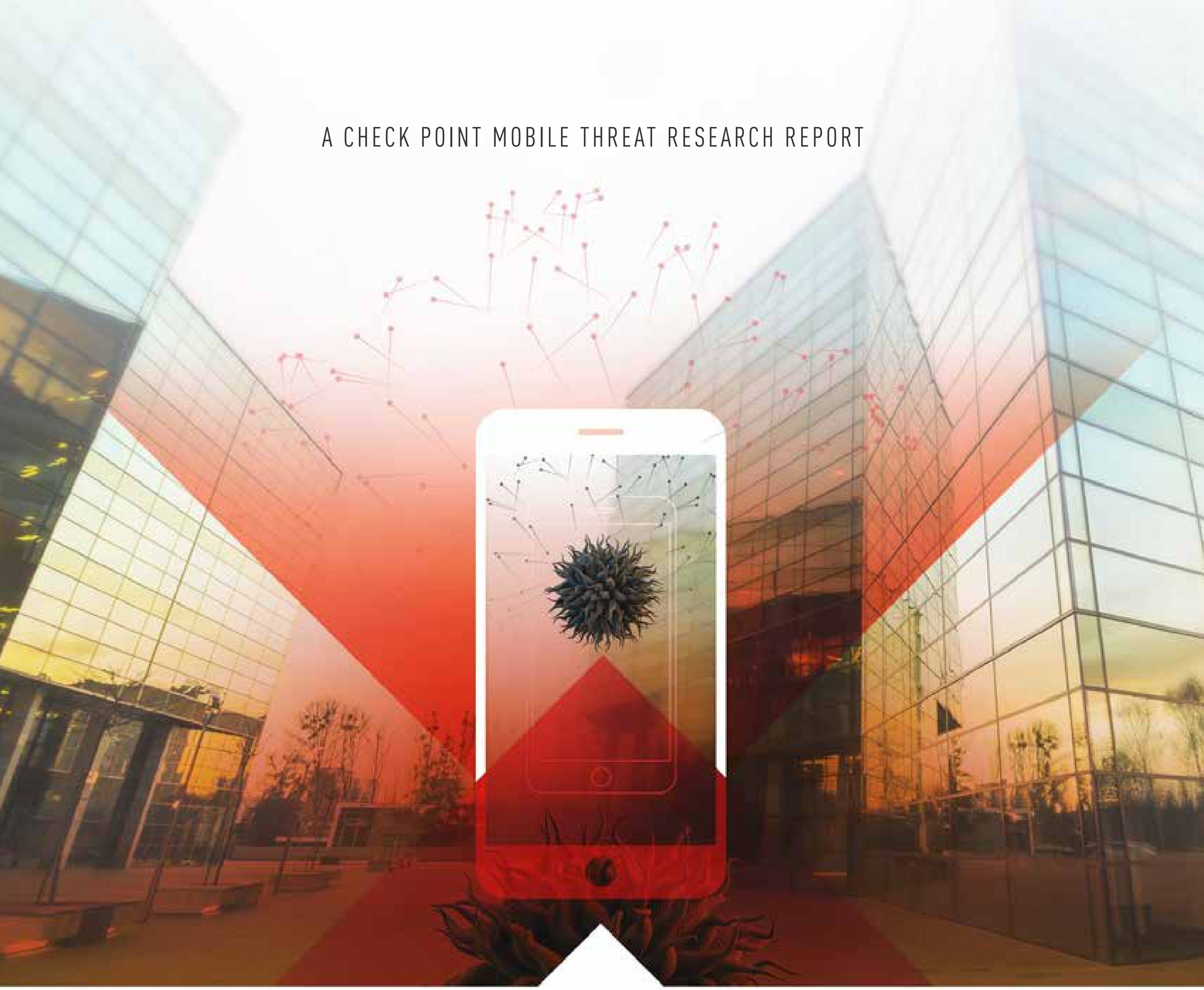
A CHECK POINT MOBILE THREAT RESEARCH REPORT



MOBILE CYBERATTACKS IMPACT EVERY BUSINESS

CHECK POINT RESEARCH

INTRODUCTION

As businesses around the globe increasingly adopt mobility programs to boost productivity and profitability, cyberattacks continue to grow in sophistication and frequency. Yet today nearly two-thirds of security professionals doubt their organizations can prevent a breach to employees' devices, while 94% expect the frequency of mobile attacks to increase.[1]

This report, prepared by Check Point's mobile threat research team, is the first to study the impact of mobile attacks in enterprise environments by assessing actual threat telemetry of corporate-owned and bring-your-own devices. The results are stark: enterprise mobility is under constant attack, affecting all regions and industries, on both major mobile platforms, Android and iOS. Threats to mobile users are myriad and powerful, and ultimately capable of compromising any device, accessing sensitive data at any time.

