Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
Camp BGen Rafael T Crame, Quezon City
https://www.itms.pnp.gov.ph

MEMORANDUM

FOR	:	See Distribution
FROM	:	D, ITMS
SUBJECT	:	**Computer Security Bulletin: (CSB18-04 SamSam Ransomware)**
DATE	:	May 11, 2018

1. References:
   a. Computer Security Bulletin CSB17-010 "Ransomware" revised; and
   b. Republic Act 10175 "Cybercrime Prevention Act of 2012" Chapter 2, Section 4a, 3 and 4.

2. Please be informed that there is an escalation of SamSam ransomware cyber-attack threats which uses drive-by attack. With this, awareness and prevention on protecting PNP computer systems and data against SamSam ransomware is paramount.

3. In this regard, attached is the Computer Security Bulletin learning material produced by this Service on the subject matter which is a form of ransomware that steal, corrupt and encrypt files stored in a computer then spread stealthily across networks and display a ransom note for the decryption of files.

4. For widest dissemination.

REMATO C ANGARA
Police Chief Superintendent

Distribution:

Command Group
D-Staff
P-Staff
D, NSUs
RD, PROs

PNP Computer Security Bulletin CSB18-04

SamSam Ransomware

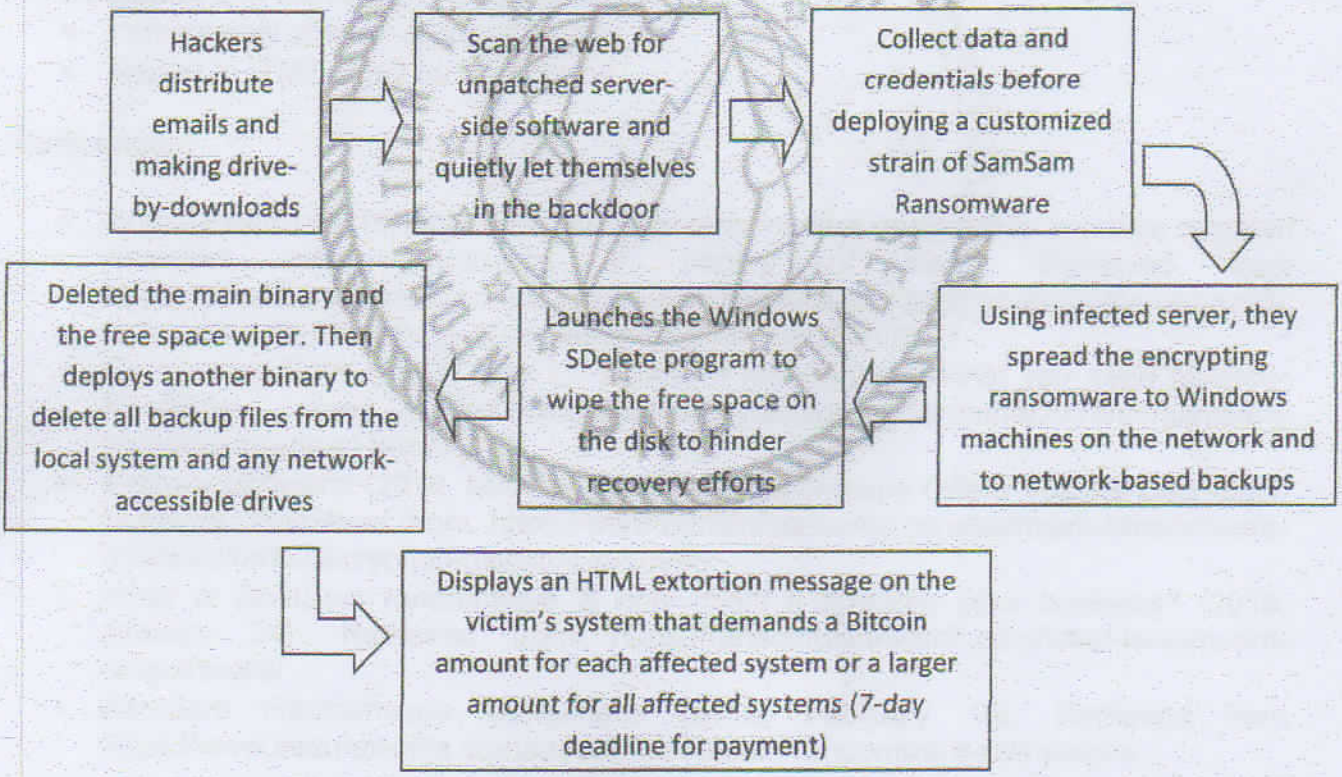
Risk/Impact Rating: **SERIOUS**

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:



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

Modus Operandi:

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