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

CYBER GUIDANCE ISSUE 00249

EMOTET SPREADS THROUGH MALICIOUS EXCEL FILES

DATE ISSUED: 1st March 2022

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Emotet has been a hot favourite for attackers throughout 2021 and is looking to follow through in 2022. While it is distributed in many different ways, the most recent attack of note spotted by Palo Alto has the malware hidden in Microsoft Excel files delivered via social engineering emails that harbour an obfuscated Excel 4.0 macro.

BREAKDOWN

Emotet is known for it's high infection rates and continuous ability to modify and change characteristics and attack vectors to evade detection and this new attack is just another feather in the cap. The new attack chain "reveals multiple stages with different file types and obfuscates script before arriving at the final payload." The latest vehicle is an encrypted .ZIP file – with the password contained in the email body which holds a Microsoft Excel document. This is laced with a macro which downloads and executes an HTML application upon activation. This application then uses PowerShell to connect to the command and control (C2) server before executing a second command to retrieve the final Emotet payload and execute it. From the sample analysed by Palo Alto, the second script contained 14 URLs to try to ensure the malware is successfully downloaded – in case one or more is shut down by authorities. Emotet is favoured among hackers as a means to deliver other malware such as ransomware and establish a wide-reaching botnet or backdoor for persistence. The malicious content is only able to execute on a device that has macros enabled. Microsoft has committed to disabling macros by default in some applications to prevent malware delivery via this means and add additional layers of protection, rather than a single click.

REMEDIATION STEPS

- Disable macros by default and only enable editing on documents from trusted sources
- Educate users on how to spot phishing and social engineering emails and what to do with them in your organisation.
- Avoid opening ZIP files and attachments unless they are from a known trusted source and are expected.

REFERENCES & RESOURCES

Palo Alto https://unit42.paloaltonetworks.com/new-emotet-infection-method/
Threatpost https://threatpost.com/emotet-spreading-malicious-excel-files/178444/ZDNet