HC3: Analyst Note

January 6, 2022 TLP: White Report: 202201061700

Mespinoza/GoldBurlap/CYBORG SPIDER

Executive Summary

Mespinioza (also known as GOLD BURLAP and CYBORG SPIDER) is a cybercriminal group who operates PYSA ransomware, among other cyber weapons, and have been active since 2018. They have a history of targeting many industries, including healthcare, and continue to develop their capabilities and increase their targeting frequency.

Report

Mespinoza (also known as GOLD BURLAP and CYBORG SPIDER) is a financially-motivated cybercriminal group initially observed engaging in cyberattacks in October 2018. They developed and operated their own ransomware variant (PYSA), which after undergoing several updates, began encrypting victim files with the .pysa extension in December 2019. They also regularly use a number of other tools including ADRecon, Advanced Port Scanner, DNSGo RAT, Mimikatz, PEASS and PowerShell Empire. By the end of 2020, Intel471 considered them to be a "rising power" and as of November 2021, they are known to have accumulated at least 190 global victims via ransomware attacks alone. PYSA is cross-platform ransomware and versions are developed in both the C++ and Python languages.

Mespinoza operates a leak site called, "Pysa's Partners", which it uses to leverage "name and shame" tactics to apply additional pressure to compel victims to pay ransoms. Mespinoza is not known to operate as ransomware as a service (RaaS). The top five countries targeted by Pysa are the US, UK, Canada, Spain, and Brazil. Figure 1 depicts their total global targeting, with the color corresponding to the number of victims in each country (scale at bottom):

