CIBERBOLETÍN

ENERO 2022

TEMA DEL MES

Las autoridades rusas arrestan 14 personas con la ayuda de EE. UU.

VULNERABILIDADES

Estas han sido las 10 vulnerabilidades más representativas que fueron identificadas en el mes de enero de 2022, tomando en cuenta el tipo de componente que afectan, si se encuentra ligado con alguna campaña de compromiso y el nivel de criticidad con base a CVSS V 3.1.

THREAT INTELLIGENCE

Una amenaza novel que incorpora funciones de troyano y spyware, además de ser multiplataforma y modular.

EN NUESTRA REGIÓN

Se denuncian ciberataques relacionados con el conflicto Rusia-Ucrania

MNEMO

TEMA DEL MES

Detienen a miembros del ransomware REvil

Las autoridades rusas arrestan 14 personas con la ayuda de EE. UU.

REvil, también conocido como **Sodinokibi**, es un programa malicioso de tipo **ransomware** que ha estado activo desde abril de 2019 y ha sido distribuido bajo la modalidad de "**RaaS**" (Ransomware como servicio), donde los actores de amenaza ofrecen el software a otros atacantes y reciben un porcentaje por el rescate solicitado a las víctimas. REvil se cree que es la evolución del ransomware **GandCrab**, que fue identificado por primera vez en enero de 2018; sin embargo, este terminó con sus operaciones en marzo de 2019. Durante el año pasado, REvil afectó a grandes organizaciones, como el proveedor de carne JBS, el cliente del software desarrollado por Kaseya y Apple, entre otros.

En el mes de julio de 2021, REvil suspendió sus actividades tras comprometer a diversas organizaciones mediante la **vulnerabilidad presente en el software** de Kaseya, y después de que el gobierno de **Estados Unidos** solicitara a **Rusia** tomar acciones ante los grupos de ransomware que operan en el país. Lo anterior, ocasionó que el sitio web y la infraestructura de REvil quedara fuera de línea. No obstante, en el mes de septiembre del mismo año se reestablecieron operaciones del ransomware.

Imagen 1. Yaroslav Vasinskyi de 22 años.

Imagen 2. Yevgeniy Polyanin.

Durante el mes de octubre del **2021**, se vio un **aumento en las campañas** maliciosas relacionadas con este programa. Además, en el mismo periodo, se **arrestaron en Polonia a dos presuntos afiliados** de nombres Yaroslav Vasinskyi y Yevgeniy Polyanin; sin embargo, estas personas quedaron en espera de extradición por parte de Estados Unidos. En noviembre fueron arrestadas de manera oficial por el gobierno.

En el mes de octubre, autoridades de Alemania vincularon a un hombre nombrado "Nikolay K." como un posible autor intelectual del ransomware, tras descubrirse una serie de **transacciones en bitcoin** relacionadas con **pagos de rescates**, una cuenta de **correo electrónico registrado en 60 sitios web**,su número de teléfono asociado a una **cuenta de Telegram** de comercio de **criptomonedas** y pagos de rescate. A pesar de ello, no pudo ser detenido debido al acuerdo de extradición del país.

Posteriormente, Europol detuvo a algunas personas como presuntos afiliados de REvil y GandCrab. Hasta el momento no se conoce información acerca del nombre de las personas detenidas.

Las campañas de REvil continuaron a lo largo de los meses aunque el 14 de enero de **2022,** el Servicio Federal de Seguridad (FSB) de **Rusia**, en cooperación con el Departamento de Investigación del Ministerio Interior del país, informaron acerca del **arresto de 14 miembros** en 25 direcciones en Moscú, San Petersburgo, Leningrado y Lipetsk. En adición, las autoridades también lograron identificar a todos los miembros del grupo REvil y pudieron documentar su actividad y establecer su participación en transacciones fraudulentas. No obstante, hasta la fecha se desconoce si los 14 detenidos son la totalidad de la operación o hay más personas involucradas.

.

La FSB comunicó que el arresto se logró gracias a la **información proporcionada por Estados Unidos** sobre el líder criminal debido a su participación en ataques a organizaciones de ese país. Con esta información, **la autoridad logró confiscar** la cantidad aproximada de **6.6 millones de dólares**, los cuales de forma detallada fueron:

- Más de 426 **millones** de **rublos**
- 600 mil **dólares** americanos
- 500 mil **euros**
- 20 **autos de lujo**
- **Equipos** informáticos
- Un estimado en 6,698,728 rublos de cuentas de **criptomonedas**

Según las investigaciones, se cree que la **operación** del ransomware REvil **generó más de 200 millones de dólares** y **afectó** al menos a **175 mil sistemas alrededor del mundo**.

Las 14 personas arrestadas fueron acusadas de ser parte de la operación de REvil, de la creación de este y de la implementación del ransomware en redes empresariales en todo el mundo.

Imagen 3. FSB arresta a 14 miembros del ransomware REvil

Además, de acuerdo con los informes emitidos por las autoridades rusas, se comunicó que **los miembros del ransomware REvil no serán extraditados a Estados Unidos**, ya que, el gobierno ruso no cuenta con un mecanismo legal para extraditar a sus propios ciudadanos.

Imagen 4. FSB arresta a 14 miembros del ransomware REvil.

Durante varios años se ha visto como algunos grupos de ransomware desaparecen pero, otros nuevos surgen, siendo una mejora del primero. Un ejemplo de ello es el ransomware REvil/Sodinokibi que fue la **evolución** de GandCrab y ahora se ha visto al ransomware **BlackMatter** que asegura ser la evolución de REvil.

