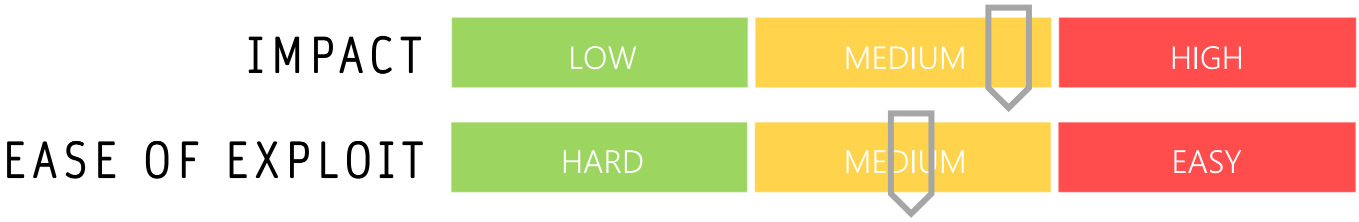
UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00139

PHISHING SCAM USES .TXT ATTACHMENTS

DATE ISSUED: 27th April 2021



OVERVIEW

A new email phishing attack has been seen to use a secre-stealing Trojan known as Poulight through txt file attachments with the title “ReadMe_knl.txt” displayed with the Notepad icon to make it seem more legitimate.

BREAKDOWN

Opening the attachment prompts the execution of the code hidden within the file through a PowerShell command customized to the target or victim to download https[:]//iwillcreatemedia[.]com/build.exe that is set as a hidden attribute, and then proceed to run the executable file. This customisation is determined in the preliminary stages of the attack where the Trojan will perform an environmental inspection to determine wht operating system and download the appropriate configuration of the malware executable. It will record user names, machine names, system names and other machine information including any anti-malware software in use and graphics card and processor information, writing the information to a file for exfiltration. Following this, it will gain a list of currently running processes and decode and run the executable malware. Poulight then proceeds to download all information relating to current processes, any stored credentials and any BitCoin wallet information and send it off to the Command and Control Center.

REMEDIATION STEPS

- Use SPAM and Secure Email Gateway filtering to prevent malicious emails from reaching your user.
- Prevent users from running executable files on their devices.
- Use URL filtering to prevent access to known malicious URLs.
- Educate users to raise awareness around social engineering and phishing emails and what to do within your organisation if they suspect an email is malicious.

REFERENCES & RESOURCES

360 Security	https://blog.360totalsecurity.com/en/a-txt-file-can-steal-all-your-secrets/
KnowBe4	https://blog.knowbe4.com/heads-up-new-phishing-attack-with-.txt-attachment-can-steal-all-your-secrets