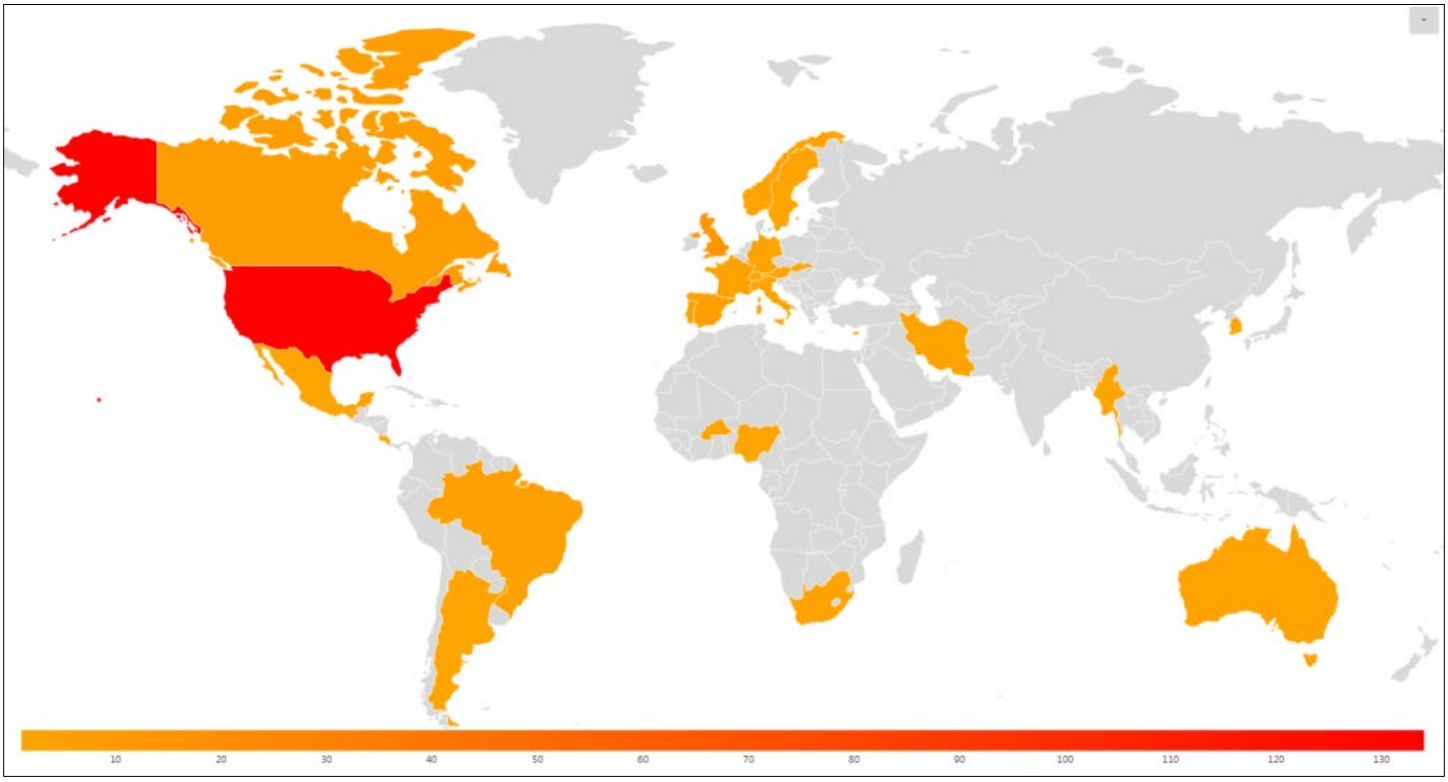

Figure 1: PYSA Ransomware Heat Map (Source: Cyble)

HC3: Analyst Note

January 6, 2022 TLP: White Report: 202201061700

PYSA is used to target industries like education, utilities, transportation, construction, business services and, most notably, the healthcare and public health (HPH) sector. Although the Pysa variant has only been known to be operating since December 2019, it quickly became one of the more prolific threats against healthcare. In 2020, it was one of the top ten ransomware variants used to target healthcare (per Crowdstrike data, see figure 2), beating out many other well-known variants such as Clop, Lockbit, Nemty, RagnarLocker, Avvadon, MountLocker and SunCrypt.

