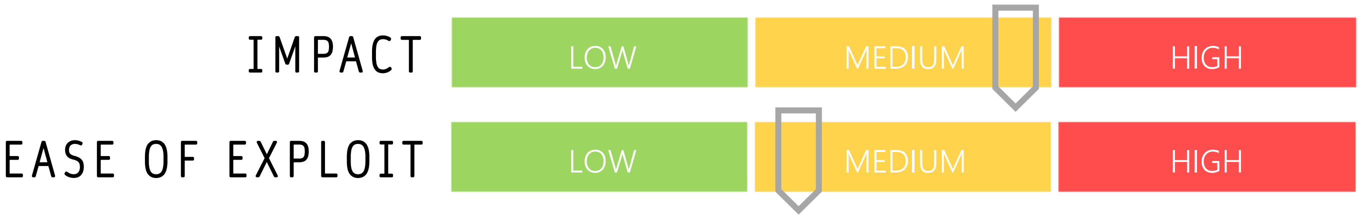
UNISPHERE SOLUTIONS

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

# CYBER GUIDANCE ISSUE 0004

## GOLANG WORM

DATE ISSUED: 25th June 2020


IMPACT LOW MEDIUM HIGH

EASE OF EXPLOIT LOW MEDIUM HIGH

## OVERVIEW

Known as a "first-stage malware loader" positioning itself as a backdoor with aims to install crypto-miners and other damaging malware has evolved from Linux targeting to exploit vulnerabilities in Windows Servers

## BREAKDOWN

When initially discovered in 2019, the loader is spread by worm, searching for and infecting vulnerable machines to download the XMRig crypto-miner to begin harvesting Monero cryptocurrency using valuable computing and power resources. The new variant adds a payload capacity and attacks web application frameworks (ThinkPHP) and applications servers (see CVE-2017-10271, CVE-2015-1427, CVE-2014-3120, CVE-2018-7600 & CVE-2018-20062). For Hadoop, Redis and MSSQL the malware uses brute force or dictionary attacks to gain credentials for remote code executions and downloading of file sets customised to the platform that is being attacked containing the loader payload, crypto-miner with configurations, a watchdog and a scanner for further propagation. In Windows machines, a backdoor user is added to the system through an unauthorised SSH key.

## REMEDIATION STEPS

- Ensure security updates and patching is up to date on all devices
- Ensure web application firewalls are updated and configured correctly
- Ensure your organization has up to date Endpoint and Network Protection in place on all devices
- Ensure network monitoring and analysis is conducted regularly to detect any abnormal network behaviours

## REFERENCES & RESOURCES

| | |
|---|---|
| Threatpost: | https://threatpost.com/worm-golang-malware-windows-payloads/156924/ |
| Cyware Social | https://cyware.com/news/golang-worm-broadens-its-horizons-8c500fe8 |