Cloud Systems Are the New Battleground for Crypto Mining Threat Actors

Trend Micro report warns of growing attack surface for CPU-mining

DALLAS, March 29, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced a new report revealing a fierce, hour-by-hour battle for resources among malicious cryptocurrency mining groups.

To read a full copy of the report, *A Floating Battleground Navigating the Landscape of Cloud-Based Cryptocurrency Mining,* please visit: *https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/probing-the-activities-of-cloud-based-cryptocurrency-mining-groups*

"Just a few hours of compromise could result in profits for the perpetrators. That's why we're seeing a continuous fight for cloud CPU resources. It's akin to a real-life capture-the-flag, with the victim's cloud infrastructure the battleground," said Stephen Hilt, Senior Threat Researcher at Trend Micro. "Threats like this need joined-up, platform-based security to ensure the bad guys have nowhere to hide. The right platform will help teams map their attack surface, assess risk, and apply for the right protection without adding excessive overheads."

Threat actors are increasingly scanning for and exploiting these exposed instances, as well as brute-forcing SecureShell (SSH) credentials, in order to compromise cloud assets for cryptocurrency mining, the report reveals. Targets are often characterized by having outdated cloud software in the cloud environment, poor cloud security hygiene, or inadequate knowledge on how to secure cloud services and thus easily exploited by threat actors to gain access to the systems.

Cloud computing investments have surged during the pandemic. But the ease with which new assets can be deployed has also left many cloud instances online for longer than needed—unpatched and misconfigured.

On one hand, this extra computing workload threatens to slow key user-facing services for victim organizations, as well as increasing operating costs by up to 600% for every infected system.

Crypto mining can also be a precursor to more serious compromise. Many mature threat actors deploy mining software to generate additional revenue before online buyers purchase access for ransomware, data theft, and more.

The Trend Micro report details the activity of multiple threat actor groups in this space, including:

Outlaw, which compromises IoT devices and Linux cloud servers by exploiting known vulnerabilities or performing brute-force SSH attacks.

TeamTNT, which exploits vulnerable software to compromise hosts before stealing credentials for other services to help it move around to new hosts and abuse any misconfigured services.

Kinsing, which sets up an XMRig kit for mining Monero and kicks any other miners off a victim system.

8220, which has been observed fighting Kinsing over the same resources. They frequently eject each other from a host and then install their own cryptocurrency miners.

Kek Security, which has been associated with IoT malware and running botnet services.

To mitigate the threat from cryptocurrency mining attacks in the cloud, Trend Micro recommends organizations to:

- Ensure systems are up-to-date and running only the required services
- Deploy firewall, IDS/IPS, and cloud endpoint security to limit and filter network traffic to and from known bad hosts
- Eliminate configuration errors via Cloud Security Posture Management tools
- Monitor traffic to and from cloud instances and filter out domains associated with known mining pools
- Deploy rules that monitor open ports, changes to DNS routing, and utilization of CPU resources from a cost perspective

For more insights into cloud crypto mining and the benefits of leveraging a unified cybersecurity platform, check out these resources: https://www.trendmicro.com/en_us/ciso/22/c/stop-cryptomining-malware.html

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

---