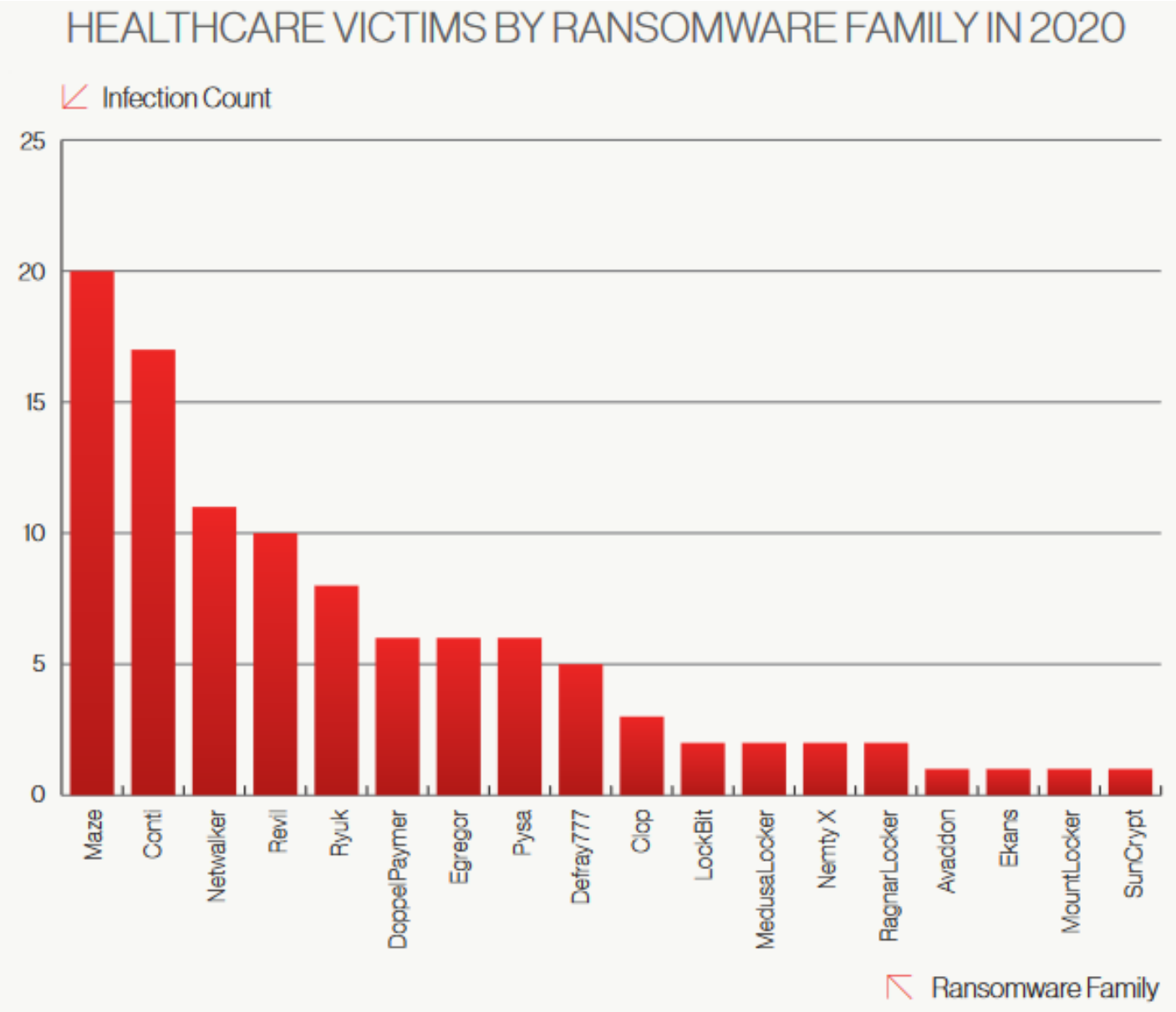

Figure 2: Source: Crowdstrike

The Cyber Peace Institute has also reported on ransomware groups targeting healthcare during the pandemic. They found Pysa was one of the most aggressive among all ransomware groups in targeting healthcare over the last two years. (see figure 3) Furthermore, they noted that unlike some cybercriminal groups who made public promises to

refrain from targeting healthcare during the pandemic or others who simply didn't make any statement, Pysa threatened healthcare specifically and then followed through with those promises.

