MNEMO

CIBERBOLETÍN

Diciembre 2020

CONTENIDOS

ARCHIVOS VHD COMO CONTENEDORES DE MALWARE

Un método sencillo para una distribución evasiva

Entre noviembre y diciembre investigadores identificaron y analizaron una nueva campaña que implicaba el uso de ficheros VHD como un método para distribuir una nueva versión de un malware conocido, el troyano **Zebrocy**, que se encuentra escrito en Go.

Mediante el uso de la técnica del *spear-phishing* acompañado de una temática relativa a la pandemia producida por la Covid-19, se suplantaba la identidad de **Sinopharm International Organization.** El objetivo era inducir a sus víctimas a que ejecutaran el contenido malicioso que albergaban los ficheros VHD.

El usuario debía **montar el archivo VHD para poder acceder al interior del disco duro virtual**, en él se encontraba un documento en formato PDF y otro que era **un ejecutable que se hacía pasar por un documento Word**. Tras la ejecución del falso documento Word, se iniciaba la infección del dispositivo de la víctima con Zebrocy. Los cibercriminales usaron la funcionalidad por defecto de Windows de ocultar extensiones de archivo, lo que hacía más creíble el engaño ya que el documento disponía de un icono de Microsoft Word.

El formato de fichero **VHD** (*Virtual Hard Drive*) puede almacenar contenido como si fuera un disco duro. La tecnología de virtualización de Microsoft, **Hyper-V,** adoptó este formato como su formato nativo, que en este caso permite al usuario montarlo y acceder a su contenido.

Por otro lado, el formato **VHDX** es compatible con Microsoft Server 8 y tiene algunas funciones más modernas respecto a su formato antecesor, entre las que se destacan la capacidad de redimensionar su tamaño hasta 64 terabytes o sus mecanismos de prevención de corrupción de datos.

Desde Windows 8 y versiones superiores, un usuario puede montar este fichero solamente haciendo doble clic. Una vez es montado el fichero VHD, una imagen de disco duro VHD se muestra al sistema operativo de Windows. Es posible acceder a la información que contiene a través de herramientas de descompresión como 7-zip, WinRar o VHDtool.

Esta no es la primera vez que cibercriminales han empleado este tipo de distribución a través de VHD para evadir los sistemas de detección, si bien, no es el método más comúnmente empleado. En septiembre de 2019, fueron reportados incidentes donde **Windows, Google y otras soluciones antivirus fallaban al detectar el malware almacenado dentro de archivos VHD**.

Para poder realizar un escaneo de los documentos que un VHD contiene, previamente se debe montar como se haría con un disco duro. Las tecnologías como Gmail o Chrome no son capaces de montar/descomprimir archivos VHD dado que no son considerados como posibles contenedores de malware. Cabe destacar que este tipo de extensiones de archivos (VHD y VHDX) no se encuentran en la lista negra de Gmail en la actualidad.

El equipo de analistas de Cyber Threat Intelligence de Mnemo ha realizado trabajos de comprobación de la vigencia de este método evasivo en el año 2020, por lo tanto, se han realizado pruebas para comprobar la evasión de los sistemas defensivos en diferentes clientes de correo electrónico y soluciones antivirus.

A continuación, se muestra el resultado de las pruebas realizadas, pudiendo comprobar de forma explícita cómo se puede enviar un fichero VHD que contiene una muestra del malware **PyXie**, catalogada como malicioso. Es necesario destacar que la misma prueba se realizó con un archivo ZIP que contenía la misma muestra de malware.

El malware, en el caso del archivo VHD, no fue detectado por lo que este método de distribución representa una ciberamenaza más en el panorama de la ciberseguridad. Por el lado contrario, el malware que se encontraba dentro del archivo ZIP si era detectado por los diferentes servicios como Gmail.

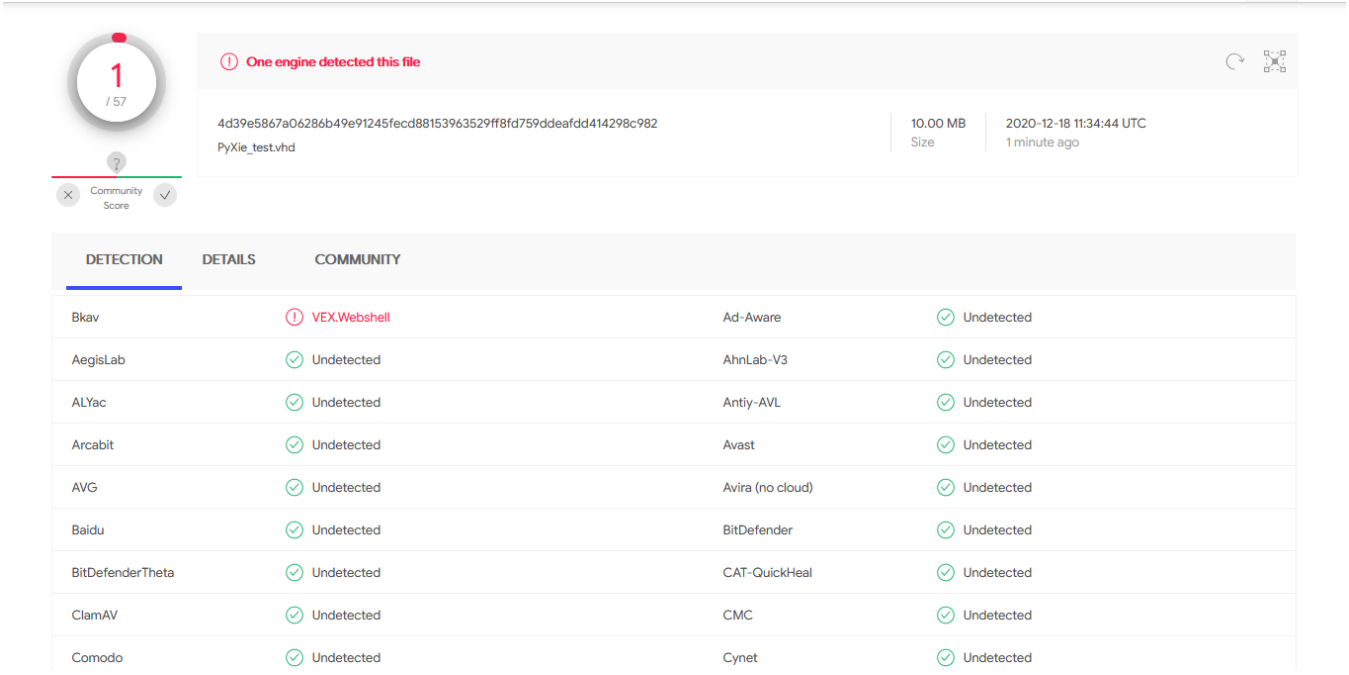
GMAIL

- Fichero ZIP detectado

- Fichero VHD no detectado

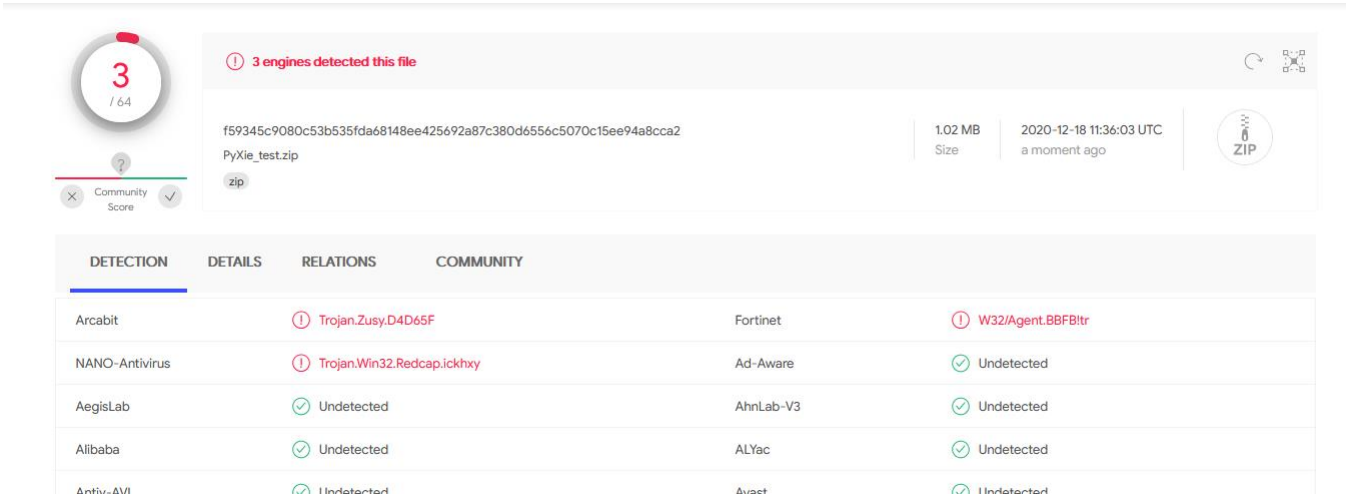
VIRUSTOTAL

El fichero VHD empleado para esta prueba se subió a la plataforma de VirusTotal. El resultado determinó que existían unos niveles de detección muy bajos (1/57), tal y como se puede comprobar en la imagen a continuación.



Añadido a esto, no se han obtenido evidencias de que ninguno de los escáneres configurados en VirusTotal hayan conseguido escanear satisfactoriamente este fichero, salvo Bkav.

No obstante, el fichero ZIP ha obtenido una mejor detección dado que este formato de fichero si es contemplado como un contenedor de malware.



Dada la sencillez en la que un cibercriminal puede utilizar un fichero VHD como un vehículo para alojar malware, así como las dificultades técnicas de los clientes de correo o el software antivirus presentan para analizar dichos ficheros, sería previsible que atacantes de toda índole y habilidad comiencen a emplear de forma más asidua este sencillo método de evasión.

Dada la vigencia actual del empleo de archivos VHD o VHDX para distribuir malware, se recomienda restringir la descarga de este tipo de archivos a través de las puertas de enlace de correo electrónico y navegadores, ya que este método es muy atractivo para cualquier atacante y no presenta una actual remediación de los sistemas de detección de soluciones antivirus o software de correo electrónico.

Silvia Hernández Sánchez Cyber Threat Intelligence Analyst

Principales vulnerabilidades en diciembre de 2020

SolarWinds, SAP y Cisco

MNEMO-CERT presenta las 10 vulnerabilidades más representativas que fueron identificadas en el mes de diciembre de 2020, considerando el tipo de componente que afectan y el nivel de criticidad con base a CVSS V 3.1.

