Check Point
SOFTWARE TECHNOLOGIES LTD

2016 H2 GLOBAL THREAT INTELLIGENCE TRENDS

INTRODUCTION

New, sophisticated threats continue to emerge on a daily basis across multiple platforms: social media, mobile platforms, email and web pages. At the same time, new, high-profile malware and attack methods continue to evolve, bypassing existing security solutions and tailoring attacks against the largest companies in the world. The devices we use every day are now subject to compromise and can be leveraged for attacks. Even the recent U.S. elections were targeted. The Check Point 2016 H2 Global Threat Intelligence Trends report provides you with the best overview of the cyber landscape, threats and attacks and predictions, based on data drawn from the ThreatCloud World Cyber Threat Map between July and December 2016. Information about threats, trends and attacks divided by region can be found in our Check Point 2016 H2 Regional Threat Intelligence Trends report.

GLOBAL TRENDS

DDOS ATTACKS VIA IOT DEVICES

August marked the introduction of the now infamous Mirai Botnet – a first of its kind Internet-of-Things (IoT) Botnet, which attacks vulnerable Internet-enabled digital video recorders (DVR), surveillance cameras (CCTV), and other Internet-enabled devices. It turns them into bots, using the compromised devices to launch multiple high-volume Distributed Denial of Service (DDoS) attacks.

Victims so far include Amazon, Twitter and Spotify as well as the entire internet infrastructure of Liberia. It is estimated that approximately 500,000 Mirai-powered bots have spread worldwide. In October, the botnet and scanner source code were released publicly—an act which opens the door for future botnet attacks of this kind. It is now clear that vulnerable IoT devices are in use in almost every home. Therefore, we will continue to see massive DDoS attacks that utilize such devices, ushering in an era in which every smart device in everyday use should be meticulously protected and updated.

THE MONOPOLY IN THE RANSOMWARE MARKET

In our previous Threat Intelligence half-year review, we marked 2016 as the year for ransomware—a prophecy that was realized emphatically. There was an increase in the overall attack rank as well as a variety of new methods for infection, communication, and anti-detection. Although thousands new of ransomware variants were observed in 2016, in recent months we witnessed a change in the ransomware landscape as it became more and more centralized, with a few significant malware families dominating the market and hitting organizations of all sizes. Cerber and Locky, the ransomware families at the top of the list, were first introduced in spring 2016. Over the last few months, new versions of those ransomware families were constantly discovered. Our data even shows that Cerber is ranked among the top 20 malware family attacks in the APAC region.

NEW FILE EXTENSIONS USED IN SPAM CAMPAIGNS

According to statistics collected by our researchers, the most prevalent infection vector used in malicious spam campaigns throughout the second half 2016 was downloaders based on Windows Script engine (WScript). Downloaders written in Javascript (JS) and VBScript (VBS) dominated the mal-spam distribution field together with similar yet less familiar formats such as JSE, WSF, and VBE. WScript-based downloaders, such as those mentioned below, have several features which make them popular among threat actors in the spam industry:

- The functionality is consistent across different Windows versions.
- The default behavior of a WScript file format dictates that the contained code is executed—for example, when it is double-clicked.
- Script files are very easy to manipulate and generate polymorphic variants of a single downloader, which is undetectable by security products based on a static signature.
- While scripts that are run in the browser are sandboxed, WScript code is able to run using permissions similar to those of the victim and its abilities within the machine is simply unlimited.
- When it comes to the security industry, script files get a lot less attention.

The second most common malicious attachment type was MS-Office documents, and we detected a substantial increase in the use of less common formats, such as document-templates and macro-enabled documents. Examples included the .dotm extension, prominently used by Cerber ransomware distributors, and .xlsm used mainly by Locky ransomware.

Different malicious attachments were often sent in zip and rar archives. As many email services, and even clients, block such files by default, Office documents and PDF files are exceptional and commonly sent "as is." Although there was an increase in large-scale spam campaigns with reasonable social engineering applied, our observations show that the majority of the malicious spam is still poorly written and does very little to convince users of its legitimacy.

