Check Point
SOFTWARE TECHNOLOGIES LTD

2016 H2 REGIONAL 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, prominent malware and attack methods continue to evolve, bypassing existing security solutions, and tailoring attacks against the largest companies in the world. Devices in our everyday use are now subject to compromise and can be leveraged for attacks. Even the recent U.S. elections were targeted with significant attacks. 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.

REGIONAL SUMMARY—AMERICAS

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.

MAJOR CYBER BREACHES

- **Jul-Nov, 2016:** Cyberattacks were at the heart of the U.S. presidential campaign, as over 19,000 emails from the Democratic National Committee (DNC) were published on WikiLeaks (July 22). The data breach also included an analytical data program maintained by the DNC and used by the Clinton campaign. The hacker claiming to be behind the DNC attack also published (August 12) personal information of nearly 200 Congressional Democrats, including House Minority Leader Nancy Pelosi. U.S. President Obama ordered intelligence agencies to review cyberattacks carried out during the 2016 presidential campaign, following reports of Russian intervention in favor of President-elect Trump.

- **October 17, 2016:** The popular casual dating site, Adult Friend Finder, suffered a security breach for the second time. Over 300 million account credentials were stolen. The attackers took advantage of the poor encryption methods used for sensitive information stored in the site's database.

- **November 23, 2016:** The United States Navy announced that personal data of over 130,000 ex and current sailors, was stolen from a private contractor. According to the Navy, an unknown attacker breached a private contractor's computer and stole the file containing the sailors' private information.

- **December 14, 2016:** Yahoo admitted it suffered a massive data breach in August 2013, exposing the personal data of over one billion users. The data breach was exposed by law enforcement agencies, and is probably unrelated to the 2014 data breach that was announced in September. In that breach, account information tied to over 500 million user accounts was disclosed.

TOP MALWARE FAMILIES (AMERICAS)

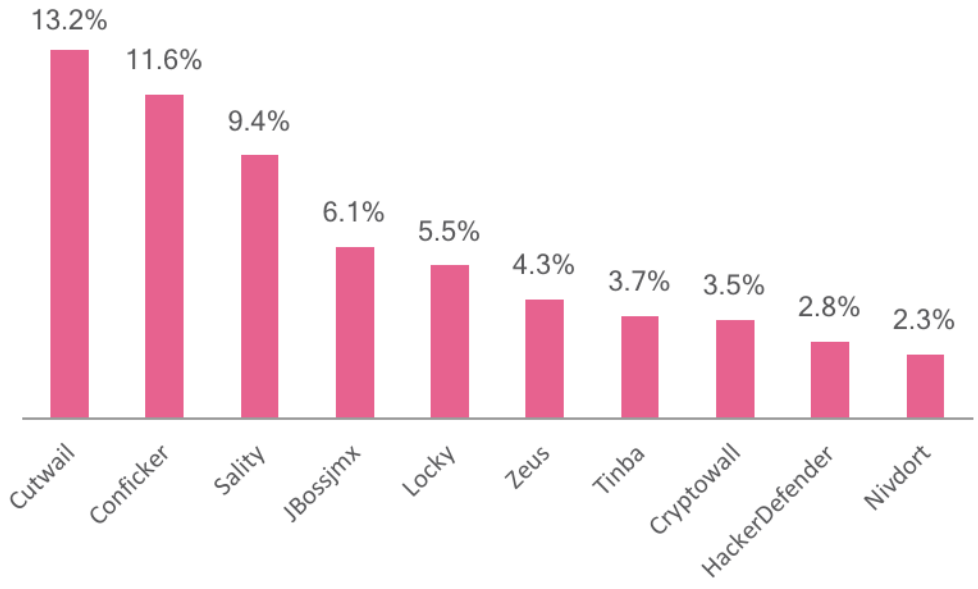


Figure 1: Most Prevalent Malware in the Americas

TOP RANSOMWARE (AMERICAS)

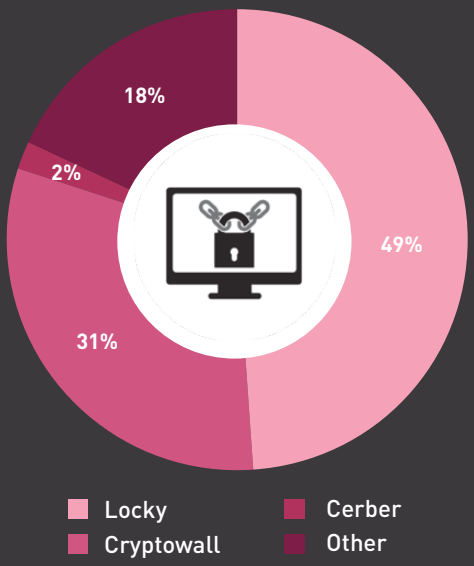


Figure 2: Most Prevalent Ransomware in the Americas

TOP BANKING MALWARE (AMERICAS)