Titulo	Identificador	CVSS	Descripción
Error en **SolarWinds** produce afectaciones a miles de organizaciones[1]	N/A	Crítico	Error presente en la cadena de suministro de SolarWinds que ocasionó que usuarios maliciosos modificaran el sistema de compilación de **SolarWinds Orion.**
Falla de seguridad presente en **SAP NetWeaver**	CVE-2020-268292	CVSS v3.1: 10.0 [Crítico]	Vulnerabilidad presente en las versiones **7.11, 7.20, 7.30, 7.31, 7.40, 7.50 de SAP NetWeaver AS JAVA**, la cual puede ocasionar que un usuario ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **Cisco Jabber**	CVE-2020-271273	CVSS v3.1: 9.9 [Crítico]	Vulnerabilidad presente en algunas versiones de **Cisco Jabber**, la cual puede ocasionar que un usuario ejecute código arbitrario de manera remota en el dispositivo afectado.
Falla de seguridad presente en **Cisco Jabber**	CVE-2020-271324	CVSS v3.1: 9.9 [Crítico]	Vulnerabilidad presente en algunas versiones de **Cisco Jabber**, la cual puede permitir a un usuario ejecutar código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **Microsoft**	CVE-2020-170955	CVSS v3.1: 9.9 [Crítico]	Vulnerabilidad presente en algunas versiones de **Hyper-V**, la cual puede ocasionar que un usuario ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **Microsoft**	CVE-2020-171186	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en algunas versiones de **Microsoft SharePoint Server**, la cual puede permitir a un usuario ejecutar código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **HPE Edgeline Infrastructure Manager**	CVE-2020-71997	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en **HPE Edgeline Infrastructure Manager**, la cual puede ocasionar que un usuario ejecute código de manera arbitraria en el dispositivo afectado.
Falla de seguridad presente en **ArubaOS**	CVE-2020-246338	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en versiones de **ArubaOS**, la cual puede permitir a un usuario ejecutar código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **Docker**	CVE-2020-295759	CVSS v3.1: 9.8 [Crítico]	Vulnerabilidad presente en las versiones anteriores a la **1.8.0-alpine de Docker**, la cual puede ocasionar que un usuario ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **SAP Solution Manager**	CVE-2020-2683710	CVSS v3.1: 9.1 [Crítico]	Vulnerabilidad presente en la versión 7.2 de **SAP Solution Manager**, la cual puede permitir a un usuario ejecutar código de manera remota en el dispositivo afectado.

[1] https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/
[2] https://nvd.nist.gov/vuln/detail/CVE-2020-26829
[3] https://nvd.nist.gov/vuln/detail/CVE-2020-27127
[4] https://nvd.nist.gov/vuln/detail/CVE-2020-27132
[5] https://nvd.nist.gov/vuln/detail/CVE-2020-17095
[6] https://nvd.nist.gov/vuln/detail/CVE-2020-17118
[7] https://nvd.nist.gov/vuln/detail/CVE-2020-7199
[8] https://nvd.nist.gov/vuln/detail/CVE-2020-24633
[9] https://nvd.nist.gov/vuln/detail/CVE-2020-29575
[10] https://nvd.nist.gov/vuln/detail/CVE-2020-26837

La lista está encabezada por un fallo presente en la cadena de suministro de SolarWinds, el cual ha afectado a diferentes organizaciones en todo el mundo. Esta falla se debe al acceso al sistema de compilación SolarWinds Orion, ocasionando que agregaran una "backdoor" en una DLL legítima del programa, que posteriormente provocó que varios clientes de SolarWinds sufrieran incidentes cibernéticos.

Entre las compañías afectadas por estos ataques se encuentran FireEye, Microsoft, Cisco, VMware, y varias organizaciones gubernamentales de Estados Unidos, como el Departamento del Tesoro de EE. UU., la Administración Nacional de Telecomunicaciones, el Departamento de Seguridad Nacional, entre otros.

MNEMO-CERT publicó avisos de seguridad referentes a este incidente, los cuales pueden consultar en la siguiente URLs:

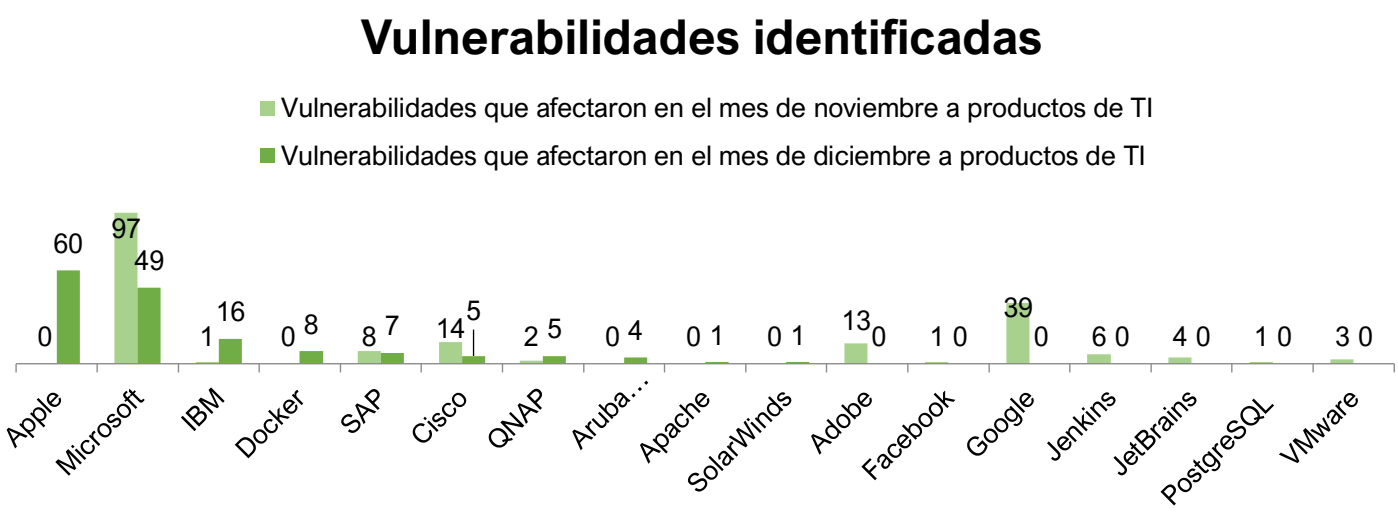
- https://cert.mnemo.com/aviso-de-seguridad-continua-campana-maliciosa-dirigida-a-sistemas-solarwinds-orion/
- https://cert.mnemo.com/aviso-de-seguridad-apt-emiten-alerta-a-las-organizaciones-sobre-una-campana-de-ciberespionaje-a-traves-de-productos-de-solarwinds/

Por otra parte, la vulnerabilidad presente en **SAP NetWeaver** es causada por una falta de verificación de autenticación, la cual puede permitir acceder a ciertas funciones que están restringidas, permitiendo la ejecución de código de manera remota con privilegios de administrador. MNEMO-CERT publicó un aviso de seguridad referente a esta falla el cual se puede consultar en la siguiente URL:

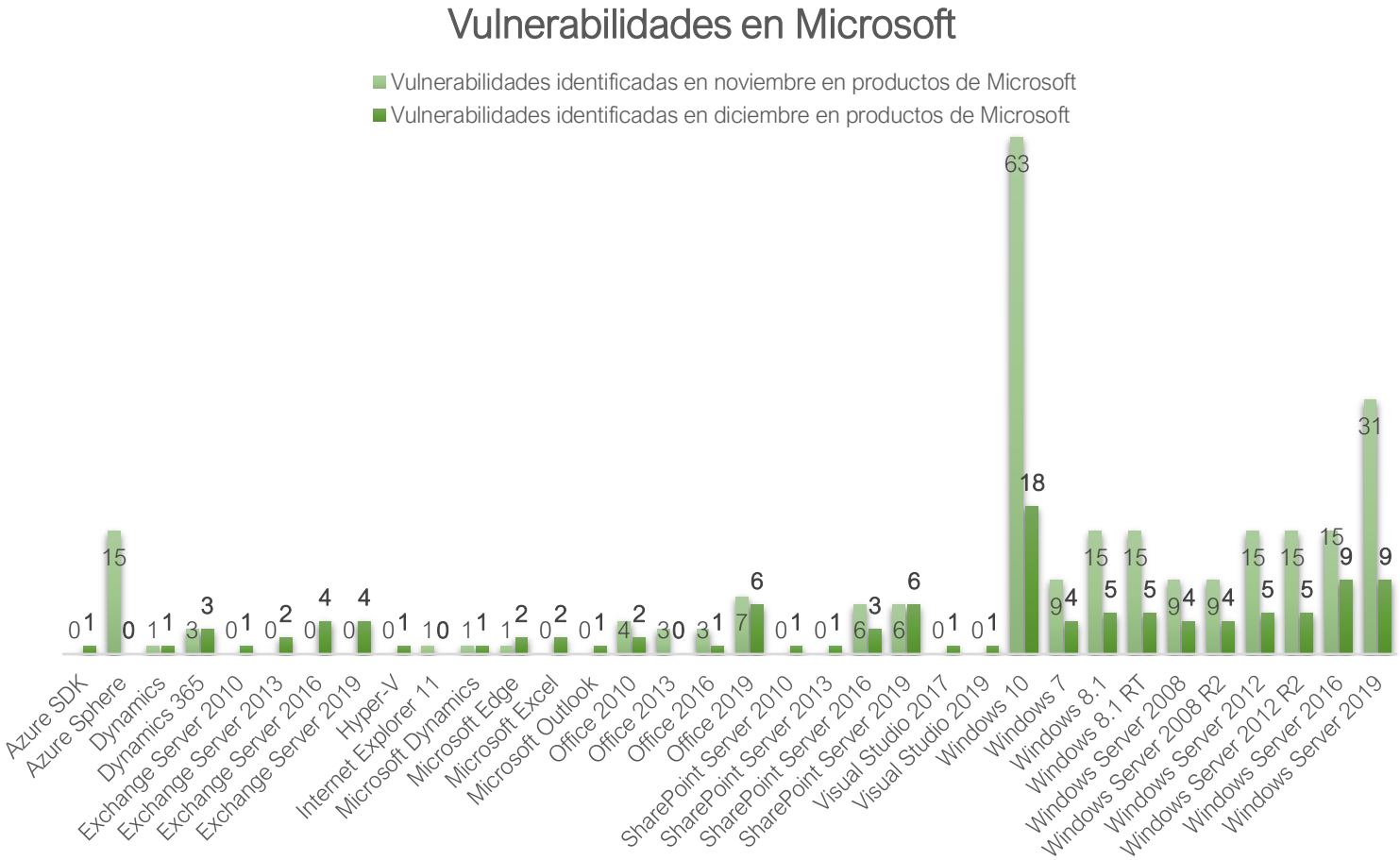
- https://cert.mnemo.com/aviso-de-seguridad-sap-publica-actualizaciones-para-corregir-fallas-de-seguridad-en-varios-de-sus-productos/