This report reveals the major trends in mobile malware and other attack vectors, where they operate, and which industries are the most frequent targets.

THE KEY FINDINGS OF THIS RESEARCH ARE:

EVERY COMPANY IS UNDER SOME FORM OF MOBILE ATTACK

THE MOST AFFECTED INDUSTRIES ARE FINANCIAL SERVICES AND GOVERNMENT

THE MOST MOBILE ATTACKS OCCUR ON BUSINESSES IN THE AMERICAS

iOS DEVICES ARE NOT IMMUNE TO BREACHES,
WHILE THE VAST MAJORITY OF ATTACKS ARE ON ANDROID DEVICES

[1] "The Growing Threat of Mobile Device Security Breaches," Dimensional Research, April 2017. https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf

METHODOLOGY

The data in this report was collected from deployments of Check Point SandBlast Mobile in 850 organizations that secured a minimum of 500 devices from July 1, 2016 to July 1, 2017. All data was normalized for the purpose of this analysis.

This study's findings are grouped regionally to include EMEA (Europe, Middle East, and Africa), APAC (Asia and the Pacific), and the Americas. Vertical sectors are grouped into seven categories: Financial Services (banks, insurance, and brokerage firms), Government, Technology, Manufacturing, Telcos, which refer to mobile carriers, and Other, which includes a number of vertical industries that are not well represented in SandBlast Mobile's customer base.

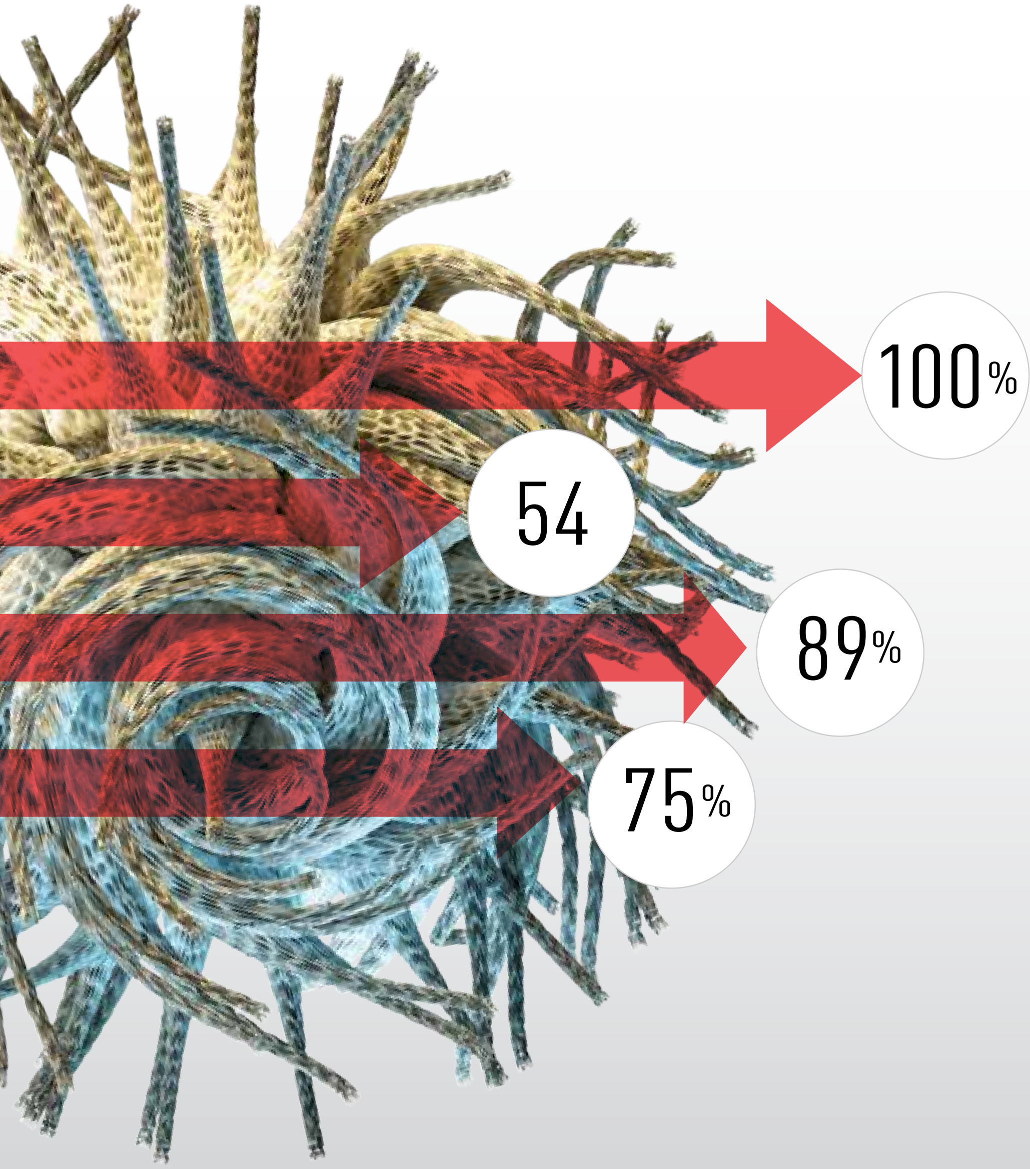
EVERY ENTERPRISE HAS EXPERIENCED A MOBILE ATTACK. THEY JUST DON'T KNOW IT.