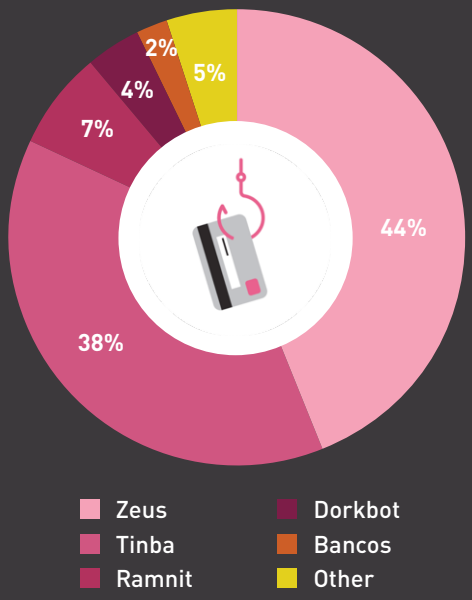


Figure 3: Most Prevalent Banking Malware in the Americas

TOP MOBILE MALWARE (AMERICAS)

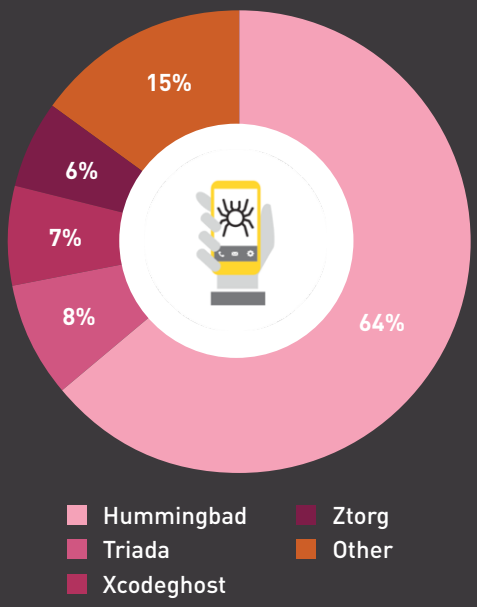


Figure 4: Most Prevalent Mobile Malware in the Americas

TOP TARGETED MALWARE WITH REGIONAL COMPARISON (AMERICAS)

The graph below displays the malware families with the highest presence in the Americas compared to the other regions, along with the spread of the family between the three regions.

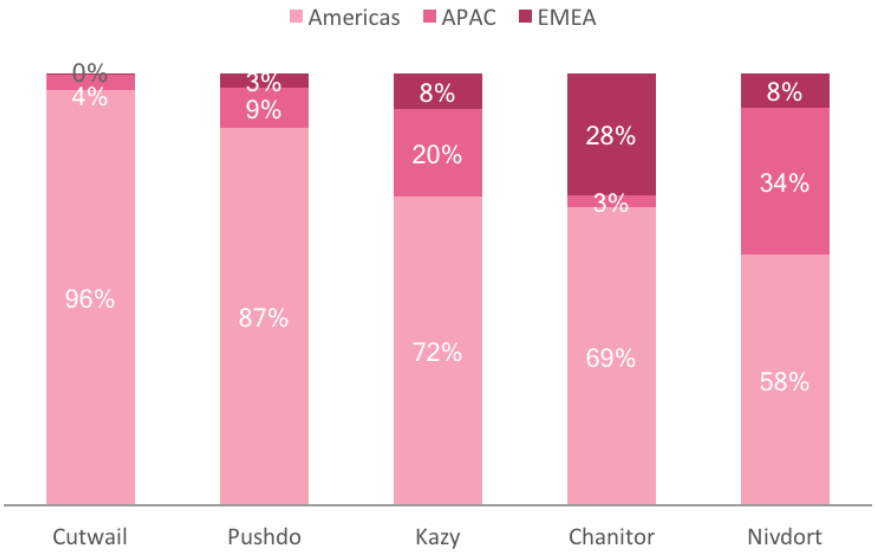


Figure 5: Top Targeted Malware in the Americas with regional comparison

REGIONAL SUMMARY—EMEA (EUROPE, THE MIDDLE EAST AND AFRICA)

MAJOR CYBER BREACHES

- **July 7, 2016:** Netia, Poland's second largest telecom operator, suffered a breach in its servers caused by a hacker named Pravy Sektor, who is associated with the far-right Ukrainian nationalist political party. The hacker published 14GB of data from the servers, including over 300,000 records of customer names, home addresses and IP addresses. In addition, over 600,000 unique email addresses from various domains were published, as well as sales transactions, device and product offers.