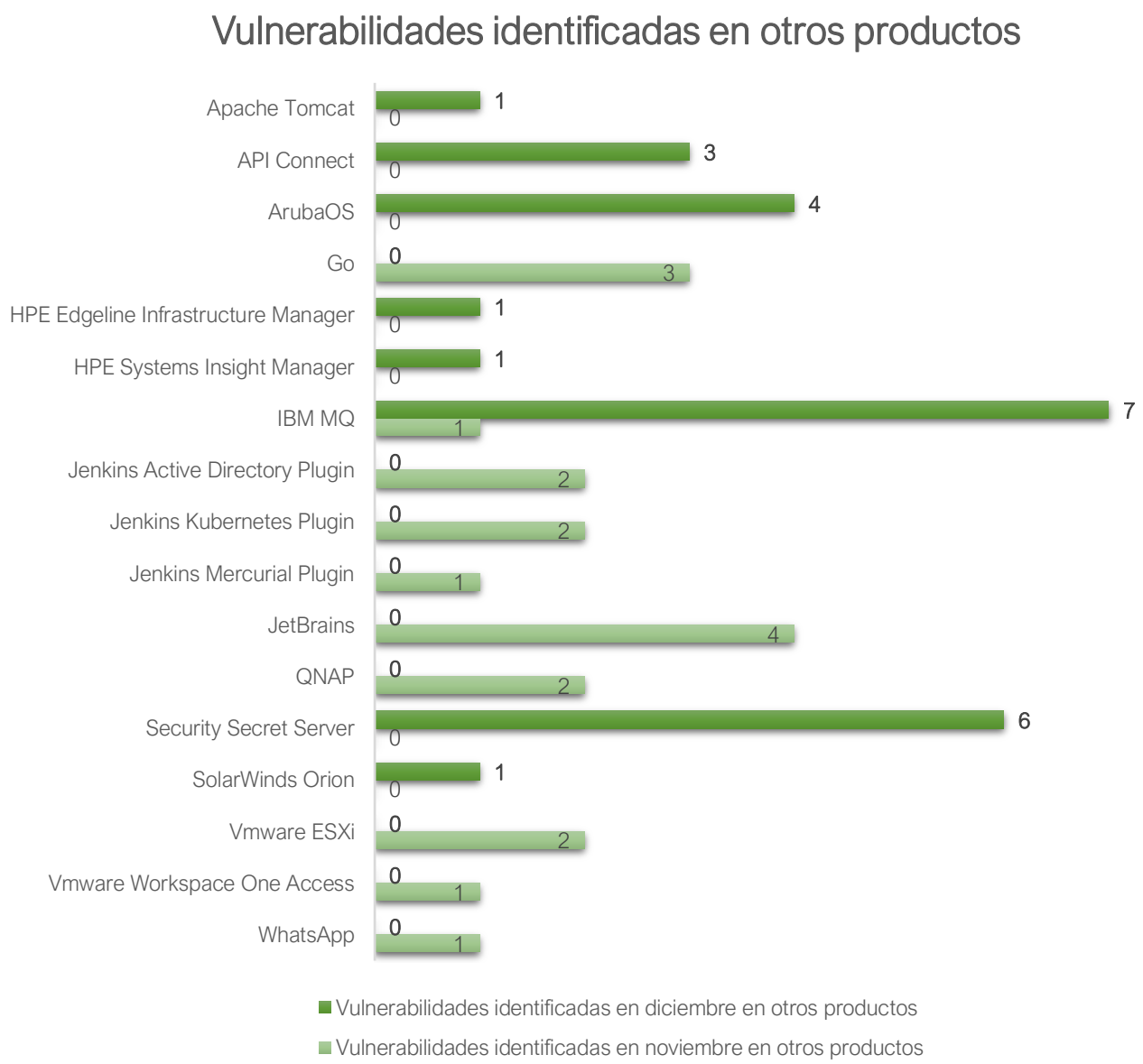
Respecto a la vulnerabilidad presente en **Cisco Jabber**, la cual afecta a los sistemas Windows, MacOS y plataformas móviles, puede ocasionar que se ejecuten programas arbitrarios en el sistema operativo donde se tiene instalada la versión de Jabber afectada.

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



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 diciembre de 2020 y un comparativo con el mes de noviembre del mismo año.





De acuerdo con un análisis de vulnerabilidades realizado durante el 2020, se ha identificado un incremento en comparación de años anteriores. Esta cifra, según los expertos, está relacionada con la manera de trabajo actual, derivado de la pandemia que enfrentamos, ya que varias organizaciones se han visto obligadas a llevar a sus aplicativos rápidamente al mercado y en muchas ocasiones estas son liberadas sin implementar controles de seguridad adecuados.

MNEMO-CERT también destacada las vulnerabilidades más representativas de este año, considerando si estas fueron aprovechadas, el tipo de componente que afectan y el nivel de criticidad con base a CVSS versión 3.1.

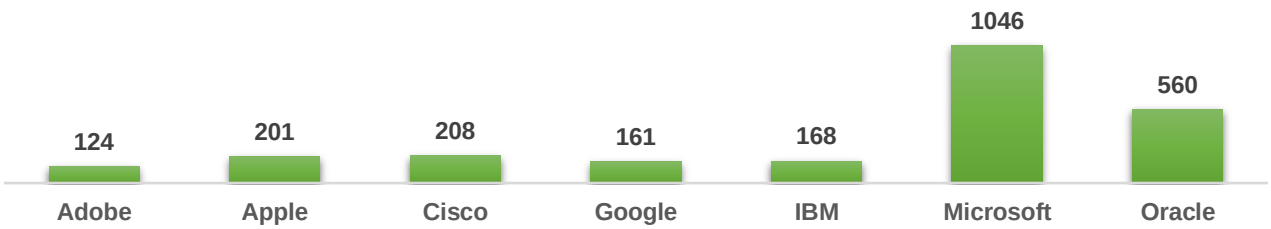
VULNERABILIDADES

Titulo	Identificador	CVSS	Descripción
Campañas maliciosas aprovechan vulnerabilidad en Windows Server	CVE-20202-1472	CVSS v3.1: 10.0 [Crítico]	Esta falla se encuentra presente en algunas versiones de Microsoft Windows Server, también conocida como "Zerologon", ha sido aprovechada por diferentes grupos maliciosos como "TA505" o "MuddyWater" y por los desarrolladores del ransomware "Ryuk".
Actores maliciosos aprovechan vulnerabilidad en Oracle WebLogic Server	CVE-2020-14882	CVSS v3.1: 9.8[Crítico]	Esta vulnerabilidad afecta a los servidores de Oracle WebLogic, y puede permitir a un usuario malicioso ejecutar código remoto sin requerir autenticación. Se identificó a algunos usuarios empleando esta vulnerabilidad para comprometer a organizaciones y recolectar información confidencial, entre ellos, la botnet "DarkIRC".
Actores aprovechando vulnerabilidad en Citrix	CVE-2019-19781	CVSS v3.1: 9.8[Crítico]	A principios de este año, se identificaron ataques por parte del grupo APT-41 quien realizó campañas para aprovechar el error presente en Citrix Application Delivery Controller.
Identifican vulnerabilidad en protocolo SMBv3	CVE-2020-0796	CVSS v3.1: 10.0 [Crítico]	En octubre se identificó nueva actividad maliciosa relacionada con la botnet conocida como "LemonDuck", la cual se aprovechaba de diferentes fallas de seguridad entre las que se incluyen "SMBGshost" (CVE-2020-0796) y CVE-2017-0144 vulnerabilidad que es utilizada por el programa malicioso "Eternal Blue".
Actores maliciosos aprovechan vulnerabilidad presente en complemento de WordPress	CVE-2020-25213	CVSS v3.1: 9.8[Crítico]	Presente en el complemento File-Manager para WordPress fue aprovechada junto con la vulnerabilidad "Zerologon", los atacantes la utilizaron para obtener un punto de apoyo inicial para ingresar a la red, aprovechar la vulnerabilidad Zerologon y comprometer los controladores de dominio de la organización.
Grupo malicioso aprovecha vulnerabilidad en Zoho Manage	CVE-2020-10189	CVSS v3.1: 9.8[Crítico]	"APT41" realizó campañas para aprovechar la vulnerabilidad CVE-2020-10189 (CVSS v3.1: 9.8 [Crítico]) presente en "Zoho ManageEngine Desktop Central", que permite la ejecución remota de código en instalaciones afectadas para obtener privilegios de sistema.
Actores maliciosos de Irán aprovechan vulnerabilidad en F5 BIG-IP	CVE-2020-5902	CVSS v3.1: 9.8[Crítico]	Esta falla presente en productos BIG-IP, fue utilizada en una campaña por parte de un usuario malintencionado con sede en Irán dirigida a varios sectores como TI, gobierno, atención médica, finanzas, seguros y medios, de manera central en Estados Unidos.
Usuarios maliciosos aprovechan falla de seguridad en Apache Tomcat	CVE-2020-1938	CVSS v3.1: 9.8[Crítico]	En febrero esta falla presente en Apache fue aprovechada por atacantes para hacer búsquedas de servidores vulnerables y realizar desde el reconocimiento de los sistemas hasta la implementación de mecanismos para conservar el acceso en los mismos.
Grupos aprovechan una falla en Laravel Framework	CVE-2019-9081	CVSS v3.1: 9.8[Crítico]	Los desarrolladores de "Lucifer" llevaron a cabo campañas para aprovechar esta falla presente en algunas versiones de Laravel Framework. Permite la ejecución de código en el dispositivo afectado.
Aprovechamiento de falla de seguridad en Vmware	CVE-2020-4006	CVSS v3.1: 7.2 [Alto]	Esta falla fue considerada como un zeroday que afecta a Workspace One Access e Identify Manager de VMware. Una firma de ciberseguridad alertó de la existencia de ataques que aprovechaban esta falla y tenían como objetivo robar información confidencial de las organizaciones.

