Security Advisory
Volume 2016-53-1

Ransomware – Locky

Summary

We want to alert our customers to an influx in ransom-based malware being spread through email spam campaigns. The new variant, nicknamed Locky, uses document-based macros and phishing techniques to be successful. Locky comes in the form of an email attachment masquerading as a payment invoice or tracking document. When opened it will prompt the user to enable macros which will run the code, downloading and running the malicious executable. The executable will begin to encrypt data, rendering it unusable unless the company pays a ransom for the decryption key.

Detailed Information

Users receive an email with a subject line that reads "ATTN: Invoice J-XXXXXXXX" with a .doc attachment named after the subject and a message that reads *"Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice"*. Upon opening and running the macro script a file is retrieved and stored in the %Temp% folder. Once executed it encrypts files on the victim's workstation and on accessible network shares. Locky, like CryptoWall, renames files making them harder to retrieve, then deletes Volume Snapshot Service (VSS) files, and appends ".locky" to encrypted files. The wallpaper of the infected workstation will be changed to instructions on how to purchase the decryption key. Prices for the key range between BTC 0.5 ($220) to BTC 1.0 ($440). There is currently no known way to decrypt files encrypted by Locky.

Preventive Actions

Ensure critical business files are backed up regularly and not accessible with user credentials.
Disable the running of Macros except in trusted locations.

1) Go to the Group Policy Setting in the Trust Center
2) Select "**Disable all except digitally signed macros**"
3) Set a shared folder for Macros to run in User Configuration/Administrative Templates/Microsoft Office XXX 20XX/Application Settings/Security/Trust Center/Trusted Locations
4) Instruct users to run all required macros in shared folders allowed in "Trusted Locations"

Provide user awareness training in recognizing and reporting phishing attempts

Corrective Actions

Remove the malware and restore files from back-up.

If business critical documents have been encrypted but not backed up, the only known recovery option at this time is to pay the ransom. While each company must decide whether this is an acceptable practice, affected companies have been able to recover critical business files through this action.

Additional References

Sophos "Locky" Ransomware
Palo Alto Networks Research Center - "Locky"
Hospital Pays 17k for Crypto Key
Microsoft Technet - Trusted Locations Office 2013
FBI - Ransomware on the Rise