REGIONAL ADVANCED THREAT REPORT

EUROPE, MIDDLE EAST AND AFRICA — 2H2015

FireEye

SPECIAL REPORT

CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

This report provides you with unique insights into Europe, Middle East and Africa's (EMEA's) threat landscape for the second half of 2015. For years, over 95% of businesses have unknowingly hosted compromised PCs within their corporate networks, and that has not changed. During our assessment, we identified all types of threat actors compromising our customers' networks, including suspected nation-state-backed actors looking to conduct cyber espionage, cybercriminals and hacktivists looking to make a statement.

This Regional Advanced Threat Report for EMEA provides an overview of the advanced targeted threats against computer networks that FireEye discovered during the second half of 2015. It is a follow-up to the Advanced Threat Report for EMEA 1H2015.

Turkey, Spain, Israel, Luxembourg and Germany are the countries most targeted with advanced attacks.

Motivated by many objectives, threat actors' capabilities are evolving to be able to steal personal data and business strategies, gain a competitive advantage or degrade operational reliability.

This report summarizes 2H2015 data gleaned from the FireEye Dynamic Threat Intelligence (DTI) cloud. The threat landscape has undergone dramatic changes between the first and second half of 2015. Threat actors are adapting their tools, techniques and procedures (TTPs) and shifting their target industries and countries.

- Turkey, Spain, Israel, Luxembourg and Germany are the countries most targeted with advanced attacks.
- Government, financial services, energy, telecommunications and aerospace were the most targeted verticals in EMEA.
- The use of macros is a privileged method for cyber criminals to compromise their victims in order to steal information or install ransomware.

Disclaimer: This report only covers computer network attacks that targeted FireEye (anonymized) customers, sharing their metrics with FireEye – it is by no means an authoritative source for all APT attacks in EMEA and elsewhere in the world. In this dataset, we take reasonable precautions to filter out "test" network traffic as well as traffic indicative of manual intelligence sharing among our customer base within various closed security communities. We realize that some popular targeted threat actors' TTPs (tools, techniques and procedures) can be reused and repurposed by both cyber-criminals and nation-state threat actors alike. To address this issue, we employ conservative filters and crosschecks to reduce the likelihood of misidentification.

Definitions

Advanced Targeted Threat: one or more sets of cyber tools, techniques, and procedures (TTPs) that are employed directly or indirectly by a nation-state or a sophisticated, professional criminal organization for cyber espionage or the long-term subversion of specific adversary networks. Qualifying characteristics may include regular human interaction (that is, not a scripted, automated attack), and the ability to extract sensitive information over time and at will.

Callback: an unauthorized communication between a compromised victim computer and its attacker's command-and-control (CnC) infrastructure.

Remote Access Tool (RAT): software that allows a computer user (for the purposes of this report, an attacker) to control a remote system as though he or she had physical access to that system. RATs offer numerous attractive features such as screen capture, file exfiltration, etc. Typically, an attacker installs the RAT on a target system via some other means such as spear phishing or exploiting a zero-day vulnerability, and the RAT then attempts to keep its existence hidden from the legitimate owner of the system.

Threat Actor: the nation-state or criminal organization believed to be behind an APT. This could be a military unit, an intelligence agency, a contractor organization or a non-state actor with indirect state sponsorship.

Tools, Techniques, and Procedures (TTPs): the characteristics specific to a threat actor in the cyber domain, usually referring to specific malware. Advanced targeted threats normally employ multiple TTPs, and multiple advanced targeted threats can also use the same TTPs. This dynamic frequently complicates cyber defense analysis.