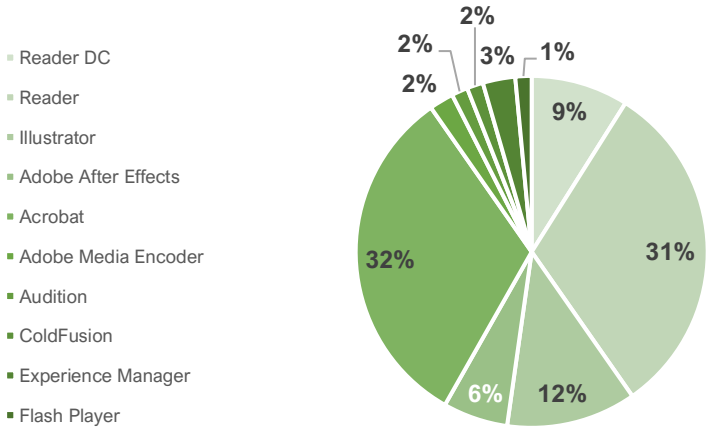
VULNERABILIDADES

Finalmente, MNEMO-CERT presenta en las siguientes gráficas las vulnerabilidades identificadas en el año para los fabricantes más conocidos y los principales productos afectados durante el 2020.

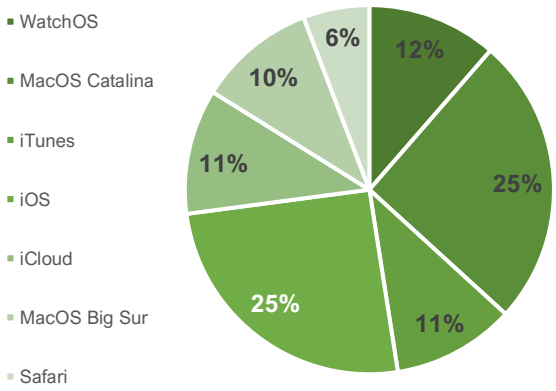
Vulnerabilidades identificadas del año por fabricante



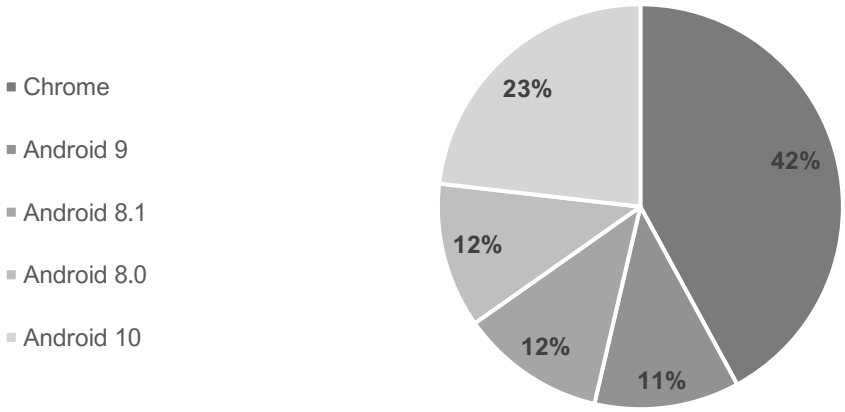
Vulnerabilidades identificadas en productos de Adobe durante el 2020



Vulnerabilidades identificadas en productos de Apple durante el 2020



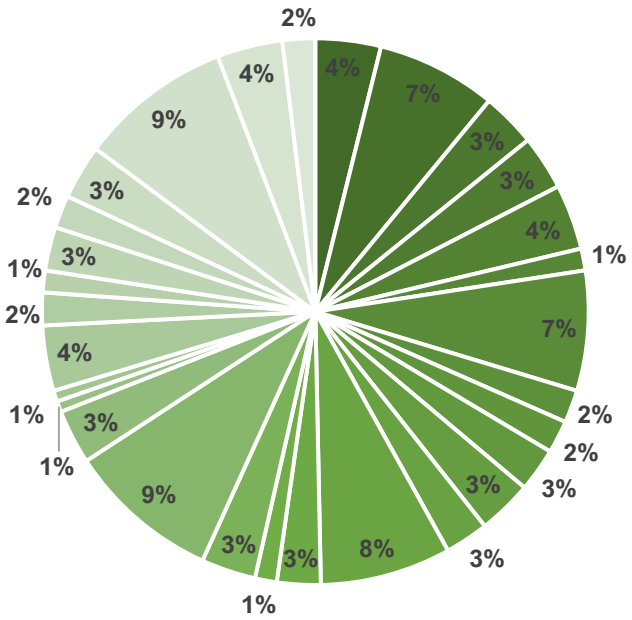
Vulnerabilidades identificadas en productos de Google durante el 2020



VULNERABILIDADES

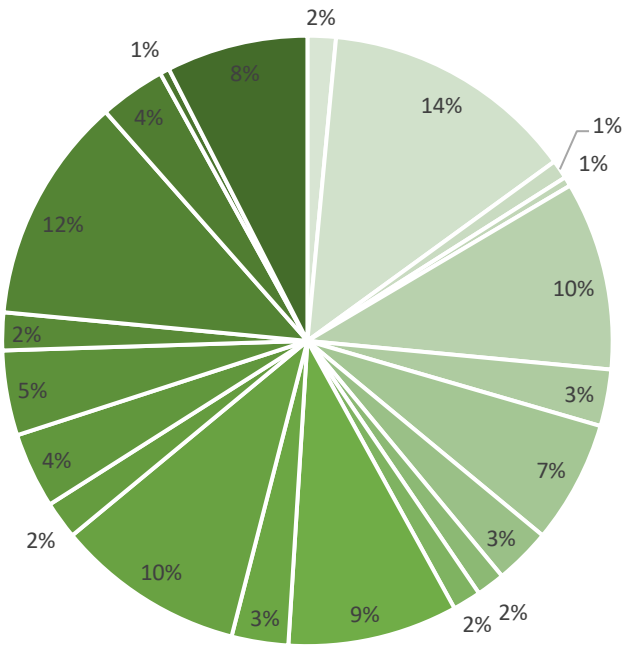
Vulnerabilidades identificadas en productos de IBM durante el 2020

- Spectrum Scale
- QRadar SIEM
- InfoSphere Information Server
- WebSphere Application Server
- Jazz Team Server
- InfoSphere Guardium
- IBM MQ
- Content Navigator
- i2 Intelligent Analyis Platform
- IBM Watson
- Planning Analytics
- Security Access Manager Appliance
- Security Identity Manager
- Security Secret Server
- Tivoli Netcool
- Security Guardium
- Maximo Asset Management
- IBM Cognos Analytics
- Spectrum Protect Operations Center
- Jazz Reporting Service
- API Connect
- Security Identity Manager Virtual Appliance
- Data Risk Manager
- Security Information Queue
- Maximo Anywhere
- Quality Manager
- Security Directory Server
- Security Information Queue
- Spectrum Protect Plus



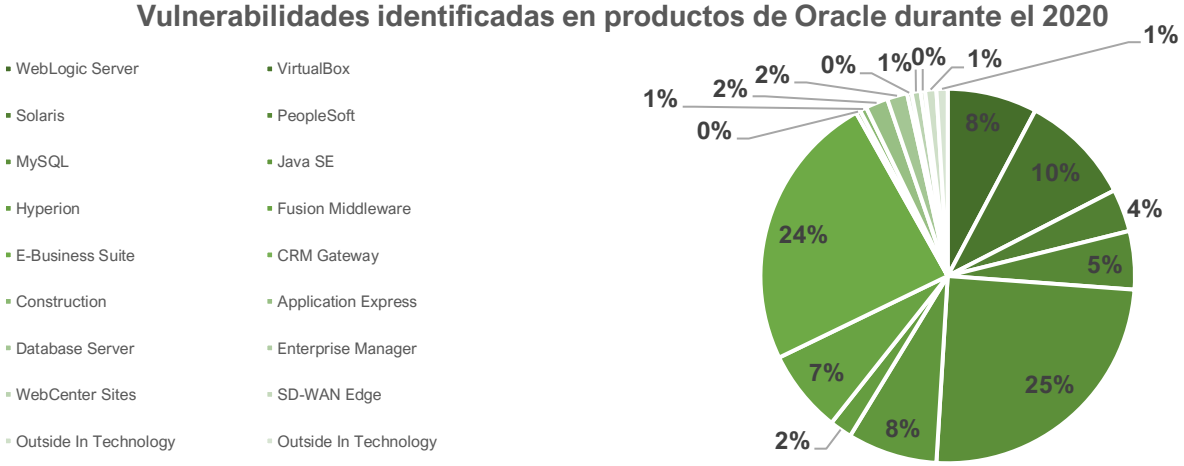
Vulnerabilidades identificadas en productos de Cisco durante el 2020

- AsyncOS
- Cisco Discovery Protocol
- Cisco FTD
- Firepower Management Center
- Identity Services Engine (ISE)
- WebEx
- SD-WAN
- Cisco Jabber
- IOS XR
- IOS Software
- Data Center Network Manager
- Cisco ASA
- Cisco DNA
- Cisco Security Manager
- FXOS Software
- SPA500 Series IP Phones
- Small Business
- Cisco Wireless
- Juniper Network Junos OS
- IOS XE
- Intelligent Proximity

