

Trend Micro Predicts 2018 Cyberattacks Will Rely on Vulnerabilities

Changing technology landscape will require reliable patch management to block latest threats

DALLAS, December 5, 2017— This year, cyberattacks continued to plague business leaders, with major breaches occurring due to known vulnerabilities. [Trend Micro Incorporated \(TYO: 4704; TSE: 4704\)](#), a global leader in cybersecurity solutions, predicts the trend of known vulnerabilities being used in major attacks will continue in 2018 as corporate attack surfaces expand and expose more security holes. Patch management and employee education should be prioritized for all executives to protect an organization's most critical data.

As information technology and operational technology (IT/OT) continue to converge, enterprise applications and platforms will be at risk of manipulation and vulnerabilities, as stated in Trend Micro's 2018 predictions report. Additionally, Trend Micro predicts an increase in Internet of Things vulnerabilities as more devices are manufactured without security regulations or industry standards. Overall, the increased connectivity and enlarged attack surface present new opportunities for cybercriminals to leverage known issues to penetrate a corporate network.

"We at Trend Micro are constantly scouting out future threats that will have the greatest impact for businesses, and we predict which vulnerabilities will make the biggest waves in the coming year," said Rik Ferguson, VP of security research for Trend Micro. "Many devastating cyberattacks in 2017 leveraged known vulnerabilities that could have been prevented had they been patched beforehand. This trend will continue next year as corporate attack surfaces expand and expose more security holes. While this remains a challenge for enterprises, executives should prioritize vulnerability management as they make 2018 cybersecurity plans, particularly in the looming shadow of GDPR implementation."

Ransomware will continue to be a mainstay due to its proven success. There will be an increase in targeted ransomware attacks, in which the criminals go after a single organization to disrupt operations and force a larger ransom payout. Business Email Compromise (BEC) attacks will also continue to gain popularity with attackers, as the return on investment for successful attacks is quite high.

"The private sector continues to be under siege from a variety of cyber threats," said Edwin Martinez, chief information security officer for CEC Entertainment. "Institutions must continue to share critical information so we can better prevent and respond to these cyber threats limiting exposure to sensitive data."

Threat actors will also leverage growing technologies, like blockchain and machine learning, to enhance obfuscation against traditional cybersecurity protections. For this reason, the company recommends a layered, [cross-generational](#) defense strategy, which combines the latest security techniques with proven tactics that reinforce nearly 30 years of experience protecting some of the biggest global brands.

To access the complete report, "Paradigm Shifts: Trend Micro Security Predictions for 2018," please visit <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018>.

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 6,000 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.

<https://newsroom.trendmicro.ca/2018-01-03-Trend-Micro-Predicts-2018-Cyberattacks-Will-Rely-on-Vulnerabilities>