PNP Computer Security Bulletin CSB18-04

SamSam Ransomware

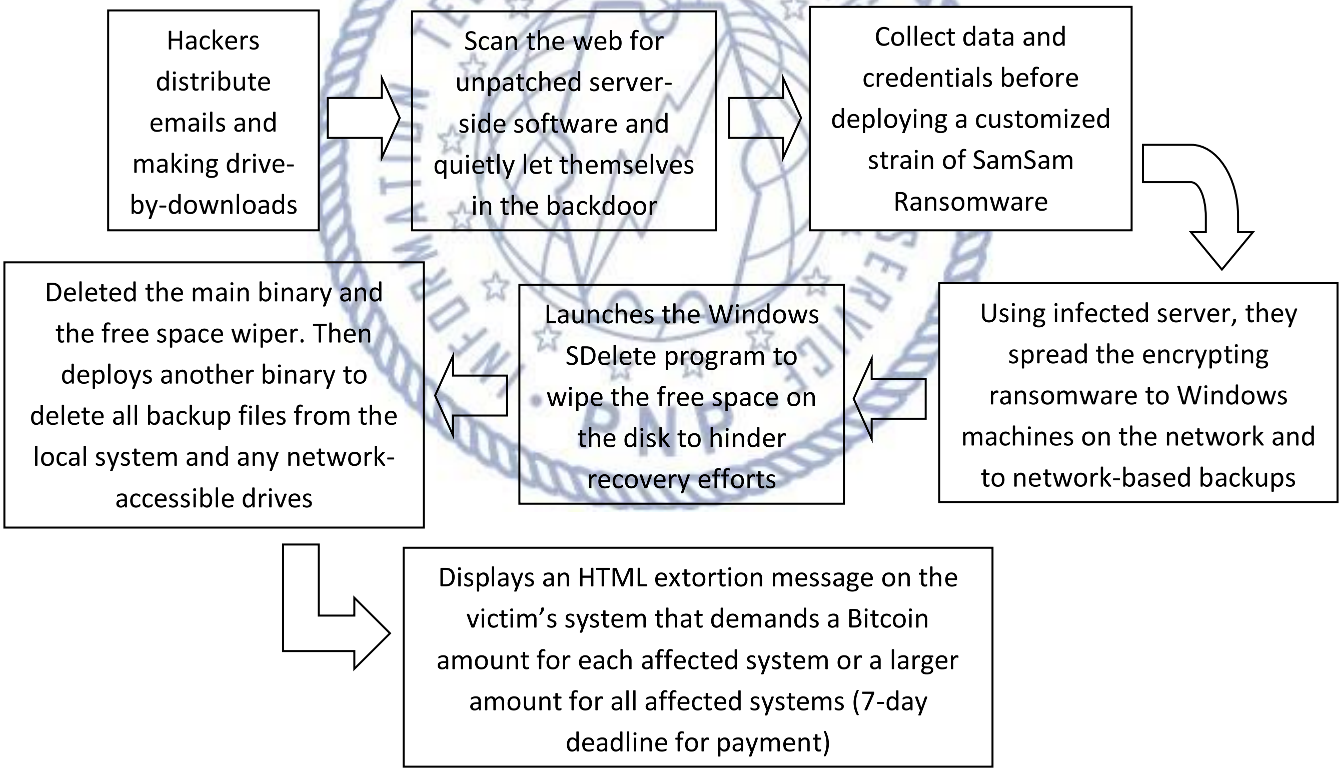
Risk/Impact Rating: **SERIOUS**

Created: May 3, 2018

Description:

- A custom infection used in targeted attacks, often deployed using a wide range of exploits or brute-force tactics.
- Attacks were made on target via vulnerable JBoss host servers in 2016 and 2017.
- In 2018, it uses either vulnerabilities in remote desktop protocols (RDP), Java-based web servers, or file transfer protocol (FTP) servers to gain access to the victims’ network or brute force against weak passwords to obtain an initial foothold.
- SamSam attacks are relatively rare and seem to be focused on the healthcare, government and education sectors.
- Its software configuration and ransom demands vary from one victim to the next and ransom demands are as high as 60,000USD.

How it works:



Hackers distribute emails and making drive-by-downloads

Scan the web for unpatched server-side software and quietly let themselves in the backdoor

Collect data and credentials before deploying a customized strain of SamSam Ransomware

Using infected server, they spread the encrypting ransomware to Windows machines on the network and to network-based backups

Launches the Windows SDelete program to wipe the free space on the disk to hinder recovery efforts

Deleted the main binary and the free space wiper. Then deploys another binary to delete all backup files from the local system and any network-accessible drives

Displays an HTML extortion message on the victim’s system that demands a Bitcoin amount for each affected system or a larger amount for all affected systems (7-day deadline for payment)

Note: Payment of ransom is no guarantee that hacker will send a key to unlock the infected computer

Modus Operandi:

- Via email or other electronic communication methods pretending to be from a legitimate source that trick users into clicking the malicious link or downloading attachments with malicious code.

Security Risks to PNP Computer Systems and Data:

- Data can be altered, damaged, deleted, and infused with additional computer viruses.
- Interfere with the normal functioning of the computer system or prevent its utilization.

Mitigation Measures:

- Use hard passwords and never reuse the same password at multiple sites;
- Backup and test your data regularly;
- Always check the spelling of the URLs in email links before clicking or entering sensitive information;
- Avoid opening e-mails from unverified or questionable sources;
- Avoid posting personal data on social media;
- Use genuine software and patch/update;
- Scan your computer regularly using antivirus software;
- Configure email client for security;
- Scan all emails and filter executable files from reaching the end users; and
- Run regular penetration tests as often as possible and practical.

If infected:

- Report it to the network administrators;
- Immediately change any passwords; or
- Report to ITMS ISSD for assistance.

References:

- Bradley Barth (2018, April 30). *SamSam ransomware designed to inundate targeted networks with thousands of copies of itself*. Retrieved from https://www.scmagazine.com/samsam-ransomware-designed-to-inundate-targeted-networks-with-thousands-of-copies-of-itself/article/762178/
- Christopher Boyd (2018, May 1). *SamSam ransomware: what you need to know*. Retrieved from https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/
- Mathew Schwartz (2018, May 2). *SamSam Ransomware Offers Volume Decryption Discount.* Retrieved from https://www.bankinfosecurity.com/samsam-ransomware-offers-volume-decryption-discount-a-10956
- *What is SamSam ransomware & how might it threaten your business?* (2018, January 24). Retrieved from https://ransomwarewatch.com/what-is-samsam-ransomware/
- *SamSam Ransomware Campaigns* (2018, February 15). Retrieved from https://www.secureworks.com/research/samsam-ransomware-campaigns

For further inquiries, contact ITMS ISSD:

- Telephone Number: **(02) 723-0401 local 4225**;
- E-mail address: **issditms@gmail.com**; and
- Website: **www.itms.pnp.gov.ph**.