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

CYBER GUIDANCE ISSUE 00117

OBLIQUE RAT HIDES WITH STEGANOGRAPHY

DATE ISSUED: 8th March 2021

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

OVERVIEW

Users who click on malicious email attachments could be redirected to compromised websites hiding the ObliqueRAT Remote Access Trojan hidden within images on the site using steganography.

BREAKDOWN

First discovered in 2019, this malware is circulated through emails originally containing Microsoft Office documents with malicious code embedded within. Now users who click on the attachments are being redirected to malicious websites that hide the malware in images using steganography techniques to download the payload and exfiltrate system and other sensitive information from victim's systems. The modification to the malware comes as a step to avoid detection by traditional signature-based anti-virus and detection mechanisms. This obfuscation occurs through a seemingly benign bitmap image file (BMP) that contains both legitimate data and malicious executables. A file shortcut is also installed to create persistence to initiate upon the computer's reboot.

REMEDIATION STEPS

- Use endpoint protection and remediation anti-malware software to protect individual hosts.
- Use behaviour monitoring and network detection and remediation software and/or devices to detect, alert on, and isolate anomalous network behaviour.
- Educate users on the dangers of malicious email attachments and how they should handle suspicious emails.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/website-images-obliquerat-malware/164395/
Security Affairs https://securityaffairs.co/wordpress/98290/malware/obliquerat-targets-govn-entities.html
Cisco Talos https://blog.talosintelligence.com/2020/02/obliquerat-hits-victims-via-maldocs.html