H1 2016 GLOBAL AND REGIONAL TRENDS OF THE 'MOST WANTED' MALWARE

Check Point
SOFTWARE TECHNOLOGIES LTD.

TABLE OF CONTENTS

H1 2016 GLOBAL AND REGIONAL TRENDS OF THE 'MOST WANTED' MALWARE

INTRODUCTION

The malware world continues to develop rapidly and dynamically. New malware, with increasingly sophisticated abilities, appears on a daily basis, as the cat and mouse game between attackers and defenders persists. To provide organizations with the best level of protection, security experts must stay conversant about the ever-changing threat landscape. The Check Point H1 2016 Global and Regional Trends of the 'Most Wanted' Malware report provides you with a comprehensive overview of the malware landscape in the top categories – ransomware, banking and mobile – based on threat intelligence data drawn from the ThreatCloud World Cyber Threat Map between January and June of 2016.

GLOBAL TRENDS

RANSOMWARE: THE DAWN OF A NEW ERA

Without a doubt, 2016 will go down as a prime year for ransomware. Ransomware has consistently been in the news for the past several months, and for a good reason, as attacks have increased in quantity, variety, efficiency, and sophistication. Barraging users and organizations of all sizes, criminals are now creating new and revamped ransomware using every possible type of attack vector. For more information about the ransomware epidemic, download our whitepaper, Ransomware: Attacks, Trends, and Response.

TURMOIL IN THE EXPLOIT KIT LANDSCAPE

Attackers use exploit kits to spread malware. These kits, which have an alarming success rate, leverage vulnerabilities in the users' web browsers or operating system to install malware without the user's consent or knowledge. As we have seen in the case of the Nuclear Exploit Kit, this can be an extremely profitable business for developers who rent their kit to attackers worldwide. Interestingly, there has been a shift in the exploit kit arena since the beginning of 2016. We have witnessed the decline of two of the largest exploit kits in the wild, Angler and Nuclear, and the rise of Neutrino and Rig Exploit Kits, as seen in the recent Cerber campaign.

THE RISE OF MOBILE BOTNETS

In 2016, a new form of malware appeared in the mobile world – botnets. A botnet is a group of devices (PCs, laptops, or mobile phones) controlled by hackers without the owner's knowledge. The larger the botnet, the greater its capabilities. The botnets we detected, such as Viking Horde and DressCode, even managed to infiltrate Google Play and target hundreds of thousands of users. So far, mobile botnets have been used mainly to generate fraudulent traffic and ad clicks. However, they can be leveraged to achieve disruptive goals, such as DDoS attacks which can have a devastating effect on organizations of all sizes.

GLOBAL MALWARE STATISTICS

The following statistics are based on data drawn from the ThreatCloud World Cyber Threat Map between January and June of 2016. The percentage of each malware family represents its portion of all the recognized malware attacks on organizations worldwide.

