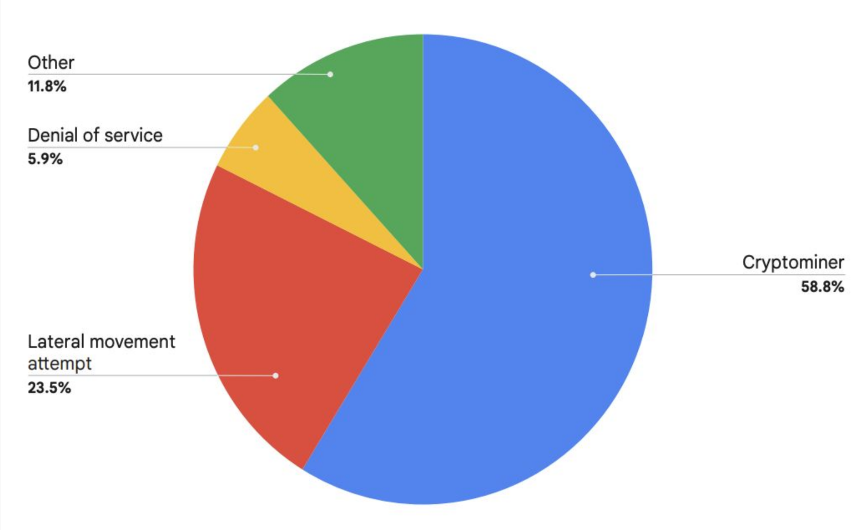
Threat Hunting for Cryptojacking in the Cloud

Megan Roddie-Fonseca
SANS FOR509 Co-Author
Sr. Security Engineer, Datadog

What is Cryptojacking?

“Cryptojacking is a type of cybercrime where a criminal secretly uses a victim’s computing power to generate cryptocurrency.” - Interpol

Cryptojacking is one of the most prevalent threats in cloud environments. According to Google’s Threat Horizons Report, almost 60% of attacks in H1 2024 were motivated by cryptomining.



The Risks of Cryptojacking

Increased Costs

The resources required by cryptominers do not come cheap. You do not want to find out there was a cryptominer running when you get your monthly bill!

Performance Issues

Cryptominers installed on existing infrastructure can impact performance of servers by mass resource consumption.

Opportunities for hunting!

Threat Hunting Opportunities

01

GPU-Enabled VM Creation

GPU-Enabled VM Creation

AWS

- **RunInstance** events
- Look for **instanceType** of **g*.*xlarge**

Azure

- **MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE** events
- Look for **VmSize** associated with **N-Series**

Google Cloud

- **v1.compute.instances.insert** or **v1.compute.instances.attachDisk** events
- Look for **A3, A2, G2,** or **N1** VM types

02

Cryptomining Domain Connections

Cryptomining Domain Connections

Log Sources

- **DNS Resolver** Logs
- **NGFW** Logs
- **Sysmon** Logs

Threat Intel

- **GitHub - Crypto mining pools aggregator (domains + IPs)**
- Microsoft - Top 10 Mining Domains Observed

03

Billing Tracking

The Cost of Cryptojacking

“In attacks observed by Microsoft, cryptojacking activities were seen to incur compute fees more than $300,000”
- Microsoft

AWS Cost Explorer

Azure Cost Management

Google Cloud Cost Management

Thank You!