Mespinoza Ransomware Threat Brief

Pysa

Table of Contents

Mespinoza is a variant of ransomware operated by a cybercrime group since at least October 2018.

While it has been stated that Mespinoza is operated under a Ransomware-as-a-Service (RaaS) model, there is no conclusive evidence of this, and it is more likely that Mespinoza is run and maintained by a closed group of actors.

The name 'Pysa' is likely due to the use of the abbreviation in various parts of the ransomware's functionality. The most visible instances are encrypted files' extension being changed to '.pysa' and the phrase 'Protect Your System, Amigo' used in the ransom note.

Motives

The Mespinoza group is financially motivated, leading them to employ alternative techniques to maximize victim ransom payments. To achieve this outcome the Mespinoza operators run a double-extortion model, where valuable files are exfiltrated from the victim network before encryption. The group then threatens to publicize this stolen data to their dedicated leaks site ensuring the victim is properly incentivized to send payment.

Tactics, Techniques, and Procedures (TTPs)

A common initial access vector used by Mespinoza actors, reported by both The DFIR Report and Unit 42, is Remote Desktop Protocol (RDP). RDP is a very common method of initial access. It was reported in 2020 by Hewlett Packard Enterprise that over half of all ransomware attacks were via RDP.

RDP credentials are sold by initial access merchants on dark web forums. These credentials are commonly purchased by malicious actors seeking guaranteed, immediate access to a compromised network.

Once initial access has been achieved, Mespinoza actors are known to be disciplined when carrying out their attacks and perform targeted searches for data that would be the most worthwhile in exfiltrating and holding ransom. To efficiently exfiltrate valuable data an automated PowerShell script is executed. This script searches file contents against a specified wordlist and exports matching files to a remote actor-controlled server.

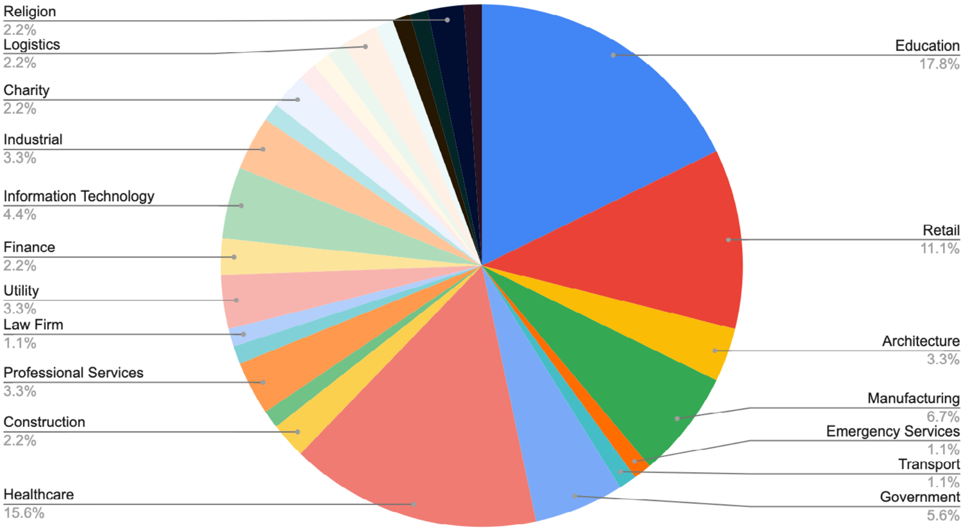
During attacks, actors have been observed utilizing the tools Advanced IP Scanner and Advanced Port Scanner to map the victim network. Mimikatz and PowerShell Empire toolsets are then used to pivot through the network.

When possible, Mespinoza actors have been observed logging into Cloud Backup platforms to delete backups. Actors leverage stolen credentials found during earlier stages of the attack to gain access. These platforms are then logged into from systems with IP addresses from the same Geo-IP location as the victim's network. It is currently theorized that Mespinoza actors have access to a network of compromised hosts that span many regions and locations.