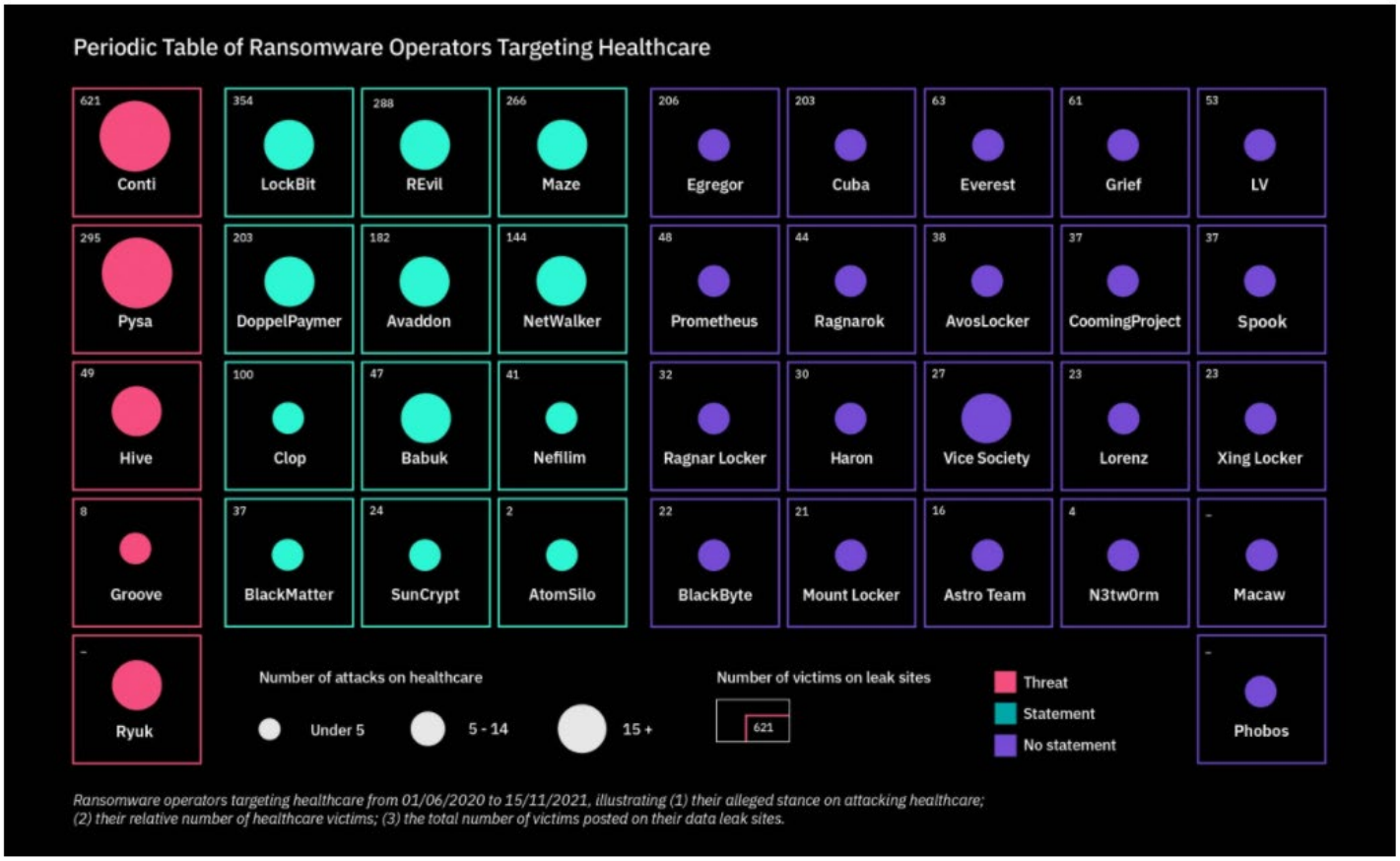

Figure 3: Ransomware targeting of healthcare during the pandemic

The Cyber Peace Institute's data also reflects Pysa as having launched some of the largest ransomware attacks against health targets during the pandemic. (see figure 4)

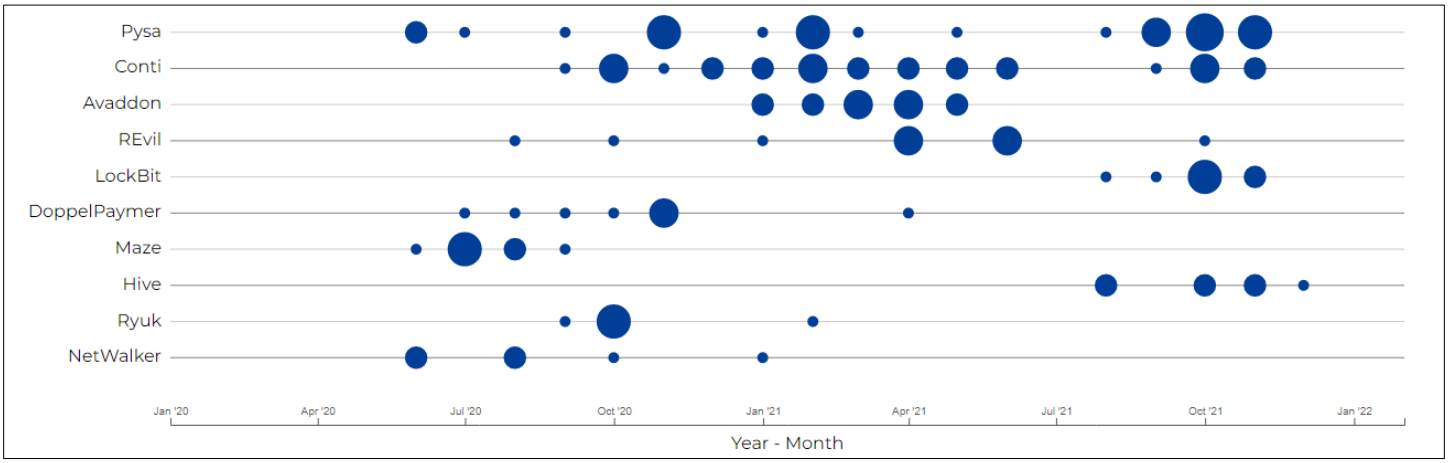

Figure 4: Top 10 Ransomware Operators vs. the Health Sector During the Pandemic

Pysa often follows a standard execution flow (see figure 5). It often begins by creating a mutual exclusion object (mutex) which it does for the same reason legitimate applications do – to ensure two processes or threads don't attempt to write to the same memory space simultaneously. It then goes on to begin its basic reconnaissance functions by enumerating the drives on the victim system by leveraging the application programming interfaces GetLogicalDriveStringsW, GetDriveTypeW and CreateThread. Once it identifies drives, it compares them to a whitelist and then begins to identify individual files for encryption, which it encrypts via Advanced Encryption Standard 256 with the extension .pysa (hence the ransomware variant name). It then creates two registry keys under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, one with the name legalnoticetext having the ransom note as its value and one named legalnoticecaption having the value "PYSA". It then releases the mutex and creates and executes a batch file (update.bat) which contains the self-deletion commands. Additional details on this execution flow and other technical details of a Pysa attack can be found on the Cyble blog, the DFIR Report analysis, as well as the report from the French national CERT.

