FILESLACK – RANSOMWARE

(Incident Response Plan)

Document

1. Overall Summary

FileSlack Ransomware is an encryption-based ransomware Trojan that first emerged in **February 2019**. This malicious software is designed to infiltrate systems, encrypt files using a **strong encryption algorithm**, and render the victim's data completely inaccessible. Once the files are encrypted, the attackers demand a **ransom payment** in exchange for the decryption key, exploiting the victims' desperation to regain access to their valuable data.

2. How FileSlack Ransomware Works

The FileSlack Ransomware operates similarly to other ransomware threats but has its unique characteristics:

1. **Infiltration:** The ransomware is typically distributed via phishing emails, malicious attachments, compromised websites, or software vulnerabilities. It may also be delivered via exploit kits or infected USB drives.
2. **Encryption Mechanism:** Once the FileSlack Ransomware infects a system, it identifies and encrypts files such as documents, images, videos, databases, and other critical data using a strong encryption algorithm. The encryption process ensures that the files are inaccessible without the decryption key held by the attackers.
3. **Ransom Demand:** After encrypting the files, the ransomware displays a ransom note, often instructing the victim to pay a specific amount of cryptocurrency (e.g., Bitcoin) to a designated wallet address. The ransom note typically threatens the permanent loss of the data if the payment is not made within a specified time frame.
4. **File Extensions:** Encrypted files may be renamed or appended with a specific extension associated with FileSlack, making it evident that they have been compromised.

3. Impact of FileSlack Ransomware

- **Data Loss:** Victims lose access to critical files, which can result in financial, operational, or reputational damage for individuals or organizations.
- **No Guarantee of Recovery:** Even if the ransom is paid, there is no guarantee that the attackers will provide the decryption key or that the decrypted data will be intact.
- **Propagation Risk:** FileSlack Ransomware may attempt to spread across networked systems, potentially infecting additional machines or servers.
- **Business Disruption:** Organizations may face downtime and operational paralysis, particularly if critical systems or backups are affected.

4. Ransomware Attack Overview

4.1 How attack gets executed:

The **FileSlack Ransomware** is a malicious program that encrypts victims' files and demands a ransom for their recovery. Upon infecting a system, it places a ransom note titled **'Readme_Restore_files.txt'** on the victim's desktop. This note instructs the victim to contact the attackers via email or instant messaging to negotiate payment.

Victims who reach out are typically asked to pay a hefty ransom, often amounting to several hundred dollars or more, using digital currencies such as **Bitcoin**. However, paying the ransom is highly discouraged, as attackers frequently fail to provide the promised decryption keys, leaving victims without their data.

The initial compromise often occurs through the exploitation of vulnerabilities in internet-facing servers, facilitated by open-source frameworks. Once access is achieved, the attackers—linked to **HAFNIUM**—exfiltrate sensitive data to file-sharing platforms such as **MEGA**. HAFNIUM, a threat actor group, primarily operates from leased **Virtual Private Servers (VPS)** within the United States to carry out its operations.

This highlights the importance of promptly patching server vulnerabilities, employing robust endpoint defenses, and maintaining secure data backups to mitigate the impact of ransomware attacks like FileSlack.

4.2 Extensions

FileSlack Ransomware uses a strong encryption algorithm to target the user-generated files found on the infected computer, which may include files with the following file extensions:

.jpg, .jpeg, .raw, .tif, .gif, .png, .bmp, .3dm, .max, .accdb, .db, .dbf, .mdb, .pdb, .sql, .dwg, .dxf, .cpp, .cs, .h, .php, .asp, .rb, .java, .jar, .class, .py, .js, .aaf, .aep, .aepx, .plb, .prel, .prproj, .aet, .ppj, .psd, .indd, .indl, .indt, .indb, .inx, .idml, .pmd, .xqx, .xqx, .ai, .eps, .ps, .svg, .swf, .fla, .as3, .as, .txt, .doc, .dot, .docx, .docm, .dotx, .dotm, .docb, .rtf, .wpd, .wps, .msg, .pdf, .xls, .xlt, .xlm, .xlsx, .xlsm, .xltx, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .ppt, .pot, .pps, .pptx, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .sldx, .sldm, .wav, .mp3, .aif, .iff, .m3u, .m4u, .mid, .mpa, .wma, .ra, .avi, .mov, .mp4, .3gp, .mpeg, .3g2, .asf, .asx, .flv, .mpg, .wmv, .vob, .m3u8, .dat, .csv, .efx, .sdf, .vcf, .xml, .ses, .qbw, .qbb, .qbm, .qbi, .qbr , .cnt, .des, .v30, .qbo, .ini, .lgb, .qwc, .qbp, .aif, .qba, .tlg, .qbx, .qby , .1pa, .qpd, .txt, .set, .iif, .nd, .rtp, .tlg, .wav, .qsm, .qss, .qst, .fx0, .fx1, .mx0, .fpx, .fxr, .fim, .ptb, .ai, .pfb, .cgn, .vsd, .cdr, .cmx, .cpt, .csl, .cur, .des, .dsf, .ds4, , .drw, .eps, .ps, .prn, .gif, .pcd, .pct, .pcx, .plt, .rif, .svg, .swf, .tga, .tiff, .psp, .ttf, .wpd, .wpg, .wi, .raw, .wmf, .txt, .cal, .cpx, .shw, .clk, .cdx, .cdt, .fpx, .fmv, .img, .gem, .xcf, .pic, .mac, .met, .pp4, .pp5, .ppf, .nap, .pat, .ps, .prn, .sct, .vsd, .wk3, .wk4, .xpm, .zip, .rar.

5. Attack Phases

Once installed, FileSlack encrypts files on the victim's system and appends the ".FileSlack" extension to each affected file (e.g., "1.jpg" becomes "1.jpg.FileSlack"). It also generates a ransom note titled "Readme_Restore_Files.txt", which is placed on the infected system.

The ransom note informs victims that their files have been encrypted and explicitly warns against attempting to modify or repair them, as this could lead to permanent data loss. To recover the encrypted files, victims are instructed to contact the attackers via the email addresses gomer@horsefucker.org or gomersimpson@keemail.me for further instructions.

This emphasizes the need for robust security measures to prevent such infections and highlights the risks of engaging with threat actors in ransom negotiations.

6. FileSlack Ransomware – Distribution Techniques

- **Phishing Emails:** Fraudulent email messages designed to trick users into clicking malicious links or downloading infected attachments.
- **Malicious Websites:** Fake or compromised sites that host malware and infect users who visit or interact with them.
- **Infected Documents:** Virus installation scripts embedded within documents, often disguised as macros, which execute when the document is opened.
- **Compromised Application Installers:** Maliciously altered software installers that deliver malware during installation.

7. Encryption Process

Once all preceding modules have executed, the FileSlack ransomware activates its encryption engine. It likely relies on a predefined list of file type extensions to identify target files for encryption using a robust cipher. The targeted file types often include:

- Backups
- Databases

- Archives
- Images
- Music
- Videos

This ensures that the ransomware focuses on high-value data, maximizing its impact on the victim.

8. Investigation and Removal Process

It is crucial to remove the **FileSlack ransomware** promptly to prevent it from spreading further across your system or network. Removing this ransomware requires a certain level of expertise in dealing with malware. The following steps will guide you in successfully eliminating the infected files and mitigating the threat.

