SamSam Ransomware

CERT-In has been reported that new variants of ransomware named "SamSam" is spreading. The modes of spreading this malware is via malicious advertisements, spam emails etc. with crafted attachments.

Malicious activity

- The attacker's tries to access the victim machine either by exploiting the vulnerable server or through building the remote desktop connection on victim machine using brute force attack or credentials it purchase from dark Net.
- Once attacker successfully access the victim machine, it drops the SamSam Ransomware executable on the victim machine which encrypt all the files of the victim machine (excluding window file and Recycle bin folders) with dot stubbin extension. After encrypting all files of victim machine, attacker also drops a text file which contain message for paying ransom to decrypt the data.

Countermeasures and Best practices for prevention

1. Users are advised to disable their RDP if not in use, if required it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
2. Restrict execution of Power shell /WSCRIPT in enterprise environment. Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. Script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
3. Reference: https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
4. Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
5. Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
6. Don't open attachments in unsolicited e-mails, 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 e-mail and go to the organization's website directly through browser
7. 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
8. Consider encrypting the confidential data as the ransomware generally targets common file types.
9. Ensure that the operating system and third party applications (MS office, browsers, browser Plugins, antivirus) etc, are up-to-date with the latest patches.

10. Maintain updated Antivirus software. Use Quick Heal Bot Removal Tool for scanning the laptop for any malicious bot. Please refer the URL: https://www.quickheal.co.in/bot-removal-tool.
11. Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
12. Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
13. Implement strict External Device (USB drive) usage policy.
14. 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.

Indicator of Compromise

Hashes

- 5d65ebdde1aef8f23114f95454287e7410965288f144d880ece2a2b8c3128645 (prelecturedexe.exe)
- d8d919d884b86e4d5977598bc9d637ed53e21d5964629d0427077e08ddbcba68 (proteusdlll.dll)
- 2b06d2abc87f51aa7b8451da16270003ceba57184b0dd5f244670873409c75b9 (winnetuse.exe)
- 427091e1888c2bf1f2e11a1010b3ab6c8634eda4ddc34d37202d401fbaa8989d (ss2.exe)
- 594b9b42a2d7ae71ef08795fca19d027135d86e82bc0d354d18bfd766ec2424c (ss2.stubbin)
- a660cc6155b307c0957c4c6ea119a295a852d28097196d85f00f5517944a3dcb (SORRY-FORFILES.html)
- bc53f513df363dd999ac855b53831b3b31ac5516a4bf8f324489710cf06955f0 (g04inst.bat)
- da9c2ecc88e092e3b8c13c6d1a71b968aa6f705eb5966370f21e306c26cd4fb5 (sdgasfse.dll)
- 036071786d7db553e2415ec2e71f3967baf51bdc31d0a640aa4afb87d3ce3050 (samsam.exe)
- 0f2c5c39494f15b7ee637ad5b6b5d00a3e2f407b4f27d140cd5a821ff08acfac (samsam.exe)
- 32445c921079aa3e26a376d70ef6550bafeb1f6b0b7037ef152553bb5dad116f (selfdel.exe)
- 45e00fe90c8aa8578fce2b305840e368d62578c77e352974da6b8f8bc895d75b (samsam.exe)
- 553967d05b83364c6954d2b55b8cfc2ea3808a17c268b2eee49090e71976ba29
- (553967d05b83364c6954d2b55b8cfc...)
- 58ef87523184d5df3ed1568397cea65b3f44df06c73eadeb5d90faebe4390e3e (samsam.exe)
- 6245a51e78526c25510d0aa0909576119fdf0244619f670036538063b88f1c21
- (HELP_DECRYPT_YOUR_FILES.html)
- 6bc2aa391b8ef260e79b99409e44011874630c2631e4487e82b76e5cb0a49307 (samsam.exe)
- 7aa585e6fd0a895c295c4bea2ddb071eed1e5775f437602b577a54eef7f61044 (samsam.exe)
- 89b4abb78970cd524dd887053d5bcd982534558efdf25c83f96e13b56b4ee805 (samsam.exe)
- 939efdc272e8636fd63c1b58c2eec94cf10299cd2de30c329bd5378b6bbbd1c8 (samsam.exe)
- 946dd4c4f3c78e7e4819a712c7fd6497722a3d616d33e3306a556a9dc99656f4 (samsam.exe)
- 979692a34201f9fc1e1c44654dc8074a82000946deedfdf6b8985827da992868 (samsam.exe)
- 97d27e1225b472a63c88ac9cfb813019b72598b9dd2d70fe93f324f7d034fb95 (del.exe)
- a763ed678a52f77a7b75d55010124a8fccf1628eb4f7a815c6d635034227177e (samsam.exe)
- e682ac6b874e0a6cfc5ff88798315b2cb822d165a7e6f72a5eb74e6da451e155 (samsam.exe)
- ffef0f1c2df157e9c2ee65a12d5b7b0f1301c4da22e7e7f3eac6b03c6487a626 (samsam.exe)

- 738c95f5bfe63a530b200a0d73f363d46c5671c1fcbb69c217e15a3516501a86 (mswinupdate.exe)
- 9b23bfc35b18ed80104c496b2aa722b3e56ff9ceb9dae60d1aff7230321c1d12 (ClassLibrary1.dll)
- bbd4102fe25e73c0815d0c020d60d47dbbfbe79ef1e490e7b4f97640dd932b58 (g04inst.bat)

Domain

- jcmi5n4c3mvgtyt5.onion
- anonyme.com
- evilsecure9.wordpress.com
- followsec7.wordpress.com
- key88secu7.wordpress.com
- keytwocode.wordpress.com
- lordsecure4u.wordpress.com
- payforsecure7.wordpress.com
- secangel7d.wordpress.com
- union83939k.wordpress.com
- zeushelpu.wordpress.com

References

- ✓ https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2018-1673
- ✓ https://www.us-cert.gov/ncas/alerts/AA18-337A
- ✓ https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf