MSPs, Hybrid Workers and Connected Cars Face Cyber-Threat Onslaught in 2023

Trend Micro's forward-looking report predicts how the threat landscape will evolve

DALLAS, Dec. 13, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released **Future/Tense: Trend Micro Security Predictions for 2023**. The report warns that threat actors will ramp up attacks targeting security blind spots in the home office, software supply chain and cloud in the coming year.

To read a full copy of the report, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2023

Cybercriminals will target security blind spots in the home office, software supply chain and cloud in the coming year.

"The pandemic might be receding, but remote working is here to stay," said Jon Clay, vice president of threat intelligence at Trend Micro. "That means a renewed threat actor focus on unpatched VPNs, connected SOHO devices and back-end cloud infrastructure in 2023. In response, organizations will need to focus on helping overworked security teams by consolidating attack surface management and detection and response to a single, more cost-effective platform."

According to the report, VPNs represent a particularly attractive target as a single solution could be exploited to target multiple corporate networks. Home routers will also be singled out as they're often left unpatched and unmanaged by central IT.

Alongside the threat to hybrid workers, the report anticipates several trends for IT security leaders to watch out for in 2023, including:

- **A growing supply chain threat from managed service providers (MSPs)**, which will be selected because they offer access to a large volume of downstream customers, thereby maximizing the ROI of ransomware, data theft and other attacks
- **"Living off the cloud" techniques** may become the norm for groups attacking cloud infrastructure to stay hidden from conventional security tools. An example could be using a victim's backup solutions to download stolen data into the attacker's storage destination
- **Connected car threats** such as targeting of the cloud APIs which sit between in-vehicle embedded-SIMs (eSIMs) and back-end application servers. In a worst-case scenario (i.e., Tesla API) attacks could be used to gain access to vehicles. The connected car industry could also be impacted by malware lurking in open-source repositories
- **Ransomware-as-a-service (RaaS) groups may rethink their business** as the impact of double extortion fades. Some may focus on the cloud, while others could eschew ransomware altogether and try monetizing other forms of extortion like data theft
- **Social engineering will be turbo-charged** with business email compromise (BEC)-as-a-service offerings and the rise of deepfake-based BEC

Trend Micro recommends organizations mitigate these emerging threats in 2023 via:

- **Zero trust strategies** built on a "never trust, always verify" mantra, to minimize damage without sacrificing user productivity
- **Employee training and awareness raising** to turn a weak link in the security chain into an effective line of defense
- **Consolidating onto a single security platform** for all attack surface monitoring and threat detection and response. This will improve a company's ability to catch suspicious activity across their networks, reduce the burden on security teams and keep defenders sharp
- **Stress testing IT infrastructures** to ensure attack readiness in different scenarios, especially ones where a perimeter gateway has already been breached
- **A software bill of materials (SBOM)** for every application, to accelerate and enhance vulnerability management—by delivering visibility into code developed in-house, bought from commercial sources, and built from third-party sources

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Media Contact: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2022-12-13-MSPs,-Hybrid-Workers-and-Connected-Cars-Face-Cyber-Threat-Onslaught-in-2023