TOP MALWARE FAMILIES

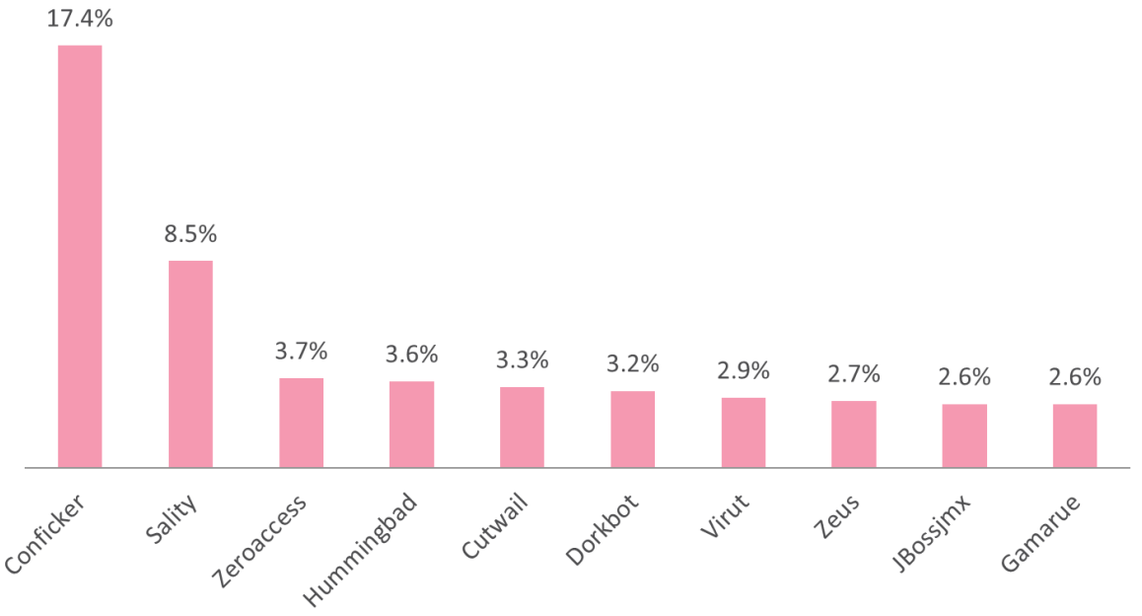

Figure 1 – Most Prevalent Malware Globally

TOP RANSOMWARE

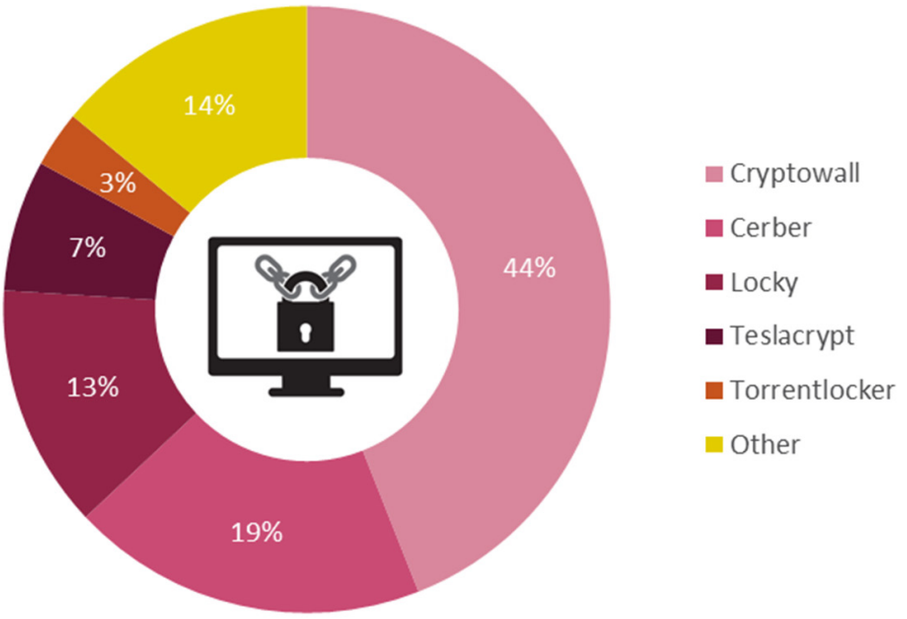

Figure 2 – Most Prevalent Ransomware Globally

TOP BANKING MALWARE

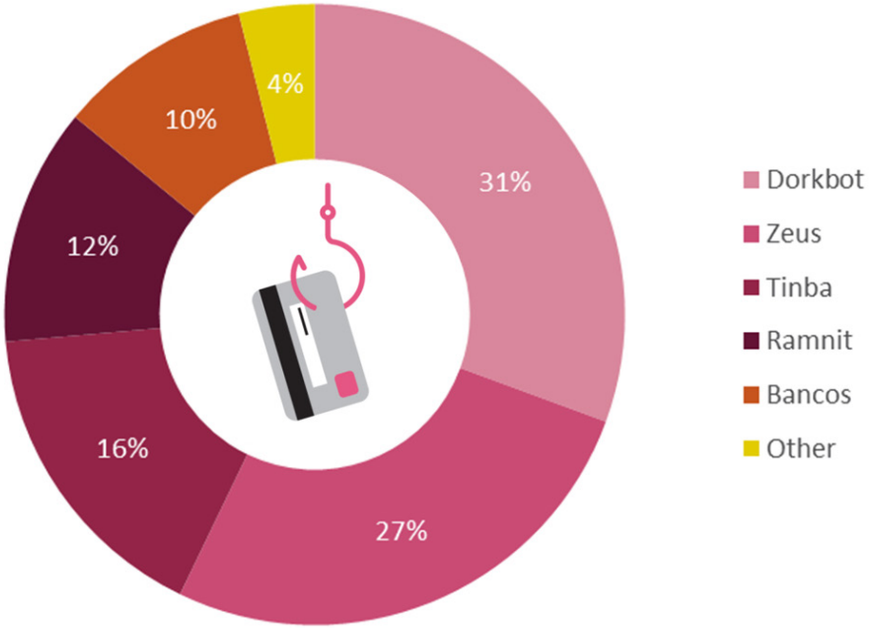

Figure 3 – Most Prevalent Banking Malware Globally

TOP MOBILE MALWARE

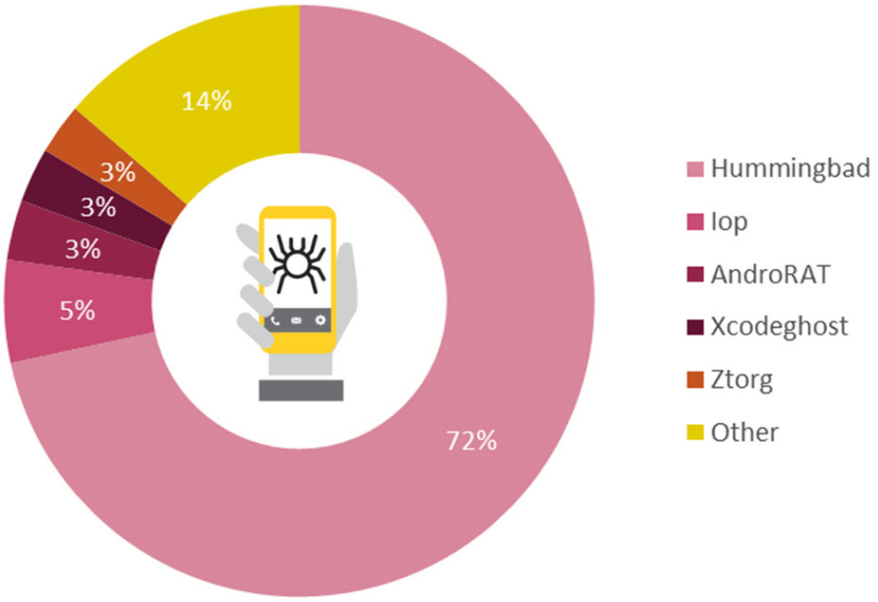

Figure 4 – Most Prevalent Mobile Malware Globally

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, as derived from the ThreatCloud World Cyber Threat Map, which tracks how and where cyberattacks are taking place worldwide in real-time.

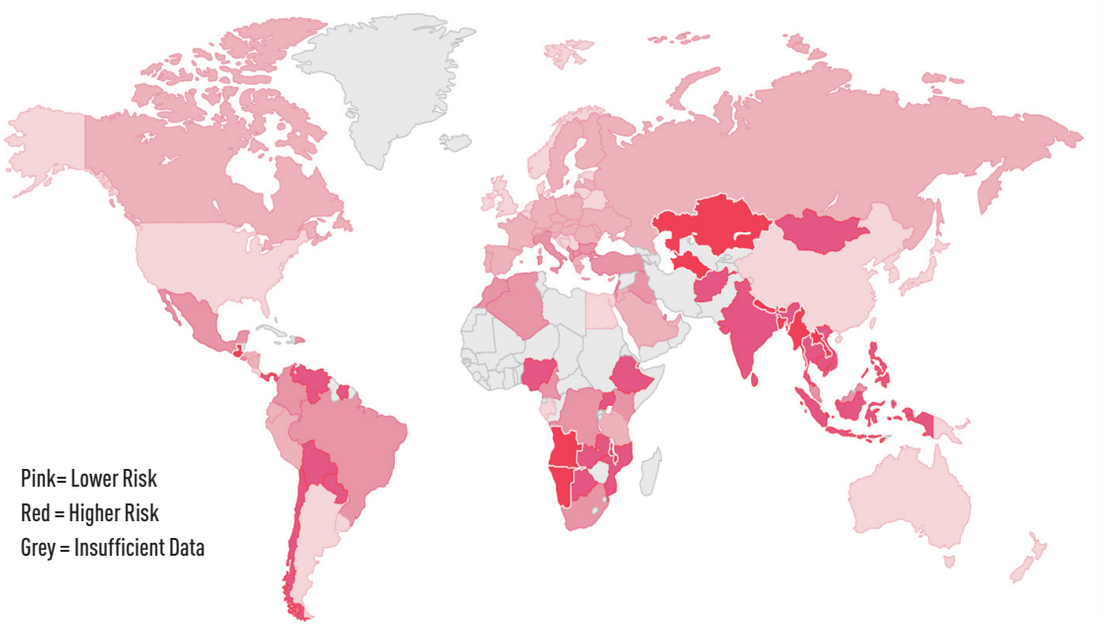

Figure 5 – World Cyber Threat Index Map

TOP MALICIOUS FILETYPES

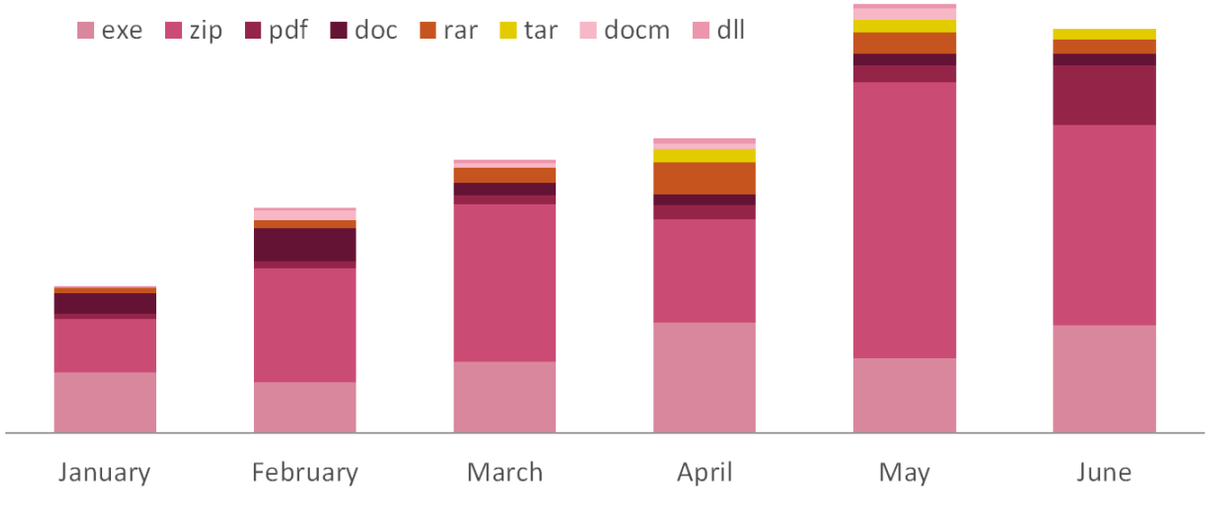

Figure 6 – Top File Types Seen in Malicious Context Globally

CYBER ATTACK CATEGORIES BY REGION

The infographic below shows the spread of three of the main malware categories detailed in this report – Banking, Mobile and Ransomware – across the different regions on the world. The regions include the Americas; Europe, Middle East and Africa (EMEA); and Asia and Pacific (APAC).

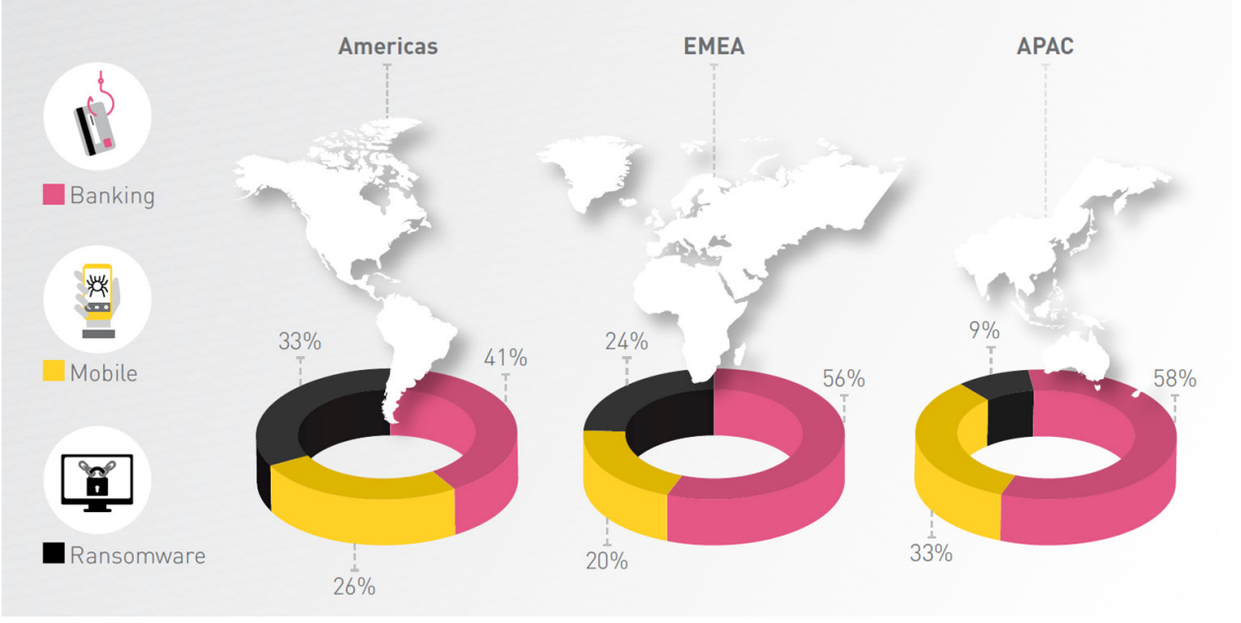

Figure 7 – Attack Categories by Region

REGIONAL SUMMARY – AMERICAS

MAJOR CYBER BREACHES

- **January 27, 2016:** The Wendy's fast food chain suffered a Point-of-Sale credit card breach that affected 1,025 locations. Similar to the Target breach of 2014, the attack was thought to originate with a third-party service provider.
- **February 5, 2016:** The Hollywood Presbyterian Medical Center in Los Angeles was targeted by ransomware which encrypted the entire system, including patient records and other sensitive information. The attackers demanded and received 40 Bitcoins – around $17,000 at the time of the payment. This attack was a major milestone in the ransomware epidemic, which has continued to grow ever since.
- **April 3, 2016:** The Panama Papers Breach where an estimated 11.5 million documents and 2.6 terabytes of private data from the Panama-based law firm Mossack Fonseca, which is involved in off-shore tax havens, was published in an act referred to as the world's largest data leakage event. Recent research estimates that the law firm's website was hacked through a vulnerable version of Revolution Slider, a WordPress Plugin used by the website.

