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

CYBER GUIDANCE ISSUE 00184

CHAOS MALWARE – WIPER OR RANSOMWARE?

DATE ISSUED: 16th August 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	PRESENTLY UNKNOWN	EASY

OVERVIEW

An 'under-construction' malware dubbed "Chaos" has been discovered which has been under development since June and v5 is set to be released into the wild very soon. The malware is said to be a ransomware but after analysis by researchers, it seem to be a wiper instead.

BREAKDOWN

While this malware hasn't yet been released, the developers appear poised to release very soon as iteration 5 of the software is currently under development. In the beginning, the malware looked poised to be a .NET variant of the Ryuk ransomware, however researchers from Trend Micro have discovered that in fact it appears to behave more like a destructive Trojan. Rather than encrypting files like malware normally would, Chaos v2 replaces files with random bytes and encodes these with Base64, making the file unrecoverable. It drops a ransomware note however the unrecoverable files means victims are not incentivised to pay. Chaos v3 became more akin to ransomware adding AES/RSA encryption functions with a feature for operators to add a proprietary file extension and change their victim's desktop background to customise their attacks. A worming function allows the malware to spread to all drives found on the affected system potentially allowing the malware to shift to removable drives or escape air-gapped systems. The malware elevates privileges and searches for backups and shadow volume copies as well as files to destroy and disables the Windows recovery mode. Although this malware is not yet in circulation, Proof of Concepts (PoCs) are available suggesting it won't be long now.

REMEDIATION STEPS

- Download your copy of our free Ransomware Defence Strategy Checklist to ensure your business/organisation is prepared for ransomware attacks.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/chaos-malware-ransomware-wiper/168520/