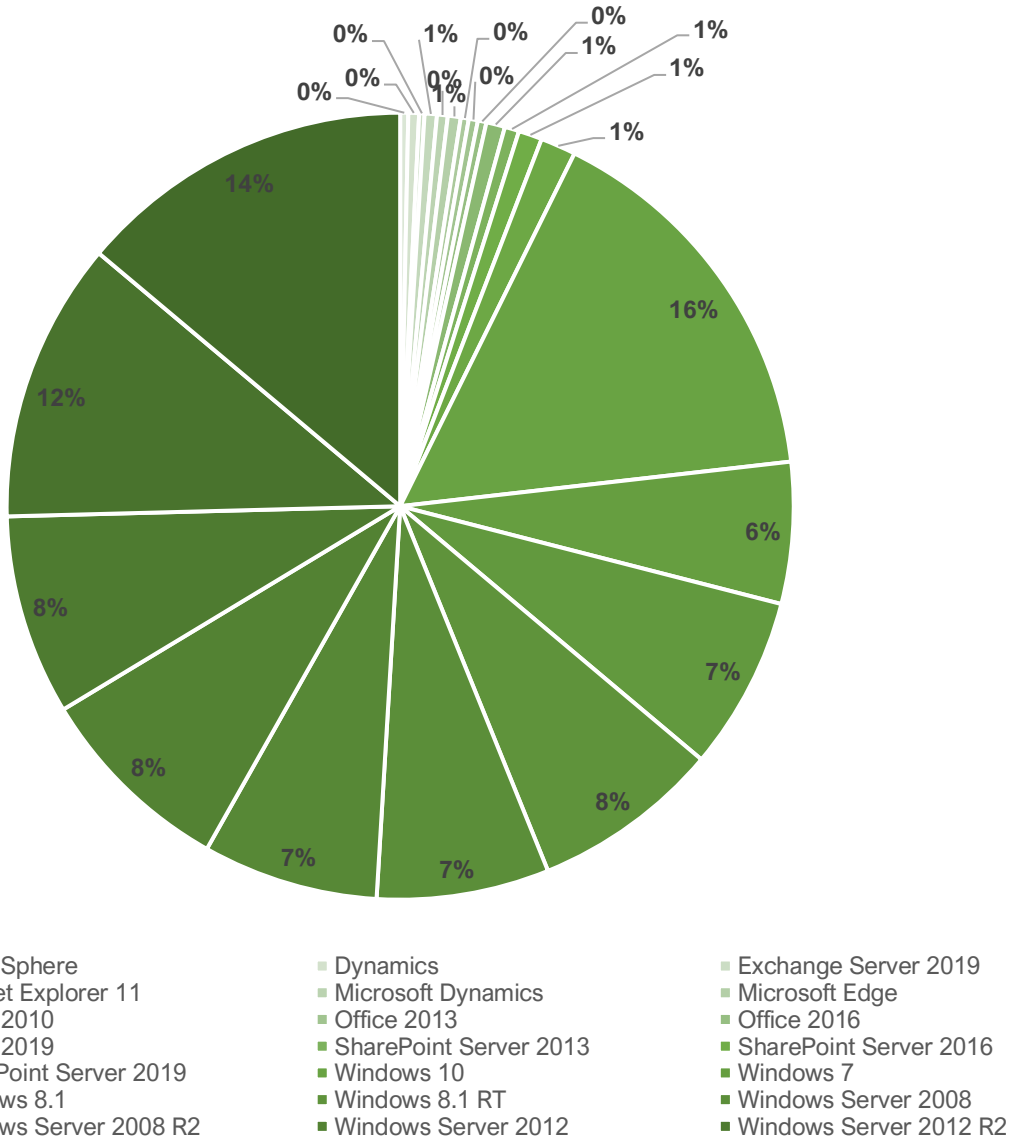


VULNERABILIDADES

Vulnerabilidades identificadas en productos de Oracle durante el 2020



Vulnerabilidades identificadas en productos de Microsoft durante el 2020



- Azure Sphere
- Dynamics
- Exchange Server 2019
- Internet Explorer 11
- Microsoft Dynamics
- Microsoft Edge
- Office 2010
- Office 2013
- Office 2016
- Office 2019
- SharePoint Server 2013
- SharePoint Server 2016
- SharePoint Server 2019
- Windows 10
- Windows 7
- Windows 8.1
- Windows 8.1 RT
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Cyber Threat Intelligence for Financial Sector

2020 – Análisis de amenazas

El camino que lleva a una organización a poder realizar acciones de seguridad activa en su infraestructura empieza por entender bien aquellas amenazas que podrían impactar potencialmente contra su entidad.

El equipo de Cyber Threat Intelligence de Mnemo estructura de manera detallada todos los análisis que realiza para poder tener un acercamiento sobre posibles tendencias o patrones que se repiten en las intrusiones contra entidades financieras principalmente. Finalmente, estos patrones y tendencias son los que ayudan a identificar los principales vacíos que pueden tener las organizaciones.

A lo largo de este artículo se pretende dar una visión general de aquellas amenazas que han sido investigadas por el equipo a lo largo de este complicado año 2020.

En primer lugar, es necesario enumerar las técnicas y tácticas (basadas en la versión 6 de ATT&CK MITRE) más utilizadas por aquellos actores que han llevado a cabo algún tipo de intrusión contra las entidades financieras. Cabe mencionar que estas técnicas y tácticas se encuentran dentro del espectro empleado por todo tipo de grupos cibercriminales.

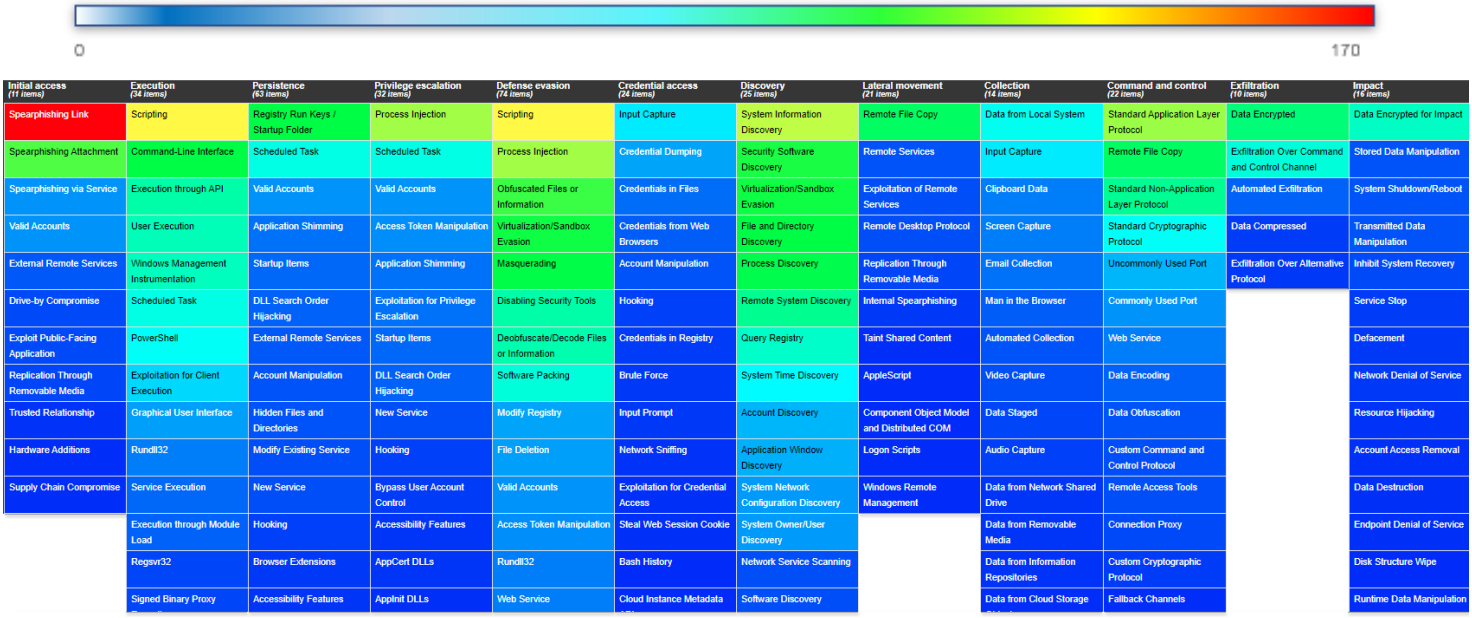


Imagen 1: Tácticas y técnicas más usadas durante el año 2020 para el sector financiero

*La matriz no contempla ninguna técnica que se haya usado en al menos cinco ocasiones en 2020.

La matriz está basada en una escala de colores donde el blanco es el valor mínimo (0 recurrencias) hasta el rojo que es el valor máximo (170 recurrencias). Las técnicas mostradas se acotan exclusivamente al año 2020 y a ciberamenazas investigadas por el equipo en el sector financiero.

Es destacable el uso excesivo de la técnica Spearphishing Link (T1192 en la versión 6.0 y T1566.002 en su actual versión). Sin ninguna duda, tanto el **Spearphishing mediante link o archivo adjunto, sigue siendo a día de hoy el vector de entrada favorito de los actores**. Los usuarios siguen siendo hoy en día la principal vulnerabilidad identificada.

Sin embargo, aunque no destaca, bajo la misma táctica de Initial Access, se puede observar que ocupa la posición número siete la técnica Exploit Public-Facing Application (T1190 mismo ID para ambas versiones). Se resalta esta técnica debido a que ha sido ampliamente utilizada en el Q4 de este mismo año, identificándose un incremento de su uso en un 70% durante los últimos 3 meses.

Este hecho está principalmente constatado por algunas vulnerabilidades que han tenido lugar en productos muy utilizados por la industria, los cuales se encuentran expuestos en Internet, como podrían ser productos de Oracle, Pulse Secure, Microsoft o Fortinet entre otros.

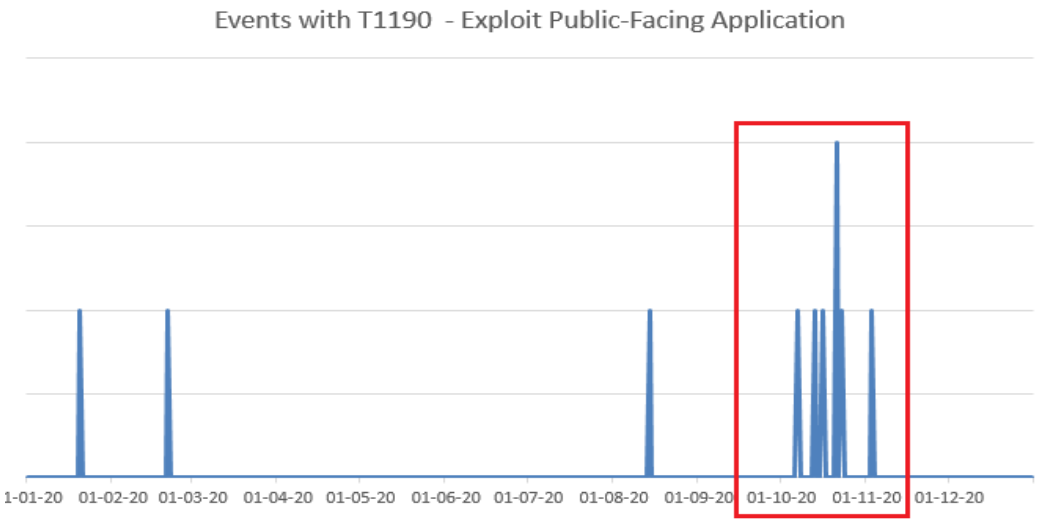


Imagen 2: Tendencia en la explotación de vulnerabilidades como vector de ataque durante el Q4

Otra técnica a destacar por su aparición en una gran parte de intrusiones, se trata del Scripting (T1064 en la versión 6.0 y T1059 en su actual versión). En la versión actual de ATT&CK, esta técnica agrupa diferentes métodos de intérpretes relacionados con el scripting que son usados por los actores para llevar a cabo ejecuciones de malware.

