Trend Micro 1H Security Roundup Report Showcases Evolution of Ransomware and BEC Scams

DALLAS--(BUSINESS WIRE)--As Trend Micro predicted, 2016 has proven to be a year of online extortion through various malicious attack methods. Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in security software and solutions, today published its security roundup report, "The Reign of Ransomware," which analyzes the trends in attacks and vulnerabilities seen throughout the first half of this year. The report provides extensive data surrounding the rise and impact of attacks, such as a 172 percent increase in ransomware and $3 billion in losses due to business email compromise (BEC) scams so far in 2016, as well as nearly 500 vulnerabilities in a variety of products.

"Ransomware is capable of crippling organizations who face it, and the cybercriminals spearheading these attacks are creatively evolving on a continuous basis to keep enterprises guessing," said Raimund Genes, chief technology officer for Trend Micro. "It has dominated the threat landscape so far in 2016, causing immense losses to businesses across multiple industries. Enterprises must adopt multi-layered security solutions to optimally combat these threats that could attempt to penetrate corporate networks at any time."

The following report findings highlight trends from the first half of 2016:

- **Ransomware dominates the threat landscape:** The occurrence of ransomware families nearly doubled, with an increase of 172 percent, in the first half of 2016 compared to 2015, further establishing ransomware as a prevalent and pervasive threat. Variants are designed to attack all levels of the network.
- **BEC scams spread across the world:** The FBI listed more than 22,000 victims in 2016 to date, with more than US $3 billion in losses. Trend Micro has found that the U.S. is the most targeted country for these attacks.
- **New vulnerabilities and ransomware strengthen attacks through exploit kits:** The declining use of Angler EK can be attributed to the arrest of 50 cybercriminals. As such, other EKs have taken its place, including new players like Rig and Sundown.
- **Rising number of vulnerabilities found in Adobe Flash and IoT platforms:** Trend Micro and the ZDI reported several significant browser and kernel vulnerabilities, which were identified during the Pwn2Own competition
- **Incidents of data breaches plague various industries:** Both private and public sectors fell victim to data breaches in the first half of the year, including Myspace and Verizon, several hospitals and government entities.
- **Updates in Point-of-Sale malware give rise to new attacks:** FastPoS came equipped with efficient credit card theft capabilities, affecting small to medium businesses across the globe, including some in the U.S. FighterPoS also made its debut, showing worm-like qualities that allowed cross-network infection.
- **Exploits revive old vulnerabilities in their attacks:** Shellshock exploits increased in the first half of the year, despite available patches, with thousands of new exploits seen each month. This is another example of the benefit to virtual patching, which provides faster protection to enterprise networks when vulnerabilities surface.
- **Cybercriminals defy the odds with banking Trojans:** Trojans like QAKBOT increased their attacks following the arrest of the creators of DYRE. This variant goes after crucial information including banking credentials, browsing habits and other sensitive user data.

In total, 79 new ransomware families were identified in the first six months of the year, which surpasses the total number of new families found in all of 2015. Both new and old variants caused a total of US $209 million in monetary losses to enterprises. Ransomware attacks found in the first half of 2016, like BEC scams, originated from emails 58 percent of the time.

Research shows both growth and evolution in vulnerabilities and exploit kits (EKs), as well. Angler was found to steadily decrease in use, while other EKs, like Neutrino, filled the void. New vulnerabilities and ransomware were added to keep EKs up to date and effective. Unpatched software continues to provide additional opportunities for attackers to infect networks via EKs.

In the first half of 2016, Trend Micro discovered 473 vulnerabilities in a variety of products, with 28 coming from Adobe Flash and 108 from Advantech's Web Access, demonstrating the full capabilities of the company's research teams.

"While it's unfortunate for us, cybercriminals are resilient and flexible when it comes to altering an attack method each time we find a patch or solution," said Ed Cabrera, chief cybersecurity officer for Trend Micro. "This creates massive problems for enterprises and individuals alike since the threats change as often as solutions are provided. It bodes well for businesses to anticipate being targeted and to prepare accordingly, implementing the latest security solutions, virtual patching and employee education to mitigate risks from all angles."

For the complete report, please visit: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-reign-of-ransomware.

About Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital

information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables users to enjoy their digital lives safely. For more information, visit www.trendmicro.com.

Contact:

Trend Micro Incorporated
Jerrod Resweber, 972-499-6614
publicrelations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NYSE:
TMICY

---

https://newsroom.trendmicro.ca/2016-08-23-Trend-Micro-1H-Security-Roundup-Report-Showcases-Evolution-of-Ransomware-and-BEC-Scams