MOBILE TRENDS

THREAT FACTORS

Banking Trojans and fake ad-networks remained the main money-making vectors for large scale malware campaigns, with mobile ransomware found to be on the rise. Interestingly, many banking Trojans have started developing ransomware capabilities as a secondary attack vector. Fake ad-networks still have the technological edge with highly sophisticated rootkits that enable total takeover of mobile devices, and compromise of digital identities, as shown by the Gooligan botnet.

As reported above, IoT devices have become an increasing security concern in 2016, with the spectacular DDOS attacks unleashed by the Mirai botnet from low-end IoT hardware such as IP-based cameras. Google has announced "Android Things", an IoT OS which will presumably address such security issues and will further extend Android's relevance.

THREAT ACTORS

2016 put the spotlight on mobile technology used by threat actors. Following the terrorist acts in Paris and San Bernardino, there has been a lot of discussion regarding the role of mobile security and secured apps, such as Telegram, in facilitating stealthy communications for terrorists. This controversy peaked at the FBI–Apple encryption dispute, in which Apple's security mechanisms collided with law enforcement needs. On the reverse, there was the Pegasus targeted attack where surveillance tool developer NSO assisted in spying on a human rights activist based in the United Arab Emirates. These events drew serious attention to mobile-espionage, which is likely to become an increasingly active and tense cyber-warzone.

GLOBAL MALWARE STATISTICS

The statistics below are based on data drawn from the ThreatCloud World Cyber Threat Map between July and December 2016. The percentage of each malware family represents its percentage within all the recognized malware attacks on organizations worldwide.

TOP MALWARE FAMILIES (GLOBAL)

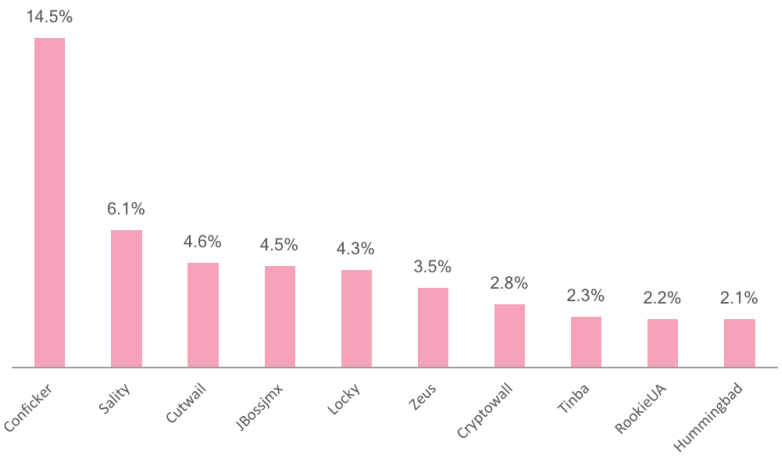


Figure 1: Most Prevalent Malware Globally

TOP RANSOMWARE (GLOBAL)

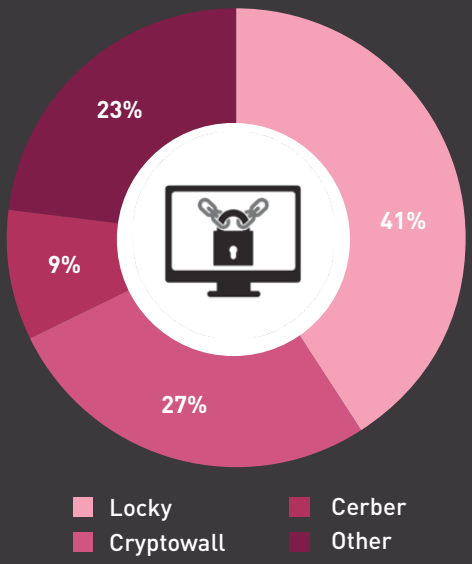


Figure 2: Most Prevalent Ransomware Globally

TOP BANKING MALWARE (GLOBAL)