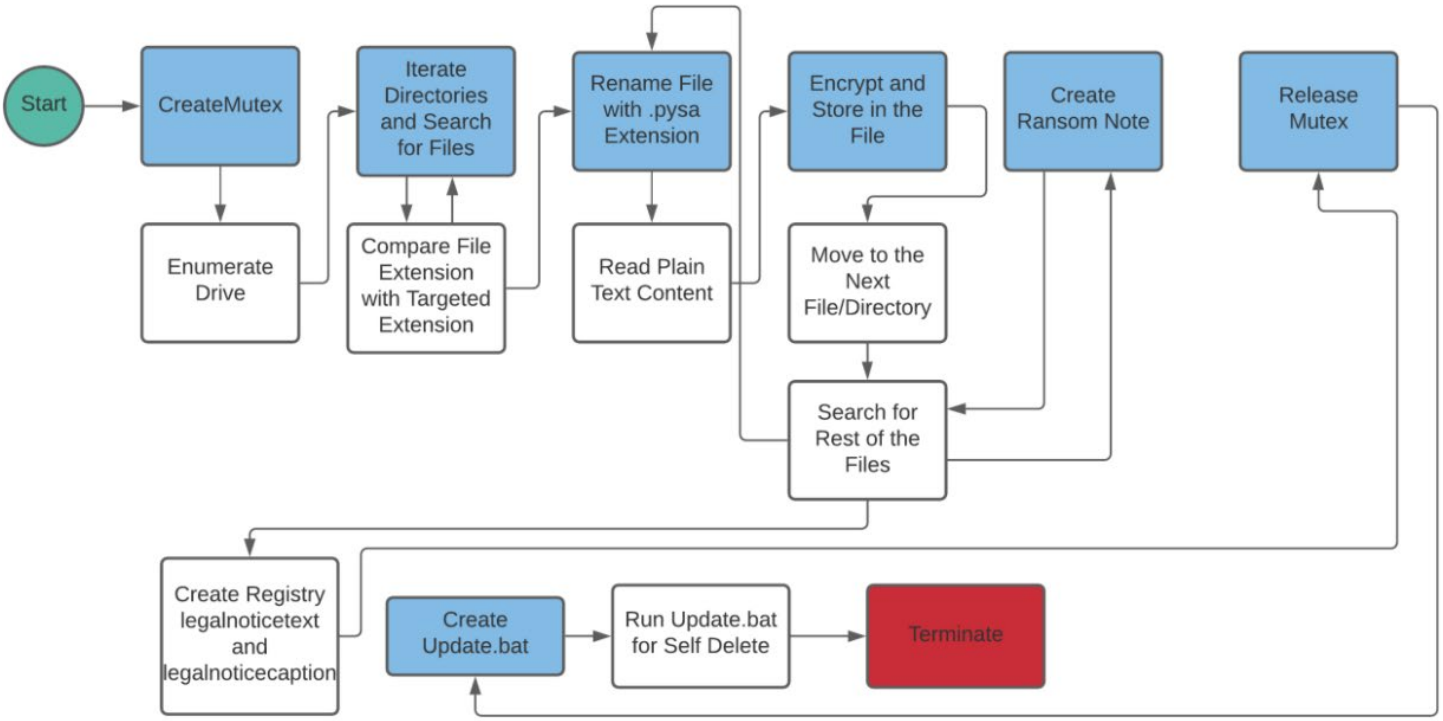

Figure 5: Execution flow of PYSA Ransomware (Source: Cyble)

Pysa has known to leverage several tools for command and control (C2) communications including RDP, PowerShell Empire and Kodiac. Beginning in May of 2021, Pysa ransomware has been used to target VMWare ESXi systems for encryption where they then move laterally via root access and enable SSH for further exploit via remote shell. The FBI released a flash alert on Pysa in March of 2021.

