Trend Micro 2016 Security Roundup Reveals 752 Percent Increase in Ransomware

81 billion cyber threats blocked, an increase of 56 percent

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released its annual security roundup report, "2016 Security Roundup: A Record Year for Enterprise Threats," which proves 2016 was truly the year of online extortion. Cyber threats reached an all-time high in 2016, with ransomware and Business Email Compromise (BEC) scams gaining increased popularity among cybercriminals looking to extort enterprises. A 752 percent increase in new ransomware families ultimately resulted in $1 billion in losses for enterprises worldwide.

Trend Micro and the Zero Day Initiative (ZDI) discovered 765 vulnerabilities in 2016. Of these, 678 were brought to ZDI through their bug bounty program, then ZDI verifies and discloses the issue to the affected vendor. Compared to vulnerabilities discovered by Trend Micro and ZDI in 2015, Apple saw a 145 percent increase in vulnerabilities, while Microsoft bugs decreased by 47 percent. Additionally, the use of new vulnerabilities in exploit kits dropped by 71 percent, which is partially due to the arrest of the threat actors behind Angler that took place in June 2016.

"As threats have diversified and grown in sophistication, cybercriminals have moved on from primarily targeting individuals to focusing on where the money is: enterprises," said Ed Cabrera, chief cybersecurity officer for Trend Micro. "Throughout 2016 we witnessed threat actors extort companies and organizations for the sake of profitability and we don't anticipate this trend slowing down. This research aims to educate enterprises on the threat tactics actively being used to compromise their data, and help companies adopt strategies to stay one step ahead and protect against potential attacks."

In 2016, the Trend Micro Smart Protection Network™ blocked more than 81 billion threats for the entire year, which is a 56 percent increase from 2015. In the second half of 2016, more than 3,000 attacks per second were blocked for customers. During this time, 75 billion of blocked attempts were email based, illustrating that email remains the top entry point for threats.

Report highlights include:

- **Growth of Ransomware –** Throughout the course of 12 months, the number of ransomware families grew from 29 to 247. One leading factor to explain this increase is the profitability of ransomware. Although individuals and organizations are encouraged not to pay the ransom, cybercriminals still managed to rake in roughly $1 billion last year.
- **BEC Scams on the Rise –** Much like ransomware, BEC scams proved to be incredibly lucrative for cybercriminals, resulting in an average of $140,000 in losses for companies around the globe. These scams also highlighted the effectiveness of social engineering techniques for threat actors targeting enterprises.
- **A Variety of Vulnerabilities –** Trend Micro and the Zero Day Initiative (ZDI) discovered a record high number of vulnerabilities in 2016, most of which were found in Adobe Acrobat Reader DC and Advantech's WebAccess. Both applications are widely used throughout enterprise and Supervisory Control and Data Acquisition (SCADA) systems.
- **Angler Exploit's Exit –** Following the arrest of 50 cybercriminals, the once dominant Angler exploit kit slowly faded out of the spotlight until it ceased to exist. While it didn't take long for new exploit kits to burst onto the scene in Angler's absence, by the end of 2016, the amount of vulnerabilities included in exploit kits had decreased by 71 percent.
- **Banking Trojans and ATM Malware –** Cybercriminals have been using ATM malware, skimming cards and banking Trojans for a while now. However, the attacks have diversified in recent years, giving threat actors access to personally identifiable information (PII) and credentials, which can also be used to gain a foothold inside enterprise networks.
- **Mirai's Massive Attack –** In October 2016, attackers took advantage of poorly secured IoT devices to issue a distributed denial-of-service (DDoS) attack that hijacked approximately 100,000 IoT devices and forced websites such as Twitter, Reddit and Spotify to go offline for several hours.
- **Yahoo's History Making Data Breach –** Yahoo experienced the largest data breach in history in August 2013, compromising 1 billion account users' information. However, the incident was not disclosed until three months after reports of a separate data breach in September 2016, which involved 500 million more accounts. These events stirred up the responsible disclosure conversation and the accountability companies have to their customers regarding the security of user data.

For the complete report, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2016-roundup-record-year-enterprise-threats.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity 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 organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

Contact:

Trend Micro Incorporated
Erin Johnson, 972-499-6627
publicrelations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.ca/2017-02-28-Trend-Micro-2016-Security-Roundup-Reveals-752-Percent-Increase-in-Ransomware