Trend Micro Blocks Over 61 Million Ransomware Attacks in 2019

Security leader records 10% rise in ransomware detections

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today released its 2019 security roundup report. The report details the most important issues and changes in the threat landscape to provide businesses with insights into best practices and strategies for protecting their infrastructures from current and emerging threats.

Ransomware continued to be a mainstay cyber threat last year. Overall, Trend Micro discovered a 10% increase in ransomware detections, despite a 57% decrease in the number of new ransomware families. The healthcare sector remained the most targeted industry, with more than 700 providers affected in 2019. Additionally, at least 110 US state and municipal governments and agencies fell victim to ransomware.

“Digital transformation has been a business buzzword for decades, and the concept has yielded very positive results over time. But security is often an afterthought, which leaves digital doors wide open for cybercriminals,” said Jon Clay, director of global threat communications for Trend Micro. “Despite the prevalent ideals of digital transformation, lack of basic security hygiene, legacy systems with outdated operating systems and unpatched vulnerabilities are still a reality. This scenario is ideal for ransomware actors looking for a quick return on investment. As long as the ransom scheme continues to be profitable, criminals will continue to leverage it.”

To improve the ransomware business process, alliances between ransomware groups were formed in 2019. For example, the Sodinokibi ransomware operators launched coordinated attacks on 22 local government units in Texas, demanding a combined US$2.5 million ransom. This attack also demonstrated the “access-as-a-service” trend, in which criminal groups rent out or sell access to company networks. This service ranges in price from $3,000 to $20,000 USD, with the most expensive offering including full access to a company’s server hosts and corporate virtual private networks (VPNs).

Known vulnerabilities remain key to successful cyber attacks, including ransomware. In 2019, Trend Micro’s Zero Day Initiative (ZDI) disclosed 171% more high severity vulnerabilities than in 2018. The criticality score reflects the likelihood of these flaws being leveraged by attackers, so high severity bugs are more likely to be weaponized and the patches should be prioritized.

To protect against today’s threat landscape, Trend Micro recommends a connected threat defense across gateways, networks, servers and endpoints. Additionally, these best practices can increase a company’s security posture:

- Mitigate ransomware with network segmentation, regular back-ups and continuous network monitoring.
- Update and patch systems and software to protect against known vulnerabilities.
- Enable virtual patching, especially for operating systems that are no longer supported by the vendor.
- Implement multi-factor authentication and least privilege access policies to prevent abuse of tools that can be accessed via admin credentials, like remote desktop protocol, PowerShell and developer tools.

For more on the cyber threat landscape of 2019, access the full report here: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-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 6,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

Contact:

Erin Johnson
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
OTC Pink:
TMICY

---

https://newsroom.trendmicro.com/2020-02-25-Trend-Micro-Blocks-Over-61-Million-Ransomware-Attacks-in-2019