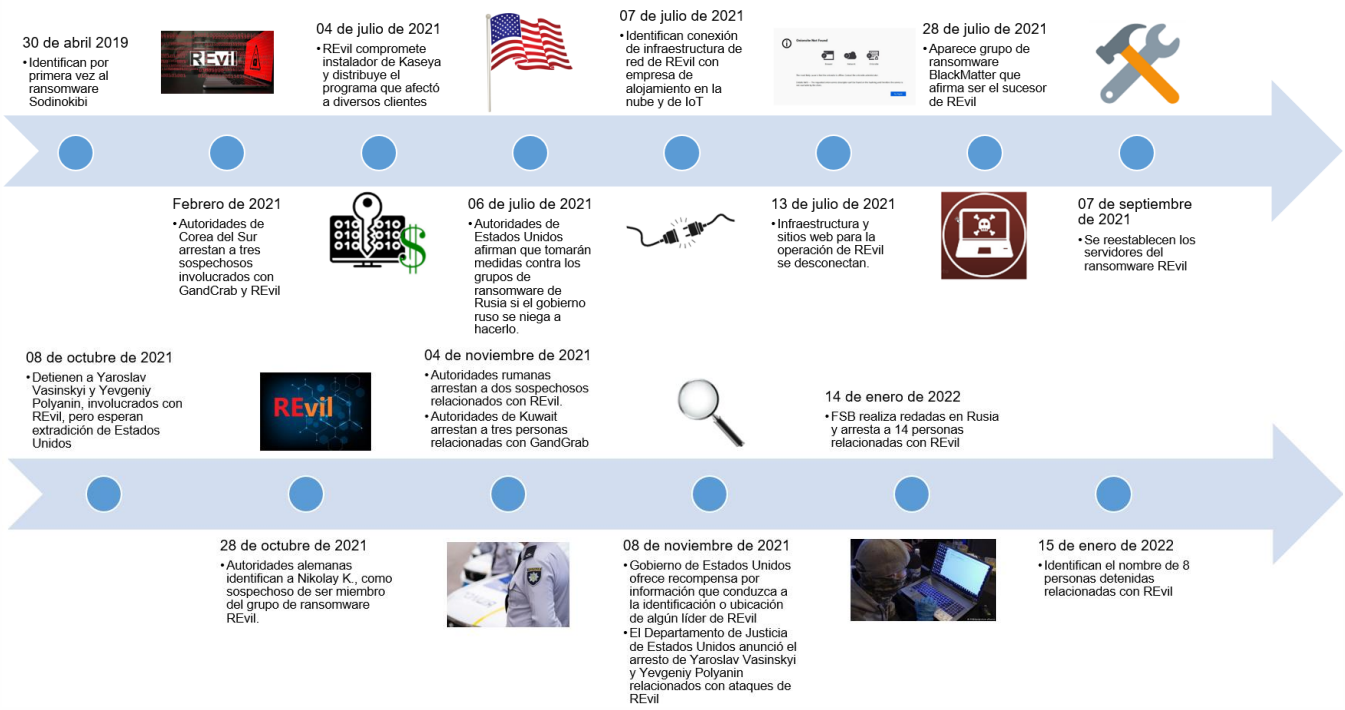


Imagen 5. Línea de tiempo de acontecimientos importante relacionados con REvil.

Santiago Gutiérrez Yazmin Yanela

Consultor de CTI

Las autoridades realizan un gran esfuerzo por detener la actividad malintencionada de grupos de amenaza. **REvil** hizo que las autoridades redoblaran esos esfuerzos tras afectar a grandes compañías en Estados Unidos, quien en conjunto con autoridades internacionales y tras ejercer presión sobre Rusia, lograron detener la actividad del grupo. Sin embargo, no está claro cuál es papel de los detenidos dentro de REVil. Por otro lado, los ucranianos Vasinskyi y Polyani extraditados a Estados Unidos enfrentan cargos que podrían darles pena máxima de 115 y 145 años de prisión, mientras que, **los afiliados detenidos en Rusia** podrían enfrentar **cargos por menos de 10 años**. No cabe duda que, el grupo obtuvo **ganancias** impresionantes a lo largo de su operación actual y que la aplicación de la **ley** en algunos países puede ser **favorable** para que estos grupos continúen. A pesar de ello, las acciones de **Rusia** han causado gran **incertidumbre** a los actores maliciosos dentro de la **Dark Web**, ya que, se comienzan a verse **observados por las autoridades**.

VULNERABILIDADES

Principales vulnerabilidades de enero 2021

Oracle, Samba, Zabbix, Microsoft, Wordpress

Titulo	Identificador	CVSS	Descripción
Falla de seguridad presente en productos de **Oracle**	CVE-2022-21275	CVSS v3.1: 10.0 [Crítico]	Vulnerabilidad presente en el componente **Connection Manager** de **Oracle Communications Applications** versiones **12.0.0.3** y **12.0.0.4**. Un atacante no autenticado con acceso a la red podría aprovechar el fallo y tomar el control del sistema afectado.
Falla de seguridad presente en productos de **Oracle**	CVE-2022-21390	CVSS v3.1: 10.0 [Crítico]	Vulnerabilidad presente en el componente **Webservices Manager** de **Oracle Communications Applications** versiones **12.0.0.3** y **12.0.0.4**. Un atacante no autenticado con acceso a la red podría aprovechar el fallo a través de HTTP y tomar el control del sistema afectado.
Falla de seguridad presente en productos de **Oracle**	CVE-2022-21389	CVSS v3.1: 10.0 [Crítico]	Vulnerabilidad presente en el componente **Connection Manager** de **Oracle Communications Applications** versiones **12.0.0.3** y **12.0.0.4**. Un atacante podría aprovechar el fallo a través de HTTP, afectar a productos adicionales y tomar el control del sistema afectado.
Falla de seguridad presente en productos de **Oracle**	CVE-2021-35683	CVSS v3.1: 9.9 [Crítico]	Vulnerabilidad presente en el componente **EAS Console** de **Oracle Essbase** versiones anteriores a **11.1.2.4.047**. Un atacante con pocos privilegios podría aprovechar el fallo a través de HTTP y tomar el control de la instancia afectada.
Falla de seguridad presente en **Samba**	CVE-2022-44142	CVSS v3.1: 9.9 [Crítico]	Vulnerabilidad presente en **Samba** versiones anteriores a **4.13.17**, es una falla de tipo out-of-bounds en las instalaciones que usan el módulo VFS vfs_fruit. Un atacante podría aprovechar el fallo y ejecutar código arbitrario como usuario administrador en la instancia afectada.
Falla de seguridad presente en **Zabbix**	CVE-2022-22704	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en el paquete **zabbix-agent2** para **Alpine Linux**, la cual podría permitir que un actor malicioso eleve privilegios en la instancia afectada.
Falla de seguridad presente en productos de **Microsoft**	CVE-2022-21907	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en la pila del protocolo **HTTP** en el componente **http[.]sys**. La falla puede ser aprovechada por los actores de amenaza para enviar paquetes especialmente diseñados y ejecutar código arbitrario de forma remota.
Falla de seguridad presente en **WordPress**	CVE-2021-25032	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en el complemento de **PublishPress Capabilities** de **WordPress** versiones anteriores a **2.3.1** debido a la falta de verificaciones CDRF. Un atacante no autenticado podría actualizar las opciones del blog vulnerable y convertir a cualquier nuevo usuario registrado como administrador.
Falla de seguridad presente en **WordPress**	CVE-2021-24949	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en un widget del plugin **The Plus Addons for Elementor** de **WordPress** anteriores a **5.0.7**. Un usuario malintencionado podría realizar una inyección de SQL y modificar la base de datos.
Falla de seguridad presente en productos de **Microsoft**	CVE-2022-21849	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en la extensión **IKE** de **Windows**. Un atacante podría aprovechar el fallo y permitir la ejecución de código en la instancia afectada de forma remota.

MNEMO-CERT presenta las 10 vulnerabilidades más representativas que fueron identificadas en el mes de enero de 2022, tomando en cuenta el tipo de componente que afectan, si se encuentra ligado con alguna campaña de compromiso y el nivel de criticidad con base a CVSS V 3.1.

En los primeros tres lugares se encuentran posicionadas vulnerabilidades presentes en productos de **Oracle** quien, en este mes, resolvió diversos problemas de seguridad en varios de sus productos. Las fallas se encuentran presentes en los componentes **Connection Manager**, **Webservices Manager** y **Connection Manager** de **Oracle Communications Applications**, permitiendo que un atacante no autenticado pueda tomar el control del sistema afectado. **MNEMO-CERT** publicó un aviso referente a estas vulnerabilidades, los cuales pueden ser consultados en la siguiente URL:

