Cyber Threat Surge: Trend Micro Blocks 160 billion Incidents in 2023

Ransomware detections fall 14% as alternative attack strategies evolve

DALLAS, March 6, 2024 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today revealed a 10% annual increase in total threats blocked in 2023 and warned that attackers are using more advanced methods to target fewer victims with the potential for higher financial gains.

To read a copy of the report, *Calibrating Expansion: Annual Cybersecurity Threat Report*, please visit: *https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/calibrating-expansion-2023-annual-cybersecurity-threat-report*

Jon Clay, VP of threat intelligence at Trend:"We're blocking more threats than ever before for our customers. But understand that adversaries showed a variety and sophistication of TTPs in their attacks, especially in defense evasion. As our report demonstrates, network defenders must continue to proactively manage risk across the entire attack surface today. Understanding the strategies favored by our adversaries is the foundation of effective defense."

Trend Micro blocked **161 billion threats** overall in 2023, compared to 82 billion threats five years ago. In 2023, threats blocked by email and web reputation dropped annually by 47% and 2%, respectively. Threats blocked by Trend's Mobile Application Reputation Service (-2%), Smart Home Network (-12%), and Internet of Things Reputation Service (-64%) also declined. However, there was a 35% annual increase in threats blocked under Trend's File Reputation Service (FRS).

This could indicate that threat actors are choosing their targets more carefully. Instead of launching attacks on a wider range of users and relying on victims clicking on malicious links in websites and emails, they're targeting a smaller number of higher-profile victims with more sophisticated attacks. This might enable them to bypass early detection layers like network and email filters—which could explain the surge in malicious file detections at endpoints.

Some other trends observed in the report include:

1. APT actors showed a variety and sophistication of their attacks against victims, especially around defense evasion tactics.

- Email malware detection surged by 349% year-on-year (YoY), while malicious and phishing URL detections declined by 27% YoY – again highlighting the trend for more using malicious attachments in their attacks.
- Business email compromise (BEC) detections increased 16% YoY.
- Ransomware detections dropped 14% YoY. However, once again, the increase in FRS detections may indicate that threat actors are getting better at evading primary detection via techniques such as Living-Off-The-Land Binaries and Scripts (LOLBINs/LOLBAs), Bring Your Own Vulnerable Driver (BYOVD), zero-day exploits, and AV termination.
- Linux and MacOS ransomware attacks were 8% of the overall ransomware detections.
- There was an increase in remote encryption, intermittent encryption, EDR bypass using unmonitored virtual machines (VMs), and multi-ransomware attacks where victims were hit more than once. Adversaries have recognized EDR as a formidable defense but are now utilizing bypass tactics to get around this technology.
- Thailand and the US were the top two ransomware victim countries, with banking as the most affected sector.
- The top MITRE ATT&CK detections were defense evasion, command & control, initial access, persistence, and impact
- Risky cloud app access was the top risk event detected by Trend's attack surface risk management (ASRM), recorded almost 83 billion times.
- Trend's Zero Day Initiative discovered and responsibly disclosed 1914 zero-days, up 12% YoY. These included 111 Adobe Acrobat and Reader bugs. Adobe was the number one vendor for vulnerability reporting, and PDFs were the number one spam attachment type.
- Windows applications were the top 3 vulnerabilities exploited through detections from our virtual patches.
- Mimikatz (used in data harvesting) and Cobalt Strike (used in Command & Control) continued to be the preferred legitimate tools to abuse to aid criminal activity.

In light of these findings, Trend advises network defenders to:

- Work with trusted security vendors with a cybersecurity platform approach to ensure resources are not only secured but also continuously monitored for new vulnerabilities.
- Prioritize SOC efficiency by monitoring cloud applications carefully as they become more closely integrated into day-to-day operations.
- Ensure all the latest patches/upgrades are applied to operating systems and applications.
- Utilize comprehensive security protocols to safeguard against vulnerabilities, tighten configuration settings, control application access, and enhance account and device security. Look to detect ransomware attacks earlier in the attack lifecycle by shifting left in defenses during initial access, lateral movement, or data exfiltration stages.

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.

---

https://newsroom.trendmicro.com/2024-03-06-Cyber-Threat-Surge-Trend-Micro-Blocks-160-billion-Incidents-in-2023