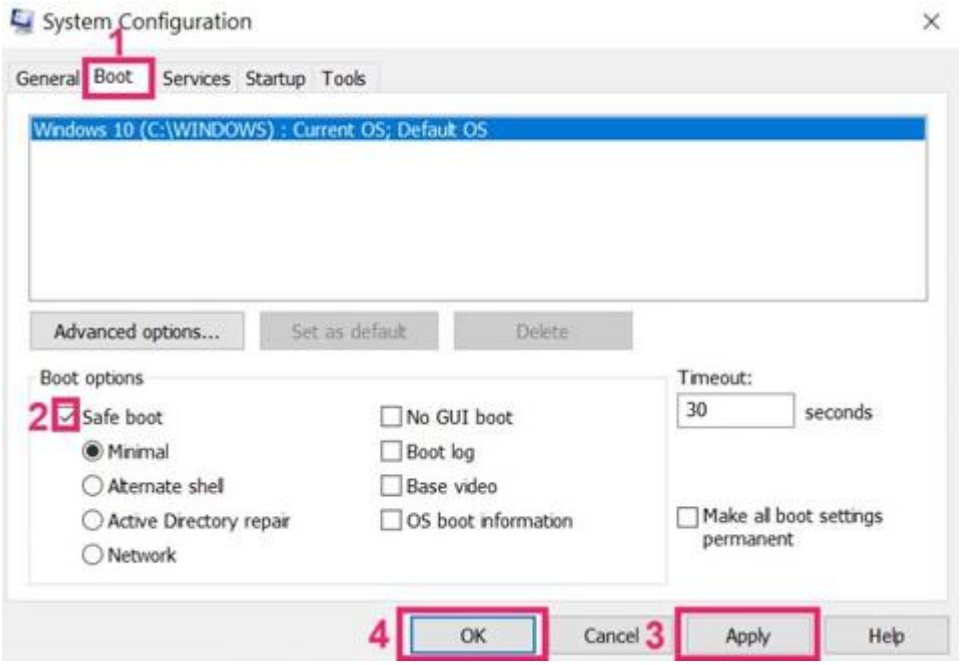
8.1 Existing Scanning Engines

- **Update Antivirus/EDR Solutions:** Ensure that your organization's Antivirus or Endpoint Detection and Response (EDR) tools are updated with the latest threat definitions. Perform a comprehensive scan to detect and remove the ransomware infection.
- **Use Third-Party Antivirus if Needed:** If your current Antivirus or EDR solutions fail to identify the ransomware, deploy a trusted third-party antivirus solution from reputable vendors approved by your organization. Conduct a deep scan to detect and eliminate the threat.
- **Isolate the Infected Machine:** Disconnect the affected system from the network immediately to prevent the ransomware from spreading to other devices or servers.
- **Examine Event Logs:** Review system and security event logs to trace the infection source and understand the scope of the attack.
- **Check for Unauthorized Processes:** Use task managers or EDR tools to identify and terminate any suspicious or unauthorized processes running on the system.
- **Restore from Backup:** If available, restore the infected system to its previous state using a clean backup. Ensure the backup is free of any ransomware traces before restoration.
- **Patch System Vulnerabilities:** Update the operating system and software on the infected machine to close any vulnerabilities that could be exploited by the ransomware.
- **Enable Threat Intelligence Feeds:** Leverage threat intelligence feeds in your security tools to detect indicators of compromise (IoCs) associated with the ransomware.
- **Report the Incident:** Notify your organization’s security team or incident response team about the infection. If required, report the attack to appropriate regulatory