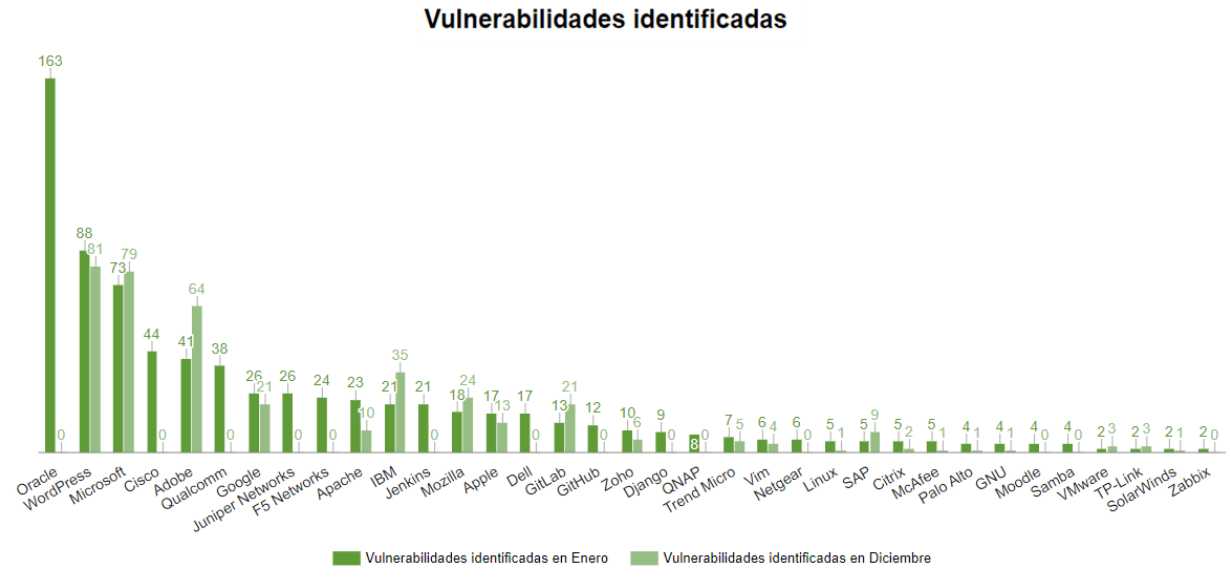
- https://mailchi.mp/mnemo.com/aviso-de-seguridad-oracle-publica-actualizaciones-de-seguridad-para-corregir-fallas-en-varios-de-sus-productos

En la siguiente posición se encuentra una vulnerabilidad presente en **Oracle Essbase**, la cual requiere baja complejidad para ser aprovechada y permite a los atacantes tomar el control de la instancia afectada.

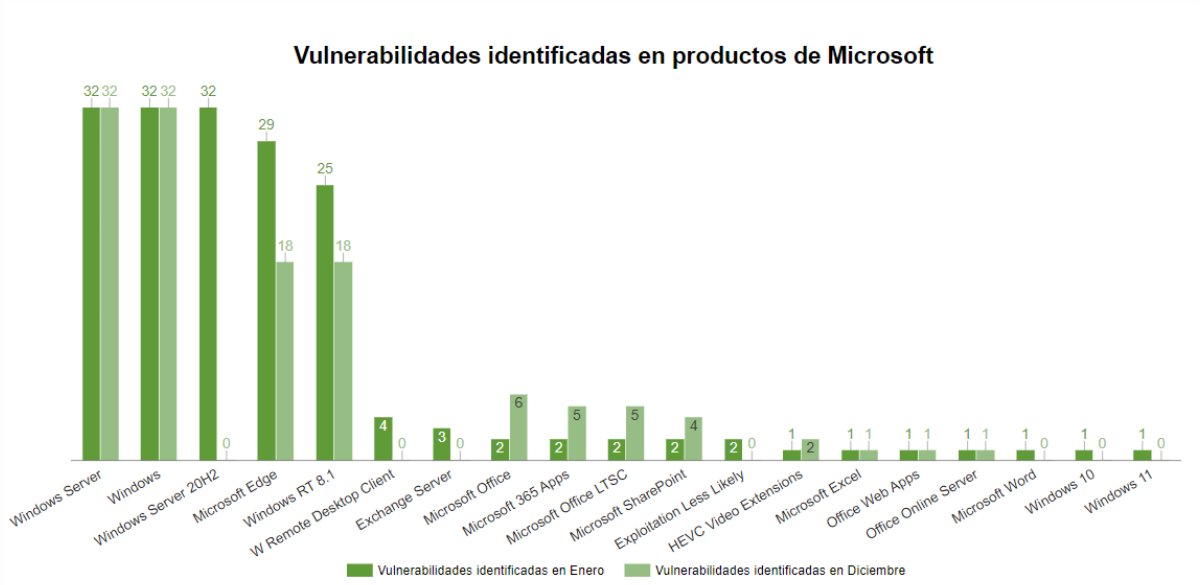
Posteriormente, se destaca una vulnerabilidad de **Samba** que permite a los actores de amenaza ejecutar código arbitrario como usuario administrador en el equipo vulnerable. **MNEMO-CERT** emitió un aviso relacionado con esta vulnerabilidad y las correcciones publicadas, el cual puede ser consultado en la siguiente URL:

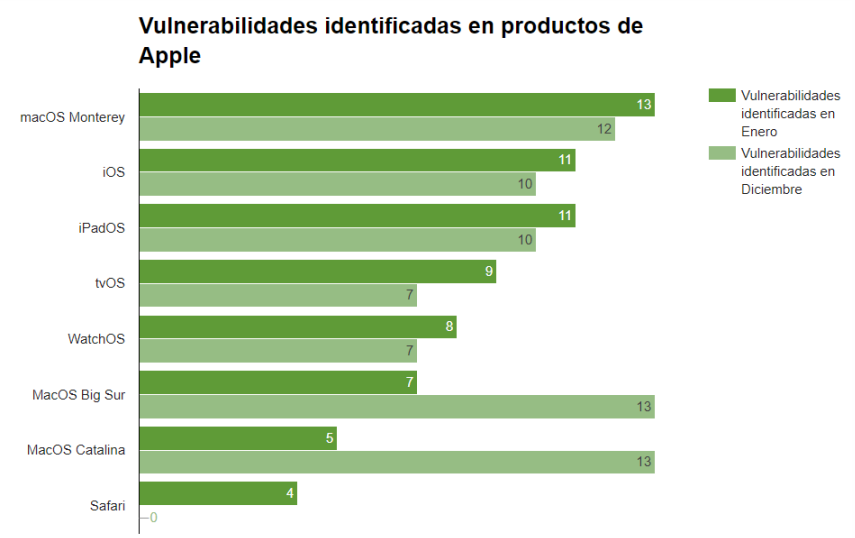
- https://mailchi.mp/mnemo.com/aviso-de-seguridad-samba-corrige-vulnerabilidades-en-su-producto