While the previously mentioned tools are well-known and publicly available, Unit 42 reported on the use of a custom-written payload written in the Go programming language (Golang). The payload, named Gasket and ChaChi by threat intelligence companies, uses command-and-control via HTTP or DNS and can execute PowerShell commands, tunnel traffic, and self-uninstall. Gasket is likely dropped onto victim devices as a backup in case RDP connectivity is lost.

Mespinoza actors have targeted organizations from a range of industries. However, the Education and Healthcare sectors appear to be a focal point of the group, making up a third of all victims published on Mespinoza's leak site in 2021.

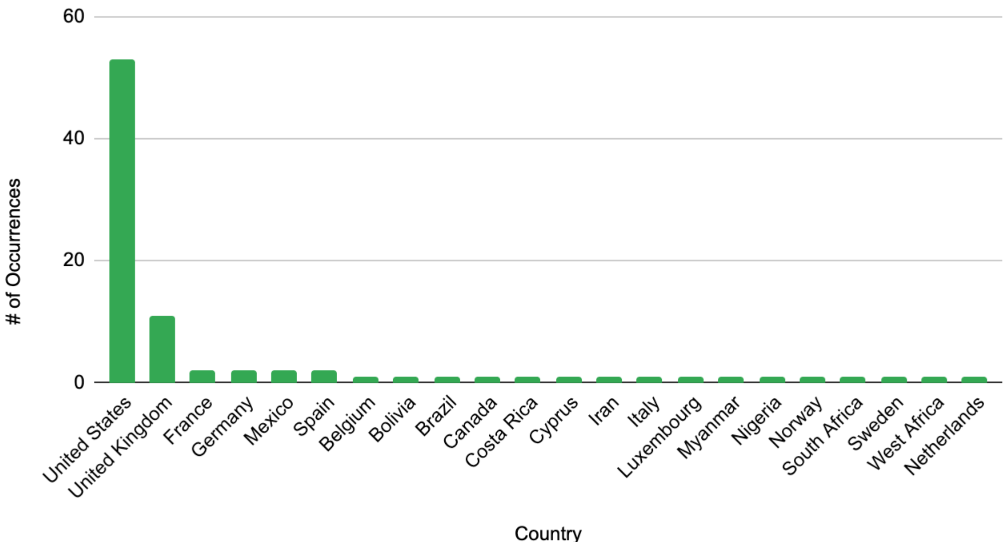
2021 Mespinoza/Pysa Victims by Industry



Statistics on victim geolocation show a strong targeting of the US, with almost 60% of 2021 victims being US organizations.

Table of Contents

2021 Mespinoza/Pysa Victims by Industry



Mitre ATT&CK

The following maps known Mespinoza ransomware attack TTPs to MITRE ATT&CK:

Initial Access

- **External Remote Services (T1133) -** Mespinoza actors have used RDP to gain initial access to victim networks.

Execution

- **System Services: Service Execution (T1569.002) -** Mespinoza actors have utilized PsExec to perform ransomware attacks.
- **Command and Scripting Interpreter:** PowerShell (T1059.001) - **Mespinoza actors have** used PowerShell scripts in their ransomware attacks.
- **Command and Scripting Interpreter: Python (T1059.006) -** Mespinoza actors have used Python scripts to deploy ransomware.

Persistence

- **Create or Modify System Process: Windows Service (T1543.003) -** Gasket can install itself as a system service.

Defense Evasion

- **Impair Defenses: Disable or Modify Tools (T1562.001) -** Mespinoza is able to stop antivirus products.
- **Indicator Removal on Host: File Deletion (T1070.004) -** Mespinoza actors have deleted batch files after executing them.
- **Masquerading:** Match Legitimate Name or Location (T1036.005) - Mespinoza actors have named the ransomware "svchost.exe" to evade detection.
- **Modify Registry (T1112) -** Mespinoza has modified the registry key SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" to store the ransom note.

Credential Access

- **Brute Force (T1110) -** Mespinoza actors have utilized brute force methods to access domain accounts.
- **Unsecured Credentials:** Credentials In Files (T1552.001) - Mespinoza actors have exfiltrated password stores before carrying out ransomware attacks.
- **OS Credential Dumping:** LSASS Memory (T1003.001) - Mespinoza actors have used Mimikatz to dump LSASS process memory and steal credentials.

Discovery

- **System Network Configuration Discovery (T1016) -** Mespinoza can perform network reconnaissance using the Advanced IP Scanner tool.
- **Network Service Scanning (T1046) -** Mespinoza can perform network reconnaissance using the Advanced Port Scanner tool.

Lateral Movement

- **Remote Services: Remote Desktop Protocol (T1021.001) -** Mespinoza actors have used RDP to move laterally around victim networks.

Collection

- **Automated Collection (T1119) -** Mespinoza actors use a PowerShell script that automatically exfiltrates files that match a list of keywords.

Command and Control

- **Application Layer Protocol:** Web Protocols (T1071.001) - Gasket has used HTTP-based C2 communications.
- **Application Layer Protocol:** DNS (T1071.004) - Gasket has used DNS tunneling for C2 communications.

Exfiltration

- **Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002) -** Mespinoza actors have utilised WinSCP to exfiltrate data from victim networks before encryption.

Impact

- **Service Stop (T1489) -** Mespinoza can stop processes and services.
- **Inhibit System Recovery (T1490) -** Mespinoza is able to delete shadow copies.
- **Data Encrypted for Impact (T1486) -** Mespinoza encrypts files that are part of a targeted list of file extensions.
- **Data Destruction (T1485) -** Mespinoza when possible has been observed logging into cloud backup platforms to delete backups.

Mitigations/Defences

The Center for Internet Security (CIS) Controls are a prioritized set of safeguards designed to defend against cyber attacks. The CIS Controls have three tiers, known as Implementation Groups, that build on each other.

The following table maps Mespinoza's MITRE ATT&CK techniques to CIS v8 Safeguards:

MITRE ATT&CK	CIS Safeguards
External Remote Services (T1133)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 6.3: Require MFA for Externally-Exposed Applications 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access
System Services: Service Execution (T1569.002)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Command and Scripting Interpreter: PowerShell (T1059.001)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Impair Defenses: Disable or Modify Tools (T1562.001)	**IG1** 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage

Table of Contents

Unsecured Credentials: Credentials In Files (T1552.001)	**IG1** 2.3: Address Unauthorized Software 3.1: Establish and Maintain a Data Management Process 3.2: Establish and Maintain a Data Inventory 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.5: Implement and Manage a Firewall on End-User Devices 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 11.3: Protect Recovery Data 14.3: Train Workforce Members on Authentication Best Practices 14.4: Train Workforce on Data Handling Best Practices
OS Credential Dumping: LSASS Memory (T1003.001)	**IG1** 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 11.3: Protect Recovery Data 14.1: Establish and Maintain a Security Awareness Program 14.3: Train Workforce Members on Authentication Best Practices
System Network Configuration Discovery (T1016)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process

Table of Contents

Remote Services: Remote Desktop Protocol (T1021.001)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 4.5: Implement and Manage a Firewall on End-User Devices 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access
Inhibit System Recovery (T1490)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Brute Force (T1110	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 6.3: Require MFA for Externally-Exposed Applications 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access 11.4: Establish and Maintain an Isolated Instance of Recovery Data 14.1: Establish and Maintain a Security Awareness Program 14.3: Train Workforce Members on Authentication Best Practices

Command and Scripting Interpreter: Python (T1059.006)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Data Encrypted for Impact (T1486)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.4: Implement and Manage a Firewall on Servers 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Indicator Removal on Host: File Deletion (T1070.004)	**IG1** 3.1: Establish and Maintain a Data Management Process 3.3: Configure Data Access Control Lists 3.4: Enforce Data Retention 4.1: Establish and Maintain a Secure Configuration Process 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage
Masquerading: Match Legitimate Name or Location (T1036.005)	**IG1** 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process

