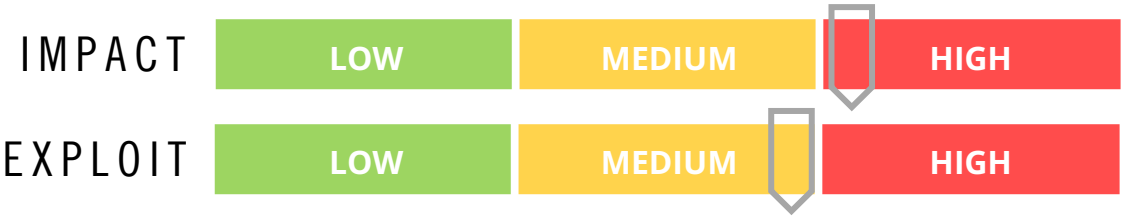
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0265

KMSDBOT INFECTS SYSTEMS & LAUNCHES DDOS ATTACKS

DATE ISSUED: 21st November 2022



OVERVIEW

Akami Security Research have discovered a new and evasive Golang-based malware KmsdBot which leverages the Secure Shell (SSH) cryptographic protocol and uses weak credentials to enter the targeted systems with the goal of mining cryptocurrency and carrying out Distributed Denial-of-Service (DDoS) attacks.

BREAKDOWN

KmsdBot has been seen to target multiple sectors, from gaming to luxury car brands to security firms. The malware gets its name from an executable named "kmsd.exe," downloaded from a remote server following a successful compromise. It supports multiple architectures, such as Winx86, Arm64, and mips64, to stay non-persistent which allows it to avoid detection. The first DDoS attack was targeted at a gaming company named FiveM, which allows gamers to host custom, private, online games servers. The malware employed specific targeted attacks along with generic Layer 4 and Layer 7 attacks. Once the system is infected, the bot downloads a list of login credentials to use when it scans for open SSH ports.

REMEDIATION STEPS

- Use strong and unique credentials for servers or deployed applications.
- Ensuring the deployed applications are up-to-date with the latest security patches and check with vendors for new releases regularly.
- Use public key authentication for the SSH connections.

REFERENCES & RESOURCES

Security Affairs: https://securityaffairs.co/wordpress/138514/malware/kmsdbot-golang-malware.html
The Hacker News: https://thehackernews.com/2022/11/new-kmsdbot-malware-hijacking-systems.html