Trend Micro Detected Over 13 Million Malware Events Targeting Linux-based Cloud Environments

Coinminers, web shells and ransomware made up 56% of malwares targeting Linux systems in the first half of 2021

DALLAS, Aug. 23, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released new research on the state of Linux security in the first half of 2021. The report gives valuable insight into how Linux operating systems are being targeted as organizations increase their digital footprint in the cloud and the pervasive threats that make up the Linux threat landscape.

To read the full report, Linux Threat Report 2021 1H: Linux Threats in the Cloud and Security Recommendations, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-threat-report-2021-1h-linux-threats-in-the-cloud-and-security-recommendations

As of 2017, 90% of public clouds workloads ran on Linux. According to Gartner®, "Rising interest in cloud-native architectures is prompting questions about the future need for server virtualization in the data center. The most common driver is Linux-OS-based virtualization, which is the basis for containers.[1]"

Linux allows organizations to make the most of their cloud-based environments and power their digital transformation strategies. Many of today's most cutting-edge IoT devices and cloud-based applications and technology run on some flavor of Linux, making it a critical area of modern technology to secure.

"In the industry, we see some very creative attacks and we have to stay ahead. Protecting the company, our employees, and our intellectual property is a priority," says John Breen, Global Head of Cybersecurity at Flowserve. "We'll continue to work closely and collaborate with Trend Micro to ensure our people and our company remain protected."

The report investigates the top malware families affecting Linux servers during the first half of 2021, with the top types of malwares being:

- **25% Coinminers** – The high prevalence of cryptocurrency miners is of little surprise given the clear motive of the seemingly endless amount of computing power the cloud holds, making it the perfect environment.
- **20% Web shells** – The recent Microsoft Exchange Attack, which leveraged web shells, showed the importance of patching against this type of malware
- **12% Ransomware** – The most prevalent detected was the modern ransomware family, DoppelPaymer, however some other notable ransomware families seen targeting Linux systems as well are RansomExx, DarkRadiation, and the DarkSide.

"It's safe to say that Linux is here to stay, and as organizations continue to move to Linux-based cloud workloads, malicious actors will follow," said Aaron Ansari, vice president of cloud security for Trend Micro. "We have seen this as a main priority to ensure our customers receive the best security across their workloads, no matter the operating system they choose to run it on."

The report revealed that most detections arose from systems running end-of-life versions of Linux distributions, including 44% from CentOS versions 7.4 to 7.9. In addition, 200 different vulnerabilities were targeted in Linux environments in just six months. This means attacks on Linux are likely taking advantage of outdated software with unpatched vulnerabilities.

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. **TrendMicro.com**.

GARTNER is the registered trademark and service mark of Gartner Inc., and/or its affiliates and has been used herein with permission. All rights reserved.

[1] Gartner - Rationalizing Applications and Infrastructure for Cloud Delivery,Philip Dawson, 28 May 2021

SOURCE Trend Micro Incorporated

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

---

https://newsroom.trendmicro.com/2021-08-23-Trend-Micro-Detected-Nearly-13-Million-Malware-Events-Targeting-Linux-based-Cloud-Environments