U UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 0277

VMWARE ESXI SERVER RANSOMWARE EVOLVES

DATE ISSUED: 13th February 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

The FBI and CISA have released a recovery script for the global ESXiArgs Ransomware campaign targeting VMware ESXi servers, but the ransomware has since been updated to elude attempts at remediation, evolving in a way that makes previous detections method ineffective.

BREAKDOWN

As previously released by French Computer Emergency Response Team (CERT-FR), the ESXiArgs Ransomware targeted more than 3,800 VMware ESXi servers globally. The ransomware encrypts configuration files on vulnerable virtual machines, making them potentially unusable. The threat actors then ask for a ransom to release the encrypted files. Recently the Cybersecurity and Infrastructure Security Agency (CISA) and FBI released a recovery script which creates new configuration files for the machine. However, a new ESXiArgs ransomware has emerged with the capability to encrypt huge amounts of data in large files making it difficult to recover the effected VMware ESXi virtual machines. The ransom note has also been changes to no longer display the bitcoin address to make it more difficult for security researchers to track ransom payments. The newer version is also capable of encrypting files even if the openSLP port (427) is disabled. See Cyber Guidance Issue 0274 for more information.

REMEDIATION STEPS

- Update the VMware ESXi servers with the latest security patch.
- Monitor network activity for any suspicious or anomalous behaviour.
- Maintain regular and robust offline backups.
- Check out our Ransomware Defence Strategy Guide for more tips on how to secure your environment.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/paypal-and-twitter-abused-in-turkey-relief-donation-scams/
CISA	https://www.cisa.gov/uscert/ncas/current-activity/2023/02/07/cisa-releases-esxiargs-ransomware-recovery-script