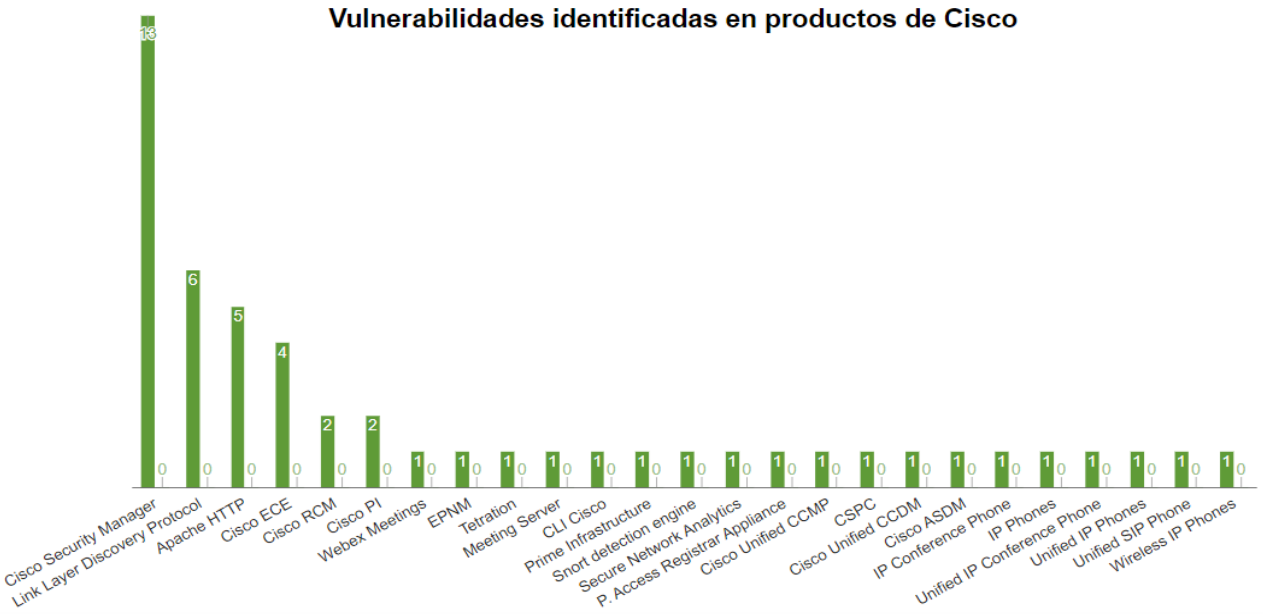
Asimismo, cabe señalar que, durante este mes varios fabricantes corrigieron diversos fallos en sus diferentes productos, siendo los más destacados "**Oracle**", "**WordPress**", "**Microsoft**" y "**Cisco**"; a comparación del mes pasado, en donde las más sobresalientes fueron "Microsoft", "WordPress", "Adobe" y "Huawei".

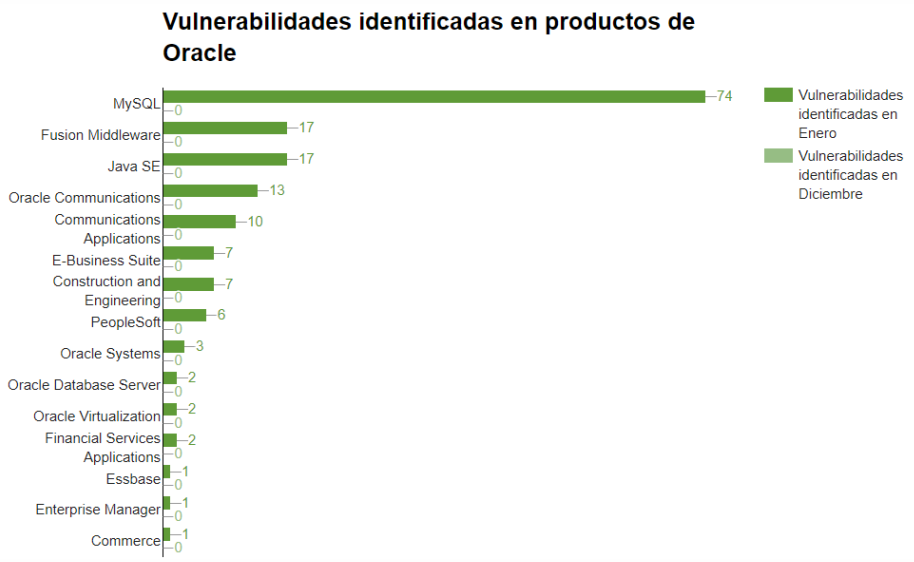


Del mismo modo, en las siguientes gráficas se muestra el **número de vulnerabilidades por producto para los fabricantes** con mayor cantidad de fallas identificadas en el mes de enero de 2022 y un comparativo con el mes de diciembre de 2021.

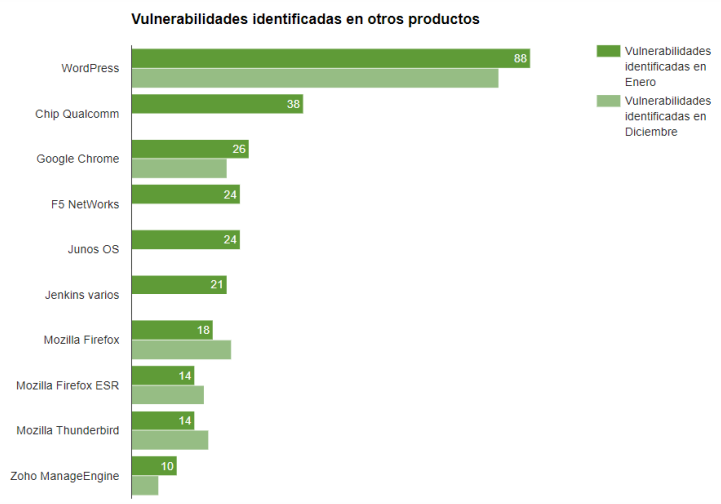





Vulnerabilidades identificadas en productos de Cisco
13
6
5
4
2
2
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
0
Cisco Security Manager
Link Layer Discovery Protocol
Apache HTTP
Cisco ECE
Cisco RCM
Cisco PI
Webex Meetings
EPNM
Tetration
Meeting Server
CLI Cisco
Prime Infrastructure
Snort detection engine
Secure Network Analytics
P. Access Registrar Appliance
Cisco Unified CCMP
CSPC
Cisco Unified CCDM
Cisco ASDM
IP Conference Phone
IP Phones
Unified IP Conference Phone
Unified IP Phones
Unified SIP Phone
Wireless IP Phones


Vulnerabilidades identificadas en productos de Oracle
MySQL
Fusion Middleware
Java SE
Oracle Communications
Communications Applications
E-Business Suite
Construction and Engineering
PeopleSoft
Oracle Systems
Oracle Database Server
Oracle Virtualization
Financial Services Applications
Essbase
Enterprise Manager
Commerce
74
17
17
13
10
7
7
6
3
2
2
2
1
1
1
0
Vulnerabilidades identificadas en Enero
Vulnerabilidades identificadas en Diciembre


Vulnerabilidades identificadas en productos de Adobe
Adobe Reader
Adobe Acrobat
Bridge
Adobe InCopy
Adobe InDesign
Illustrator
26
26
6
3
4
3
2
0
Vulnerabilidades identificadas en Enero
Vulnerabilidades identificadas en Diciembre



Producto	Vulnerabilidades identificadas en Diciembre	Vulnerabilidades identificadas en Enero
Django	1	9
GitHub	0	7
GitLab	0	7
GitLab CE/EE	16	6
Vim	4	6
NETGEAR productos	0	6
Kernel de Linux	1	5
Trens Micro Apex One	1	5
QNAP QVR Elite	0	5
Junos OS Evolved	0	5
Trend Micro Worry-Free Business Security	4	4
Palo Alto Networks Cortex XDR	0	4
Moodle	0	4
GNU	0	4
Citrix Hypervisor	0	4
Citrix XenServer	0	4
Samba	0	4
TP-Link varios	3	2
Apache NiFi	1	2
SolarWinds	1	2
zabbix	0	2
Trend Micro Deep Security	0	2
Trend Micro Cloud One	0	2
SAP Business One	1	2
QNAP QcalAgent	0	2
McAfee Agent	0	2
Workstation Pro	0	2
PowerVM Hypervisor	2	1
SAP NetWeaver	1	1
McAfeeData Loss Prevention (DLP) ePO	0	1
Citrix Workspace app	1	1
QNAP QuTS	0	1
SAP S/4HANA	1	1
VMware Cloud Foundation	0	1
Vmware ESXi	0	1
Horizon Client	0	1

SysJoker: nueva familia de malware multiplataforma

Una amenaza novel que incorpora funciones de troyano y spyware, además de ser multiplataforma y modular.

A finales del año 2021, investigadores de ciberseguridad identificaron una nueva amenaza que han denominado **SysJoker**. Se trata de un troyano modular y multiplataforma que incorpora: **técnicas de ofuscación** de información, mediante la implementación de algoritmia XOR; enumeración del **sistema comprometido**; envío de **información** de manera **cifrada** al servidor C2; y el establecimiento de **persistencia**, mediante la creación de una clave de registro.

En sistemas Linux, se ha observado como los ciberdelincuentes detrás de SysJoker explotaban vulnerabilidades en servicios expuestos para desplegar la carga final del troyano en los servidores infectados. Para dispositivos con sistemas operativos MacOS, uno de los **vectores de infección** manejados por los analistas es la **distribución de paquetes npm** (Node Package Manager) que previamente han sido modificados incluyendo el payload de SysJoker.

La hipótesis generada por el equipo de analistas de Cyber Threat Intelligence de Mnemo es que los actores de amenazas utilizan correos electrónicos de tipo **phishing**, relacionado directamente a la subtécnica Spearphishing Attachment - T1566.001, con un archivo adjunto que contiene un cargador o, en su defecto, la carga final de SysJoker y, así, poder distribuir esta amenaza al menos en sistemas operativos Windows.

El archivo desplegado por los cibercriminales es un **ejecutable desarrollado en el lenguaje C++**, el cual utiliza técnicas de **cifrado a través del algoritmo XOR**. Muchas de las cadenas, que han sido cifradas mediante este algoritmo, están relacionadas con actividades llevadas a cabo en la **fase de post-explotación del sistema comprometido**.

El **equipo de CTI de Mnemo** ha tenido la oportunidad de analizar una de las muestras relacionadas con este malware. Lo primero que destaca es que los ciberdelincuentes han **modificado** deliberadamente los **metadatos del binario**, agregando información relacionada a un driver de la empresa Intel. De esta manera, buscan persuadir al usuario **para hacerle creer que es un software legítimo** y que no sospeche de la actividad maliciosa.

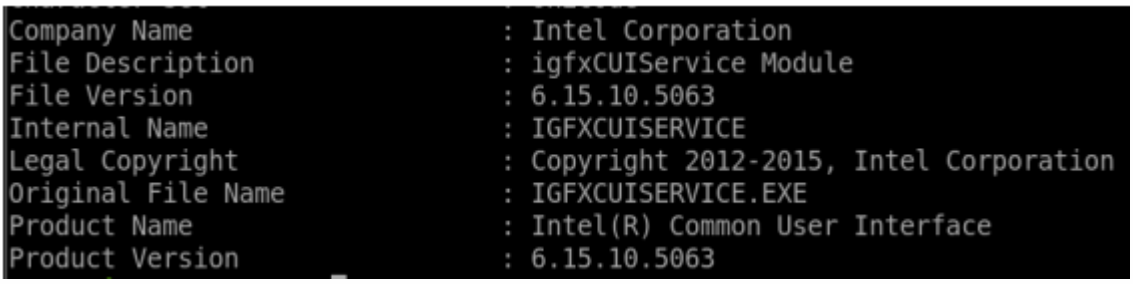


Imagen 1: Metadata de la muestra. Fuente: CTI Mnemo.

Tal y como se ha mencionado, uno de los **métodos de evasión** utilizados por este malware es la **inclusión de cadenas cifradas con el algoritmo XOR**. La clave para descifrar las cadenas se encuentra hardcodeada y, al realizar el análisis, se puede extraer y utilizar para descifrar todas las cadenas.

Además de utilizar el algoritmo XOR, usan **codificación en Base64** con el objetivo de sumar complejidad a la hora de identificar strings potencialmente maliciosas tanto para analistas de malware como para diferentes herramientas de seguridad.

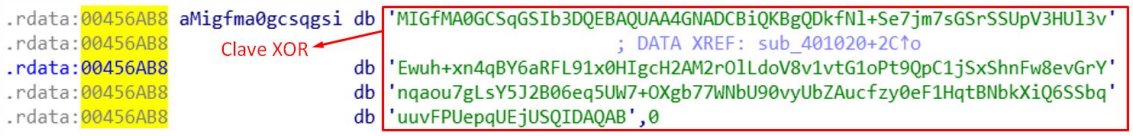


Imagen 2: Clave XOR utilizadas por SysJoker. Fuente: CTI Mnemo

Al realizar el proceso de descifrado y decodificado de varios strings, se encuentra información relacionada con: el nombre del driver legítimo que intenta suplantar SysJoker, la ejecución de comandos y el repositorio de Google Drive que contiene el dominio C2 al que debe establecer la comunicación el sistema infectado.

Imagen 3: Descifrado y decodificado de URL. Fuente: CTI Mnemo.

Este recurso de Google Drive alojaba un archivo denominado *domain.txt,* que contenía un dominio codificado que debía actuar como servidor C2. Al ya no estar disponible este recurso, no se ha permitido evidenciar más comunicaciones de la muestra de SysJoker.

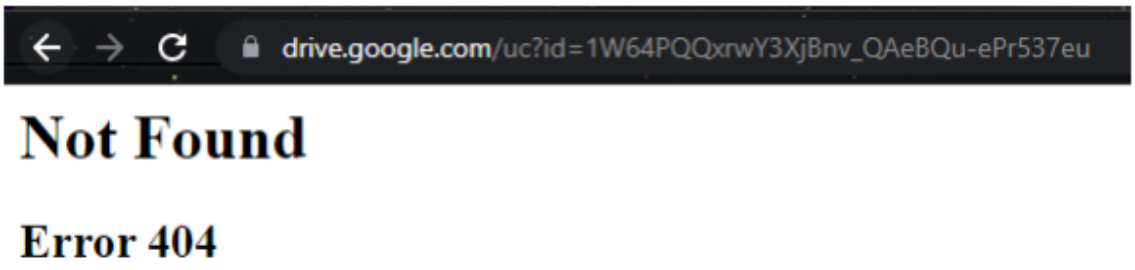


Imagen 4: Consulta del recurso en Google Drive. Fuente: CTI Mnemo.

Al realizar la **ejecución de la muestra**, se evidencia el uso de **PowerShell** para **copiarse a sí misma en la ruta** '*C:\ProgramData\SystemData*' con el nombre '*igfxCUIService.exe*', nombre de un driver legítimo de Intel que, como se había

mencionado antes, es utilizado para intentar hacer **evasión de defensas** al momento de ejecución.

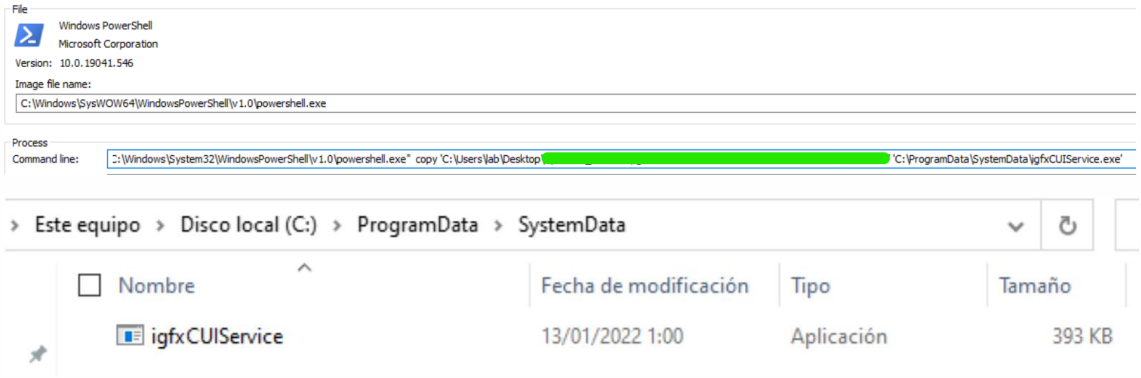


Imagen 5: Copia de la muestra en una nueva ruta del sistema. Fuente: CTI Mnemo.

