Trend Micro Foresees Evolving Technology Introducing New Threats in 2017

Attacks will broaden and differentiate to penetrate new vulnerable surfaces

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released its annual security predictions report, "The Next Tier – 8 Security Predictions for 2017." The upcoming year will include an increased breadth and depth of attacks, with malicious threat actors differentiating their tactics to capitalize on the changing technology landscape.

"Next year will take the cybersecurity industry into new territory after 2016's threat landscape opened doors for cybercriminals to explore a wider range of attacks and attack surfaces," said Raimund Genes, chief technology officer for Trend Micro. "We foresee the General Data Protection Regulation (GDPR) causing extensive data management changes for companies around the world, new attack methods threatening corporations, expanding ransomware tactics impacting more devices and cyber-propaganda swaying public opinion."

In 2016, there was a large increase in Apple® vulnerabilities, with 50 disclosed, along with 135 Adobe bugs and 76 affecting Microsoft. This apparent shift in exploits against vulnerable software will continue in 2017 as Microsoft's mitigations continue to improve and Apple is seen as a more prominent operating system.

The Internet of Things (IoT) and Industrial Internet of Things (IIoT) will play a larger role in targeted attacks in 2017. These attacks will capitalize upon the growing acceptance of connected devices by exploiting vulnerabilities and unsecured systems to disrupt business processes, as we saw with Mirai. The increasing use of mobile devices to monitor control systems in manufacturing and industrial environments will be combined with the significant number of vulnerabilities found in these systems to pose threats to organizations.

Business Email Compromise (BEC) and Business Process Compromise (BPC) will continue to grow as a cost-effective and relatively simple form of corporate extortion. A BEC attack might yield $140,000 by luring an innocent employee to transfer money to a criminal's account. Alternatively, hacking directly into a financial transaction system, while requiring more work, will result in far greater financial windfalls for criminals – as much as $81 million.

"We continue to see cybercriminals evolving to the changing technology landscape," said Ed Cabrera, chief cybersecurity officer for Trend Micro. "While new ransomware saw an exponential increase in 2016, that growth is no longer sustainable, so attackers will find new ways to use existing malware families. Similarly, changes in IoT open new doors to go after additional attack surfaces, and software changes push criminals toward finding different types of flaws."

Highlights from the 2017 predications report include:

- The number of new ransomware families is predicted to plateau, only growing 25 percent, but will branch out into IoT devices and non-desktop computing terminals, like PoS systems or ATMs
- Vendors will not secure IoT and IIoT devices in time to prevent denial of service and other attacks
- New vulnerabilities will continue to be discovered in Apple and Adobe, which will then be added to exploit kits
- With 46 percent of the world's population now connected to the internet, the rise in cyber-propaganda will continue as new world leaders are appointed, potentially influencing public opinion with inaccurate information
- As seen in the Bangladesh Bank attack early in 2016, BPC attacks can allow cybercriminals to alter business processes and gain significant profits, and BEC attacks will continue to be useful to extort businesses via unsuspecting employees
- GDPR will force policy and administrative changes that will greatly impact costs and require organizations to conduct complete reviews of data processes to ensure compliance
- New targeted attack methods will focus on evading modern detection techniques to allow threat actors to target different organizations

To learn more about Trend Micro's 2017 threat predictions, visit: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017.

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 over 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.com/2016-12-06-Trend-Micro-Foresees-Evolving-Technology-Introducing-New-Threats-in-2017