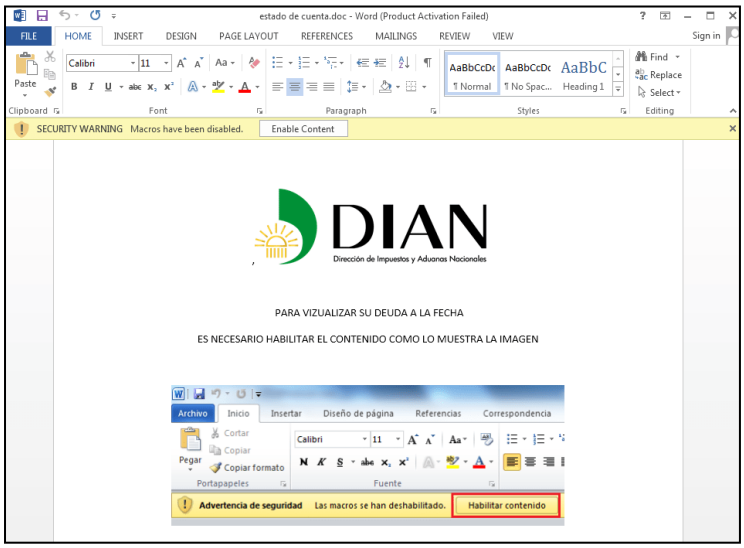


Imagen 3: Ejemplo de documento relacionado con APT-C-36 que contiene macros embebidas.

Sin duda, esta técnica es muy utilizada por el malware de primera etapa para descargar y ejecutar el de segunda etapa. Un claro ejemplo y que es ampliamente frecuentado por los actores, es a través de Microsoft Office y macros de Visual Basic.

Mucho malware, con ayuda de la interacción por parte de sus víctimas, a la hora de abrir documentos Word o Excel y habilitar el contenido, tienen la capacidad de ejecutar código VBS para realizar la descarga de otra pieza de malware.

Al igual que esta técnica es muy utilizada por el malware de primera etapa, existen otras como Process Injection o System Information Discovery que son, por lo general, usadas también mediante técnicas de scripting, ya sea a través de VBS, PowerShell, Python, etc…

Por otro lado, se hace necesario también analizar en todas las intrusiones los intereses que pudieran existir desde el punto de vista geopolítico, ya que, es bien sabido que muchos conflictos entre países han sido extrapolados en forma de ciberataques para lograr impacto geopolítico o ganancias económicas.

Tanto el origen como el destino de los eventos son importantes para llegar a determinar si existe algún tipo de motivación o interés por parte del actor. Estas localizaciones no son obtenidas desde los indicadores de compromiso, como direcciones IP, sino desde los actores cuando las líneas de investigación permiten atribuir la intrusión a uno de ellos.

ORIGEN DE LOS EVENTOS ANALIZADOS

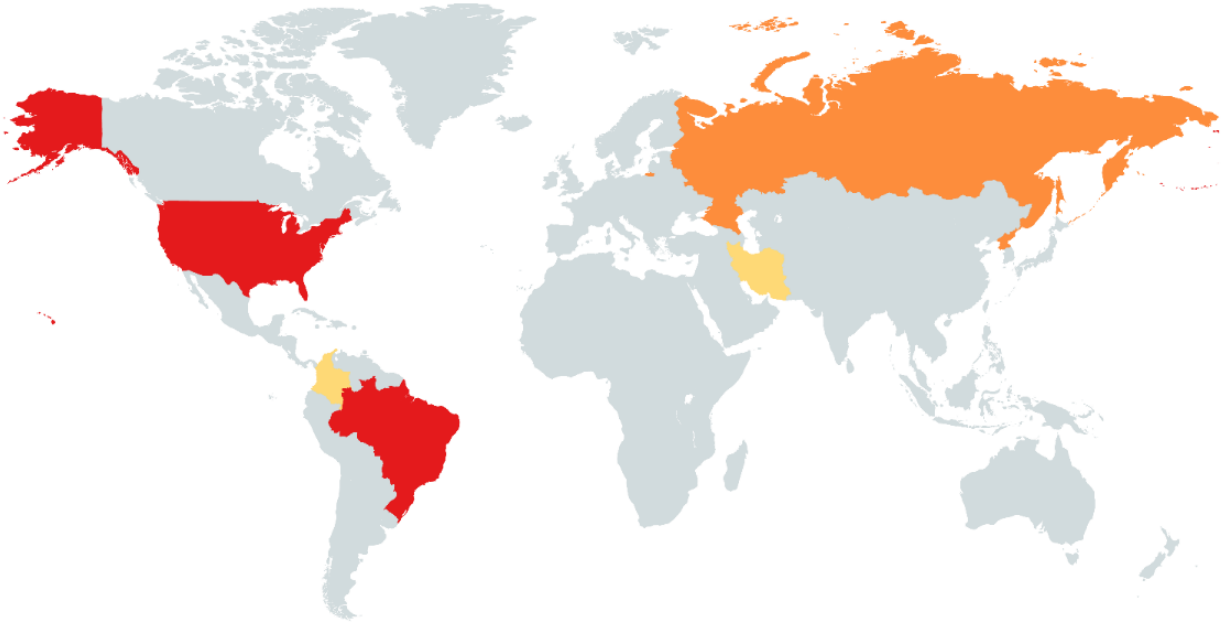


Imagen 4: Origen de los eventos analizados por CTI

El anterior mapa ilustra el top 6 de los países en los cuales se ha podido identificar el origen, ya sea por error humano del actor, colaboración en cuanto a inteligencia o analítica rigurosa de la intrusión. Es importante mencionar que el origen es sobre el actor/es que lleva a cabo la operación, desconociendo así si hubiese por detrás un estado patrocinando al grupo.

1. Brasil
2. Estados Unidos
3. Rusia
4. Corea del Norte
5. Irán
6. Colombia

Este Top 6 se ha generado en base a los eventos que el equipo de Cyber Threat Intelligence ha investigado con objetivos y motivaciones sobre el sector financiero, no abarcando completamente todo el espectro del sector financiero ni de otros sectores.

Por contraparte, a continuación, se muestra el mapa desde la perspectiva de aquellos países que fueron receptores de los ciberataques. Tal y como se puede contemplar, tres de los seis países que corresponden a los más activos sobre la cuestión de origen de los ciberataques, se repiten, esta vez como destinos.

Imagen 5: Destino de los eventos analizados por CTI

1. Colombia
2. Brasil
3. Estados Unidos
4. México
5. España
6. Perú

Brasil, a diferencia de otros países, contiene muchos grupos cibercriminales que son establecidos localmente y tienen como objetivo su propio país, llevando a cabo operaciones principalmente contra el sector financiero y gubernamental.

Los conocidos troyanos brasileños fueron principalmente identificados en intrusiones de origen y destino brasileño, sin embargo, se ha visto cómo estas familias de malware se están expandiendo por toda la región Latinoamericana y la península ibérica.

Basado en las muestras obtenidas y analizadas de los troyanos brasileños, se pudo observar cómo dichos malware tenían mucha relación entre sí, no sólo en el comportamiento una vez es ejecutado, sino también en la propia intrusión orquestada por el actor que lo despliega.

La siguiente imagen ilustra los grafos de actividad-ataque que han sido extraídos de eventos relacionados con los principales troyanos brasileños, donde se muestran únicamente los pasos que han sido similares en sus respectivas intrusiones, es decir, esta imagen no representa la intrusión al completo de cada troyano.

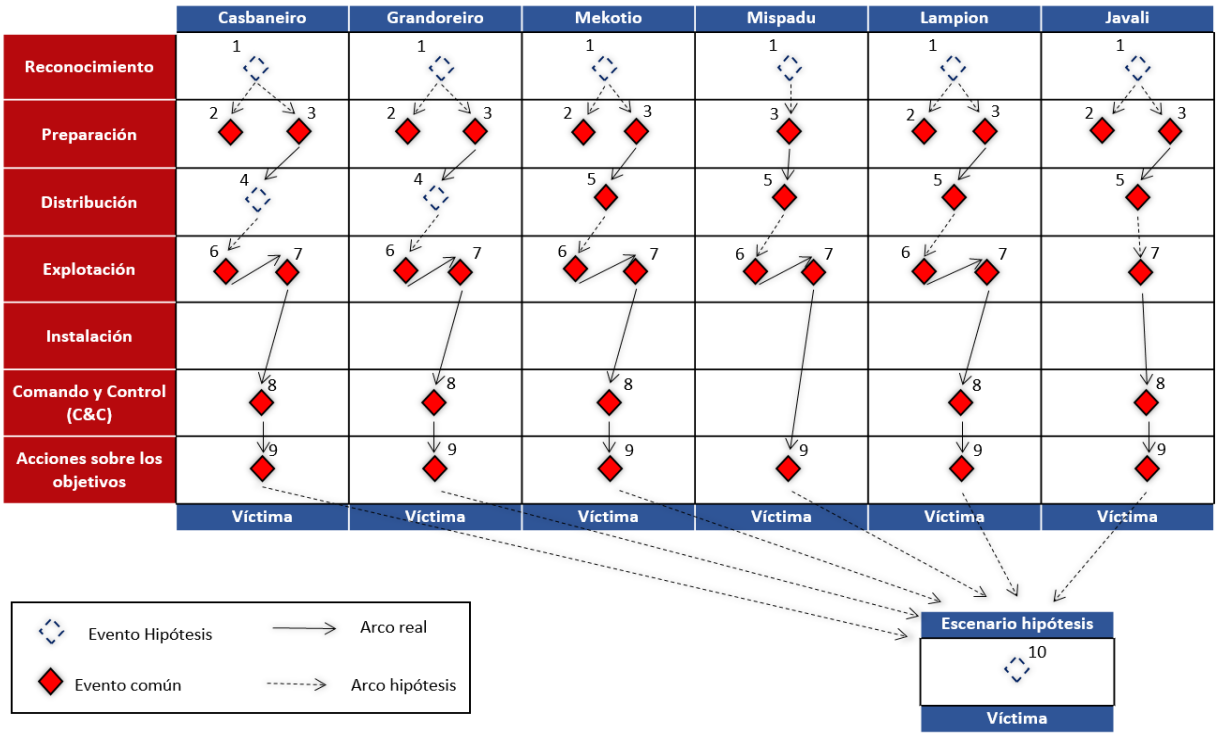


Imagen 6: Grafo de actividad-ataque realizado por CTI

Como se puede apreciar, la fase donde principalmente existen diferencias entre estos troyanos se trata de la instalación, es decir, momento en el que los actores realizan persistencia. Muchos de estos troyanos no tienen como objetivo realizar persistencia, y otros, sin embargo, la realizan pero de diferentes formas.