Posteriormente, como **medidas de enumeración**, los ciberdelincuentes utilizan servicios legítimos del sistema operativo como ***getmac*** y el uso de consultas **WMI** (Windows Management Instrumentation) para **obtener información relacionada con el equipo** que ha sido **comprometido**.

Las consultas realizadas se exponen a continuación.

CONSULTAS	OBJETIVO
get Caption	Enumerar la versión del sistema operativo
get CSDVersion	Enumerar el Service pack instalado en el equipo
get OSArchitecture	Enumerar la arquitectura de la plataforma que ejecuta la aplicación
get Version	Enumerar la versión del sistema operativo

Este comando se encuentra codificado y puede ser descifrado con la clave hardcodeada enumerada previamente.

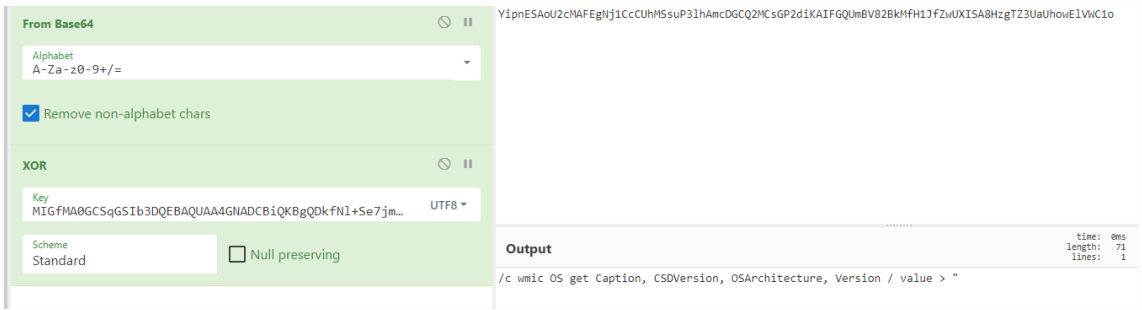


Imagen 6: Data decodificada y descifrada. Fuente: CTI Mnemo.

El output de esta ejecución de comandos va a ser redireccionado a un archivo situado en la carpeta previamente creada por los cibercriminales (*C:\ProgramData\SystemData*).

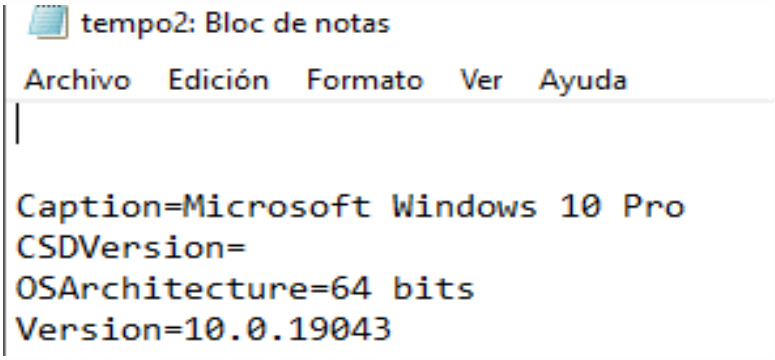


Imagen 7: Información recolectada por SysJoker. Fuente: CTI Mnemo.

Posteriormente, a través de PowerShell, se enumera la variable de entorno que almacena el nombre del usuario que ha ejecutado la muestra, redirigiendo la salida del comando a otro archivo creado en la misma carpeta.

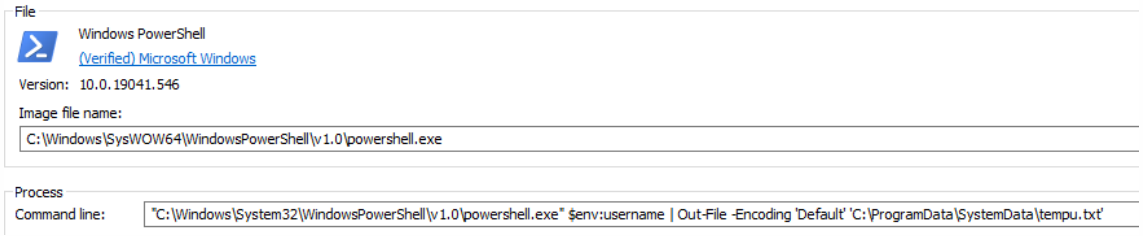


Imagen 8. Uso de Powershell para obtener información del sistema. Fuente: CTI Mnemo.

El último recurso que es generado en esta carpeta tiene el nombre ***Microsoft_Windows.dll*** y se trata de un archivo de texto que contiene **otra cadena codificada en base64 y cifrada**. Este será enviado hacia el servidor C2 que, como se mencionó al inicio del análisis, es obtenido desde un repositorio en Google Drive.

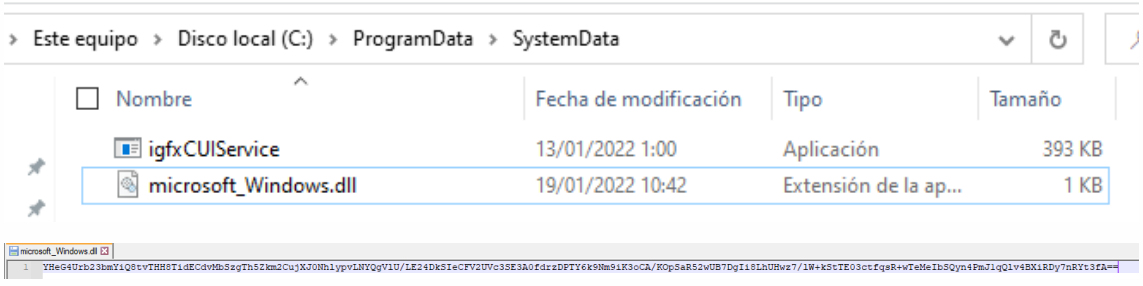


Imagen 9: Contenido del supuesto archivo DLL. Fuente: CTI Mnemo.

Además, se define el user-agent utilizado para enviar la información almacenada en los archivos de texto creados por los atacantes, objeto de la enumeración del sistema mediante los comandos expuestos previamente.

