Windsor Day 4: Ransomware

Disclaimer: Cyber Range does not allow file transfers so all information is stored as screenshots As well, with day 4 it's the last day at the range and we ran too low on time to document everything we should have.

PRE-ASSESSMENT/RESEARCH

- Types of Cyber insurance
    - First-party coverage — the insurer pays the organization's expenses incurred directly due to a security breach.
    - Third-party coverage — this policy covers damages or settlements the organization must pay due to suits or claims for injuries resulting from the organization's actions or failure to take action.
    - Privacy Liability Coverage
    - Network Security
    - Network Business Interruption
    - Errors and Omissions Coverage
    - Media Liability Coverage
- Things not usually covered by cyber insurance
    - Poor security processes
    - Prior breaches
    - Human error
    - Insider attacks
    - Pre-existing vulnerabilities
    - Technology system improvements

Ransomware attacks can vary in severity, and the impact of a ransomware attack depends on several factors, including the specific variant of ransomware, the target's preparedness, and the attacker's objectives. Severity levels can be categorized roughly as follows:

Low Severity:

Minor inconvenience: Some ransomware attacks may not have a significant impact on the victim's operations. For example, the ransomware may target less critical data or systems, resulting in minimal disruption.

Moderate Severity:

Partial data loss: In some cases, ransomware may encrypt critical data, causing disruptions and potential data loss. However, the victim organization may have backups or be able to recover the data without paying the ransom.

High Severity:

Major disruption: High-severity ransomware attacks can cripple an organization's operations. They may encrypt critical systems, making them inaccessible and causing significant downtime. Recovering from such an attack can be costly and time-consuming.

Critical Severity:

Widespread damage: Some ransomware variants are designed to spread rapidly within an organization's network, affecting numerous systems and causing extensive damage. These attacks can lead to severe financial and reputational consequences.

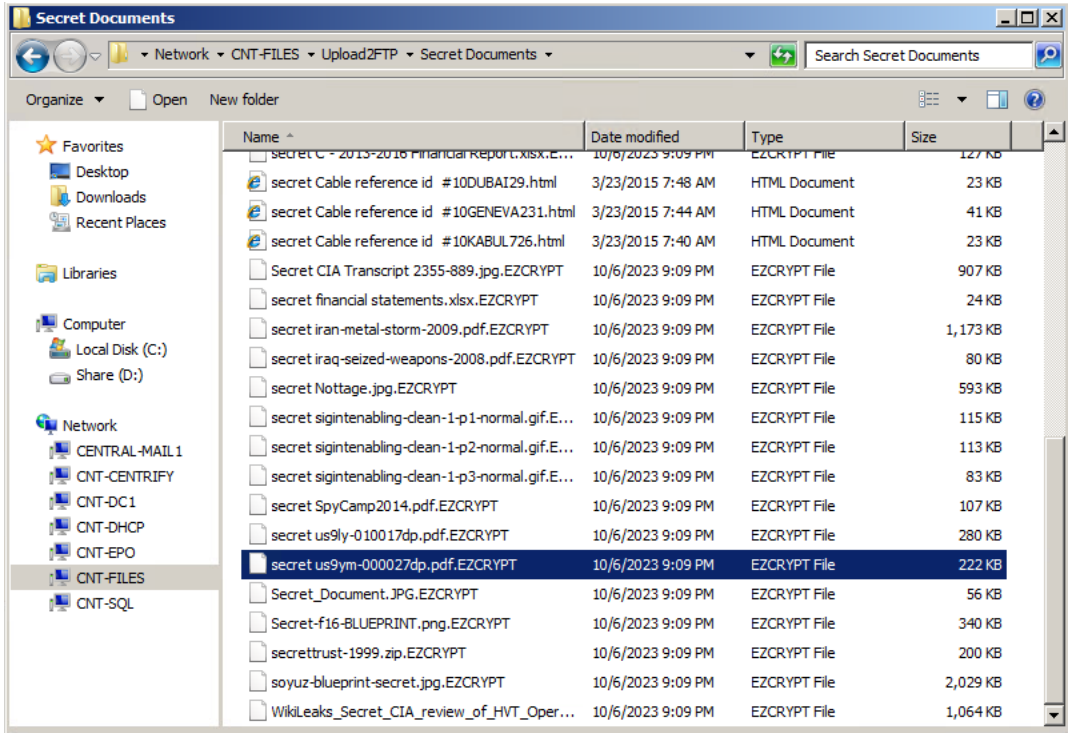
Catastrophic Severity:

System-wide or organizational collapse: In rare cases, ransomware attacks can lead to the complete breakdown of an organization's operations. This might occur when essential systems, including those related to safety or critical infrastructure, are compromised.

