FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

16 MAR 2021

Alert Number

CP-000142-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Increase in PYSA Ransomware Targeting Education Institutions

Summary

FBI reporting has indicated a recent increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom. PYSA, also known as Mespinoza, is a malware capable of exfiltrating data and encrypting users' critical files and data stored on their systems. The unidentified cyber actors have specifically targeted higher education, K-12 schools, and seminaries. These actors use PYSA to exfiltrate data from victims prior to encrypting victim's systems to use as leverage in eliciting ransom payments.

Technical Details

Since March 2020, the FBI has become aware of PYSA ransomware attacks against US and foreign government entities, educational institutions, private companies, and the healthcare sector by unidentified cyber actors. PYSA typically gains unauthorized access to victim networks by compromising Remote Desktop Protocol (RDP) credentials and/or through phishing emails. The cyber actors use Advanced Port Scanner and Advanced IP Scanner[1] to conduct network reconnaissance, and proceed to install open source tools, such as PowerShell Empire[2], Koadic[3], and Mimikatz[4]. The cyber actors execute commands to deactivate antivirus capabilities on the victim network prior to deploying the ransomware.

The cyber actors then exfiltrate files from the victim's network, sometimes using the free open-source tool WinSCP[5], and proceed to encrypt all connected Windows and/or Linux devices and data, rendering critical files, databases, virtual machines, backups, and applications inaccessible to users. In previous incidents, cyber actors exfiltrated employment records that contained personally identifiable information (PII), payroll tax information, and other data that could be used to extort victims to pay a ransom.

Upon malware execution, a detailed ransom message is generated and displayed on the victim's login or lock screen. The ransom message contains information on how to contact the actors via email, displays frequently asked questions (FAQs), and offers to decrypt the affected files. If the ransom is not met, the actors warn that the information will be uploaded and monetized on the darknet. Additionally, the malware is dropped in a user folder, such as *C:\Users\%username%\Downloads*. Observed instances of the malware showed a filename of *svchost.exe*, which is most likely an effort by the cyber actors to trick victims and disguise the

[1] They cyber actors used the Advanced Port Scanner and Advanced IP Scanner by FAMATECH, which is an open source tool that allows users to find open network computers and discover the versions of programs on those ports.
[2] PowerShell Empire is a post exploitation toolkit that provides the ability to run PowerShell agents without needing powershell.exe, as well as provide modules ranging from keyloggers to Mimikatz, and adaptable communication to avoid network detection.
[3] Koadic is an open source penetration toolkit that has several options for staging payloads and creating implants.
[4] Mimikatz is an open source post exploitation toolkit that pulls passwords from memory, as well as hashes, and other authentication credentials.
[5] WinSCP is an open source tool that provides secure file transfer between local and remote computer systems.

ransomware as the generic Windows host process name. In some instances, the actors removed the malicious files after deployment, resulting in victims not finding any malicious files on their systems.

The cyber actors have uploaded stolen data to MEGA.NZ, a cloud storage and file sharing service, by uploading the data through the MEGA website or by installing the MEGA client application directly on a victim's computer. However, in the past actors have used other methods of exfiltrating data that leaves less evidence of what was stolen.

Indicators

The following are characteristics of the compromise:

Indicators		
File Extension of encrypted files:	.pysa	
Observed malware filename:	\Users\%username%\Downloads\svchost.exe	
SHA1 Hashes[6]:	Unknown	07cb2a3fe86414b054e2b002f283935bb0cb993c
	svchost.exe	52b2fc13ec0dbf8a0250c066cd3486b635a27827
	svchost.exe	728CB56F98EDBADA697FE66FBF7D367215271F10
	17535.pyz	c74378a93806628b62276195f9657487310a96fd
	Step2.ps1	24c592ad9b21df380cb4f39a85d4375b6a8a6175
	sshs.exe or explorer.exe	f2dda8720a5549d4666269b8ca9d629ea8b76bdf
Tor URLs:	pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad.onion na47pldl5eoqxt42.onion	

The following domains are associated with this activity:

Domains Found in Ransom Notes	
ced_cririele93@protonmail.com	veronabello@onionmail.org
irvingalfie@protonmail.com	giuliacabello@onionmail.org
gustaf.wixon@protonmail.com	avitacabrera@protonmail.com
ralfgriffin@protonmail.com	domenikuvoker@protonmail.com

[6] As the cyber actors continue to develop the malicious codes, the filenames and SHA1 hashes will change and evolve.

korgy.torky@protonmail.com	mespinoza980@protonmail.com
astion11@protonmail.com	ellershaw.kiley@protonmail.com
Bfgkwethnsb@protonmail.com	jonivaeng@protonmail.com
Logan_A_Gray@protonmail.com	alanson_street8@protonmail.com
rafaeldari@onionmail.org	raingemaximo@protonmail.com
Abelzackary@onionmail.org	mcpherson.artair@protonmail.com
Elliotstaarss1@protonmail.com	lambchristoffer@protonmail.com
TimWestbrook@onionmail.org	gareth.mckie3l@protonmail.com
PaulDade@onionmail.org	rohrbacherlucho@protonmail.com
CarmenWashingtonGton@portonmail.com	aireyeric@protonmail.com
cozmo.storton@protonmail.com	noblecocking@protonmail.com
karim.abson@protonmail.com	presleybarry63@protonmail.com
chettle.willem@protonmail.com	duncan_cautherey@protonmail.com
dalliss.prout96@protonmail.com	shdujdsh@protonmail.com
karkeck.arch@protonmail.com	ihdtwesfs@portonmail.com
keefe.mcmeckan@protonmail.com	williamjohnson1963@protonmail.com
keepupchell@protonmail.com	casualstroons@portonmail.com
gabriel8970@protonmail.com	izak.pollington@protonmail.com
masonhoyt@onionmail.org	t_trstram@protonmail.com
merry.lane@mailfence.com	willmottlem01@protonmail.com
Jamesy.kettlewell@protonmail.com	BettyRacine@protonmail.com
platt.lucais@protonmail.com	Ohsgsuywb@protonmail.com
jarret.wharram@protonmail.com	Lojdgseywu@protonmail.copm
hewitt_rogers@protonmail.com	Johnbeamvv@protonmail.com
thorvald_beattie@protonmail.com	rewhgsch@protonmail.com
warden_riddoch@protonmail.com	lhdbeysdq@protonmail.com
cowland_lothaire@protonmail.com	mario1@mailfence.com
Nickola_men@protonmail.com	

Information Requested:

The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees and customers. Regardless of whether your organization decided

to pay the ransom, the FBI urges you to report ransomware incidents to your local FBI field office or the FBI's Internet Crime Complaint Center (IC3) (https://ic3.gov). Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under U.S. law.

Recommended Mitigations

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication where possible.
- Regularly, change passwords to network systems and accounts, and avoid reusing passwords for different accounts. Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on awareness and training. Provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.