Bajando un poco más de nivel, situándonos en el tradecraft extraído de cada troyano brasileño y analizado, se obtuvieron resultados muy similares de semejanza, donde pudiesen empezar a generarse hipótesis de que compartan código entre ellos.

La siguiente imagen representa el número de características relacionadas a nivel de tradecraft con cada troyano brasileño.

De esta manera, se puede comprobar que Casbaneiro y Mekotio tienen una gran similitud.

Pasa algo similar si vemos a Casbaneiro con Javali y Grandoreiro.

Por otro lado, Casbaneiro y Grandoreiro son los que más características tienen en común con cada uno de los troyanos.

	Amavaldo	Casbaneiro	Grandoreiro	Guildma	Javali	Lampion	Mekotio	Mispadu	Unknown1	Unknown2	totales
Amavaldo	0	7	7	4	6	6	8	8	5	3	54
Casbaneiro	7	0	10	4	10	7	13	8	6	4	69
Grandoreiro	7	10	0	5	7	10	9	9	6	6	69
Guildma	4	4	5	0	4	4	4	6	1	4	36
Javali	6	10	7	4	0	12	8	7	5	3	62
Lampion	6	7	10	4	12	0	6	7	7	6	65
Mekotio	8	13	9	4	8	6	0	8	5	3	64
Mispadu	8	8	9	6	7	7	8	0	5	4	62
Unknown1	5	6	6	1	5	7	5	5	0	3	43
Unknown2	3	4	6	4	3	6	3	4	3	0	36

Imagen 7: Tradecraft extraído y analizado por CTI

La siguiente relación se obtuvo a través del laboratorio de malware financiero interno "BugStation" del equipo de Cyber Threat Intelligence. Se obtuvieron relaciones a nivel de código entre diferentes muestras, inclusive, entre una muestra de un troyano brasileño con otra muestra de una familia completamente diferente y que ha estado involucrada en recientes eventos.

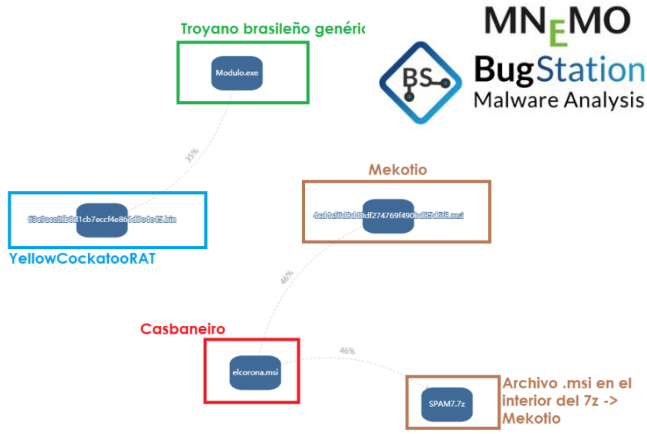


Imagen 8. Relaciones a nivel de código obtenidas por CTI

Finalmente, relacionado con los troyanos brasileños, se generó un Activity Group que contemplase el principal tradecraft que se ha visto en común por cada troyano. Por ejemplo, el uso de Googledocs es algo que se ha visto prácticamente en todas las intrusiones de estos troyanos, independientemente de que familia fuese (Grandoreiro, Mekotio, Lampion, etc…).

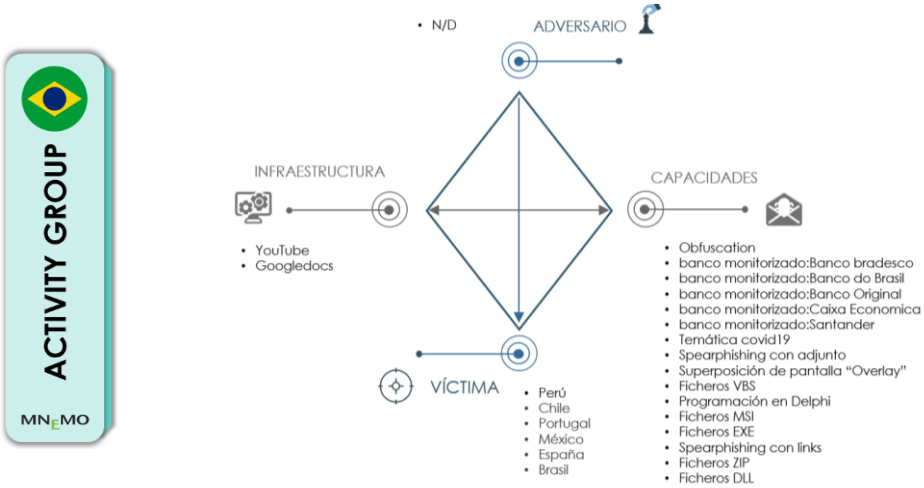


Imagen 9: Activity Group realizado por CTI

Los troyanos brasileños han tenido gran repercusión en el sector, y sin embargo, no se encuentran en el top 5 de familias de malware que han impactado en el sector y que se han podido analizar.

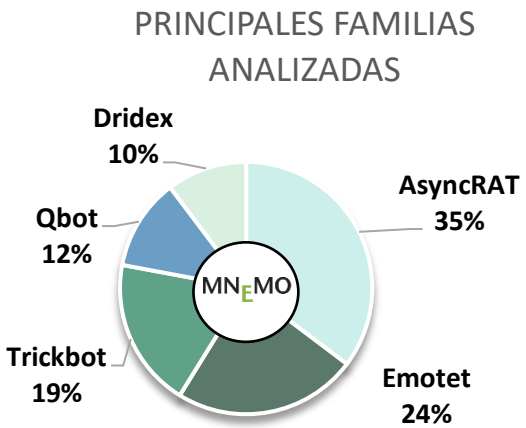


Imagen 10: Principales familias analizadas durante 2020 por CTI

AsyncRAT es la principal familia de "malware" que tiene impacto sobre las entidades financieras, esencialmente en Colombia.

Indicamos "malware" entre comillas debido a que realmente se trata de una herramienta de acceso remoto, disponible en GitHub para usarse.

En nuestro canal de YouTube, existe un análisis realizado donde se explica con detalle las líneas de investigación realizadas sobre diferentes intrusiones de APT-C-36 que ha desplegado AsyncRAT.

Emotet y Trickbot cerraron un año 2019 lleno de intrusiones, donde en España se vio afectada especialmente. A lo largo de 2020 también se han detectado numerosos eventos donde han estado presentes en entidades financieras.

Son múltiples las intrusiones que se han analizado y las cuales tienen como objetivo desplegar AsyncRAT. De la misma manera que con los troyanos brasileños, se ha llevado a cabo un Activity Group para ver esas características que se repiten en diferentes intrusiones relacionadas con AsyncRAT.

De igual modo, se manifestaron correlaciones entre eventos de APT-C-36 y de AsyncRAT, lo que llevó a realizar una investigación profunda para comprobar si pudiesen estar relacionados. El grafo de actividad-ataque recopila dichos eventos comunes durante las cadenas de infección analizadas.

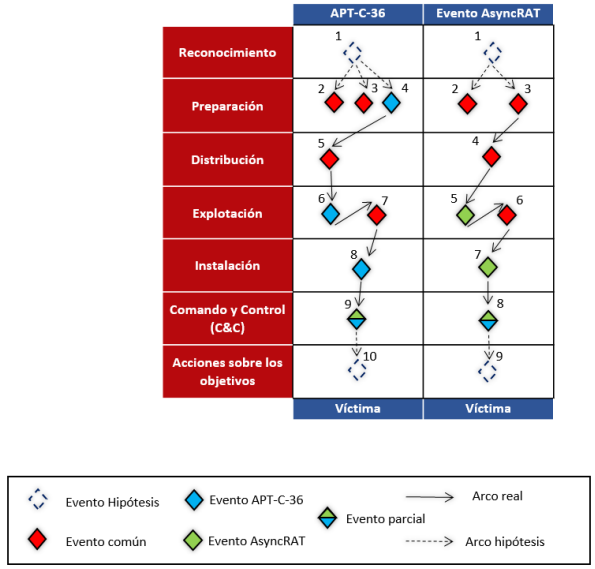


Imagen 11: Grafo de actividad ataque APT-C-36 y AsyncRAT

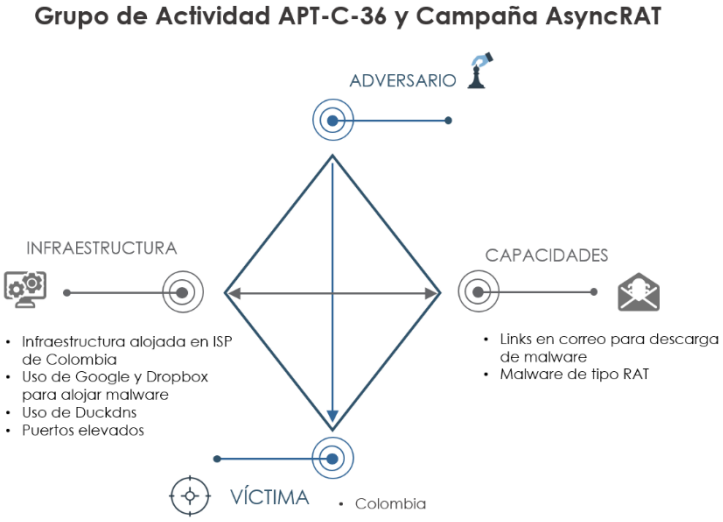


Imagen 12: Activity Group de los eventos relacionados con AsyncRAT

Al igual que durante los primeros meses del año 2020 donde se utilizaron temáticas de la Covid-19 para distribuir malware a través de spearphishing y spam, en este 2021 se verán nuevas temáticas como la vacunación y la tarjeta de vacunación como nuevas formas de ingeniería social que permitirán un engaño más real hacia las víctimas.