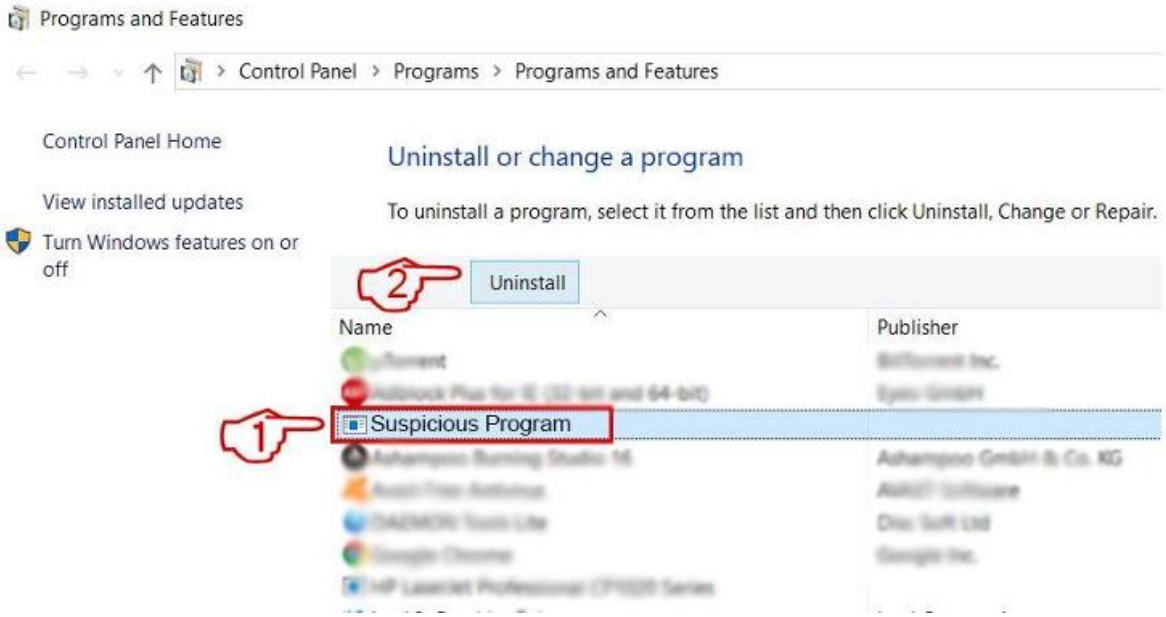
bodies or law enforcement. After performing the above steps, please follow 6.2 without fail for manual verification of Ransomware file extension presence.

8.2 Manual Confirmation & Removal Steps

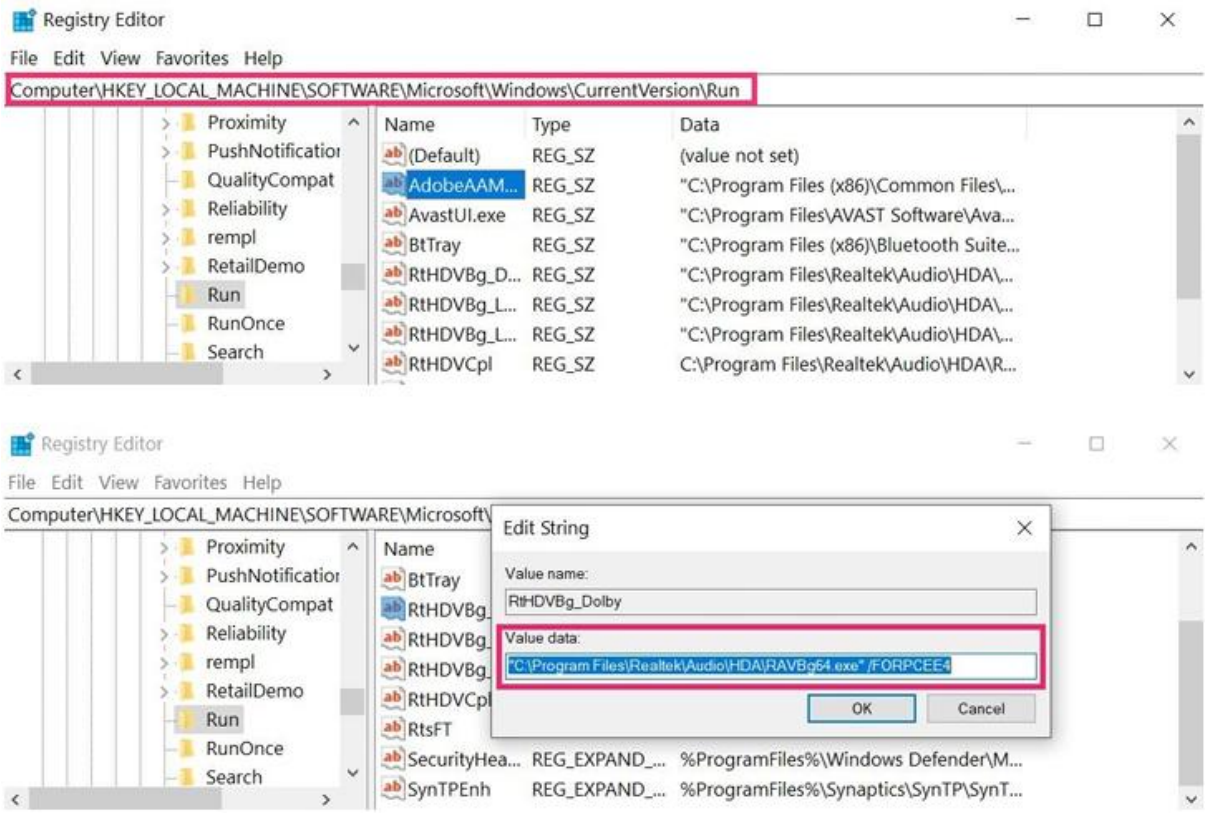
Boot Your PC In Safe Mode → MSCONFIG → Boot" tab. There select "Safe Boot" and then click "Apply" and "OK"