Each organization in our sample experienced at least one mobile malware attack during the past year. That said, the average number of mobile malware attacks per organization was 54.

BUSINESSES AVERAGED
54 MOBILE MALWARE INFECTIONS

Organizations suffer from different types of mobile attacks beyond malware. 89% experienced at least one man-in-the-middle attack over a Wi-Fi network.

Even though enterprise mobility management (EMM) solutions were in place, 75% of the organizations in our sample had at least one jailbroken iOS device or rooted Android device connected to their corporate networks. The average number of rooted or jailbroken devices in our sample was 35 per company. These results are concerning because the process of rooting or jailbreaking a device strips away all built-in security provided by the iOS and Android operating systems.



EVERY ENTERPRISE IS UNDER ATTACK

100% OF ALL BUSINESSES HAD A MALWARE ATTACK

54 IS THE AVERAGE NUMBER OF MOBILE MALWARE ATTACKS PER BUSINESS

89% EXPERIENCED A MAN-IN-THE-MIDDLE ATTACK OVER WI-FI

75% AVERAGED 35 ROOTED OR JAILBROKEN DEVICES ON NETWORK

AN INDUSTRY-BY-INDUSTRY VIEW OF THE SURVEY SAMPLE

Technology companies represent the largest percentage (32%) of protected devices in our sample, followed by financial services (21%), such as banks, brokerages, and insurance firms (Chart 1). Manufacturers composed 15% of our sample, with telecommunication companies (12%), retailers (7%), and government agencies (5%) rounding out the analysis.

