Trend Micro Predicts Escalating Cloud and Supply Chain Risk

Cyber risk increases at all layers of the corporate network as we enter a new decade

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced its 2020 predictions report, which states that organizations will face a growing risk from their cloud and the supply chain. The growing popularity of cloud and DevOps environments will continue to drive business agility while exposing organizations, from enterprises to manufacturers, to third-party risk.

“As we enter a new decade, organizations of all industries and sizes will increasingly rely on third party software, open-source, and modern working practices to drive the digital innovation and growth they crave,” said Jon Clay, director of global threat communications for Trend Micro. “Our threat experts predict that this fast growth and change will bring new risks of supply chain attacks. From the cloud layer all the way down to the home network, IT security leaders will need to reassess their cyber risk and protection strategy in 2020.”

Attackers will increasingly go after corporate data stored in the cloud via code injection attacks such as deserialization bugs, cross-site scripting and SQL injection. They will either target cloud providers directly or compromise third-party libraries to do this.

In fact, the increasing use of third-party code by organizations employing a DevOps culture will increase business risk in 2020 and beyond. Compromised container components and libraries used in serverless and microservices architectures will further broaden the enterprise attack surface, as traditional security practices struggle to keep up.

Managed service providers (MSPs) will be targeted in 2020 as an avenue for compromising multiple organizations via a single target. They will not only be looking to steal valuable corporate and customer data, but also install malware to sabotage smart factories and extort money via ransomware.

The new year will also see a relatively new kind of supply chain risk, as remote workers introduce threats to the corporate network via weak Wi-Fi security. Additionally, vulnerabilities in connected home devices can serve as a point of entry into the corporate network.

Amidst this ever-volatile threat landscape, Trend Micro recommends organizations:

- Improve due diligence of cloud providers and MSPs
- Conduct regular vulnerability and risk assessments on third parties
- Invest in security tools to scan for vulnerabilities and malware in third-party components
- Consider Cloud Security Posture Management (CSPM) tools to help minimize the risk of misconfigurations
- Revisit security policies regarding home and remote workers

To read the full report, *The New Norm: Trend Micro Security Predictions for 2020*, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2020.

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