TOP MALWARE FAMILIES

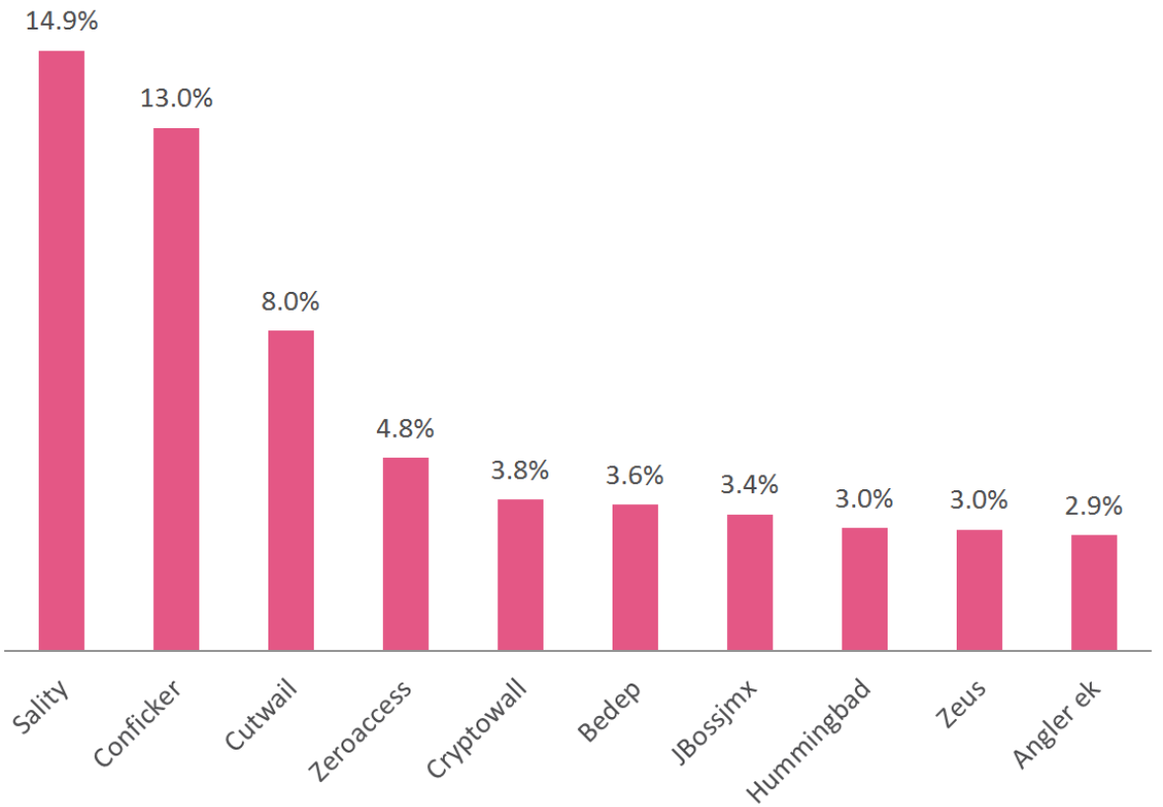

Figure 8 – Most Prevalent Malware in the Americas

TOP RANSOMWARE

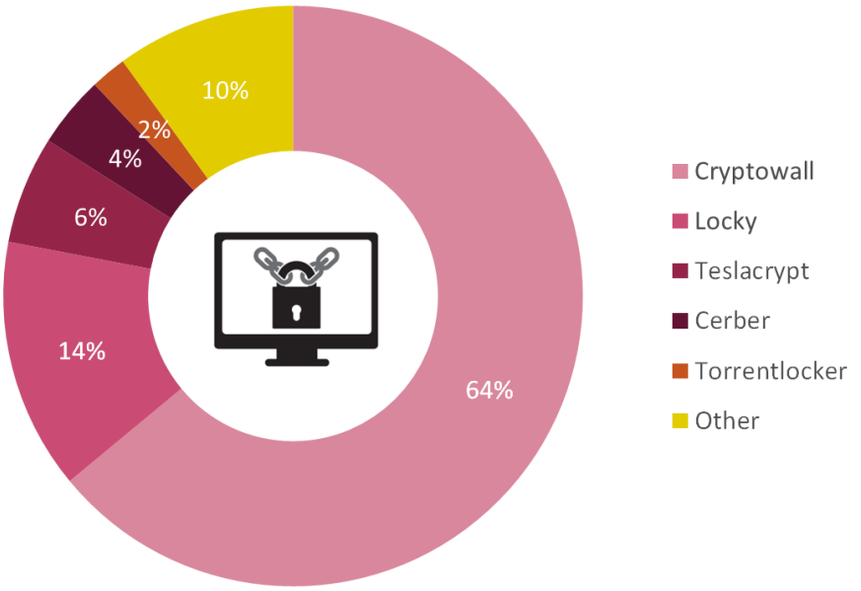

Figure 9 – Most Prevalent Ransomware in the Americas

TOP BANKING MALWARE

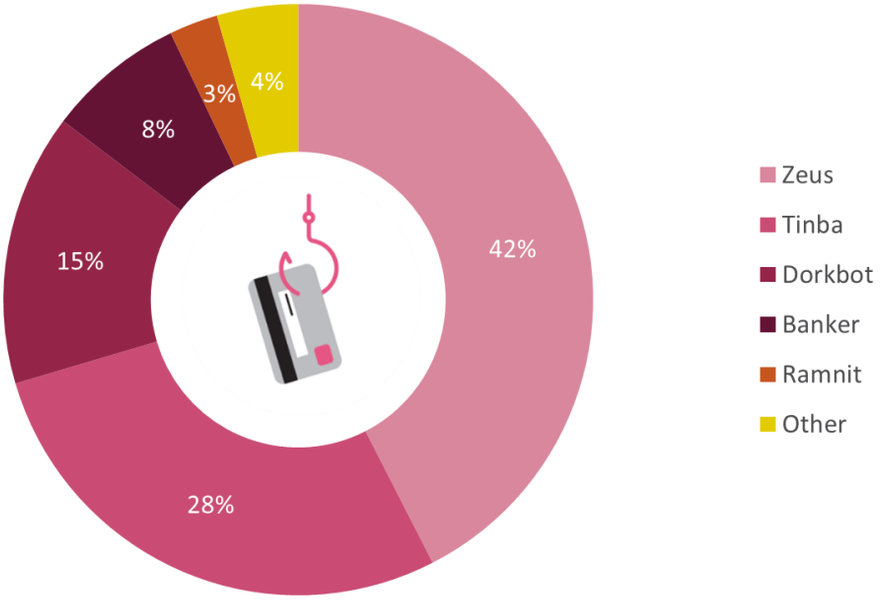

Figure 10 – Most Prevalent Banking Malware in the Americas

TOP MOBILE MALWARE

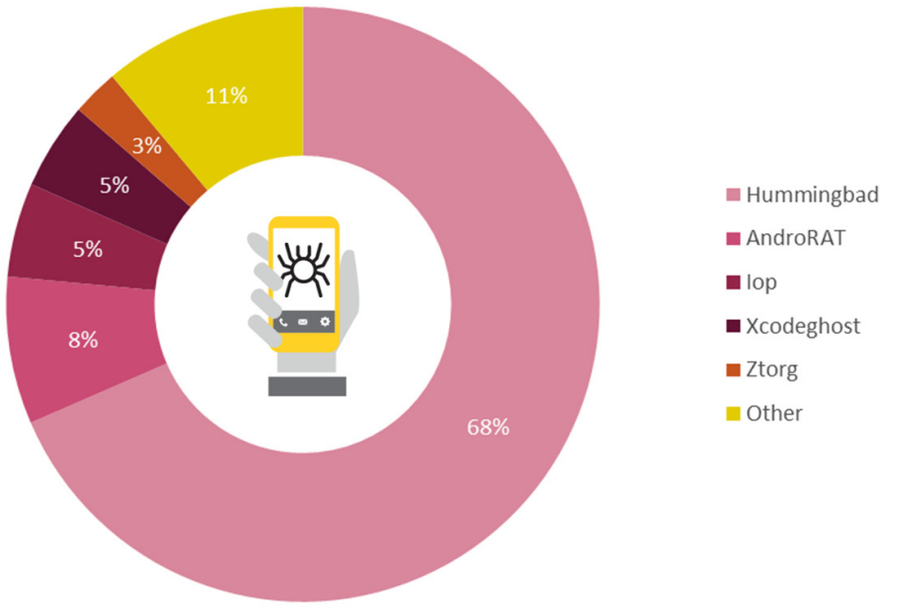

Figure 11 – Most Prevalent Mobile Malware in the Americas

TOP MALWARE WITH REGIONAL COMPARISON

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

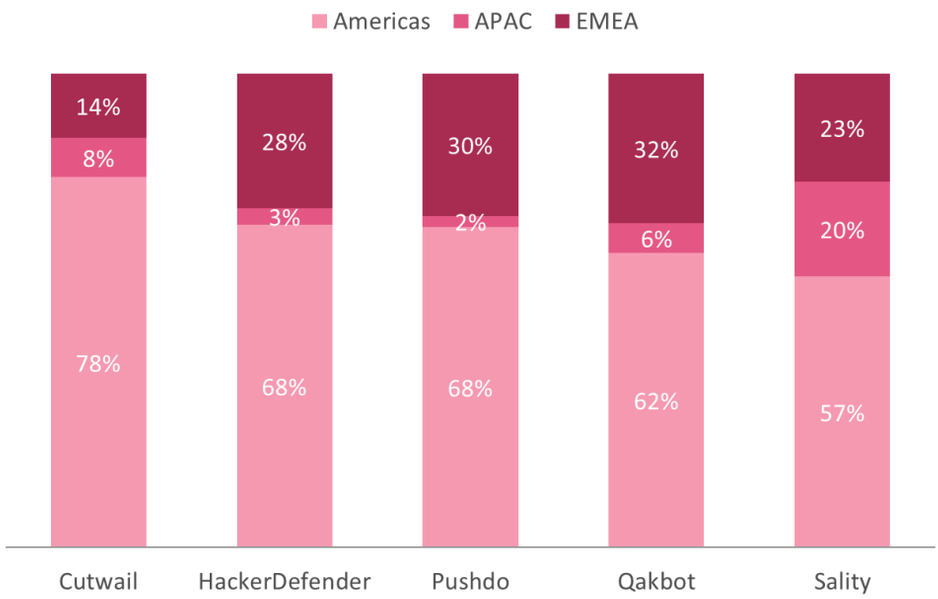

Figure 12 – Top Malware in the Americas with Regional Comparison

REGIONAL SUMMARY – EMEA

MAJOR CYBER BREACHES

- **December 23, 2015:** The Ivano-Frankivsk region in western Ukraine experienced a power outage due to what was later identified as a cyberattack. The attack targeted the power company Prykarpattyaoblenergo and affected at least 80,000 people, approximately half of the region's population. This was the first proven cyberattack to successfully damage an electric power grid.
- **April 28, 2016:** As part of its OpAfrica operation against child abuse, child labor, and corruption in African countries, the Anonymous hacktivist group breached Kenya's Ministry of Foreign Affairs server. The group stole 1TB of data and published portions of it on the Dark Web, including classified documents and email conversations regarding security issues and international trade agreements.
- **May 5, 2016:** A young Russian hacker dubbed "The Collector" obtained credentials for major email services, mainly the Russian service mail.ru, totaling 1.17 billion records. The Collector has shown he is willing to sell the data for a small price of less than $1 per record.

