Confidential

From

The Addl. Director General of Police,
CID, Haryana, Panchkula.

To

The Chief Secretary,
Government of Haryana,
Chandigarh.

No. 1150 /HITAC, CID (H), dated 28/06/2021

Subject: Threat advisory regarding Sarbloh ransomware.

Memo.

Kindly refer to the subject sited above

2. The Ransomware is a type of malicious software that cyber criminals use to block victim from accessing their own data. The digital extortionists encrypt the files on victim's computer system and add extensions to the attacked data and hold it "hostage" until the demanded ransom is paid.

29/6/21

3. It has been observed that a new variant of ransomware by the name of 'Sarbloh Ransomware' created by 'The Khalsa Cyber Fauj' outfit is being propagated via email attachments (spearphishing), targeting Government employees and among others especially those departments/bodies that are associated with Political agenda regarding recent farmer protests. This ransomware is dangerous as it does not demand money but it wants the recently enacted Farm laws to be abolished. The latest cyber security and threat intelligence companies have not been able to find any flaws in aforesaid ransomware so there is no remedy available for the same.

DSIT

PSIT 01/07/2021

SSIT

4. In view of the above, it is essential to take extra precautionary measures to prevent computer systems getting infected. This ransomware comes in the form of a word document file attached with an email. As soon as this document is opened on a computer system, the ransomware installs and infects that system and locks all the data of

Office of PS, DITECH
Diary No. (Tel) 2474
Date 2/7/21

Head Com. 1247

CISO

the machine. The removal of ransomware is possible only through formatting that machine leading to important data loss.

5. Recommendations to avoid Sarbloh ransomware are given below:

i) Maintain updated Antivirus software on all systems.

ii) Keep the operating system and third-party applications (MS Office, browsers, browser Plugins) up-to-date via latest patches.

iii) Do not open attachments in unsolicited emails, even if they come from people in personal contact list, and never click on a URL appended in an unsolicited e-mail, even if the link seems legitimate. In cases of genuine URLs, close out the email and go to the organization's website directly through the browser.

iv) Do not enable Macros if prompted by documents received from untrusted sources.

v) Follow safe practices while internet browsing and ensure the web browsers are secured with appropriate content controls.

vi) Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, the backup data should be kept on separate offline devices like external hard drives or USB drives.

vii) Check for the integrity of the information stored in the databases regularly.

viii) Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements (backdoors /malicious scripts.)

ix) If not required, consider disabling PowerShell / windows script hosting.

x) Restrict users' abilities (permissions) to install and run unwanted software applications.

xi) Enable personal firewalls on workstations.

xii) Enabled Windows Defender Application Guard with designated the trusted sites as whitelisted, so that all locations will be open in the container to block the access to memory, local storage, other installed applications or any other resources of interest to the attacker.

xiii) Enable Exploit Protection using EMET (Enhanced Mitigation Experience Toolkit) that includes several client-side mitigation steps. Detailed configuration steps can be seen in https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoftdefender-atp/enable-exploit-protection. Turn on attack surface reduction rules, including rules that block credential theft, ransomware activity, and suspicious use of PS Exec (Portable Software Executible) and WMI (Windows Management Instrumentation).

xiv) Implement strict External Device (USB drive) usage policy.

xv) Employ data-at-rest and data-in-transit encryption.

xvi) Consider installing Enhanced Mitigation Experience Toolkit or similar host-level antiexploitation tools.

xvii) Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf

xviii) Carry out Vulnerability Assessment and Penetration Testing (VAPT), and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors.

xix) Repeat audits at regular intervals.

xx) Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies.

xxi) Refer following CERTIN advisory hyperlink for additional best practices to prevent ransomware attacks
https://www.csk.gov.in/alerts/ransomware.html
CSK: Cyber Swachhta Kendra

6. This threat requires wide publicity and awareness amongst all concerned offices of Haryana Government for better understanding its concept and preventive measures.

28/6/2021

(Alok Mittal)
Addl. Director General of Police,
CID Haryana
Telefax- 0172-2566686
Email: spl-haryana@nic.in