Por último, se exponen los parámetros que van a ser enviados a través del método POST a los servidores C2 mediante el protocolo seguro HTTPs, enviando información relacionada con el sistema comprometido.

```
.rdata:00456CA8                 text "UTF-16LE", 'Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) G'
.rdata:00456CA8                 text "UTF-16LE", 'ecko/20100101 Firefox/47.0',0
.rdata:00456D44 aContentLength:                         ; DATA XREF: sub_407A30+17D↑o
.rdata:00456D44                 text "UTF-16LE", 'Content-Length: ',0
.rdata:00456D66                 align 4
.rdata:00456D68 aContentTypeApp:                        ; DATA XREF: sub_407A30+1B2↑o
.rdata:00456D68                 text "UTF-16LE", 0Dh,0Ah
.rdata:00456D68                 text "UTF-16LE", 'Content-Type: application/x-www-form-urlencoded',0Dh
.rdata:00456D68                 text "UTF-16LE", 0Ah,0
.rdata:00456DD0 aDomain         db 'domain',0           ; DATA XREF: sub_4082E0+23E↑o
.rdata:00456DD0                                         ; sub_41A110+30↑r ...
.rdata:00456DD7                 align 4
.rdata:00456DD8 aIp             db '&ip=',0             ; DATA XREF: sub_408770+35E↑o
.rdata:00456DDD                 align 10h
.rdata:00456DE0 aAnti           db '&anti=',0           ; DATA XREF: sub_408770+2E6↑o
.rdata:00456DE7                 align 4
.rdata:00456DE8 aOs             db '&os=',0             ; DATA XREF: sub_408770+277↑o
.rdata:00456DED                 align 10h
.rdata:00456DF0 aUserToken87234 db '&user_token=8723478873487',0
.rdata:00456DF0                                         ; DATA XREF: sub_408770+22B↑o
.rdata:00456E0A                 align 4
.rdata:00456E0C aName           db '&name=',0           ; DATA XREF: sub_408770+1BC↑o
```

Imagen 10: Parámetros enviados mediante las comunicaciones con el C2. Fuente: CTI Mnemo.

Para establecer la **persistencia** en el equipo comprometido, se genera una **clave de registro de autoarranque**, creando un nuevo valor con el nombre del servicio legítimo de Intel (***igfxCUIService***) apuntando al archivo ejecutable que ha sido copiado en la carpeta creada previamente.

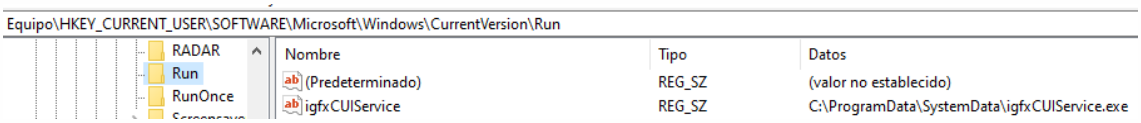


Imagen 11: Llave de registro creda para generar persistencia. Fuente: CTI Mnemo.

Esta clave genera persistencia únicamente para el usuario que haya ejecutado la muestra debido a que es creada en el hive del Current User (HKCU) y no de la Local Machine (HKLM). Esta última, permitiría que cada vez que cualquier usuario iniciase sesión en el sistema, se ejecutáse la muestra de SysJoker.

Otra de las funcionalidades desarrolladas por los cibercriminales, es la **creación de diversas funciones** que serán llamadas o ejecutadas desde los **servidores C2**. Los comandos funcionales son los siguientes:

Comando	Uso
Exe	Descarga y posterior ejecución de familias de malware adicionales.
Cmd	Ejecución de comandos y subida del resultado al servidor C2
Exit	Salida del cliente del troyano.
Remove_reg	Eliminación de clave de registro generada para la persistencia.

SysJoker es una **amenaza novel** debido a que su actividad maliciosa fue identificada a finales del año 2021 y **no se han detectado campañas relacionadas** con esta familia. Sin embargo, las investigaciones declaran que su **carga final se encuentra desarrollada desde cero**, lo cual indica que los actores de amenazas detrás de SysJoker podrían haber adquirido **el código fuente de terceros** o haberlo **desarrollado de forma íntegra**. Por lo anterior, se podría predecir que las campañas en que sea utilizado serán sumamente prolíficas, debido a las múltiples funcionalidades que contiene y a su categorización como un troyano multiplataforma.

Desde el equipo de analistas de CTI de Mnemo, se prevé que este nuevo malware podría ser muy utilizado en futuras campañas de infección a nivel mundial pero además, que podrá ser **utilizado como malware de primera etapa para la entrega y ejecución de otras** familias de malware como **ransomware**.

Además del análisis que se ha realizado a la muestra de SysJoker, se han generado las siguientes reglas de tipo Yara y de tipo SIGMA para su identificación.

REGLA YARA

```
rule MN_SysJoker {
      meta:
      description = "Detects suspicious strings related to SysJoker
Trojan"
      reference = "Internal Research"
      author = "Cyber Threat Intelligence de Mnemo"
      strings:
            $a1 = "user_token"
            $a2 = "/api/attach"
            $a3 = "token"
            $a4 = "/api/req/res"
            $a5 = "tempu.txt"
            $a6 = "temps1.txt"
            $a7 = "temps2.txt"
            $a8 = "tempo1.txt"
            $a9 = "tempo2.txt"
            $a10 = "961c151d2e87f2686a955a9be24d316f1362bf21"
            $xorDomain                                          =
"JT0zFj57H2gnIRgxNmcFXCs2KSdvMjosbkEkcSggfnM+Z38SNgA8GREXX3M5J1kcMmYy
IhEjJn4wICQGe2IJRg=="
            $xorWMIip                                           =
"YipnESAoU2ctOhIkPCcEWiNxMiokIzBhZn0XCy8lIS4MNWt/RwU2HgNpTEw2ERcDHVYX
IyEXICB1TnYR"
```

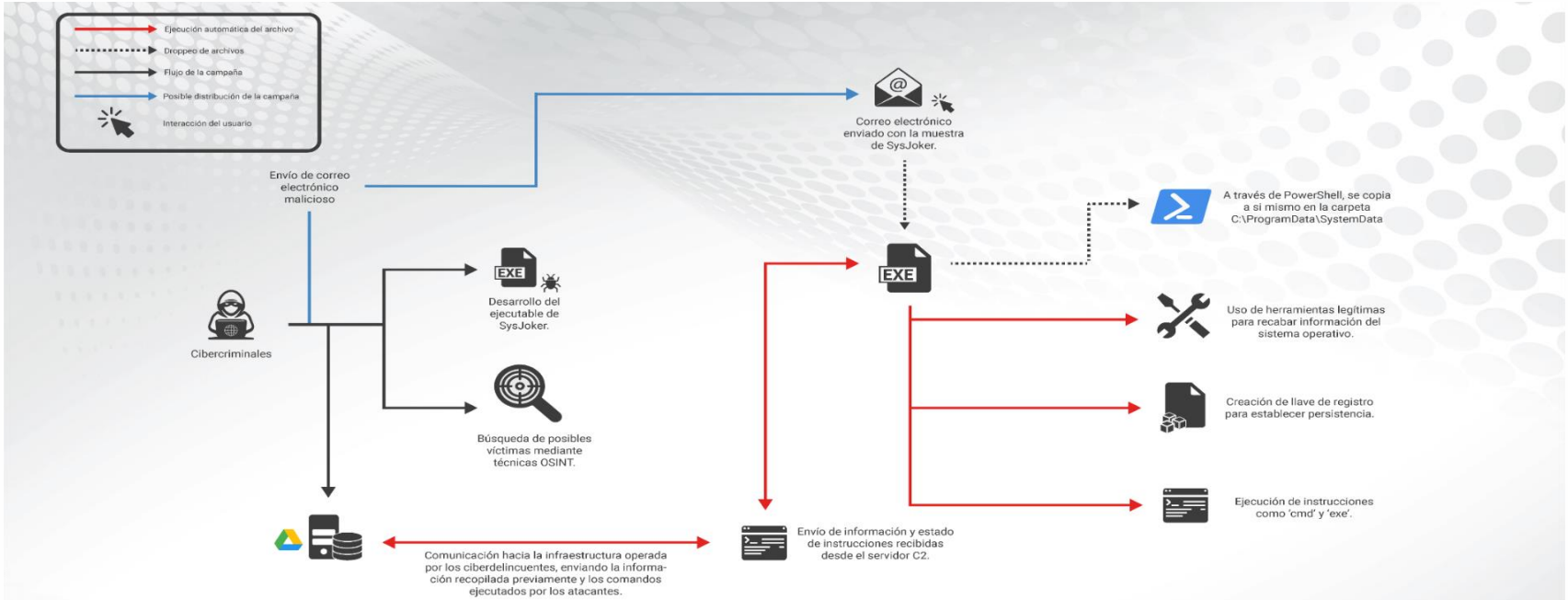
```
            $xorWMIcommand                                                  =
"YipnESAoU2cMAFEgNj1CcCUhMSsuP3lhAmcDGCQ2MCsGP2diKAIFGQUmBV82BkMfH1Jf
ZwUXISA8HzgTZ3UaUhowElVWC1o"
            $xorKey                                                         =
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDkfNl+Se7jm7sGSrSSUpV3HUl3vEwu
h+xn4qBY6aRFL91x0HIgcH2AM2rOlLdoV8v1vtG1oPt9QpC1jSxShnFw8evGrYnqaou7g
LsY5J2B06eq5UW7+OXgb77WNbU90vyUbZAucfzy0eF1HqtBNbkXiQ6SSbquuvFPUepqUE
jUSQIDAQAB"
            $xorProgramData = "ERk1CSozUSoHMgUm"
            $xorSystemData = "ERo+FTkkXQMiJxA="
            $xorName = "JC4hHg4UeRQmIQcuMCxMVjw0"
            $xorDLL = "ESQuBT8uQyglJy4QOicGXDMiayYtPQ"
            $xorPowerShell = "PSYwAz8yWCIvP18iKyw"
      condition:
            uint16(0) == 0x5A4D and 9 of ($a*) and 6 of ($xor*)


}
```

