FINISHED INTELLIGENCE REPORTS

Increase in PYSA Ransomware

TLP:WHITE

Mar 18, 2021

The Federal Bureau of Investigation has published CP-000142-MW, an alert focused on an Increase in PYSA Ransomware targeting multiple sectors including educational institutions and healthcare organizations.

PYSA, also known as Mespinoza, is malware capable of exfiltrating data and encrypting users' critical files and data stored on their systems. The unidentified cyber actors have specifically targeted the healthcare sector, higher education, K-12 schools, and seminaries. The actors use PYSA ransomware to exfiltrate data from victims prior

to encrypting victim's systems to use as leverage in eliciting ransom payments.

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 to conduct network reconnaissance, and proceed to install open-source tools, such as PowerShell Empire, Koadic, and Mimikatz.

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, 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 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.

Reference(s)	Bleeping Computer, IC3, Threat Post, ZDNet, mytechdecisions
Report Source(s)	FBI

Recommendations
The most effective mitigations for ransomware and other malware will include a defense in-depth approach that makes it more difficult to successfully deploy malware and reduce the impact or spread of a successful infection. We therefore recommend that long term, Health-ISAC member organizations should seek to:

- Provide social engineering and phishing training to employees. Most incidents originate from successful phishing campaigns.
- Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.
- Ensure emails originating from outside the organization are automatically marked before received.
- Apply applicable patches and updates immediately after testing; Develop and maintain patching program if necessary.
- Implement Intrusion Detection System (IDS).
- Implement spam filters at the email gateways.
- Block suspicious IP addresses at the firewall.
- Implement whitelisting technology on appropriate assets to ensure that only authorized software is allowed to execute.
- Implement access control based on the principal of least privilege.
- Implement and maintain anti-malware solution.
- Conduct system hardening to ensure proper configurations.
- Disable the use of Remote Desktop Protocol (RDP) or, if absolutely needed, restrict its use applying the principle of least privilege and monitor/log its usage.

Release Date

Mar 18, 2021

Sources
FBI Warns Of Increase in PYSA Ransomware Targeting Education

FBI Warns of Rise in PYSA Ransomware Operators Targeting US, UK Schools

FBI Warns of Escalating Pysa Ransomware Attacks on Education Orgs
PYSA Ransomware Pillages Education Sector, Feds Warn

Threat Indicator(s)

SHA1:
07cb2a3fe86414b054e2b002f283935bb0cb993c
24c592ad9b21df380cb4f39a85d4375b6a8a6175
52b2fc13ec0dbf8a0250c066cd3486b635a27827
728CB56F98EDBADA697FE66FBF7D367215271F10
C74378a93806628b62276195f9657487310a96fd
f2dda8720a5549d4666269b8ca9d629ea8b76bdf

Email(s):
rewhgsch@protonmail.com
gabriel8970@protonmail.com
thorvald_beattie@protonmail.com
TimWestbrook@onionmail.org
williamjohnson1963@protonmail.com
astion11@protonmail.com
PaulDade@onionmail.org
masonhoyt@onionmail.org
Johnbeamvv@protonmail.com
mcpherson.artair@protonmail.com
alanson_street8@protonmail.com
Ohsgsuywb@protonmail.com
jonivaeng@protonmail.com
pmhewitt_rogers@protonmail.com
korgy.torky@protonmail.com
rafaeldari@onionmail.org
veronabello@onionmail.org
ralfgriffin@protonmail.com
irvingalfie@protonmail.com
keefe.mcmeckan@protonmail.com
ced_cririele93@protonmail.com
domenikuvoker@protonmail.com

t_trstram@protonmail.com
Jamesy.kettlewell@protonmail.com
gareth.mckie3l@protonmail.com
BettyRacine@protonmail.com
mespinoza980@protonmail.com
chettle.willem@protonmail.com
merry.lane@mailfence.com
mario1@mailfence.com
Elliotstaarss1@protonmail.com
ihdtwesfs@portonmail.com
aireyeric@protonmail.com
Bfgkwethnsb@protonmail.com
gustaf.wixon@protonmail.com
shdujdsh@protonmail.com
casualstroons@portonmail.com
raingemaximo@protonmail.com
rohrbacherlucho@protonmail.com
ellershaw.kiley@protonmail.com
karkeck.arch@protonmail.com
izak.pollington@protonmail.com
jarret.wharram@protonmail.com
willmottlem01@protonmail.com
cozmo.storton@protonmail.com
warden_riddoch@protonmail.com
lhdbeysdq@protonmail.com
Logan_A_Gray@protonmail.com
noblecocking@protonmail.com
dalliss.prout96@protonmail.com
keepupchell@protonmail.com
CarmenWashingtonGton@portonmail.com
avitacabrera@protonmail.com
karim.abson@protonmail.com
Lojdgseywu@protonmail.co
Nickola_men@protonmail.com
platt.lucais@protonmail.com
Abelzackary@onionmail.org
duncan_cautherey@protonmail.com
giuliacabello@onionmail.org
cowland_lothaire@protonmail.com
presleybarry63@protonmail.com
lambchristoffer@protonmail.com

Domain(s):
a47pldl5eoqxt42.onion

Alert ID 5fb289cd

View Alert

Tags PYSA, FBI

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

FBI The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**