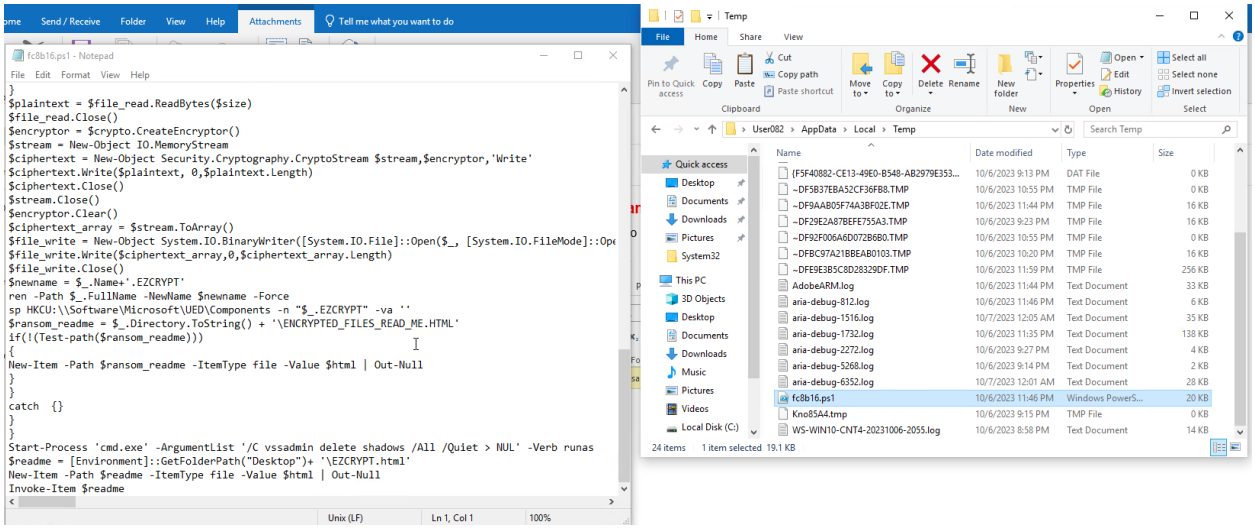
READ THIS!!! ----->
https://www.repairwin.com/how-to-remove-locky-virus-and-restore-locky-files/

21:14 - Discovered ransomware message on CNT-1,2,4
21:29 - FTP server has mapped drive named “secret documents” (CNT-FILES 192.168.200.6).

EZCRYPT file type found on CNT FTP File Server



.ps1 file found in User082 temp folder



Brief Notes

We are in the midst of a ransomware attack, the scope so far is not looking great for us, with access in our FTP server, or our file server, including our secret documents folder. Thankfully our SQL server and Domain Controller so far seems unaffected. So far we believe none of our customer PHI or PCI/DSS has been compromised. However with ransomware in our FTP server and inside our User Segment our employees and business information has been acquitted. 100k-150k.

What files are being held hostage.
Only Upload2FTP files are encrypted
Secret CIA Guide
Legend of Zorro Strategy
Secret Iran Metal Storm
Secret Iraq seized weapons
WikiLeaks Secret CIA HVT Operations

What information is being held on user workstations
5 sentence summary for customers.

Personal - All documents uploaded to the Secret Documents folder on the FTP server
Customer - No customer data as of right now
Scope - Upload2FTP/FTP file server and all CNT workstations

Initial vector - CNT-4/User082 clicked on ransomware link via phishing email
Lateral movement - High probability, quarantine CNT workstations and FTP server
Ransomware encryption - .Locky
Quarantine exploration - Unmap FTP drives, should quarantine CNT-4 and FTP server

We can download files sent through outlook to John Smith from User 082

User082 clicked on phishing email sent by John Smith
User082 sending all encrypted files to John Smith

Only Upload2FTP files are encrypted

Seemingly targeting ex-military COO rather than the rest of the company.

End statement - We recommend we do not pay the ransom, as John Smith has copies of all the data pertaining only to files our COO was never allowed to share on the company network. With less than 100k in our company bank account and a ransom of 100k, which we could bargain to what we do have. This is a case of the livelihood of the COO vs the entirety of the company.