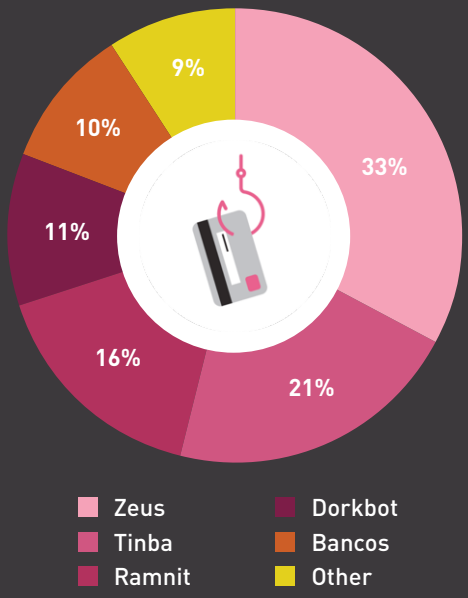


Figure 3: 2016 H2 Most Prevalent Banking Malware Globally

TOP MOBILE MALWARE (GLOBAL)

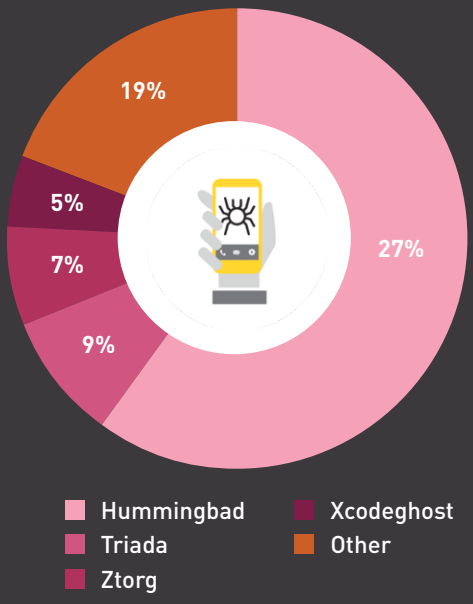


Figure 4: 2016 H2 Most Prevalent Mobile Malware Globally

GLOBAL THREAT INDEX MAP

Check Point's Threat Index is based on the probability that a machine in a certain country will be attacked by malware. This is derived from the ThreatCloud World Cyber Threat Map, which tracks how and where cyberattacks are taking place worldwide in real time.