REGLA SIGMA

```
title: SysJoker Windows detection
id: 85343fd0-00a0-477a-8c70-d79abd81f937
status: experimental
description: Rule to detect malicious behaviour related to
command-line based SysJoker activity in a Windows system
author: Mnemo Cyber Threat Intelligence Team
references:
    -      https://threatpost.com/undetected-sysjoker-backdoor-
malwarewindows-linux-macos/177532/
date: 2022/01/28
tags:
    - attack.t1059.003 # Command and Scripting Interpreter -
Windows Command Shell
    - attack.1047 # Windows Management Instrumentation
    - attack.execution
    - attack.1547.001 # Registry Run Keys / Startup Folder
    - attack.persistence
logsource:
```

```
        product: windows
        category: process_creation
    detection:
        selection1:
            CommandLine|contains|all:
                - 'ProgramData'
                - 'SystemData'
                - 'igfxCUIService'
        selection2:
            CommandLine|contains:
                - 'wmic OS get Caption, CSDVersion, OSArchitecture,
    Version'
                - 'wmic nicconfig'
                - 'get ipaddress'
        selection3:
            CommandLine|contains:
                - 'tempu.txt'
                - 'tempo1.txt'
                - 'tempi1.txt'
                - 'temps1.txt'
                - 'temps2.txt'
        condition: selection1 or selection2 or selection3
    falsepositives:
        - Unknown
    level: high
```

THREAT INTELLIGENCE



Reconnaisance / Weaponization / Delivery

- Los actores de amenazas que distribuyen SysJoker utilizan técnicas de búsquedas en fuentes abiertas de información en busca de potenciales víctimas.
- Los ciberdelincuentes desarrollan un archivo ejecutable con múltiples capacidades, que contiene la carga maliciosa del troyano SysJoker.
- A través de técnicas de ingeniería social, los cibercriminales envían la muestra de SysJoker a las víctimas que han identificado en la fase de reconocimiento.

Exploitation / Installation

- Las víctimas ejecutan de manera manual el archivo ejecutable de SysJoker. De forma automática, a través de PowerShell, se realiza la copia del propio archivo malicioso en la carpeta previamente creada C:\ProgramData\SystemData.
- Mediante la ejecución de PowerShell a través del ejecutable de SysJoker, se genera una clave de registro para establecer la persistencia.

C2 / Actions on Objectives

- Los actores de amenazas realizan consultas a través de WMI y getmac para realizar una enumeración del sistema comprometido, redirigiendo la salida de los comandos a archivos ubicados en la carpeta C:\ProgramData\SystemData.
- Cuando finalizan las labores de enumeración, los atacantes envían de manera cifrada a través de HTTPs la información que ha sido recopilada a los servidores de Comando y Control ubicados en la infraestructura de los ciberdelincuentes. Además, los atacantes definen ciertas variables que son llamadas para enviar información desde los servidores de Comando y Control.

EN NUESTRA REGIÓN

Riesgo inminente de guerra cibernética

Se denuncian ciberataques relacionados con el conflicto Rusia-Ucrania

En noviembre de 2021 **Rusia comenzó a desplegar tropas frente a la frontera con Ucrania**, iniciando una **crisis internacional** en la que se ven implicadas la Unión Europea y la OTAN, entre otros. Esta crisis, lejos de resolverse, sigue aumentando cada día debido al fracaso de las conversaciones entre los actores implicados. Sin embargo, durante el mes de enero se ha dado un paso más, puesto que se han iniciado diversos **ciberataques vinculados al conflicto**. Por tanto, se abre el posible escenario de guerra en el mundo ciber.

Recientemente, **Ucrania** ha denunciado un **ciberataque masivo** contra varios **sitios web del gobierno**, que logró incluir en ellos **mensajes amenazantes contra los ciudadanos**. Estos mensajes, escritos en ruso, polaco y ucraniano decían: "*¡Ucranianos! Todos vuestros datos personales han sido colgados en la red.* ***Tened miedo y esperad lo peor****. Todos los datos que hay en el ordenador se destruyen y es imposible recuperarlos. Toda la información sobre vosotros se ha hecho pública (...) Esto es por vuestro pasado, presente y futuro*". Aunque por el momento **no se puede atribuir el ataque a Rusia**, es evidente que está relacionado con el actual conflicto entre ambas naciones y que busca generar sentimientos y emociones de miedo en la ciudadanía, lo que puede considerarse como **guerra psicológica**.

Por otro lado, el grupo conocido como **Belarusian Cyber-Partisans** han declarado que **violaron y cifraron servidores** de la compañía **ferroviaria estatal nacional** de Bielorrusia, en **señal de protesta** por haber permitido que **Rusia utilizara** la red de **transporte ferroviario** para **trasladar unidades y equipos militares al país**. Para devolver la normalidad a los sistemas piden la liberación de 50 presos políticos que necesitan asistencia médica y quieren que las tropas rusas salgan de Bielorrusia. Los piratas informáticos afirman que este ataque es parte de una **campaña** más extensa que denominan "**Infierno: los ciberataques de sabotaje más grandes en la historia de Bielorrusia**"

Ante esto, y en base a sus fuentes de inteligencia, el **Departamento de Seguridad Nacional de Estados Unidos**, ha emitido un informe en el que declara que si EE. UU. responde a las crecientes tensiones, el **gobierno ruso o sus actores patrocinados** por el estado podrían iniciar un **ataque cibernético**. Desde un posible ataque de denegación de servicio de bajo nivel hasta un ataque destructivo en infraestructura crítica.

Se hace evidente que todos aquellos **países e instituciones que tomen partido** en este conflicto se convierten en **víctimas potenciales de ciberataques** como represalia.

Nuestras redes

LINKEDIN @mnemo

TWITTER @_mnemo

FACEBOOK @mnemo

YOUTUBE @GrupoMnemo

INSTAGRAM @mnemo_ciber

www.mnemo.com

info@mnemo.com

MNEMO