Security Experts Face Record Cyber Threats, Overwhelming Workload

Organizations seek new ways to protect their expanding attack surface, maintain stability

DALLAS, March 17, 2022 /PRNewswire/ -- New research from Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, warns of spiraling risk to digital infrastructure and remote workers as threat actors increase their rate of attack on organizations and individuals.

"Attackers are always working to increase their victim count and profit, whether through quantity or effectiveness of attacks," said Jon Clay, vice president of threat intelligence at Trend Micro. "The breadth and depth of our global threat intelligence allows us to identify shifts in how malicious actors target their victims across the world. Our latest research shows that while Trend Micro threat detections rose 42% year-on-year in 2021 to over 94 billion, they shrank in some areas as attacks became more precisely targeted."

Ransomware attackers are shifting their focus to critical businesses and industries more likely to pay, and double extortion tactics ensure that they are able to profit. Ransomware-as-a-service offerings have opened the market to attackers with limited technical knowledge – but also given rise to more specialization, such as initial access brokers who are now an essential part of the cybercrime supply chain.

Threat actors are also getting better at exploiting human error to compromise cloud infrastructure and remote workers. Trend Micro Cloud App Security (CAS) detected and prevented 25.7 million email threats in 2021 compared to 16.7 million in 2020, with the volume of blocked phishing attempts nearly doubling over the period. Research shows home workers are often prone to take more risks than those in the office, which makes phishing a particular risk.

In the cloud, incorrectly configured systems continue to plague organizations. Services such as Amazon Elastic Block Store and Microsoft Azure's Virtual Machine were among the services that had relatively high misconfiguration rates. Trend Micro also found that Docker REST APIs are frequently misconfigured, exposing them to attacks from groups like TeamTNT that deploy crypto-mining malware on affected systems.

Business email compromise (BEC) saw detections drop 11%. However, CAS blocked a higher percentage of advanced BEC emails, which could be detected only by comparing the writing style of the attacker with that of the intended sender. These attacks comprised 47% of all BEC attempts in 2021 versus 23% in 2020.

While 2021 was a record year for new vulnerabilities, Trend Micro research shows that 22% of the exploits sold in the cybercrime underground last year were over three years old. Patching old vulnerabilities remains an essential task alongside monitoring for new threats to prevent cyber-attacks and ensure strong security posture.

**To learn more about* Navigating New Frontiers: Trend Micro 2021 Annual Cybersecurity Report*, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report*

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: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---