UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00023

AWS CRYPTOJACKING WORM

DATE ISSUED: 19th August 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	LOW	[✓ MEDIUM]	HIGH

OVERVIEW

The TeamTNT group is spreading a worm through the Amazon Web Services cloud in an effort to harvest login credentials to deploy the XMRig Monero crypto-miner and numerous other malware on the targeted cloud instance.

BREAKDOWN

Cryptojacking is the practice of unauthorised use of resources to mine cryptocurrency, in this case Monero. This can be an expensive exercise for the account holder when this type of attack occurs in the cloud, as the user pays based in incoming and outgoing traffic and bandwidth consumption. Other malware deployed by the worm include an SSH post-exploitation tool 'punk.py' and backdoor 'Tsunami IRC' as well as a log cleaning tools and the Diamorphine rootkit. It will also delete any other mining software, reconfigure firewall rules and create a Linux container to host the miner and a DDoS bot, as well as collecting system information to send to the Command and Control Server. The anchoring script for this worm is based on the Kinsing malware that scans the internet for and attacks misconfigured server, Docker accounts and Kubernetes orchestrations. The worm scans for credentials that are stored in the AWS command line interface shell in an unencrypted file.

REMEDIATION STEPS

- Identify which systems are storing AWS credentials and delete any that are not needed
- Use firewalls to limit Docker API access
- Review network traffic and logs to identify any connections to mining pools or using Stratum mining protocol as well as AWS credentials being sent over HTTP
- Check cloud security configuration for AWS hosted instances

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/aws-cryptojacking-worm-cloud/158427/
IT News:	https://www.itnews.com.au/news/researchers-find-aws-creds-stealing-worm-551922
HelpNet Security:	https://www.helpnetsecurity.com/2020/08/18/worm-steals-aws-credentials/
ZDNet:	https://www.zdnet.com/article/crypto-mining-worm-steal-aws-credentials/