STUDY SAMPLE BY INDUSTRY

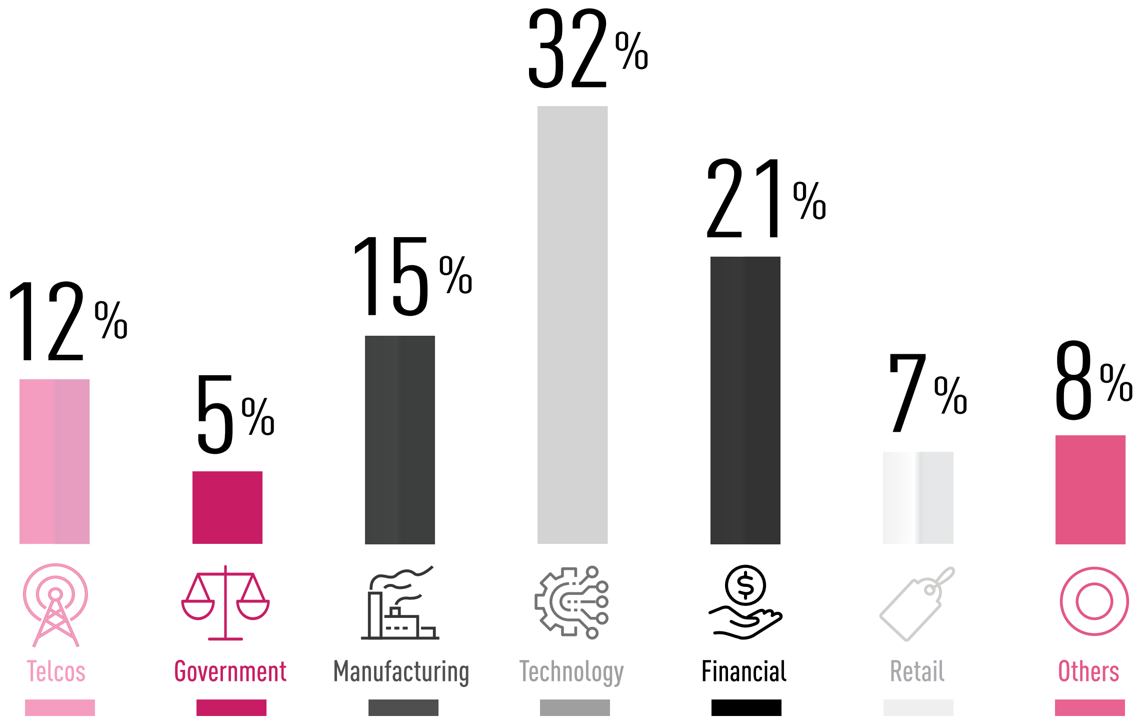


Chart 1

MOBILE MALWARE HITS GOVERNMENT AND FINANCIAL SERVICES THE MOST

One can easily see in Chart 2 that financial services (29%) and government (26%) experienced the most mobile malware attacks, far beyond their proportional representation in the sample we analyzed. Both industries offer valuable caches for attackers, such as large repositories of financial and personal information. Technology firms were also heavily impacted by malware.

MALWARE ATTACKS BY INDUSTRY

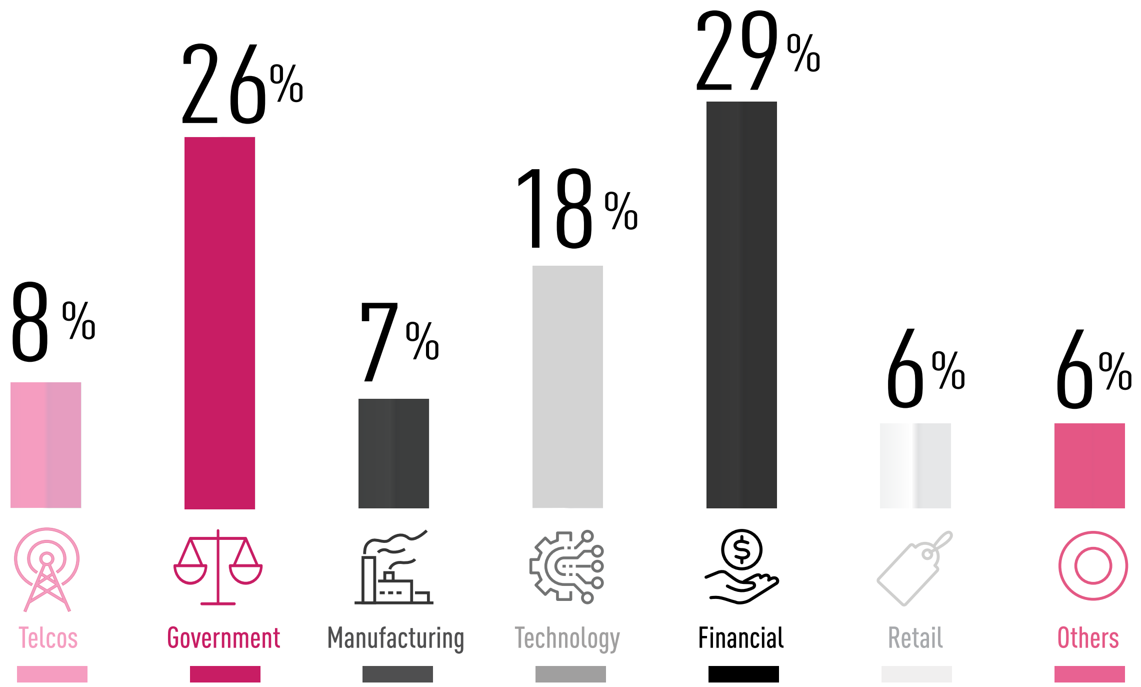


Chart 2

MALWARE TARGETS iOS DEVICES IN FINANCIAL SERVICES

Chart 3 reveals the percentage of iOS malware attacks in different industries. Financial services was the overwhelming leader, accounting for 40% of all attacks. Government (20%) devices were also heavily targeted, followed by technology companies (9%) and the manufacturers (9%). While many financial services organizations require employees to use iOS devices for better security, this data reveals that iPhones and iPads are not immune to mobile malware attacks.