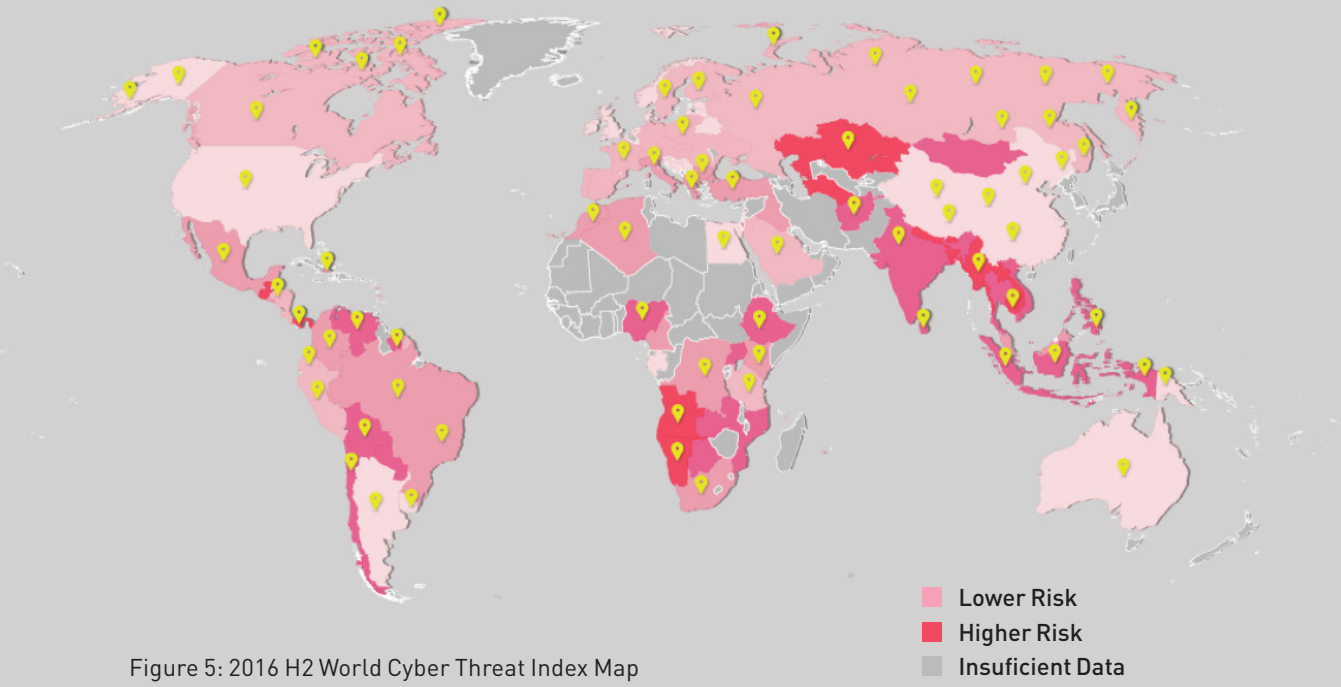


Figure 5: 2016 H2 World Cyber Threat Index Map

CYBER ATTACK CATEGORIES BY REGION

The infographic below shows the spread of three of the main malware categories in this report—Banking, Mobile and Ransomware—across the different regions on the world.

