A FLOATING BATTLEGROUND

Navigating the Landscape of Cloud-Based Cryptocurrency Mining

The rise of both cloud infrastructure and cryptocurrency has led to a convergence of the two in the world of cybercrime, with malicious actors targeting cloud-based systems with cryptocurrency-mining attacks. In our research paper, we take a close look at such actors and attacks, and examine their impact on affected organizations.

KEY FINDINGS

- A successful cryptocurrency-mining attack means that a malicious actor was able to capitalize on weak security software or other security flaws to gain access to a system. This is a red flag for organizations since a failure to address these weaknesses could lead to more damaging attacks such as ransomware or data exfiltration.
- Because of the scalability of the cloud and because cryptocurrency-mining groups normally try to maximize profits by deploying their software in all of a victim's cloud instances, the monetary impact of an attack could rise significantly in a short time.
- A cryptocurrency-mining attack could lead to disruptions in the operations of a business, which in turn could result in loss of revenue and even reputation.
- The most prominent cloud-based cryptocurrency-mining groups, such as TeamTNT and Kinsing, vary in terms of their skills, tools, infrastructure, and social media use.
- Cloud-based cryptocurrency-mining groups not only have to contend with their targets' security systems but also have to fight among themselves over their victims' resources.

SECURITY RECOMMENDATION

- Organizations should ensure that their cloud systems are up to date and running only the services that are required to minimize the chance of a successful cryptocurrency-mining attack.
- Organizations that have cloud systems directly exposed to the internet should deploy tools such as firewalls and cloud endpoint security products in order to minimize the attack surface.
- Organizations should deploy rules that can help with cloud security, such as those that can be used for monitoring resources, tracking open ports, and checking DNS changes and usage.

As organizations become more reliant on cloud infrastructure, malicious cloud-based cryptocurrency mining becomes a bigger threat, not only to their resources but also to other aspects of their cloud deployments, such as sensitive data and even the use of the infrastructure itself. Rather than considering cryptocurrency mining as a low-risk attack, organizations should treat its presence as a warning sign of deeper security weaknesses within the system that could lead to direr consequences.

Read our full paper at
https://research.trendmicro.com/cloudcryptomining.

TREND MICRO™ | research