Trend Micro Warns of 75% Surge in Ransomware Attacks on Linux as Systems Adoptions Soared

63 billion threats blocked by Trend Micro in 1H 2022

DALLAS, Aug. 31, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today predicted that ransomware groups will increasingly target Linux servers and embedded systems over the coming years. It recorded a double-digit year-on-year (YoY) increase in attacks on these systems in 1H 2022.

To read a full copy of the *Trend Micro 2022 Midyear Roundup Report*, please visit: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report

Trend Micro blocked 63 billion threats in the first half of 2022.

Jon Clay, VP of threat intelligence for Trend Micro, said:"New and emerging threat groups continue to evolve their business model, focusing their attacks with even greater precision. That's why it's essential that organizations get better at mapping, understanding, and protecting their expanding digital attack surface. A single, unified cybersecurity platform is the best place to start."

According to Trend Micro data:

- 63 billion threats blocked by Trend Micro in 1H 2022
- 52% more threats in the first half of the year than the same period in 2021
- Government, manufacturing and healthcare are the top three sectors targeted with malware

Detection of attacks from ransomware-as-a-service surged in the first half of 2022. Major players like LockBit and Conti were detected with a 500% YoY increase and nearly doubled the number of detections in six months, respectively. The ransomware-as-a-service model has generated significant profits for ransomware developers and their affiliates.

New ransomware groups are emerging all the time. The most notable one in the first half of 2022 is Black Basta. The group hit 50 organizations in just two months. Many persist with the "big game-hunting" of large enterprises, although SMBs are an increasingly popular target.

One of the primary attack vectors for ransomware is vulnerability exploitation. Trend Micro's Zero Day Initiative published advisories on 944 vulnerabilities in the period, a 23% YoY increase. The number of critical bug advisories published soared by 400% YoY.

APT groups continue to evolve their methods by employing expansive infrastructure and combining multiple malware tools. The ten-fold increase in the number of detections is another proof point that threat actors are increasingly integrating Emotet as part of their elaborate cybercrime operations.

The concern is that threat actors are able to weaponize these flaws faster than vendors can release patch updates and/or customers can patch them.

Unpatched vulnerabilities add to a growing digital attack surface many organizations are struggling to manage securely as the hybrid workplace expands their IT environment. Over two-fifths (43%) of global organizations believe it is "spiraling out of control."

Cloud visibility is particularly important given the continued threat of third parties exploiting misconfigured environments and using novel techniques like cloud-based crypto mining and cloud tunneling. The latter is frequently abused by threat actors to route malware traffic or host phishing websites.

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

SOURCE Trend Micro Incorporated

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

---

Additional assets available online: Video (1)

https://newsroom.trendmicro.com/2022-08-31-Trend-Micro-Warns-of-75-Surge-in-Ransomware-Attacks-on-Linux-as-Systems-Adoptions-Soared