- **August 14, 2016:** Sage, a large software company based in the United Kingdom which provides business software for accounting and payroll services, suffered a data breach that could affect hundreds of companies throughout Europe. Though it is yet unclear which information was revealed, Sage holds data on their clients' addresses, National Insurance Numbers, bank accounts and other financial information.

- **October 26, 2016:** Danish firm Nets announced it suffered a breach which compromised up to 100,000 credit cards. Local banks advised the clients affected by this breach to replace their cards.

- **December 6, 2016:** ThyssenKrupp, a German industrial conglomerate which is one of the largest steel manufacturers globally, admitted it was a victim of industrial espionage. Sensitive trade secrets were stolen. The breach, which was discovered in April, is suspected to have originated from Southeast-Asia.

TOP MALWARE FAMILIES (EMEA)

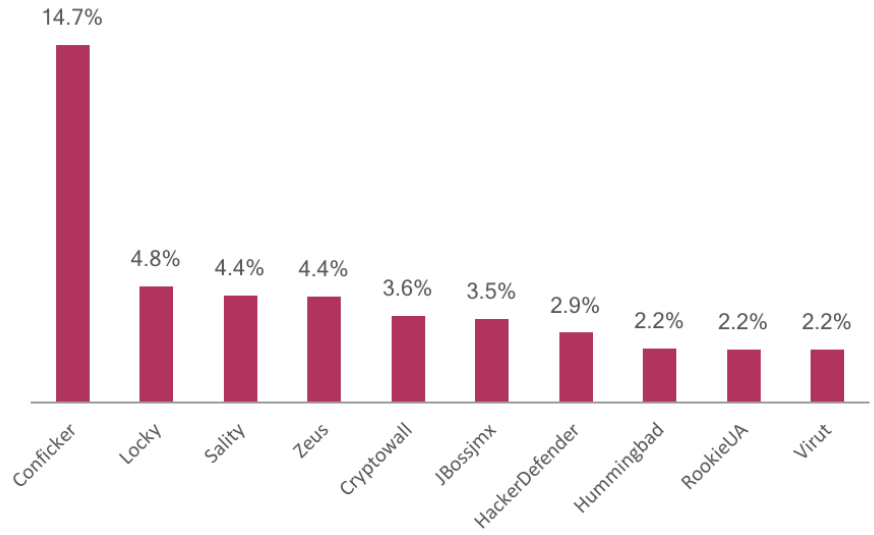
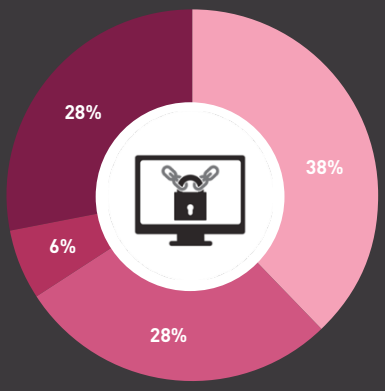


Figure 6: Most Prevalent Malware in EMEA

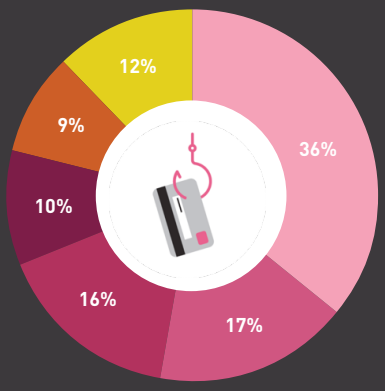
TOP RANSOMWARE (EMEA)



Locky
Cerber
Cryptowall
Other

Figure 7: Most Prevalent Ransomware in EMEA

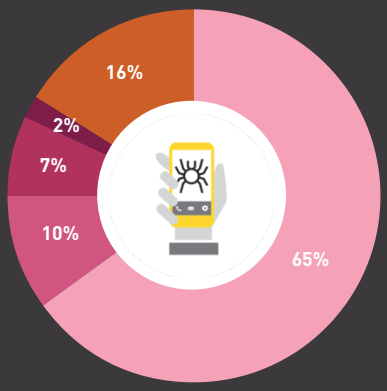
TOP BANKING MALWARE (EMEA)



Zeus
Bancos
Ramnit
Dorkbot
Tinba
Other

Figure 8: Most Prevalent Banking Malware in EMEA

TOP MOBILE MALWARE (EMEA)



Hummingbad
Xcodeghost
Triada
Other
Ztorg

Figure 9: Most Prevalent Mobile Malware in EMEA

TOP TARGETED MALWARE WITH REGIONAL COMPARISON (EMEA)

The graph below displays the malware families that have the highest presence in EMEA compared to the other regions, along with the spread of the family between the three regions.

