Trend Micro Warns of GDPR Extortion Attempts from Strategic Cybercriminals

Cybersecurity roundup report reveals growth in targeted, strategic, money-making attacks

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced its Security Roundup for 2017, revealing an increase in ransomware, cryptocurrency mining and BEC attempts over the past 12 months as cybercriminals refined and targeted their attacks for greater financial return. The trend will continue in 2018, with extortion attempts likely to target organizations trying to comply with new EU privacy laws.

The new report, *The Paradox of Cyberthreats*, validates Trend Micro's previous predictions for 2018, with cybercriminals increasingly abandoning exploit kits and spray-and-pray tactics in favor of more strategic attacks designed to improve their return on investment. Based on this trend, it's likely that some will try to extort money from enterprises by first determining the GDPR penalty that could result from an attack, and then demanding a ransom of slightly less than that fine, which CEOs might opt to pay.

"The 2017 roundup report reveals a threat landscape as volatile as anything we've seen, with cybercriminals increasingly finding they're able to gain more — whether it's money or data or reputation damage — by strategically targeting companies' most valuable assets," says Jon Clay, director of global threat communications for Trend Micro.

"It confirms our view that there is no silver bullet when it comes to the sheer range of cyberthreats facing organizations. Businesses instead need a cross-generational security solution that uses a blend of proven security protections with the best new defenses to mitigate risk effectively."

The report also reveals: a 32 percent increase in new ransomware families from 2016 to 2017; a doubling of BEC attempts between the first and second half of 2017; and soaring rates of cryptocurrency mining malware, peaking at 100,000 detections in October.

Vulnerable IoT devices are also a major security risk across several trending threats. Trend Micro detected more than 45.6 million cryptocurrency mining events during the year, representing a large percentage of all IoT events observed. Software vulnerabilities also continued to be targeted, with 1,009 new flaws discovered and disclosed in 2017 through Trend Micro's Zero Day Initiative and their 3,500+ independent whitehat researchers.

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 nearly 6,000 employees in more than 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.