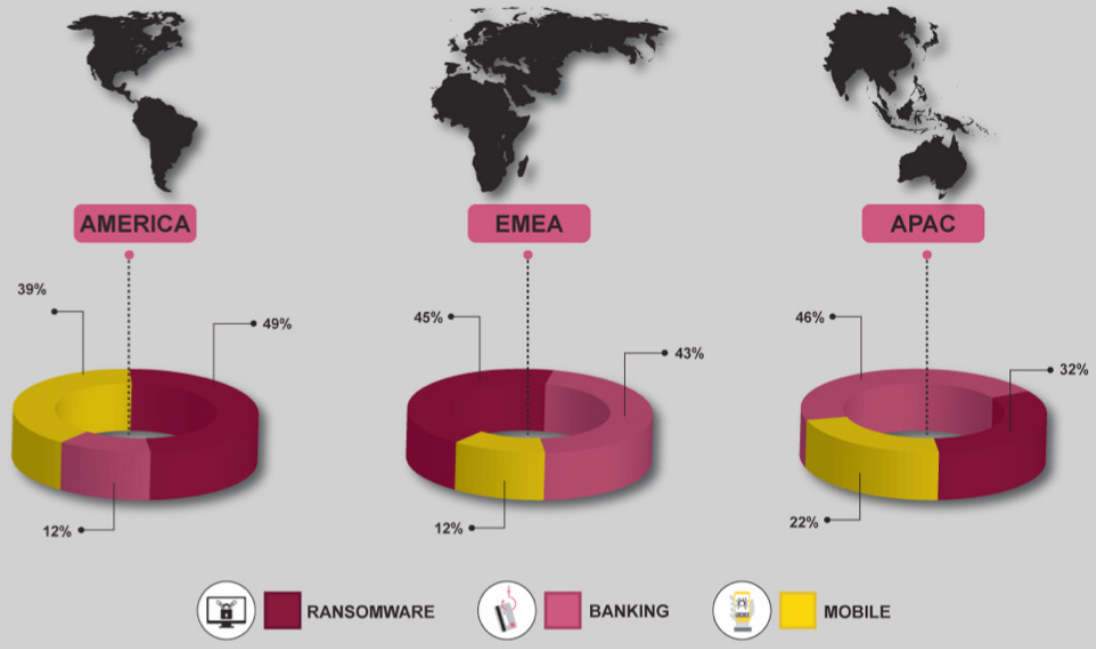
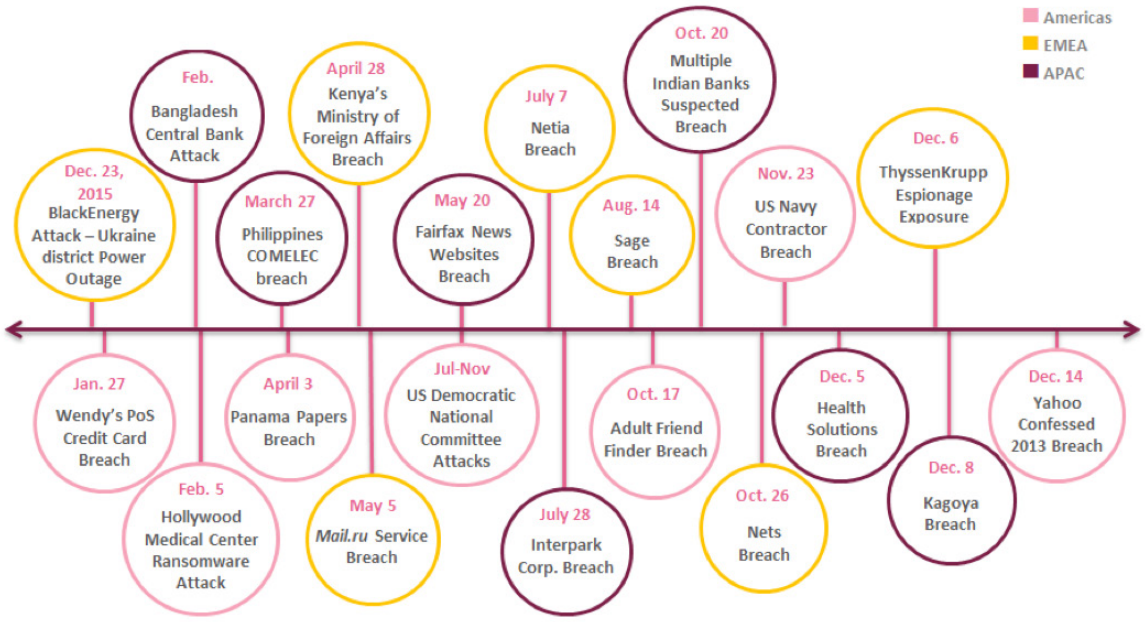


Figure 6: Attack Categories by Region

YEARLY DATA BREACHES TIMELINE



YEARLY TRENDS

- Conficker and Sality, two major botnets that have been around for over 8 years, maintained their place at the top of the global rank. Additional malware families which kept their places at the top of the malware chart for the second half of 2016 include the Zeus banking Trojan, Cutwail botnet, Hummingbad Android malware, and JBossjmx, worm.
- The percentage of ransomware attacks out of all recognized attacks globally almost doubled in the second half of 2016, from 5.5% to 10.5% of all malware attacks worldwide.

