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

CYBER GUIDANCE ISSUE 00137

WEB FORMS USED TO CIRCULATE ICEDID MALWARE

DATE ISSUED: 19th April 2021

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

OVERVIEW

Attackers are using web-based forms such as "Contact Us" and Google Forms URLs in an effort to evade email spam filters and dispense the IcedID malware.

BREAKDOWN

Using fear as a motivator, attackers are sending messages to organisations with legal threats such as copyright infringements by filling out their web-based forms and sending links to items of evidence. In reality, the link leads the victim to a Google page that automatically downloads the payload for IcedID – also known as BokBot, which is a notorious information exfiltration malware and loader for other malware – in this case Cobalt Strike. The attacker has been seen to use aliases including Mel, Melanie, Meleena and email addresses including mphotographer550@yahoo.com or megallery736@aol.com. Researchers have reverse engineered the ZIP file and discovered a heavily obfuscated .JS file which is executed by WScript, creating a shell object to launch PowerShell and download a .DAT file as the IcedID payload. The .DAT is run via rundll32 and information gathering commences. The attacker has a secondary attack chain in place for if the Google site is removed.

REMEDIATION STEPS

- Educate all users on social engineering attacks and the various points of entry attackers will attempt to exploit.
- Use URL filtering to prevent users from access known malicious or suspicious websites.
- Use Endpoint protection such as Next Generation Anti-Malware to detect and respond to anomalous behaviours.
- Prevent running of PowerShell and executable files for all users other than those which might interfere with their normal work duties.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/attackers-target-proxylogon-cryptojacker/165418/
Sophos https://news.sophos.com/en-us/2021/04/13/compromised-exchange-server-hosting-cryptojacker-targeting-other-exchange-servers/
https://github.com/sophoslabs/IoCs/blob/master/PUA-QuickCPU_xmr-stak.csv