iOS MALWARE BY INDUSTRY

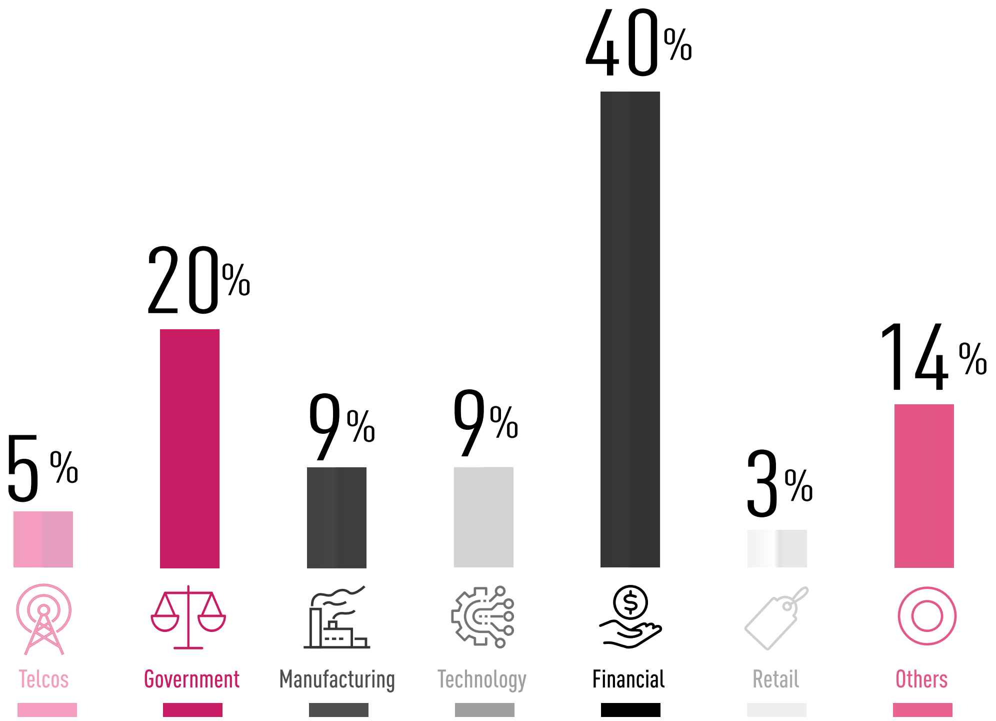


Chart 3

BUSINESSES FROM MOST INDUSTRIES FACE A WIDE VARIETY OF ATTACKS

The financial services sector has the dubious distinction of experiencing the most dangerous kinds of malware, as seen in Chart 4. For instance, 44% of all mobile remote access trojans (mRATs) were detected on devices used at financial services.

MALWARE TYPES BY INDUSTRY (%)