click on "Restart" to go into Safe Mode and goto APPWIZ.CPL and remove unwanted programs if any.



Also, Cross verify the presence of the Registry key in REGEDIT.



9. Immediate Mitigation Steps:

- **Confiscate the Affected Device:** Secure the compromised laptop or endpoint immediately to prevent further unauthorized access.
- **Disconnect from Networks:** Disable the device's connection to the official network and any other connected networks to contain the spread of the ransomware.
- **Log Out of Cloud Accounts:** Sign out of all cloud storage accounts linked to the device to protect online data from being accessed or compromised.
- **Review File Access and Transfers:** Verify whether any files have been accessed, transferred, or sent outside the organization through corporate emails or other channels.
- **Backup Critical Files:** Create a backup of critical files from the device, ensuring the backup is stored securely and scanned for potential infections before use.
- **Avoid Opening Suspicious Files:** Do not attempt to open any files with unknown or suspicious extensions, as they may trigger further ransomware activity.

10. Permanent Remediation Steps

- **Engage with the User:** Conduct an investigation with the affected user to understand how the infection originated, including any suspicious activities or downloads.
- **Analyze Logs:** Examine network and endpoint logs to trace the infection's source and identify the root cause.
- **Implement Remediation Measures:** Based on the identified root cause, take appropriate steps to enhance the organization's security posture and prevent similar incidents in the future.
- **Review Antivirus/EDR Policies:** Reevaluate the organization's Antivirus/EDR policies and procedures to understand why the solution failed to detect or block the infection source. Update configurations as necessary.
- **Format and Rebuild the Endpoint:** After securely backing up files from the infected machine, perform a full system format, reinstall the operating system, and set up all required business applications.
- **Monitor for Lateral Movement:** Check network logs to determine whether any files were transferred to other systems within the organization and take appropriate containment actions.

11. Lessons from FileSlack Ransomware Attacks

The emergence of ransomware like FileSlack highlights the importance of a **multi-layered security approach**:

- Organizations must focus on **prevention, detection, and recovery** mechanisms.
- Businesses should invest in **cybersecurity frameworks** like **Zero Trust Architecture** to limit attack surfaces and prevent lateral movement within networks.
- Incident response teams should conduct regular simulations to prepare for ransomware scenarios.

12. Final Thoughts

FileSlack Ransomware underscores the critical need for vigilance and proactive measures in combating ransomware threats. The evolving sophistication of such attacks demands that individuals and organizations remain prepared, leveraging a combination of technological solutions, employee awareness, and robust data recovery strategies. By adopting a proactive stance, you can ensure that your data remains beyond the reach of cybercriminals.

References:

https://sensorstechforum.com/fileslack-ransomware-remove/

https://www.2-spyware.com/remove-fileslack-ransomware.html