UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00097

NEW FREAKOUT MALWARE TARGETS LINUX

DATE ISSUED: 26th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

FreakOut malware is targeting Linux devices and adding infected endpoints to a botnet designed to be used for cryptomining and DDoS attack operations.

BREAKDOWN

The new malware uses port scanning, information gathering and data packet and network sniffing to seek out vulnerable Linux machines and infect them to harness their resources for attack purposes. The specific products sought out are TerraMaster TOS with versions prior to 4.2.06 (CVE-2020-28188), Zend Framework in versions higher than 3.0.0 (CVE-2021-3007) and the Liferay Portal 7.2 CE GA2 version 7.2.1 and above (CVE-2020-7961). Post exploitation, the attacker will attempt to run Python 2 which went out of support (reached end of life EOL) at the end of 2020, to run a script to carry out data and information gathering and send it back to the C2 and attempts to move laterally across the network. While most of these attacks thus far have been carried out overseas, it is recommended to take this opportunity to assess systems and apply security patches where necessary.

REMEDIATION STEPS

- Install patches available for all products listed above from the appropriate vendor
- Take any Linux device that may be vulnerable offline until remediation work can be carried out.
- Use Intrusion Prevention Systems (IPS) and monitor network traffic for abnormal activity and scan devices using anti-malware endpoint protection to detect and remediate infected devices where possible.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/linux-attack-freakout-malware/163137/
Checkpoint	https://blog.checkpoint.com/2021/01/19/linux-users-should-patch-now-to-block-new-freakout-malware-which-exploits-new-vulnerabilities/
Security Week	https://www.securityweek.com/new-freakout-malware-ensnares-linux-devices-botnet
Cyware	https://cyware.com/news/new-freakout-malware-actively-targeting-linux-devices-e94d46d2