Cyber-Threat Detections Hit a Record-Breaking 146 billion in 2022

Trend Micro annual roundup report warns of exponentially expanding attack surface

DALLAS, March 7, 2023 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced a massive 55% increase in overall threat detections in 2022 and a 242% surge in blocked malicious files, as threat actors indiscriminately targeted consumers and organizations across all sectors.

To read a full copy of the report, *Rethinking Tactics: 2022 Annual Cybersecurity Report*, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/rethinking-tactics-annual-cybersecurity-roundup-2022

Jon Clay, VP of threat intelligence at Trend Micro:"The unrivaled breadth of Trend Micro threat intelligence* reveals 2022 as a year when threat actors went 'all-in' to boost profits. A surge in backdoor detections is particularly concerning in showing us their success in making landfall inside networks. To manage risk effectively across a rapidly expanding attack surface, stretched security teams need a more streamlined, platform-based approach."

The roundup report reveals several interesting trends for 2022 and beyond:

The top three MITRE ATT&CK techniques show us that threat actors are gaining initial access through remote services, then expanding their footprint within the environment through credential dumping to utilize valid accounts.

An 86% increase in backdoor malware detections reveals threat actors trying to maintain their presence inside networks for a future attack. These backdoors primarily targeted web server platform vulnerabilities.

A record number of Zero Day Initiative (ZDI) advisories (1,706) for the third year in a row is the result of a rapidly expanding corporate attack surface and researcher investment in automated analysis tools, which are finding more bugs. The number of critical vulnerabilities doubled in 2022. Two out of the top three CVEs reported in 2022 were related to Log4j.

The ZDI observed an increase in failed patches and confusing advisories, adding extra time and money to corporate remediation efforts and exposing organizations to unnecessary cyber risk.

Webshells were the top-detected malware of the year, surging 103% on 2021 figures. Emotet detections were second after undergoing something of a resurgence. LockBit and BlackCat were the top ransomware families of 2022.

Ransomware groups rebranded and diversified in a bid to address declining profits. In the future, we expect these groups to move into adjacent areas that monetize initial access, such as stock fraud, business email compromise (BEC), money laundering, and cryptocurrency theft.

Trend Micro recommends that organizations adopt a platform-based approach to managing the cyber-attack surface, mitigate security skills shortages and coverage gaps, and minimize the costs associated with point solutions. This should cover the following:

- **Asset management.** Examine assets and determine their criticality, any potential vulnerabilities, the level of threat activity, and how much threat intelligence is being gathered from the asset.
- **Cloud security**. Ensure that cloud infrastructure is configured with security in mind to prevent attackers from capitalizing on known gaps and vulnerabilities.
- **Proper security protocols**. Prioritize updating software as soon as possible to minimize the exploitation of vulnerabilities. Options such as virtual patching can help organizations until vendors provide official security updates.
- **Attack surface visibility**. Monitor disparate technologies and networks within the organization, as well as any security system that protects them. It may be difficult to correlate different data points from siloed sources.

** It covers endpoints (Android & iOS, IoT, IIoT, PCs, Macs, Linux, servers), email, web and network layers, OT networks, cloud, home networks, vulnerabilities, consumers, businesses, and governments globally.*

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/2023-03-07-Cyber-Threat-Detections-Hit-a-Record-Breaking-146-billion-in-2022