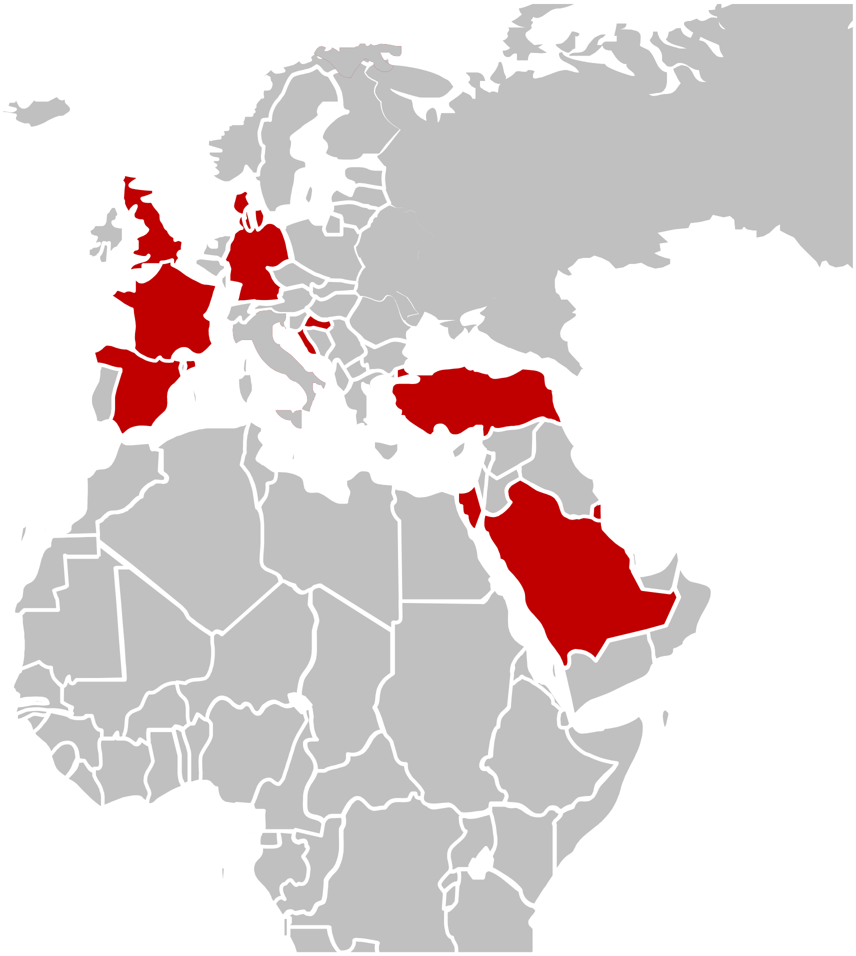
Vertical: one of 20 distinct industry categories: aerospace, chemicals, construction, e-commerce, education, energy, entertainment, finance, government, healthcare, high-tech, insurance, legal, manufacturing, other, retail, services, telecommunications, transportation, and wholesalers.

Advanced Targeted Threat Detection

Country Analysis

Turkey, Spain, Israel, Luxembourg and Germany are the most targeted countries in EMEA.

FIGURE 1. ADVANCED TARGETED THREATS DETECTED BY COUNTRY



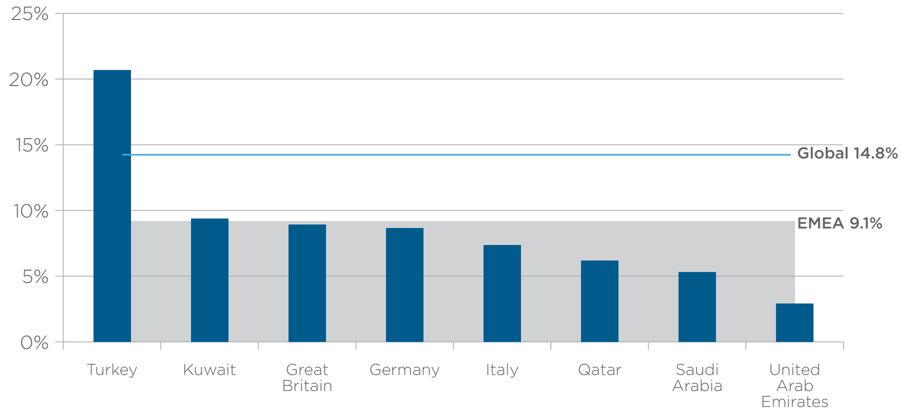
Percentage of all advanced targeted threats malware detected in EMEA, by country:

1. Turkey (27%)
2. Spain (10%)
3. Israel (9%)
4. Belgium/Luxembourg (9%)
5. Germany (9%)
6. Great Britain (9%)
7. Saudi Arabia (4%)
8. France (3%)
9. Kuwait (3%)
10. Croatia (3%)

Turkey continued to be in the crosshairs for targeted attacks in the second half of 2015. Persistent regional tensions and conflicts in neighboring states were a likely driver of nation-state threat activity. The country's high level of internet connectivity also makes it ripe for opportunistic and more advanced cyber crime operations.

The following figure shows the exposure rate in EMEA by country. The exposure rate enables a broad-level comparison of how advanced targeted threats affect the different EMEA countries.

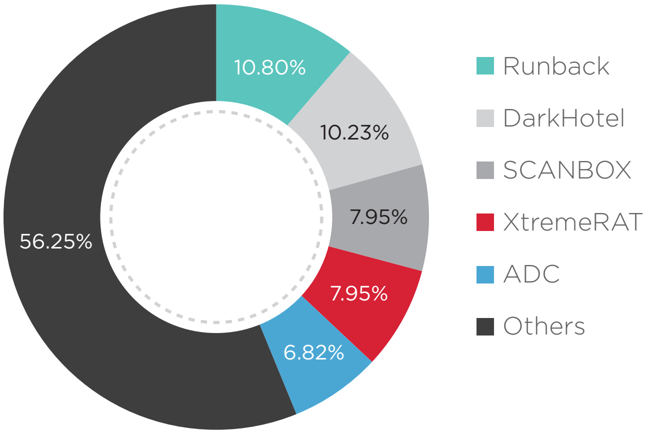
FIGURE 2. ADVANCED TARGETED THREAT EXPOSURE BY EMEA COUNTRY



Targeted Malware Families

The following graph represents the top targeted malware families identified during this report. The malware families are important to track from a risk perspective, as each family presents different capabilities and threats. They are tied to TTPs that enable an understanding of how the attackers operate. This becomes significant when we can link specific malware use to threat actors or threat types, which aids in attribution and enables people to respond more effectively.

FIGURE 3. TOP TARGETED MALWARE FAMILIES DETECTED IN EMEA



The top targeted malware families are Runback, DarkHotel and SCANBOX.

Runback

Runback, also known as Gholee[1] is a set of malware families associated with "Operation Protective Edge." Artifacts in this malware family show a possible connection to Iranian threat actors. These threat actors use social engineering tactics to persuade the target to open the document and enable macros so that the malicious macro can execute.

We believe Runback may be connected to Iranian threat actors. Those threat actors use social engineering to persuade the victims to open Ms Office documents that include a malicious macro. The top industries targeted by Runback are: high-tech, education and government.

DarkHotel

Threat actors behind the DarkHotel[2] malware family have been active since at least 2008. These threat actors use hotel wireless networks to compromise the laptops of senior executives' staying at that hotel. The actors have employed zero-day exploits, code-signing techniques and a kernel-mode keystroke logger. The sophisticated and targeted nature of the intrusions has led some to conclude DarkHotel is a nation-state campaign. The top industries targeted by these DarkHotel threat actors are: education, financial services and high-tech. **The use of shared infrastructure as a vehicle to compromise users will continue to increase as employees and senior executives become and more mobile.**

[1] http://securityaffairs.co/wordpress/28170/cyber-crime/gholee-malware.html
[2] https://securelist.com/blog/research/66779/the-darkhotel-apt/