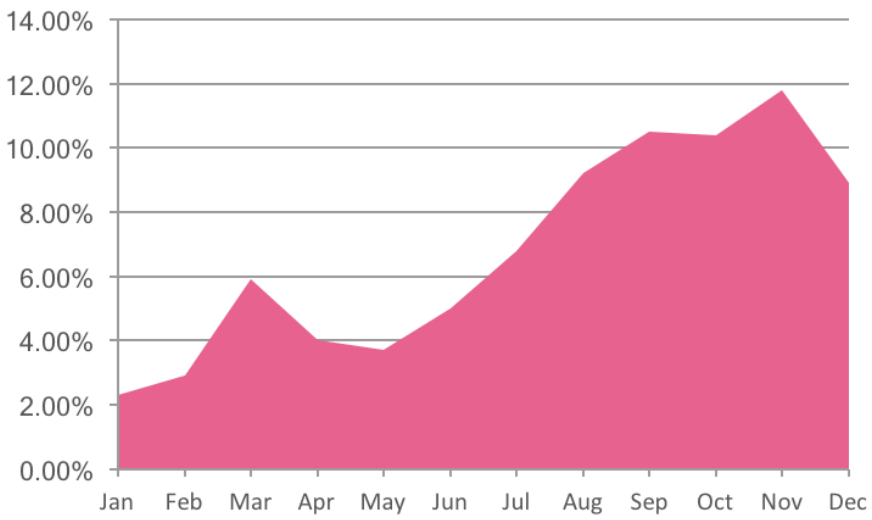


Figure 8: Percentage of Ransomware within All Recognized Attacks Worldwide

- Locky climbed the rankings from number 30 in the first half of 2016 to number five in the second half of the year. At the end of 2016, Locky ransomware made it to the top three malware families, and became the leading ransomware family, surpassing Cryptowall which had previously been dominant.
- As opposed to the significant increase in the percentage of ransomware out of all recognized attacks, the relative percentage of banking malware remained relatively stable in the second half of the year.
- The three leading banking malware families. Zeus, Tinba and Ramnit, all moved up the ranking compared to the first half of 2016. This was at the expense of Dorkbot, which was the leading banker in first half and dropped twelve spots in the global ranking and three spots in the banking malware ranking.

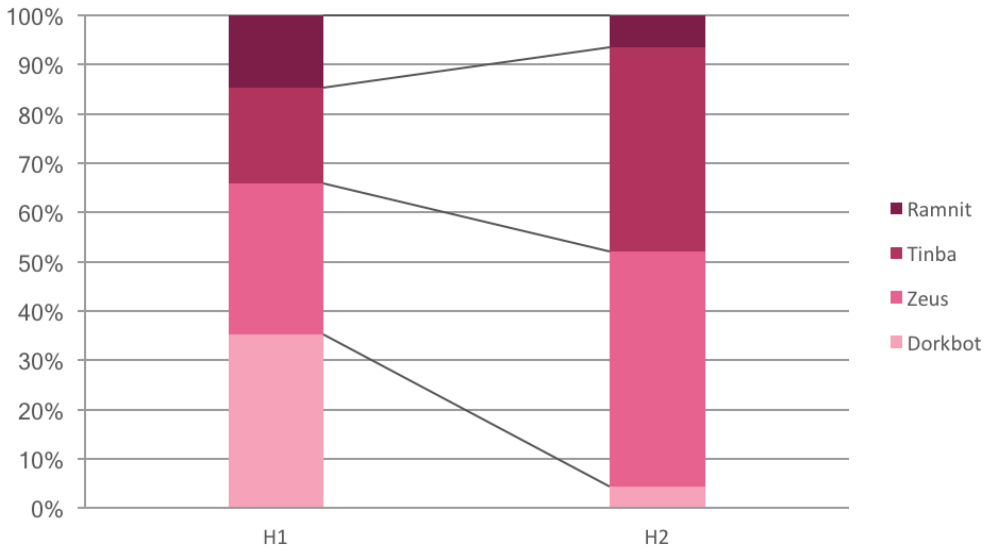


Figure 9: Proportion of attacks by the leading Banking Trojans during 2016

- The amount of organizations that suffered from mobile related security incidents increased by 23% from the first half of 2016 during the second half of the year.

