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

CYBER GUIDANCE ISSUE 00210

VMWARE ESXI SERVERS ENCRYPTED BY PYTHON SCRIPT

DATE ISSUED: 11th October 2021

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

OVERVIEW

An attack group has launched a new ransomware in the form of a short Python code that takes less than 3 hours to fully encrypt a system, and have set their sights on ESXi and Virtual Machines (VMs).

BREAKDOWN

With such precision targeting, Sophos have stated that this ransomware is one of the fastest to take down its victims. Python comes pre-installed on the ESXi Linux-based bare-metal hypervisor that installs easily onto VMs so it makes sense that the group chose this language to script their attack. Researchers also noted that this brand of ransomware creates a new set of keys to encrypt files each time it is run, which could be multiple times across each targeted datastore in a single environment and this behaviour is considered unusual. Thereafter the script then encodes a copy of these secret keys using the public key. The Python script gathers a list of files, for each file it then generates a "unique, 32-byte random code it calls the aesky which is used to encrypt the file into the /tmp path. This aesky is prepended to the encrypted file, adds a new file suffix to the name, overwrite all file contents and replaces it with the word "fuck" thereafter the original file is then deleted. The new encrypted version is moved from the /tmp back to the original file location.

REMEDIATION STEPS

- Always use unique passwords across all accounts that are long and difficult to guess – such as a passphrase.
- Enable MFA on all services wherever possible and enforce its use on administrative accounts.
- Turn off Shell when not in use.
- Limit access to your VM environments on a need-to-know or least-access principle.

REFERENCES & RESOURCES

Sophos Labs https://news.sophos.com/en-us/2021/10/05/python-ransomware-script-targets-esxi-server-for-encryption/
Threatpost https://threatpost.com/vmware-esxi-encrypted-python-script-ransomware/175374/