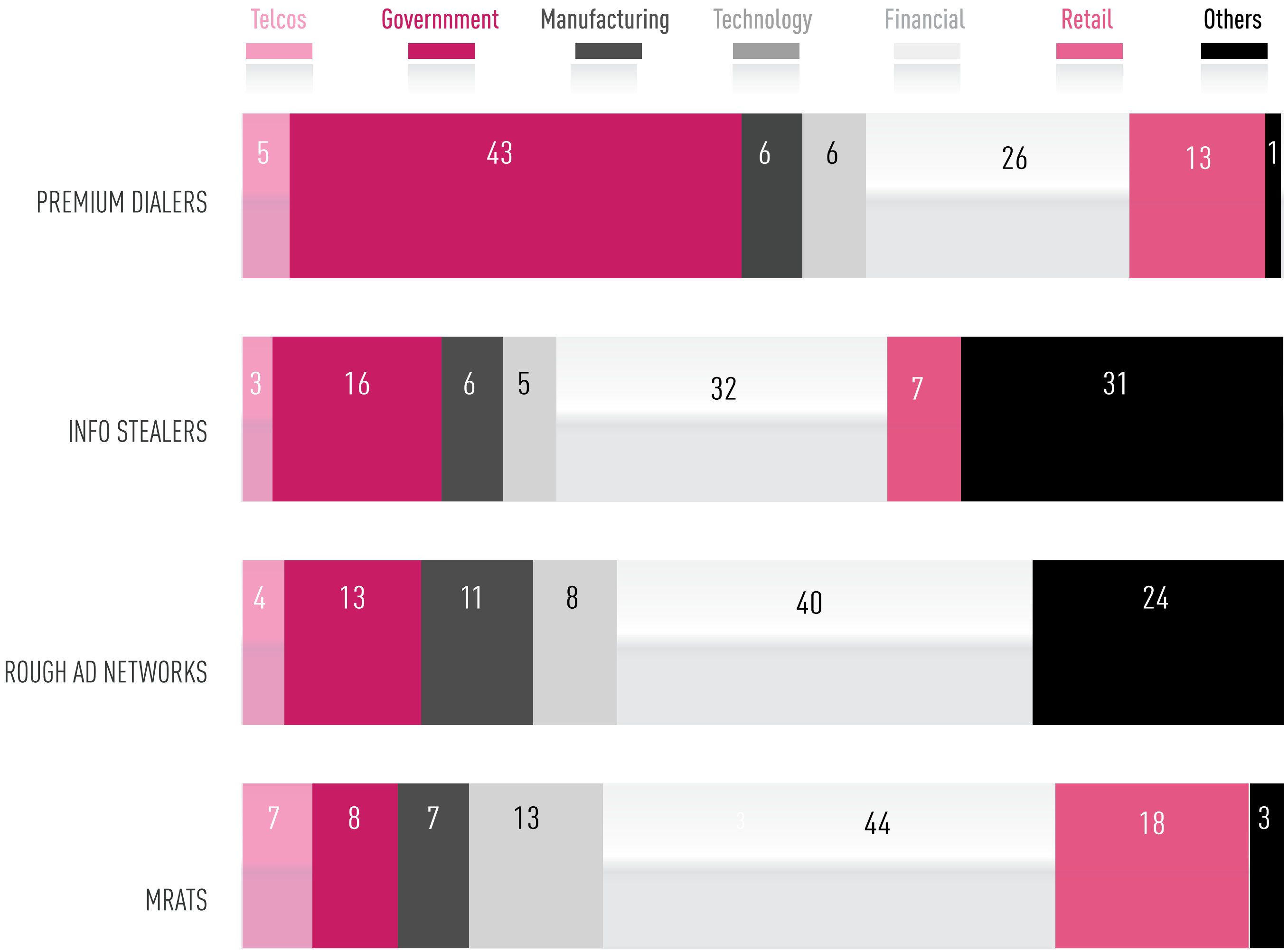


Chart 4

firms. These tools allow an attacker to access the infected device remotely and gather information from all the sensors available on the device, such as its camera, microphone, message and call directories, and much more. In a recent example, an mRAT was spotted on the mobile device of the security officer of a major European bank. This particular malware was a strain of Ispyoo, based upon an existing framework that was sold commercially as "parental protection" under different names, such as Copy9, OmegaSpy and many more.

Government employees were targeted by premium dialers, which abuse SMS and call permissions to charge the device's owner for fraudulent calls and text messages to premium services. These pesky malware, such as ExpensiveWall, operate silently and sometimes can be found on official app stores.

Clearly businesses from most industries can count on a wide variety of attacks. While some malware represents targeted attacks that are aimed at a specific organization, others try to infect as many devices as possible, compromising the security of entire networks along the way.

THE FINANCIAL SERVICES SECTOR HAS THE DUBIOUS DISTINCTION OF EXPERIENCING THE MOST DANGEROUS KINDS OF MALWARE

WHERE MOBILE MALWARE IMPACTS THE MOST BUSINESSES

The study's sample was composed of companies from every corner of the world (Chart 5). When grouped by region, 51% of the companies were located in EMEA (Europe, Middle East, and Africa), 31% from the Americas, and the remaining 18% from APAC (Asia and the Pacific).

