18 February 2016

Alert Number

MC-000068-MW

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Local Field Offices:
www.fbi.gov/contact-us/field

FBI Liaison Alert System

This product is released at TLP: GREEN. The information in this product is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

The FBI is providing the following information with **high confidence**:

Summary

The threat of ransomware continues to grow due to the relative availability of necessary tools, as well as the potential for extorting large sums of money. Modern ransomware uses strong encryption to render victims' files unreadable until the attackers are paid, often in Bitcoin, and release the encryption keys. In a new scheme, cyber criminals attempt to infect whole networks with ransomware and use persistent access to locate and delete network backups.

Technical Details

The FBI is providing indicators regarding businesses that were recently infected with a ransomware variant known as MSIL/Samas.A (a.k.a. Gen.Variant.Kazy or RDN/Ransom). Many of the executables and tools used in this intrusion are available for free through Windows or open source projects. The malware encrypts most file types with RSA-2048. In addition, the actor(s) attempt to manually locate and delete network backups. The FBI is distributing these indicators to enable network defense activities and reduce the risk of similar attacks in the future.

Federal Bureau of Investigation, Cyber Division

Flash Notification

FBI indicators based on an ongoing investigation:

- Several victims have reported initial intrusion occurring via outdated JBOSS applications.
- After an initial compromise, attackers map, connect to, and infect hosts on the network using several uploaded files, which may include the following:

Filename	MD5 Hash
samsam.exe	a14ea969014b1145382ffcd508d10156
csvde.exe	9f5f35227c9e5133e4ada83011adfd63
del.exe	e189b5ce11618bb7880e9b09d53a588f
selfdel.exe	710a45e007502b8f42a27ee05dcd2fba
tunnel.jsp	caa05dd2f9fee1923a2b94b27187d48f
tunnel.class	1a9403307958f52bcbbd985509241047

- csvde.exe is used to create a list of all hosts reporting to the active directory in a .csv file.
- The actor(s) then distribute the malware to each host in the network using a copy of Microsoft's psexec.exe, which may be named ps.exe.
- Ransomware is dropped in the C:\Windows\System32 directory as samsam.exe with a key file *<ComputerName>_PublicKey.xml*, which is used to encrypt most file types in the system.
- It renames the encrypted files by adding "encrypted.RSA" to their extension.
- It then creates the file HELP_DECRYPT_YOUR_FILES.html in the root folder of the encrypted files, as well as in the %Desktop% folder.
- This html file contains the instructions on how to decrypt the files by asking you to pay a fee.

The following are additional indicators of the executable file, samsam.exe:

SHA 256 Hash	0f2c5c39494f15b7ee637ad5b6b5d00a3e2f407b4f27d140cd5a821ff08acfac
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	213.50 KB (218624 bytes)
Comments	MicrosoftSAM
CompanyName	Microsoft
FileDescription	MicrosoftSAM
FileVersion	2.4.8.4
InternalName	samsam.exe
LegalCopyright	Copyright © 2014
OriginalFilename	samsam.exe
ProductName	MicrosoftSAM
ProductVersion	2.4.8.4

Federal Bureau of Investigation, Cyber Division

Flash Notification

Defending Against Ransomware

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.