Modify Registry (T1112)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 6.3: Require MFA for Externally-Exposed Applications 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access 11.4: Establish and Maintain an Isolated Instance of Recovery Data 14.1: Establish and Maintain a Security Awareness Program 14.3: Train Workforce Members on Authentication Best Practices
Network Service Scanning (T1046)	**IG1** 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 4.6: Securely Manage Enterprise Assets and Software 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access 9.2: Use DNS Filtering Services
Service Stop (T1489)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.4: Implement and Manage a Firewall on Servers 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002)	**IG1** 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 9.2: Use DNS Filtering Services

Create or Modify System Process: Windows Service (T1543.003)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Automated Collection (T1119)	**IG1** 11.4: Establish and Maintain an Isolated Instance of Recovery Data **IG2** 3.11: Encrypt Sensitive Data At Rest
Application Layer Protocol: Web Protocols (T1071.001)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution **IG3** 13.8: Deploy a Network Intrusion Prevention Solution
Application Layer Protocol: DNS (T1071.004)	**IG1** 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 9.2: Use DNS Filtering Services
Data Destruction (T1485)	**IG1** 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Table of Contents

Detection Opportunities

The following detection opportunities are mapped to MITRE ATT&CK v9 methods, CIS v8 Safeguards, and provide appropriate Red Canary Atomic Red Team tests to undertake for validation:

Detection Opportunity 1: Shadow Copy Deletion

MITRE ATT&CK: Inhibit System Recovery (T1490)

CIS Control(s): 4.1, 4.2, 4.7, 5.3, 5.4, 7.1, 7.2, 7.3, 11.1, 11.2, 11.3, 11.4

Red Canary Atomic Red Team Test(s): T1490 - Inhibit System Recovery Test #1

Part of the pre-deployment activities performed by Mespinoza actors is the deletion of volume shadow copies from endpoints. This action is intended to prevent victims from recovering from the attack and make them more likely to pay the ransom. Enabling PowerShell Transcription and exporting the transcripts to a remote location will allow you and your team to defend against malicious actors utilizing PowerShell to perform their activities. Searching for the following command within PowerShell logs will allow you to detect potentially malicious pre-deployment activity on your endpoints:

Command: vssadmin.exe delete shadows*

Detection Opportunity 2: PowerShell Empire detection

MITRE ATT&CK: Command and Scripting Interpreter: PowerShell (T1059.001)

CIS Control(s): 2.1, 2.2, 2.3, 4.1, 4.7, 5.3, 5.4, 6.1, 6.2, 10.1, 10.2

Red Canary Atomic Red Team Test(s): N/A

PowerShell Empire has been observed in use by Mespinoza actors during their ransomware attacks. PowerShell Empire obfuscates its activity by encoding its Powershell commands. This is an opportunity for defenders to detect potential PowerShell Empire activity on endpoints. As in Detection Opportunity 1, enablement of PowerShell Transcription, preferably to a remote location, is required to detect PowerShell commands being executed. Searching for the following 6 commands will allow network defenders to detect and investigate potential PowerShell Empire commands being executed:

Command: *-nop -sta -w 1 -enc*

Command: *-nop -NonI -w hidden -enc*

Command: *-enc SQB*

Command: *-nop -exec bypass -EncodedCommand SQB*.

Detections from these alerts should be investigated, with encoded commands being decoded and checked for malicious intent as not all encoded PowerShell commands are truly malicious:

To test your new detection logic, you can run the following command in a PowerShell window. This command mimics PowerShell Empire generating a stager but instead, the Base64 encoded string simply exits.

Command: powershell -noP -sta -w 1 -enc ZXhpdA==

Note: Remember to always check commands you intend to run, especially obfuscated commands, to ensure they are safe to execute.

References/Appendix/Resources

cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf

attack.mitre.org/software/S0583/

thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/

unit42.paloaltonetworks.com/gasket-and-magicsocks-tools-install-mespinoza-ransomware/

hpe.com/us/en/insights/articles/2020-ransomware-attacks-still-mostly-through-unsecured-rdp-2005.html