Analyst Comment

Many of the fundamental operational aspects of the Mespinioza group or Pysa ransomware variant are not significantly different than other similar cybercriminal groups or ransomware. The same basic principles apply, and any organization wishing to protect itself from Mespinioza/Pysa should consider the following guidance:

1. Design and operate enterprise networks with basic cybersecurity principles in mind, especially defense of depth and the principle-of-least-privilege. This includes architecting the network in a segmented way that balances security with operations, managing multiple layers of filtering and threat detection applications, and ensuring periodic reviews of user requirements and privileges. For healthcare operations, ransomware used to disrupt operations and data theft (for subsequent sale on the dark web) are two of the more significant threats and these principles can help defend against such attacks.

2. Protect against the common infection vectors. Operating and maintaining an effective vulnerability management program is critical to this aspect of enterprise cybersecurity. Ensure remote access technologies such as virtual private networks (VPNs) and applications that leverage the Remote Desktop Protocol (RDP) are locked down and configured in such a way to minimize their exposure. Ensure the principle-of-least-privilege also applies to these tools as well in terms of who can use them, when and how. Continuous, real-time monitoring should ensure enterprise policy compliance for all aspects of their use. Phishing attacks should be taken seriously and efforts to curtail them include awareness training, filtering and endpoint security.

3. Continuously ensure your organization's attack surface is minimized. This begins with the previously mentioned vulnerability management efforts and also includes 24/7/365 monitoring of the enterprise nework. Furthermore, ensuring indicators of compromise (IoCs) are appropriately operationalized and continuous monitoring for incidents is ongoing. Hunt efforts are also recommended in this effort.

An effort should be made to constantly gather and deploy indicators of compromise in accordance with the organizational risk management plan. It's worth noting that infrastructure associated IoCs often are often abandoned by cybercriminals after they become public but can also be reused over time as well. Some indicators of compromise of Pysa can be found in these three sources:

Cyble - Pysa Ransomware Under The Lens: A Deep-Dive Analysis
https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/

FBI flash: Increase in PYSA Ransomware Targeting Education Institutions
https://www.ic3.gov/Media/News/2021/210316.pdf

The DFIR Report: PYSA/Mespinoza Ransomware
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/

YARA is a free, signature-based malware analysis tool often used to detect adversarial presence on a network. The Yara tool, along with documentation and support, can be found at http://virustotal.github.io/yara/. Yara rules for Pysa can be found in these two sources:

Cyble - Pysa Ransomware Under The Lens: A Deep-Dive Analysis
https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/

The DFIR Report: PYSA/Mespinoza Ransomware
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/

References

Secureworks: GOLD BURLAP
https://www.secureworks.com/research/threat-profiles/gold-burlap

Cyble - Pysa Ransomware Under The Lens: A Deep-Dive Analysis
https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/

Leakware-Ransomware-Hybrid Attacks
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

CERT-FR Mespinoza/Pysa alert
https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-003/

Hypervisor Jackpotting, Part 2: eCrime Actors Increase Targeting of ESXi Servers with Ransomware
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

France warns of new ransomware gang targeting local governments
https://www.zdnet.com/article/france-warns-of-new-ransomware-gang-targeting-local-governments/

FBI flash: Increase in PYSA Ransomware Targeting Education Institutions
https://www.ic3.gov/Media/News/2021/210316.pdf

Intel471: Ransomware-as-a-service: The pandemic within a pandemic
https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

Malware.News: Another one for the collection - Mespinoza (Pysa) Ransomware
https://malware.news/t/another-one-for-the-collection-mespinoza-pysa-ransomware/35626

Cyber Peace Institute Blog Series: Reconceptualizing Ransomware
https://cyberpeaceinstitute.org/blog-series-reconceptualizing-ransomware/

39 Ransomware Groups Targeted Healthcare in the Past 18 Months
https://healthitsecurity.com/news/39-ransomware-groups-targeted-healthcare-in-the-past-18-months

The DFIR Report: PYSA/Mespinoza Ransomware
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/

Ransomware Profile: Mespinoza / PYSA
https://blog.emsisoft.com/en/38840/ransomware-profile-mespinoza-pysa/

Cynet Ransomware Report: Mespinoza
https://www.cynet.com/attack-techniques-hands-on/cynet-ransomware-report-mespinoza/

Cybereason Threat Analysis Report: Inside the Destructive PYSA Ransomware
https://www.cybereason.com/blog/threat-analysis-report-inside-the-destructive-pysa-ransomware

Malwarebytes: Ransom.Mespinoza
https://blog.malwarebytes.com/detections/ransom-mespinoza/

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback