Trend Micro Midyear Report Highlights Need for Proactive Security

2017 Midyear Security review demonstrates importance of cybersecurity investments

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released its 2017 Midyear Security Roundup: The Cost of Compromise, detailing the threats from the first half of 2017, which continue to disrupt and challenge IT planning. Businesses are faced with increased ransomware, Business Email Compromise (BEC) scams and Internet of Things (IoT) attacks, and now also contend with the threat of cyberpropaganda.

Trend Micro detected more than 82 million ransomware threats in the first half of the year, along with more than 3,000 BEC attempts, reinforcing the need for security prioritization. Despite the rising percentage of security spending in IT budgets, a recent analyst report by Forrester1 notes that funds are not properly being allocated to address the growing threats facing enterprises today.

“Enterprises need to prioritize funds for effective security upfront, as the cost of a breach is frequently more than a company’s budget can sustain,” said Max Cheng, chief information officer of Trend Micro. “Major cyberattacks against enterprises globally have continued to be a hot-button topic this year, and this trend is likely to continue through the remainder of 2017. It’s integral to the continued success of organizations to stop thinking of digital security as merely protecting information, but instead as an investment in the company’s future.”

In April and June, the WannaCry and Petya ransomware attacks disrupted thousands of companies across multiple industries world-wide. The global losses from the attack, including the resultant reduction in productivity and cost of damage control, could amount to as much as US$4 billion. In addition, BEC scams raised the total of global losses to US$5.3 billion during the first half of 2017, according to the Federal Bureau of Investigation (FBI).

As predicted, January through June experienced a rise in IoT attacks, as well as the spread of cyberpropaganda. In collaboration with Politecnico di Milano (POLIMI), Trend Micro showed it is possible for industrial robots to be compromised, that could amount to massive financial damage and productivity loss, proving that smart factories can ill-afford to dismiss the importance of securing these connected devices. There was also an increased abuse of social media with the rise of cyberpropaganda.

Given the tools available in underground markets, the spread of Fake News, or bad publicity, will cause serious financial ramifications for businesses whose reputation and brand equity is damaged by cyberpropaganda.

Trend Micro XGen™ security provides proactive protection and guidance for companies facing these pressing and growing threats with a cross-generational approach to threat defense. The threats that have manifested throughout the beginning of 2017 are only a fraction of what is likely to come. Cybercriminals are getting smarter with their attacks every day and companies should be prepared by having the appropriate budgets and solutions in place.

To read the complete report, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-cost-of-compromise

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.

1 Jeff Pollard, Security Budgets 2017: Increases Help But Remain Reactionary, Benchmarks: The S&R Practice Playbook (Forrester, 2016).

Contact:

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

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY
