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

CYBER GUIDANCE ISSUE 0270

PY#RATION RAT USES PHISHING TO STEAL INFO

DATE ISSUED: 30th January 2023

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

OVERVIEW

A new Python-based Remote Access Trojan (RAT) uses phishing emails to gain complete control over the comprised systems. The malware uses WebSocket protocol to establish a connection with the Command-and-Control (C2) server by using commonly open ports 80 and 443 to exfiltrate sensitive information.

BREAKDOWN

PY#RATION malware named by Securonix cybersecurity firm attacks start with a phishing email which consists of a password protected ZIP file containing two shortcut .LNK files disguised as front and back images of a Driver's License. When a user clicks on the .LNK file malicious code is executed in stealth mode to contact the C2 and download two .TXT files that are subsequently renamed to .BAT files. When the code is launched additional batch file 'CortonaAssist.bat' is established into the user's directory. The use of the file name as "Cortona", Microsoft's virtual assistant, helps the malware to pass as a system file and remain undetected. The malware is coded in Python which converts the code into Windows executables – including all libraries. The most recent version of the malware has a layer of fernet encryption (128bit AES) which helps it to evade detection. The malware has a capability to extract passwords and cookies from web browsers, steal data from clipboard, detect anti-virus tools running on the host, and execute shell commands.

REMEDIATION STEPS

- Educate users on how to spot phishing emails, what to do with them, and where to report them.
- Use anti-malware detection and remediation software on all endpoint devices.
- Use phishing simulation exercises to assist with user awareness training.
- Monitor network activity for any suspicious or anomalous behaviour.
- Use Secure Email Gateway and SPAM filters to prevent suspicious emails from reaching users.

REFERENCES & RESOURCES

Bleeping Computers https://www.bleepingcomputer.com/news/security/new-stealthy-python-rat-malware-targets-windows-in-attacks/