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

CYBER GUIDANCE ISSUE 00150

FAKE RANSOMWARE STRRAT SPREAD BY EMAIL

DATE ISSUED: 31st May 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

The StrRAT discovered by Microsoft Security Intelligence (MSI) is being distributed in an email campaign where it poses as Ransomware, taking control of a system, stealing credentials and changes file names to appear as though it is a ransomware attack – but doesn't actually carry out encryption of files.

BREAKDOWN

Posing as Ransomware, this Java-based Remote Access Trojan (RAT) is being distributed in a mass email campaign by attackers which allows them to take remote control of infected systems – running remote command and PowerShell, steal browser credentials, activity and applications logs, and user keystrokes. The toolset also has the capability to download a secondary payload in order to distribute other malware. Filenames are changed to display the suffix ".crimson", however they do not become encrypted, they are only made to appear to be. The email campaigns are being distributed using compromised email accounts and on occasions the emails have been seen to contain the subject line "Outgoing Payments" or "Accounts Payable Department" or "Supplier" and a series of numbers. The payload is attached in a PDF file that is activated when clicked by a user, connecting the device to the Command and Control (C2) server. The version of the RAT observed in these attacks is 1.5 and is "notable more obfuscated and modular than previous versions."

REMEDIATION STEPS

- Enable Microsoft 365 Defender and ensure it is up to date.
- Use next-gen anti-malware on endpoint devices to block the download of malware.
- Use Secure Email Gateways and filtering to prevent malicious emails from reaching your users.
- Educate users on social engineering and phishing emails and what to do in your organisation if they come across and email they deem to be suspicious.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/email-campaign-fake-ransomware-rat/166378/
GitHub https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/commit/dc6037ccc9b2e62d1544b99394daf5a86540bb08