THE SAMPLE'S REGIONAL SPLIT

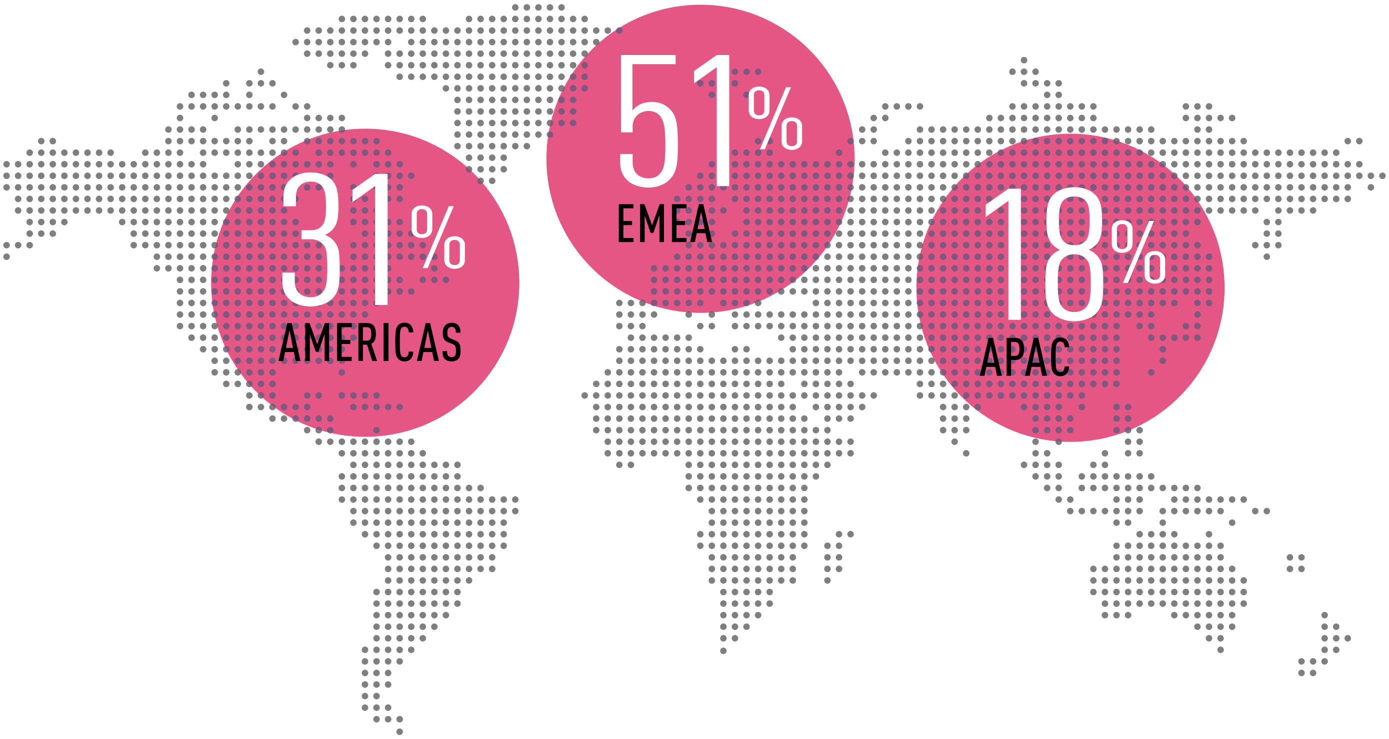


Chart 5

As seen in Chart 6, the Americas was the most impacted region in the study's sample and is composed primarily of companies in the United States. APAC accounted for a third of all mobile attacks, despite a smaller representation in the sample. This can be explained by several mass malware campaigns that have targeted Southeast Asia during the past year, including HummingBad and CopyCat. However, the bottom line is that businesses in all regions are heavily impacted by mobile malware, making it difficult to ignore this troubling trend.