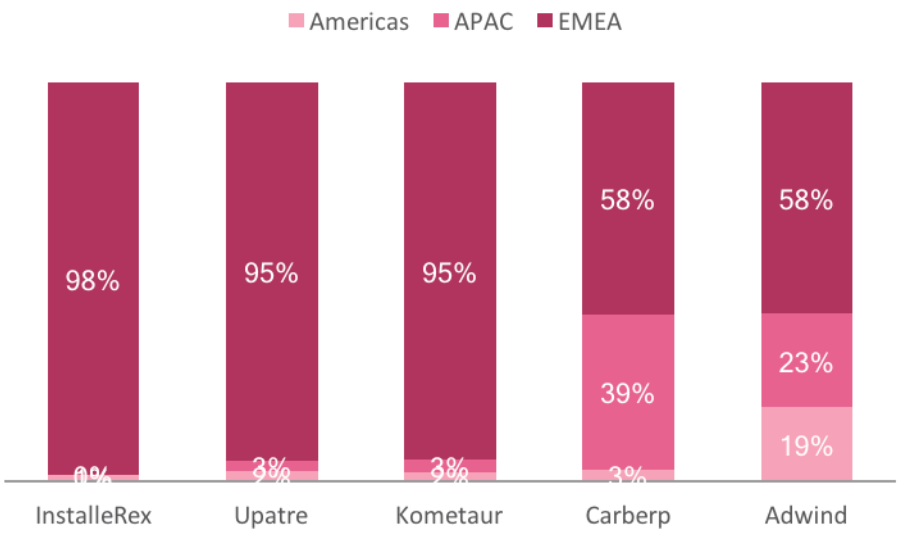


Figure 10: Top Targeted Malware in EMEA with regional comparison

REGIONAL SUMMARY—APAC (ASIA-PACIFIC)

MAJOR CYBER BREACHES

- **July 28, 2016:** Over 10 million customer records of Interpark Corp., a leading South Korean online shopping site, were stolen, including names, addresses, and phone numbers. The hacker breached the site in May, and two months later demanded a ransom of three billion South Korean Wons ($2.664M) in BitCoins to prevent the data from being published. Officials in South Korea attributed the attack to hackers from North Korea.
- **October 20, 2016:** Banks in India asked customers to replace debit card PINs, or in some cases block access to them, due to suspicions that over 3 million card details may have been disclosed in a security breach.
- **December 5, 2016:** Health Solutions, one of the biggest diagnostic laboratories in India, suffered a data breach that allowed the attackers access to over 35,000 personal medical records.
- **December 8, 2016:** Kagoya, a major hosting service provider in Japan, suffered a data breach in which 20,000 credit card details were stolen.

TOP MALWARE FAMILIES (APAC)

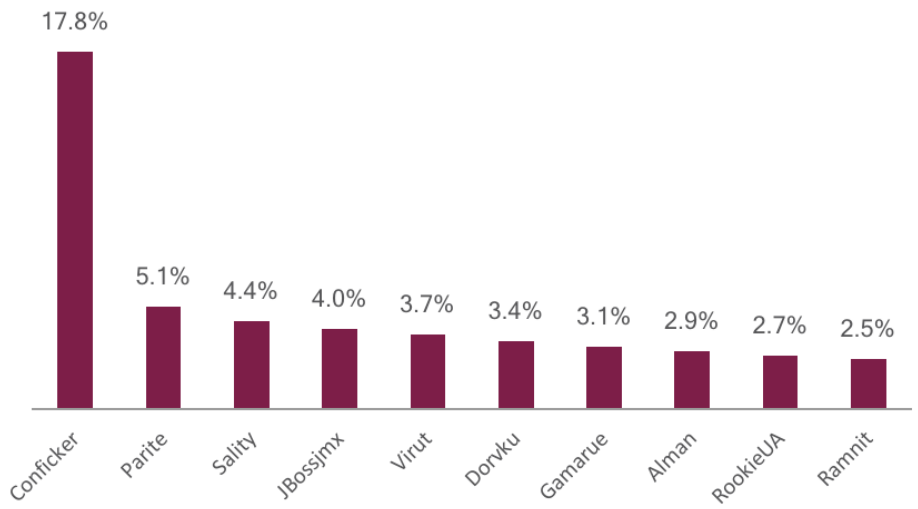


Figure 11: Most Prevalent Malware in APAC

TOP RANSOMWARE (APAC)