TOP MALWARE FAMILIES

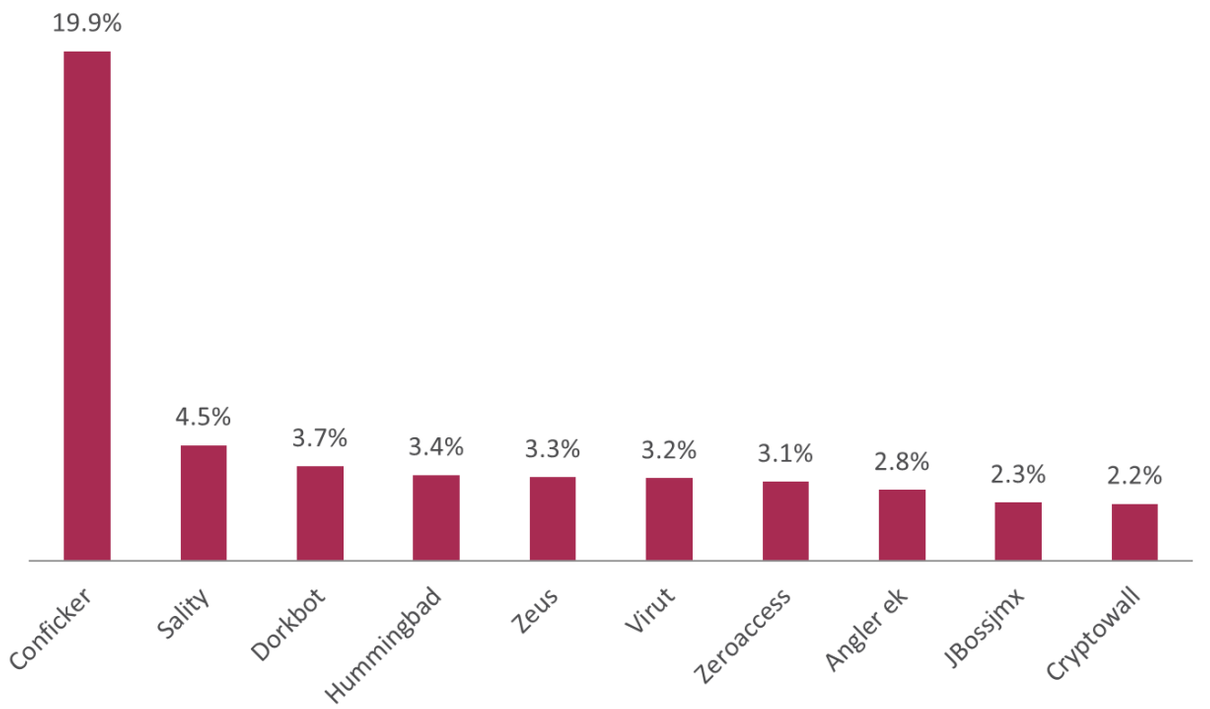

Figure 13 – Most Prevalent Malware in EMEA

TOP RANSOMWARE

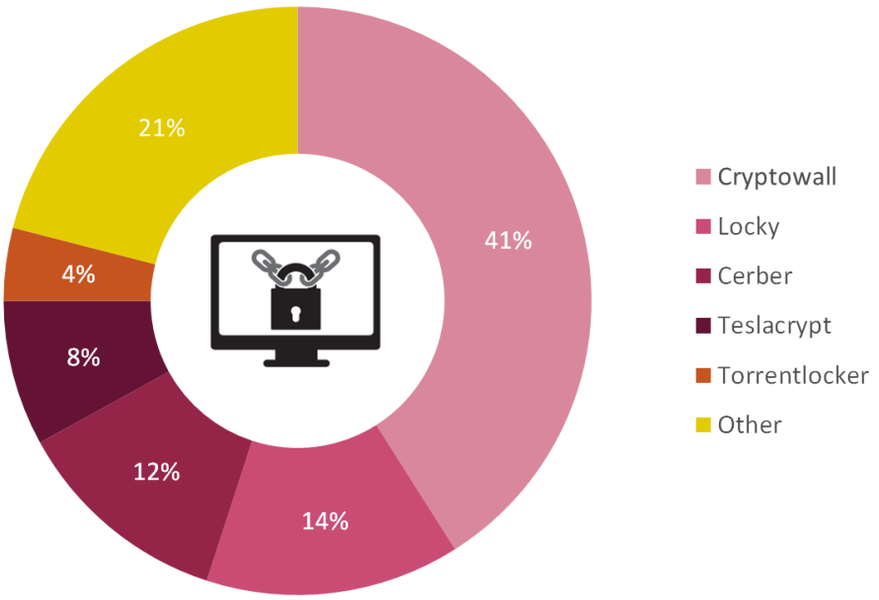

Figure 14 – Most Prevalent Ransomware in EMEA

TOP BANKING MALWARE

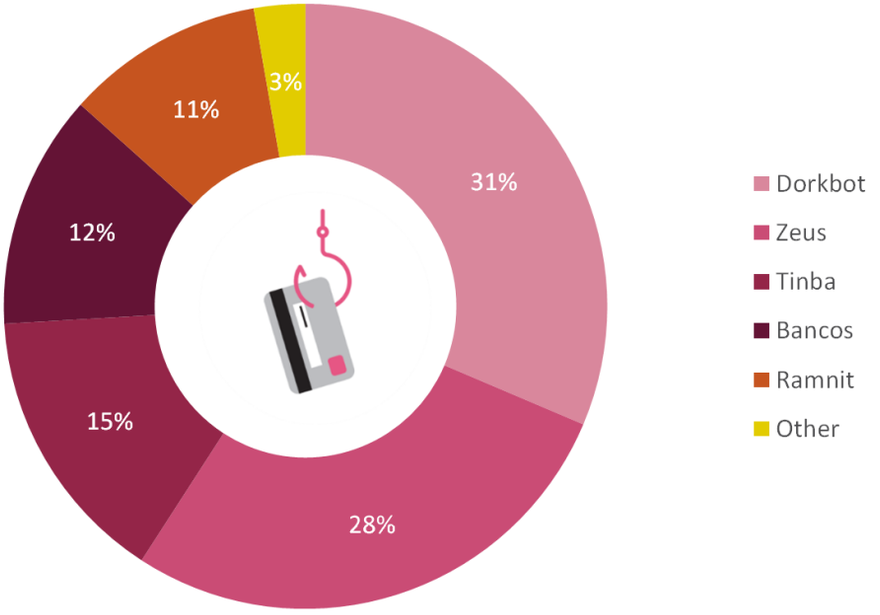

Figure 15 – Most Prevalent Banking Malware in EMEA

TOP MOBILE MALWARE

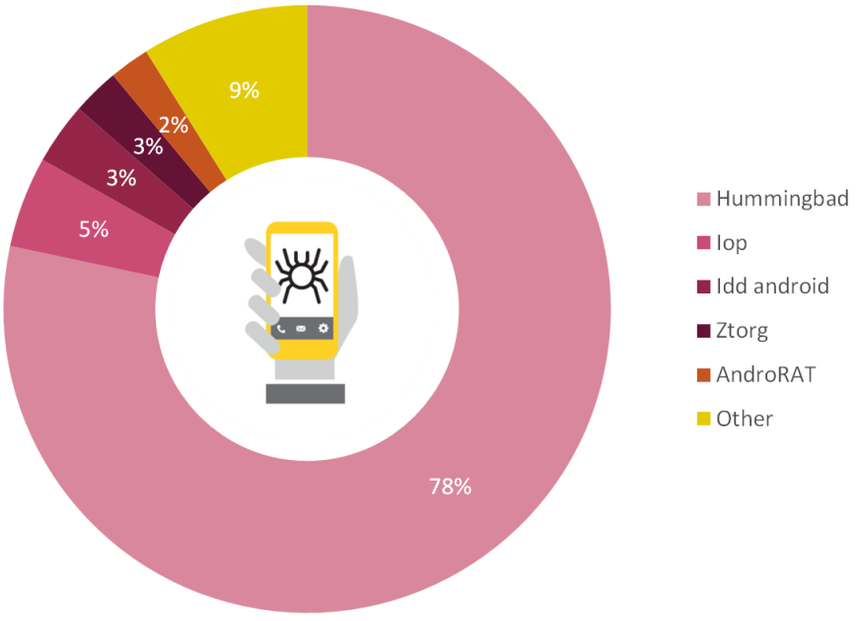

Figure 16 – Most Prevalent Mobile Malware in EMEA

TOP MALWARE WITH REGIONAL COMPARISON

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.

