T2022_14 What organizations should know about Cerber Ransomware (15th July 2022)

What is Cerber Ransomware?

Cerber, also known as CRBR Encryptor, is a ransomware-type malware that infects computers and encrypts a variety of file types, such as .jpg, .doc, .raw, .avi, etc. Each encrypted file created by Cerber receives the .cerber suffix, while some variants add .cerber2 or .cerber3.

Be aware that some ransomware variations add arbitrary file extensions, such as ".ba99," ".98a0," ".a37," ".a563," etc. Additionally, some variations of this ransomware give encrypted files a .beef extension. When an intrusion is successful, Cerber demands a ransom to unlock the files.

According to the statement, “if the ransom is not paid within the specified period (seven days), the ransom would double”.

How it works

Cerber is clear-cut as far as ransomware goes. By clicking on malicious adverts posted on otherwise trustworthy websites, phishing emails, or infected websites, victims unintentionally download ransomware onto their devices.

During encryption, Cerber creates three different files (#DECRYPT MY FILES#.txt, #DECRYPT MY FILES#.html, and #DECRYPT MY FILES#.vbs) containing step-by-step payment instructions (never variants use "_READ_THI$_FILE_.hta", "_HELP_HELP_HELP_random.hta", "_READ_THIS_FILE.hta", “_HELP_HELP_HELP_random.jpg", _R_E_A_D___T_H_I_S___random_.txt, _R_E_A_D___T_H_I_S___random_.hta and “_!!!_README_!!!_random_.hta”, “_!!!_README_!!!_random_.txt” files) in each folder containing the encrypted files.

According to the message contained in these files users can only decrypt their data using a decryptor created by cybercriminals, known as "Cerber Decryptor." Your papers, databases, and other essential files have been encrypted! played over the computer speakers when the VBScript in the #DECRYPT MY FILES#.vbs file is performed. After encrypting files, Cerber ransomware changes the desktop wallpaper.

Mitigation

The following are some steps users and administrators can take to reduce the risk of infection by Cerber ransomware:

- Use multifactor authentication
- Require multifactor authentication to remotely access networks from external sources.
- Implement network segmentation and filter traffic
- Implement and ensure robust network segmentation between networks and functions to reduce the spread of ransomware. Define a perimeter network that eliminates unregulated communication between networks.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses.
- Enable strong spam filters to prevent phishing emails from reaching end users. Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments. Filter emails containing executable files to prevent them from reaching end users.
- Implement a URL blocklist and/or allowlist to prevent users from accessing malicious websites.

Scan for vulnerabilities and keep software updated.

- Set antivirus/antimalware programs to conduct regular scans of network assets using up-to-date signatures.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner. Consider using a centralized patch management system.

Apply application controls.

- Investigate any unauthorized software, particularly remote desktop or remote monitoring and management software.
- Implement application allow listing, which only allows systems to execute programs known and permitted by the organization's security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs.
- Implement execution prevention by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.

Implement endpoint and detection response tools.

- Endpoint and detection response tools allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.

Limit access to resources over the network, especially by restricting RDP (Remote Desktop Protocol).

- After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources, and require multifactor authentication.

Secure user accounts.

- Regularly audit administrative user accounts and configure access controls under the principles of least privilege and separation of duties.
- Regularly audit logs to ensure new accounts are legitimate users.

Remediation

It is never advised to pay the attackers to decrypt your files, chances are they will take the ransom and vanish. If it is suspected that you have been infected by Cerber ransomware the following steps are recommended for isolation and remediation:

STEP 1. Isolate the infected device(s):

i. If logged into any cloud storage, be sure to log out or disconnect from same.
ii. Disconnect the infected device from the network and the internet. You may even go as far as disabling all Network Interface Cards. You can follow the link below for instructions on disabling your Network Interface Card. https://www.minitool.com/news/how-enable-disable-network-adapters-win10- 003.html
iii. Disconnect all External Storage devices

STEP 2. Reimage the infected device(s). You can follow the link below for instructions on reimaging your device.

https://www.ubackup.com/articles/how-to-reimage-a-pc-4348.html

STEP 3. Restore a clean copy of files from backups. You can follow the link below for instructions on how to backup and restore your data.

https://www.pcmag.com/how-to/how-to-back-up-and-restore-an-image-file-of-windows-10

References

- Meskauskas, Tomas. (03 December 2021). *Cerber Ransomware*. Retrieved from PC Risk. https://www.pcrisk.com/removal-guides/9842-cerber-

ransomware

- Belcic, Ivan. (27 February 2020). *Cerber Ransomware: Everything You Need to Know*. Retrieved from Avast. https://www.avast.com/c-cerber