MALWARE DISTRIBUTION BY REGION

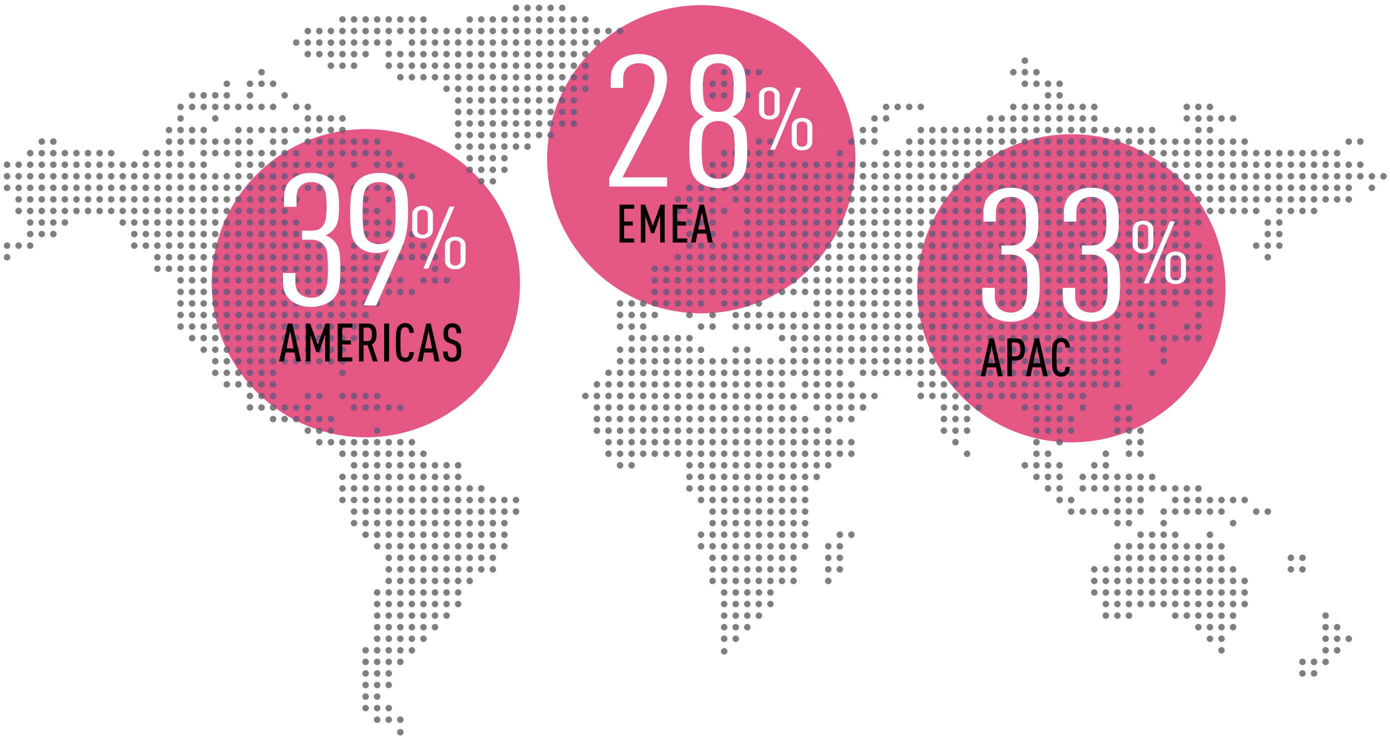


Chart 6

WHERE IS MOBILE MALWARE HEADED? IT'S NOT LOOKING PRETTY...

We can only expect mobile attacks to increase in proportion and sophistication in the years ahead. For perpetrators the world of mobile devices holds great potential: they are easier to hack and they possess even more sensitive information than PCs.

We expect the financial services sector to continue to be a primary target of cybercriminals, followed by government agencies, as these two sectors protect the most valuable assets. Malware trends indicate that the geographic distribution of mobile attacks will normalize, and every region will experience an increased amount of malware. As long as the mobile market is composed of two dominant players, iOS and Android, malware will continue to target both, and try to penetrate their defenses.

Comprehensive mobile security should be a system of components that work together cohesively to identify a wide variety of threats and to protect data while addressing employee privacy concerns. Only solutions that can analyze behavior across all vectors for indicators of attack can protect mobile devices effectively to keep them safe.

Check Point SandBlast Mobile is a multilayered security infrastructure that provides comprehensive protection. It identifies threats using on-device, network- and cloud-based algorithms, and triggers automatic defense responses. Its cloud-based risk engine identifies suspicious patterns and behaviors over time by sandboxing apps in an emulator and detecting threats at the device, app, and network levels. The infrastructure integrates with existing security investments to support incident response and provide continuous protection. As a result, organizations always have an accurate picture of the types of threats that devices on their network face, as well as detailed information about what is being done to mitigate those risks.

Next, read A CISO's Guide to Mobile Threat Defense.

For further information: www.checkpoint.com\mobilesecurity

Check Point
SOFTWARE TECHNOLOGIES LTD