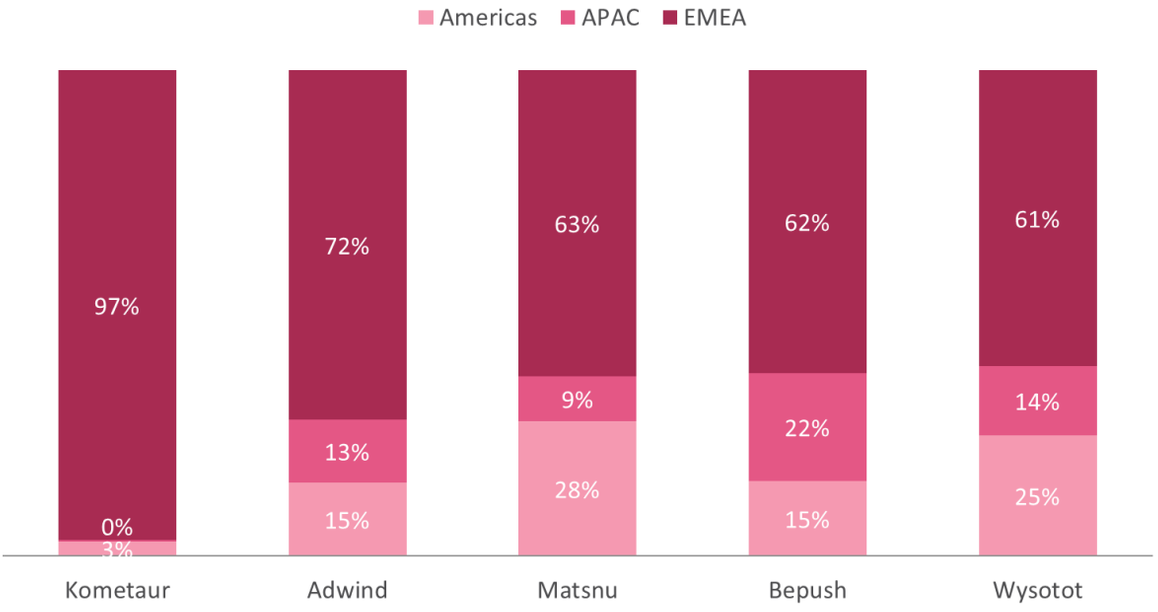

Figure 17 – Top Malware in EMEA with Regional Comparison

REGIONAL SUMMARY – APAC

MAJOR CYBER BREACHES

- **February 2016:** Cybercriminals successfully stole $81 million from Bangladesh's central bank. An investigation showed that the attack succeeded due to the lack of a firewall and other security measures on the bank's network. SWIFT, the operator of the global secure messaging system which controls financial transactions, confirmed there have since been several cyberattacks against commercial banks.
- **March 27, 2016:** A massive data breach caused a leak of the entire database of the Philippines' Commission on Elections (COMELEC), containing details of 55 million voters. The leak was comprised of personally identifiable information (PII), including passport information and fingerprint data.
- **May 20, 2016:** The Sydney Morning Herald and The Age Digital Editions, two Australian-based news websites belonging to Fairfax Media, were hacked. As a result, over 13,000 email subscriber accounts were leaked online.

