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

CYBER GUIDANCE ISSUE 00193

LOCKFILE UNIQUE ENCRYPTION AVOIDS DETECTION

DATE ISSUED: 6th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A new ransomware variety known as LockFile has been discovered in the aftermath of the ProxyShell Microsoft Exchange Server vulnerabilities which not only employs tactics from other ransomware gangs but also uses intermittent encryption to avoid detection.

BREAKDOWN

Discovered by Sophos, this new ransomware encrypts every 16bytes of a file which makes it difficult to detect for most ransomware protection solutions. This is because statistically the encrypted document appears similar to the original unencrypted file. Entry is gained through the exploitation of unpatched ProxyShell vulnerabilities (see Cyber Guidance 0114) and the PetitPotam NTLM Relay attack (see Cyber Guidance 0178) to gain control of the domain. LockFile does not connect to a C2 server to assist with further hiding its activities and uses memory mapped in I/O (Input/Output) for encryption similar to WastedLocker and Maze ransomware to reduce disk activity that might set off alerts. While LockFile is not the first to use partial encryption (LockBit 2.0, DarkSide and BlackMatter do this too) the intermittent nature of the encryption is what sets it apart. Rather than encrypting the first few blocks, the malware encrypts every second block making a text document remain partially readable, making it able to elude some ransomware detection tools. A full breakdown of the attack sequence can be viewed in the resources provided.

REMEDIATION STEPS

- Download Unisphere's Ransomware Defence Strategy Checklist to check your current ability to withstand or recover from a ransomware attack.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/lockfile-ransomware-avoid-detection/169042/
Sophos https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/