SCANBOX

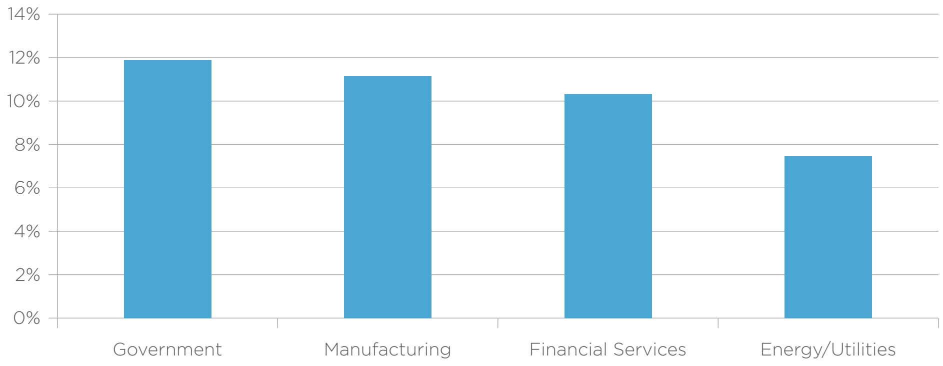
The SCANBOX malware is a profiling tool. The SCANBOX framework is sometimes installed on the victim's machine, along with several plug-ins. It installs a JavaScript-based keylogger to record all keystrokes within the compromised website to collect user names and passwords, not just system information. The threat actors likely only profile their victims for user and machine information. We continuously monitor the use of legitimate analytical tools, which we see threat actors using more frequently to collect data on their victims, which can lead to targeted attacks against individuals or industries. In November 2015, we released a report on WITCHCOVEN[3], a similar method of data collection that uses legitimate tools.

Vertical Analysis

Government, financial services, energy/utilities, telecommunications and aerospace and defense contractor were the most targeted verticals in the second half of 2015.

Figure 4 below shows which verticals in EMEA were most exposed to advanced targeted threats in the second half of 2015.

FIGURE 4. VERTICALS IN EMEA MOST EXPOSED TO ADVANCED TARGETED THREATS IN 2H2015.



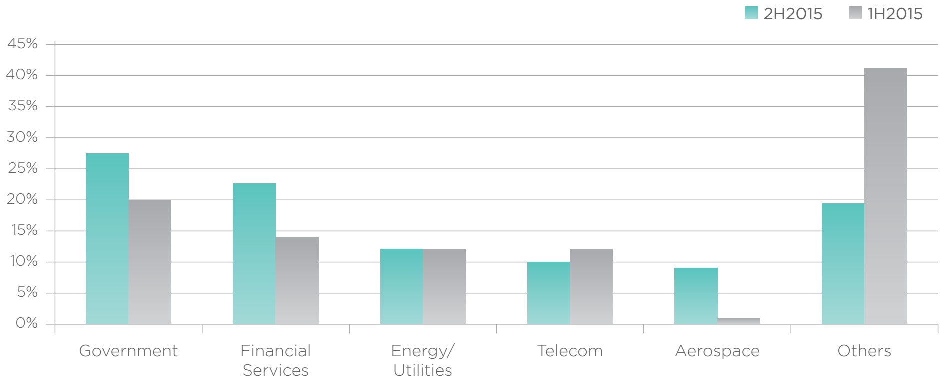
These verticals are the top industries in EMEA, accounting for most of the region's GDP.

Changes in the threat landscape in 2015

The following figures compare trends by industry between the first and second half of 2015. We looked at two different trends: all malware (inclusive of crimeware), and advanced targeted threats.

[3] https://www.fireeye.com/blog/threat-research/2015/11/pinpointing_targets.html

FIGURE 5. ALL MALWARE DETECTION BY INDUSTRY IN EMEA

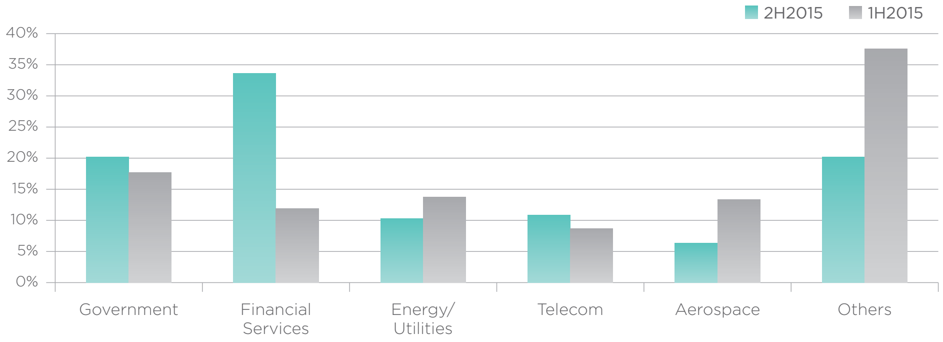


Government, financial services and aerospace saw a 70% increase in number of unique detections between the first and second half of 2015.

This clearly highlights the very fast pace at which cyber threat actors, including cyber crime groups and nation-states, are moving. **We have observed a surge in the number of unique detections for the financial services industry, suggesting that cyber criminals view the region as ripe for their nefarious activities.**

The following figure focuses on data related to the detection of advanced targeted threats in EMEA industries.

FIGURE 6. ADVANCED TARGETED THREATS DETECTED IN EMEA, BY INDUSTRY



The financial services sector saw a 300% increase in the number of advanced targeted threats detected. This data suggests that threat actors gained access to confidential information for financial gain or to understand changes happening with the European financial situation.

The rapid changes in the trends between the first and second half of 2015 suggest that what is happening in the world is reflected in cyber crime.

The financial services sector saw a 300% increase in the number of advanced targeted threats detected.

Cyber Crime Analysis

Dominant Exploit Kits

Exploit kits play a vital part in delivering malicious payloads to victims. There are many variants and frameworks of exploit kits, but in the second half of 2015, we saw one dominant kit — the Angler Exploit Kit — which delivered a variety of malicious payloads, including ransomware and information-stealing Trojans such as Dridex. The increase of Angler Exploit Kit detections in the second half of 2105 was 674%, suggesting that it is by far the most used and preferred exploit kit in the delivery of malicious payloads.

Increased Use of Macros

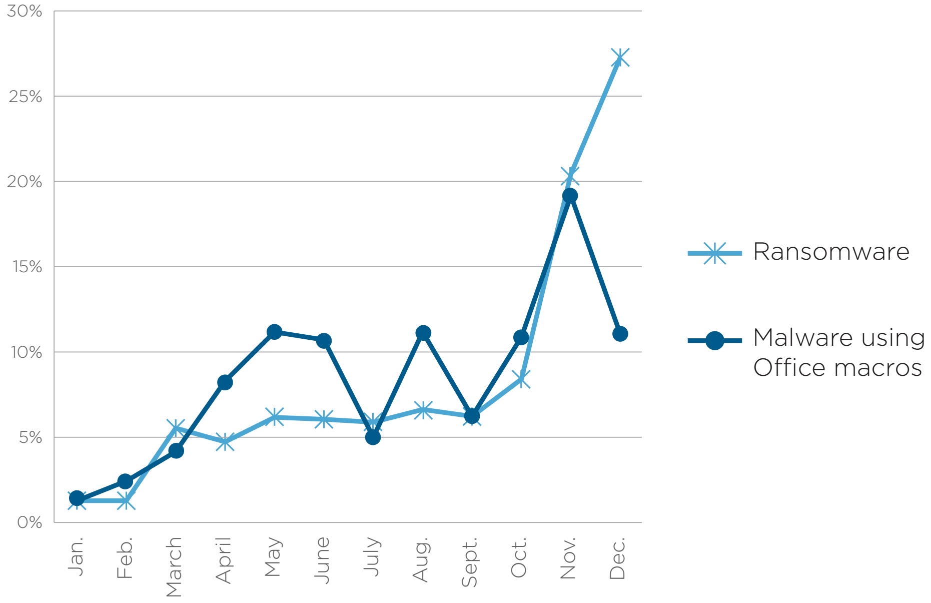
Using macros in MS Office applications is still very popular. We have seen a 10-fold increase in attacks where macros have been used to deliver malicious payloads such as ransomware, information-stealing Trojans or backdoors. Companies that allow execution of macros are vulnerable to these types of attacks, which are utilizing legitimate Windows processes to execute and download malicious payloads, making detection much more complex and difficult.