TOP MALWARE FAMILIES

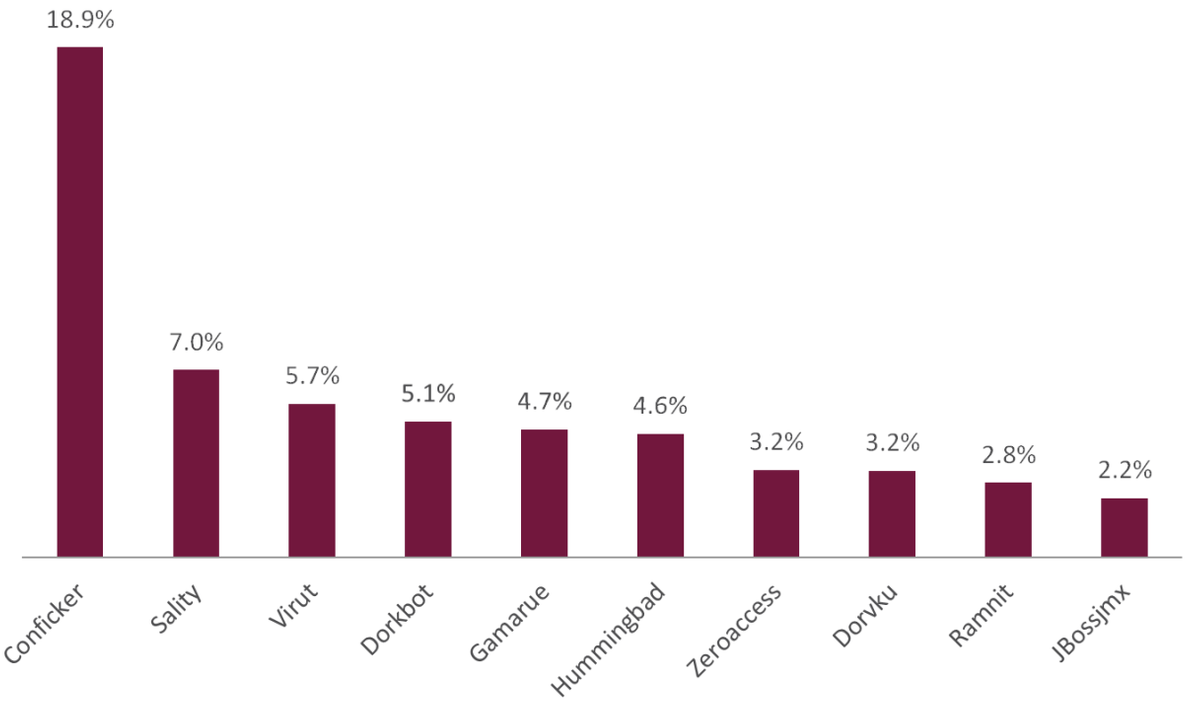

Figure 18 – Most Prevalent Malware in APAC

TOP RANSOMWARE

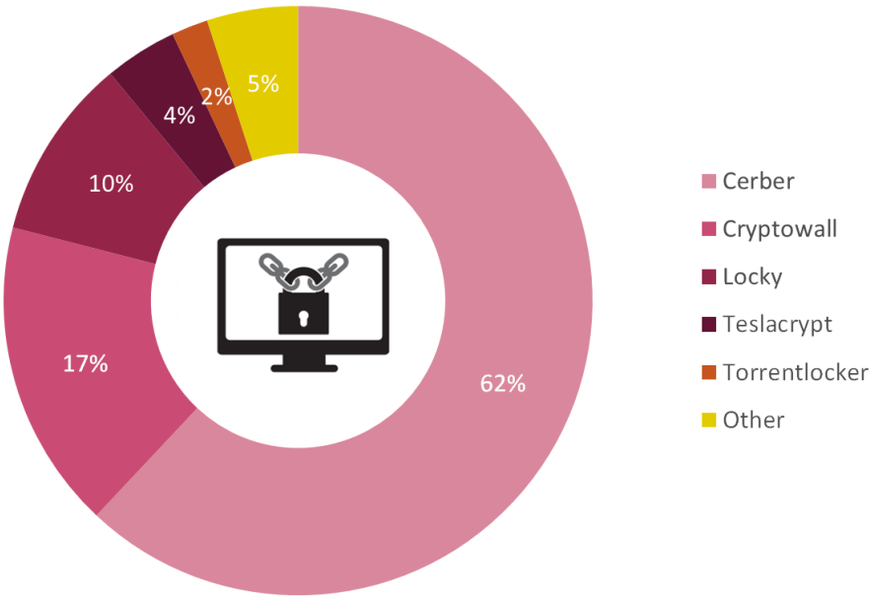

Figure 19 – Most Prevalent Ransomware in APAC

TOP BANKING MALWARE

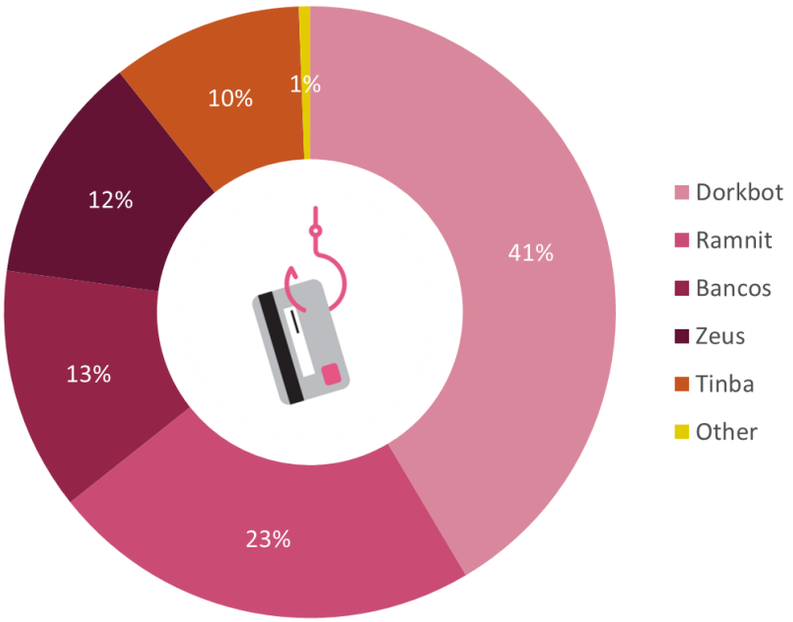

Figure 20 – Most Prevalent Banking Malware in APAC

TOP MOBILE MALWARE

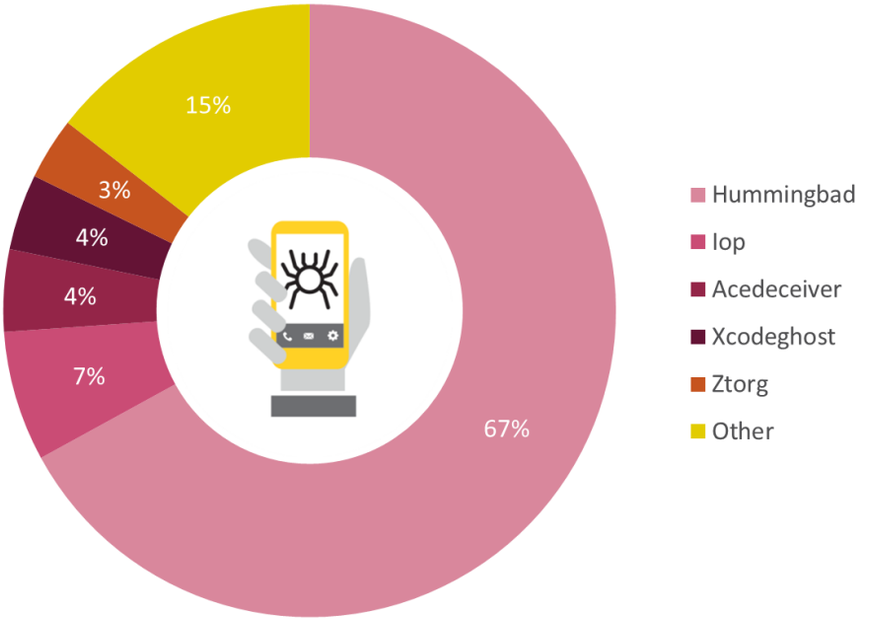

Figure 21 – Most Prevalent Mobile Malware in APAC

TOP MALWARE WITH REGIONAL COMPARISON

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.

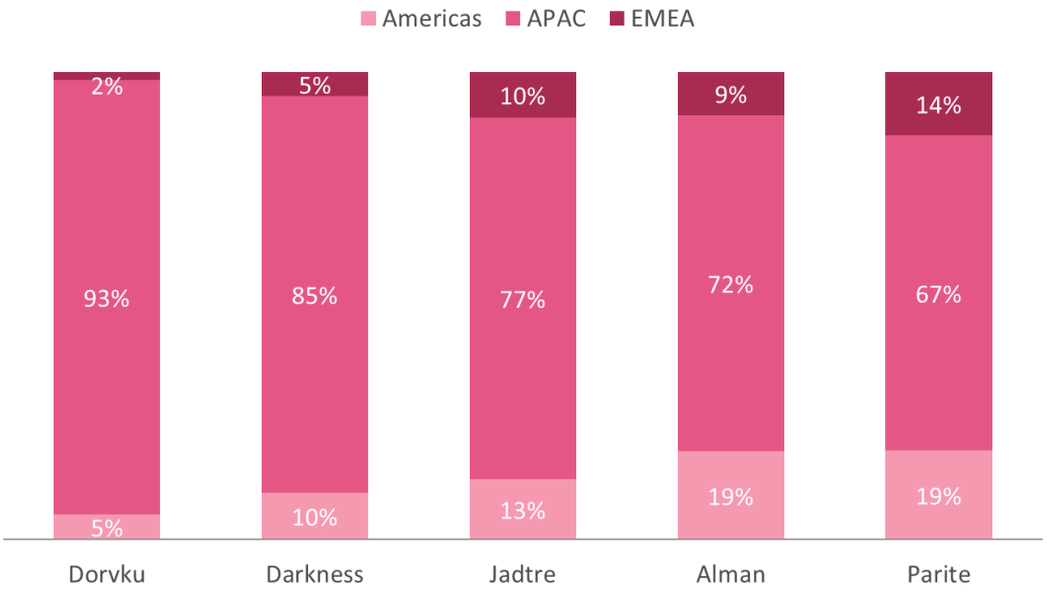

Figure 22 – Top Malware in APAC with Regional Comparison

CONCLUSION

The first half of 2016 demonstrates the nature of today's cyber threat landscape. Many old malware threats remain prominent, while at the same time newcomers arrive and take the world by storm. On top of that, malware demonstrates a long tail distribution with a small number of families responsible for a major part of the attacks, while thousands of other malware families are rarely seen. Lastly, we see that most cyber threats are global and cross-regional, with the top threats appearing in all three regions. Even seemingly region-targeted malware families have a significant presence in other regions.

The statistics in this report are based on data drawn from the ThreatCloud World Cyber Threat Map between January and June 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.

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: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com