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

CYBER GUIDANCE ISSUE 0272

NEW GOLANG BASED DATA WIPING MALWARE

DATE ISSUED: 30th January 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Cybersecurity firm ESET have found a new destructive data wiper malware used in cyberattacks attacks against Ukraine. A data wiper is malware that intentionally destroys data on a device to make the data unrecoverable and can also affect the operating system preventing it from functioning correctly going forward.

BREAKDOWN

According to ESET, the new data wiper malware is detected as SwiftSlicer that corrupt crucial files used by the Windows Operating System. It is coded in GoLang programming language making it compatible with multiple platforms and hardware. The malware is attributed to Sandworm, a nation state hacking group linked to Russia. It is distributed via the network using the Group Policy Object (GPO) – a set of rules that allows admins to configure operating systems, apps, and other user settings in an Active Directory (AD) environment. Once launched the malware deletes shadow copies (used for backup and restoration) and overwrites critical files from the Windows system directories - such as drivers, and the AD database. Specifically targeting the system drive indicates that this wiper aims to bring down an organisation's entire Windows domain. It overwrites data using 4096 bytes blocks that are filled with random bytes. The system is rebooted after the wiper destructs the data. Wipers are also commonly used in Ransomware style attacks.

REMEDIATION STEPS

- Use and update anti-malware detection and remediation software on all endpoint devices.
- Perform Regular Backups: A strong Disaster Recovery plan can minimize both data loss and downtime.
- Regularly patch operating systems and software to ensure the latest security updates are installed
- Check out our Ransomware Defence Strategy Guide for more tips on how to secure your environment

REFERENCES & RESOURCES

Bleeping Computers https://www.bleepingcomputer.com/news/security/hackers-use-new-swiftslicer-wiper-to-destroy-windows-domains/