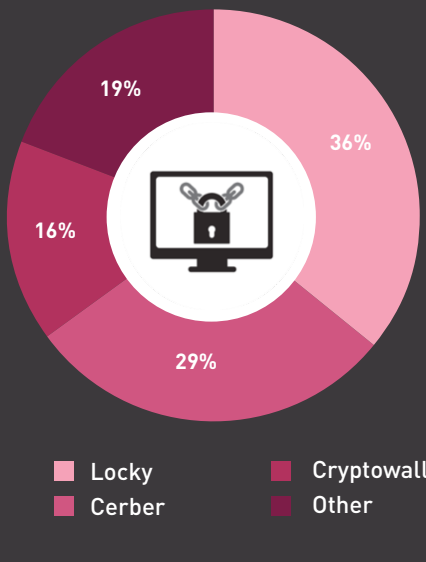


Figure 12: Most Prevalent Ransomware in APAC

TOP BANKING MALWARE (APAC)

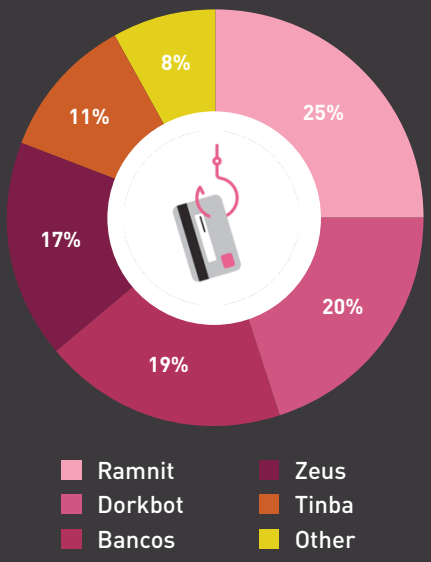


Figure 13: Most Prevalent Banking Malware in APAC

TOP MOBILE MALWARE (APAC)

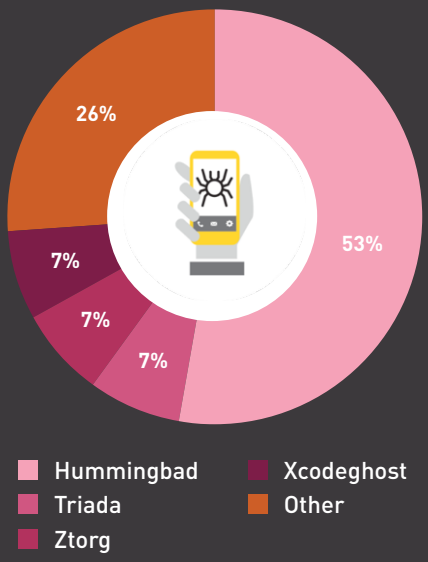


Figure 14: Most Prevalent Mobile Malware in APAC

TOP TARGETED MALWARE WITH REGIONAL COMPARISON (APAC)

The graph below displays the malware families that have the highest presence in APAC compared to the other regions, along with the spread of the family between the three regions.

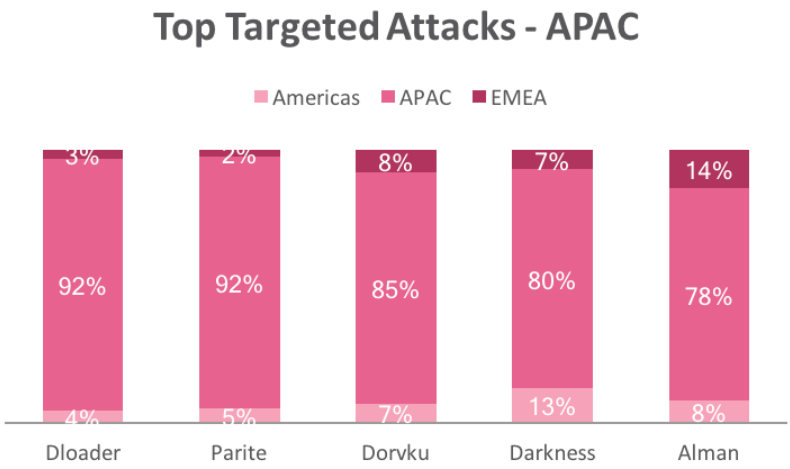


Figure 15: Top Targeted Malware in APAC with regional comparison

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.

Check Point®
SOFTWARE TECHNOLOGIES LTD.

