Trend Micro Research Finds Both On-Premise and Cloud-based Servers Compromised by Criminal Underground

Understanding the infrastructure behind cybercrime helps detect and stop operations

DALLAS, Sept. 1, 2020 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), the leader in cloud security, today released research that states organizations' on-premise and cloud-based servers are compromised, abused and rented out as part of a sophisticated criminal monetization lifecycle.

The findings come from the second of a three-part report series looking at how the underground hosting market operates. The findings show that cryptocurrency mining activity should be the indicator for IT security teams to be on high alert.

While cryptomining may not cause disruption or financial losses on its own, mining software is usually deployed to monetize compromised servers that are sitting idle while criminals plot larger money-making schemes. These include exfiltrating valuable data, selling server access for further abuse, or preparing for a targeted ransomware attack. Any servers found to contain cryptominers should be flagged for immediate remediation and investigation.

"From dedicated bulletproof hosting to anonymizing services, domain name provision and compromised legitimate assets, the cybercriminal underground boasts a sophisticated range of infrastructure offerings to support monetization campaigns of all types," said Bob McArdle, director of forward-looking threat research for Trend Micro. "Our goal is to raise awareness and understanding of cybercriminal infrastructure to help law enforcement agencies, customers and other researchers block avenues for cybercrime and drive costs up for threat actors."

The report lists the main underground hosting services available today, providing technical details of how they work and how criminals use them to run their businesses. This includes a detailed description of the typical lifecycle of a compromised server, from initial compromise to final attack.

Cloud servers are particularly exposed to compromise and use in underground hosting infrastructure as they may be lacking the protection of their on-premises equivalents.

McArdle continued, "Compromised legitimate corporate assets can be infiltrated and abused whether on-premise or in the cloud. A good rule of thumb is that whatever is most exposed is most likely to be exploited."

Cybercriminals might look to exploit vulnerabilities in server software, use brute-force attacks to compromise credentials, or steal logins and deploy malware via phishing attacks. They may even target infrastructure management software (cloud API keys), which allows them to create new instances of virtual machines or supply resources.

Once compromised, these cloud server assets could be sold on underground forums, dedicated marketplaces and even social networks for use in a range of attacks.

The report also covers emerging trends for underground infrastructure services, including abuse of telephony services and satellite infrastructure, and "parasitic" computing for rent including hidden RDP and VNC.

To read the complete second report in this series, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/commodified-cybercrime-infrastructure-exploring-the-underground-services-market-for-cybercriminals.

About Trend Micro
Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks. Our XGen™ security strategy powers our solutions with a cross-generational blend of threat-defense techniques that are optimized for key environments and leverage shared threat intelligence for better, faster protection. With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com

SOURCE Trend Micro Incorporated

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

---

https://newsroom.trendmicro.com/2020-09-01-Trend-Micro-Research-Finds-Both-On-Premise-and-Cloud-based-Servers-Compromised-by-Criminal-Underground