TOP 2017 PREDICTIONS

The trends, statistics and events presented above lead us to believe that the following events will take place in the cyber landscape of 2017:

- **IoT devices—both attack target and source**—In late December, an LG smart TV running Google TV was found to be infected by the Flocker Android ransomware. This case follows multiple other incidents that took place in 2016 in which boilers, video cameras, home alarms and a variety of other devices were attacked. The ability to track and target vulnerable IoT devices was massively exposed in 2016 and we believe that in 2017 the sophistication level, scale and diversity of such attacks will increase. Devices will be held for ransom, sensitive data will be stolen, access will be sold on the Dark Web, and compromised devices located within sensitive networks and data centers may lead to severe operational damage.

  Not only will IoT devices be subjected to various attacks, they will also be leveraged to attack other systems, and to launch massive DDoS attacks, such as the Mirai botnet operations. IoT devices can record a massive amount of data which describes their owner's everyday activities, consumer habits and even medical status. As those devices play an increasing role in today's cyber landscape, our privacy is now at risk more than ever.

- **Malware-as-a-Service industry will take on additional forms**—Drive-by attack methods, malware code and a variety of other tools are sold and traded in a business method referred to as Malware-as-a-Service. For instance, Cerber, a ransomware-as-a-service exploit, was one of the most dominant and profitable ransomware variants of 2016. Recently, a new DDoS collaboration program dubbed Sledgehammer went public, making headlines due to its unique operation mode. Participants are asked to attack targeted political websites. In return, they earn points that can be traded for rewards, such as 'Click-Fraud' bots and a DDoS tool. We estimate that new and unique collaboration frameworks will continue to emerge, each one more profitable for the actors and destructive for the public.

- **Politically-oriented attacks, or psychological warfare**—Cyber-attacks were at the heart of the U.S. presidential campaign, as the Democratic National Committee (DNC) experienced a severe security breach. Furthermore, on December 29, the American Department of Homeland Security and the FBI published a joint analysis report accusing Russian intelligence services of malicious cyber activity during the presidential elections. On that same day, President Obama expelled 35 Russian intelligence operatives from the U.S. due to the alleged attacks. Cyber actions have played a significant role in international affairs, and will become an integral part of every political actor's toolbox, from nation-state agencies to terror organizations.

- **Infection via Steganography (Image Files)**—In late November, Check Point researchers exposed a new attack vector, named ImageGate, which embeds malware in image and graphic files. Furthermore, it was discovered that, by exploiting a misconfiguration on the social media infrastructure, attackers were able to successfully upload infected image files to social media websites such as Facebook and LinkedIn. This way victims are forced to download the image file.

  Following the exposure of ImageGate, Locky ransomware has started spreading via SVG and PNG files through Facebook as well. The recently exposed Gatak backdoor also uses steganography to gain access to victims' machines and steal private information. The use of image files, which can easily be uploaded to most of today's dominant social media websites, and a variety of other platforms, creates a whole new set of tools for attackers. Indeed, dozens of less familiar malware families are now beginning to use this attack method. It seems that this concealment method will definitely become one of 2017's most prominent attack forms.

CONCLUSION

The second half of 2016 demonstrates the nature of today's cyber environment. New attack vectors targeting home devices as well as large organizations were revealed. At the same time, a few older ransomware families managed to maintain their control over the ransomware market, with constant releases of new and improved variants. Ransomware attacks stand out clearly, as the percentage of ransomware out of all recognized attacks worldwide nearly doubled in the second half of the year. Our data demonstrates a long tail distribution of some prominent families: a small number of families are responsible for a major part of the attacks, while thousands of other malware families are rarely seen. We can also see that most cyber threats are global and cross-regional, with the top threats appearing in all three regions. The APAC region stands out as its Top Malware Families chart includes 5 families which do not appear in the other regional charts.

The statistics in this report are based on data drawn from the ThreatCloud World Cyber Threat Map between July and December 2016. Check Point's ThreatCloud is the largest collaborative network to fight cybercrime, delivering the most up-to-date threat data and cyberattack trends from a global network of threat sensors. The ThreatCloud database identifies millions of malware types daily, and contains more than 250 million addresses analyzed for bot discovery, as well as over 11 million malware signatures and 5.5 million infected websites.