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

CYBER GUIDANCE ISSUE 00087

2021 NEW BABUK LOCKER RANSOMWARE

DATE ISSUED: 12th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A new ransomware strain for the new year, Babuk locker is a fairly standard ransomware but with a twist – it takes advantage of an abuses the Microsoft Windows Restart Manager.

BREAKDOWN

While many of the features of the ransomware could be considered "run of the mill," it boasts some novel features which have assisted in attack success. It is unclear how this ransomware is being distributed and presents as a 32-bit .exe file with no notable obfuscations. Once infected, the system's monitoring processes are disabled, shadow copies of files are deleted, and running applications are closed in order to encrypt their associated files – if the files are already in use by an application the encryption will fail. Babuk takes advantage of recursion techniques and multi-threading, which is nothing new, however, using the Windows Restart Manager to close active applications and services ensures that nothing will prevent the malware from opening - similar to Conti and ReEvil ransomwares. The encryption mechanism incorporates SHA hashing, ChaCha8 and Elliptical-Curve Diffie Hellman. The attacker uses their private key to randomly generate a shared secret key and a victim public key for decryption making decryption impossible without the randomly generated private key.

REMEDIATION STEPS

- Ensure your organisation has an up-to-date Business Continuity, Disaster Recovery & Incident Response plan
- Check your backup reports and routinely test response and restore procedures.
- Create archive backups and ensure they are updated at regular intervals, using varied backup types and have at least one copy store offsite and offline.
- Check network device security, access control permissions and open ports and monitor for abnormal activity.
- Implement security-in-depth/defence-in-depth multi-layered protections and scan devices using anti-malware.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/ransomware-babuk-locker-large-corporations/162836/
Bleeping Computer: https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/