In the Regional Advanced Threat Report: Europe, Middle East and Africa 1H2015, we specifically followed the evolution of Cridex/Dridex campaigns that huse macros extensively. This blog also discusses how cyber criminals use macros.

Expanded Use of Ransomware

The following graph shows how the use of macros and ransomware evolved in 2015.

FIGURE 7. MONTHLY TREND FOR MACRO-BASED MALWARE AND RANSOMWARE IN 2015.

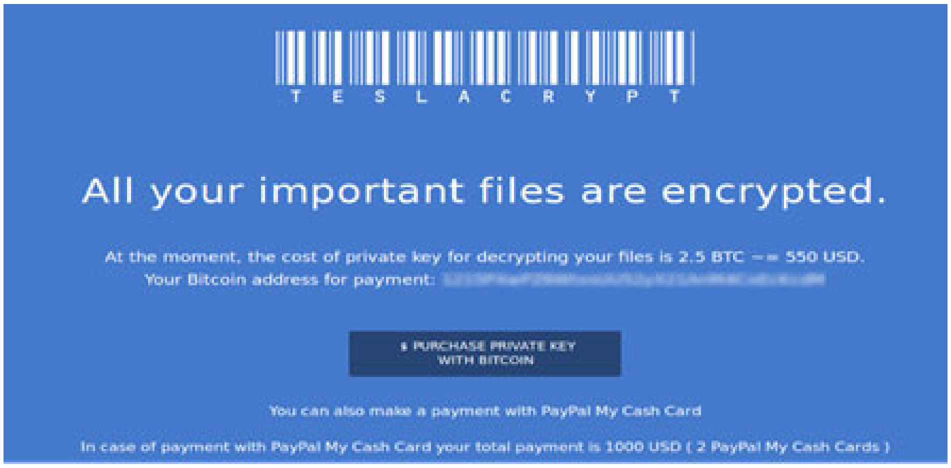


In the second half of 2015, we observed a very large increase in ransomware attacks in EMEA. The use of ransomware is evolving rapidly. The constant development of new families with new anti-detection or encryption methods suggests that there are enough victims paying at a constant rate to keep motivating cyber criminals to constantly improve their malicious code.

In the second half of 2015, we observed a very large increase in ransomware attacks in EMEA.

An example of a ransomware page experienced by victims in EMEA is presented below.

FIGURE 8. RANSOMWARE PAGE EXAMPLE



TESLACRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment: [redacted]

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

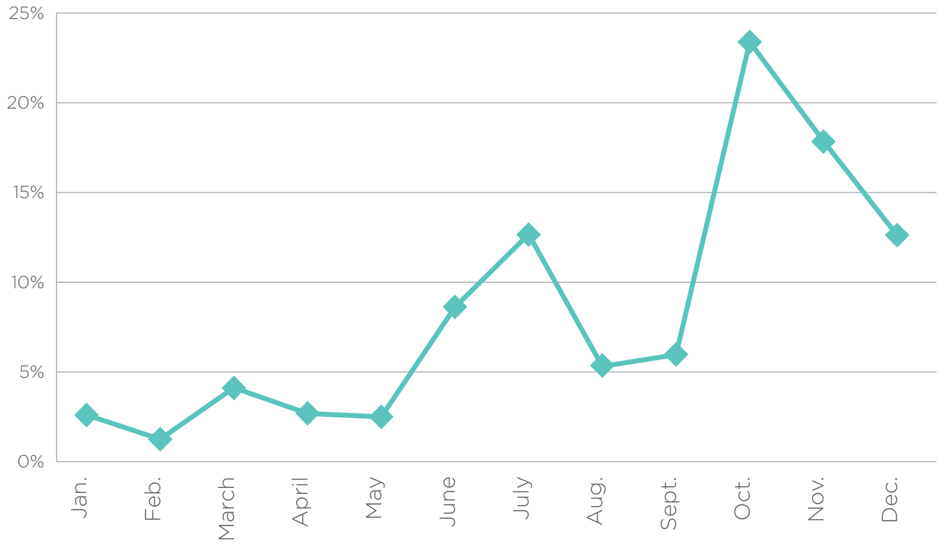
The common forms of ransomware include:

- **Cryptolocker** – The most prolific of all the file-encrypting ransomware variants, Cryptolocker was first spotted in 2013. It was spread by the “Gameover Zeus” botnet and demands a $300 to $500 ransom.
- **Cryptowall** – Cryptowall emerged a few months after Cryptolocker in 2013 and mimicked its predecessor’s behavior. The perpetrators brought in over $1 million in a six-month period in 2014.
- **CTB-Locker** – First seen in 2014, CTB-Locker was the first file-encrypting ransomware that used the Tor anonymity network. It was available for sale to cyber criminals on underground forums.
- **TorLocker** – First deployed in 2014 against Japanese users, TorLocker was marketed and sold on the now defunct Evolution marketplace.
- **Kryptovor** – This malware steals files from compromised computers but also has a ransomware component that was first seen in 2014. Kryptovor primarily targets businesses in Russia.
- **Teslacrypt** – This malware emerged in February 2015. The cyber criminals behind this operation demand that victims pay between 0.7 and 2.5 bitcoins, which is about $150 to $500, or $1,000 in PayPal My Cash cards to decrypt their files.

Point of Sale (POS) Malware

We observed a three-fold increase in POS malware, as shown in the following graph.

FIGURE 9. POS MALWARE TRENDS FOR 2015



Since late 1990s, POS terminals have undergone a lot of development and in many cases moved from being a disconnected cash register that prints customer receipts, to a fully connected device that offers many functions requiring an active connection to the company infrastructure.

This development has provided the opportunity for financially motivated threat actors to design and develop malware specifically designed to compromise POS terminals and steal sensitive information entered into these systems, typically when a customer's credit or debit card is swiped through the terminal.

The malware that targets POS terminals uses memory or RAM scrapers, which allow the attacker to obtain all data available on a credit or debit card. When a credit or debit card is swiped in a POS terminal, the information is typically stored in plain text in the POS terminal´s RAM. The data contains the card number, user name, address, security codes or other information.

The data stolen from POS terminals may be resold or duplicated into new cards and used for purchases or ATM withdrawals.

Conclusion and Recommendations

The evidence highlighted in this report demonstrates that geopolitical, financial and economic changes happening in EMEA are mirrored in the cyber security world. The changes to the threat landscape between the first and second half of 2015 were considerable, demonstrating once more the speed at which threat actors operate.

We also observed an increased volume of potential attacks by nation-state-sponsored threat actors from the Middle East. The use of shared infrastructure such as wireless networks in hotels and also user profiling are changing the TTPs used by threat actors.

We predict that threats are going to become even more disruptive as attackers modify or destroy targeted data. We already saw evidence of this with the Sandworm group targeting the Ukrainian power plant and the Kiev International Airport.

We recommend the following:

- Assume your organization is a target and that your existing security controls can be bypassed.
- Establish a cyber risk framework that enables the business with board-level sponsorship.
- Acquire threat intelligence to augment and enrich detections from your sensors.
- Establish an incident response or incident management service in a security operations center (SOC) or computer incident response team (CIRT) to be able to detect and react to an advanced targeted threat quickly.
- Bring in the right technology to identify these new threats.
- Establish a clear response plan with board and management sponsorship and involvement in the event of a breach.

Credit to Yogi Chandiramani and Jens Monrad for developing and analyzing the data for this report.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com