Los troyanos brasileños, que se aprovecharon de la Covid-19, seguirán utilizando nuevas temáticas para distribuir sus cargas útiles en los sistemas de sus víctimas. De hecho, es probable que nazca una nueva familia brasileña similar a las existentes.

Por otro lado, se sigue observando cómo hoy en día APT-C-36 lleva a cabo ataques con el objetivo final de desplegar AsyncRAT en los sistemas, consiguiendo así obtener acceso remoto. Por ello, en el momento que este grupo haya abusado de esta herramienta de conexión remota, desplegará otras existentes, posiblemente desarrollada en .NET o C#, que es donde se ha podido comprobar que tienen más conocimientos este grupo de actores y se sienten cómodos.

Malware en España: TrickBot y Conti

Nueva funcionalidad de TrickBot que inspecciona la UEFI/BIOS

Trickbot nació como un troyano bancario identificado por primera vez en 2016. A lo largo de los años, el grupo detrás de este malware ha implementado nuevas funcionalidades que lo han sofisticado, desarrollando nuevas tácticas y vías de ataque hasta llegar a ser una botnet madura y estructurada que se suma al modelo de negocio de Malware-as-a-Service (MaaS).

Entre todos los servicios que la botnet Trickbot provee, se encuentran el fraude bancario, el robo de datos confidenciales, como credenciales y datos bancarios, minería de criptomonedas y la difusión de ransomware como Ryuk o Conti, los cuales son parte de la industria del Ransomware-as-a-Service o RaaS.

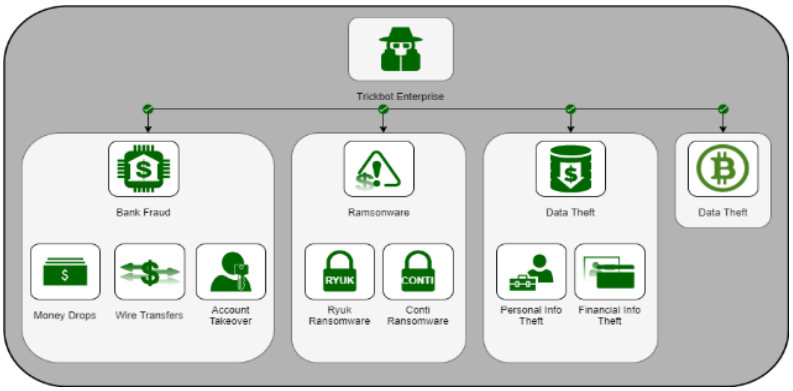


Imagen 13. Servicios de la botnet Trickbot

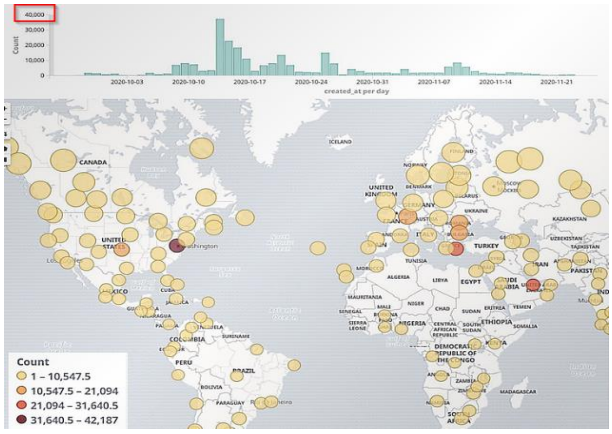


Imagen 14: infecciones por Trickbot desde octubre 2020

Durante los meses de octubre y noviembre se detectaron un número elevado de ataques por todo el mundo, habiéndose podido observar 40.000 infecciones en un solo día.

Durante el mes de octubre se llevaron a cabo operaciones entre Microsoft, ESET, Black Lotus Lab de Lumen, NTT y Symantec, para disrumpir los ataques de la botnet Trickbot. Si bien es cierto que la actividad de dicha botnet se vio reducida drásticamente, el grupo no ha desaparecido del mapa.

Durante el mes de diciembre se ha descubierto una nueva versión de Trickbot que supone una amenaza crítica para la comunidad si se consiguiera explotar.

En las versiones observadas antes del mes de diciembre, algunas de las herramientas utilizadas para comprometer los sistemas han sido PowerShell Empire o CobaltStrike, los cuales distribuían Conti y Ryuk, respectivamente. También encontramos "LightBot", un script de PowerShell capaz de realizar reconocimiento de los sistemas y recolectar información, así como Mimikatz y exploit EternalBlue.

A principios de este mes se notificó la existencia de una nueva funcionalidad de TrickBot para escanear vulnerabilidades en el firmware de la BIOS, a la que han denominado 'Trickboot'[11].

Esta nueva táctica[12] es capaz de analizar las vulnerabilidades en la UEFI/BIOS de los sistemas para poder, entre otras cosas, realizar modificaciones en el firmware además de todas las funcionalidades que ya poseía este malware. Este tipo de ataques supone una amenaza potencialmente peligrosa.

Se han distribuido muestras del malware que cuentan con la funcionalidad 'Trickboot' a países alrededor de todo el mundo, entre los que se encuentra España como objetivo. Los sectores que Trickbot ha atacado son múltiples, entre los que se el sector gubernamental, financiero, salud, telecomunicaciones, educación y otros relacionados con infraestructuras críticas.

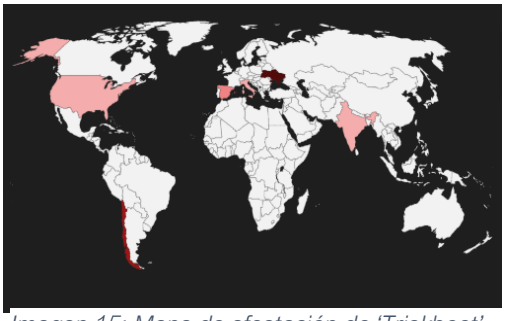


Imagen 15: Mapa de afectación de 'Trickboot'

Análisis Técnico:

```
rdata:000000018002A098 ; Export Names Table for user_platform_check.dll
rdata:000000018002A098 ;
rdata:000000018002A098 off_18002A098   dd rva aControl, rva aFreebuffer, rva aRelease, rva aStart
rdata:000000018002A098                                         ; DATA XREF: .rdata:000000018002A080↑o
rdata:000000018002A098                                         ; "Control" ...
rdata:000000018002A0A8 ;
rdata:000000018002A0A8 ; Export Ordinals Table for user_platform_check.dll
rdata:000000018002A0A8 ;
rdata:000000018002A0A8 word_18002A0A8  dw 0, 1, 2, 3           ; DATA XREF: .rdata:000000018002A084↑o
rdata:000000018002A0B0 aUserPlatformCh db 'user_platform_check.dll',0
rdata:000000018002A0B0                                         ; DATA XREF: .rdata:000000018002A06C↑o
rdata:000000018002A0C8 aControl        db 'Control',0          ; DATA XREF: .rdata:off_18002A098↑o
rdata:000000018002A0D0 aFreebuffer     db 'FreeBuffer',0       ; DATA XREF: .rdata:off_18002A098↑o
rdata:000000018002A0DB aRelease        db 'Release',0          ; DATA XREF: .rdata:off_18002A098↑o
rdata:000000018002A0E3 aStart          db 'Start',0            ; DATA XREF: .rdata:off_18002A098↑o
rdata:000000018002A0E9                 align 4
```

Imagen 16: módulo PermaDll encontrado en muestra de TrickBot

El equipo de analistas de Mnemo ha analizado una muestra cuyo nombre del nuevo módulo es el de 'PermaDll' o 'user_platform_check.dll'.

Este módulo podría ser utilizado para crear persistencia en el firmware del sistema infectado. Esto es especialmente crítico ya que explotar una vulnerabilidad de la BIOS y conseguir alojar código malicioso, supondría que se haga improbable recuperar el equipo infectado de un ataque de este tipo.

El troyano afecta a nivel de placa base y persistirá en el hardware, con independencia de la información en los discos duros. La solución a este tipo de ataques suele ser cambiar la placa base entera o resetear completamente el UEFI firmware, lo que se traduce en un altísimo coste económico.

El encargado de transmitir la información entre circuitos integrados es el SPI, que contiene el firmware UEFI/BIOS, necesario para arrancar el sistema. El chip flash SPI (Serial Peripheral Interface) recibe las peticiones de la UEFI y lo envía a través del controlador SPI, que pertenece al PCH (Platform Controller Hub) de Intel.

Este controlador cuenta con el control de acceso al firmware, que debería estar restringido para no permitir cambios en la UEFI. Sin embargo, si esta restricción no está habilitada, se

[11] https://www.advanced-intel.com/post/persist-brick-profit-trickbot-offers-new-trickboot-uefi-focused-functionality

[12] https://www.ncsc.gov.uk/news/trickbot-advisory

podría atacar esta vulnerabilidad para comprometer el firmware, hacerse con el control total del sistema y de las cuentas del equipo.

La forma en la que el TrickBot comprueba si el equipo es vulnerable a este tipo de ataques es a través de la herramienta RWEverything (read-write everything), específicamente con el driver RwDrv.sys que se adjunta ofuscado en la muestra del malware. Este driver, que se carga gracias a un módulo llamado 'permadll32_main_module', interactúa con el controlador SPI y se encarga de comprobar si el control de acceso a la BIOS está restringido y que partes pueden ser modificadas.

Herramientas como 'RWEverything' ya se habían utilizado antes en campañas de Sligshot APT y malwares como LoJax. El uso de estas nuevas funcionalidades por parte de TrickBot supone una nueva amenaza para una parte del sistema tan crítica como es el firmware.

Si el atacante consigue explotar esta vulnerabilidad y modificar el contenido del firmware, sería posible ejecutar el código malicioso antes del arranque del sistema operativo, así como esconder de la víctima y de los mecanismos de defensa del sistema la existencia de esta vía de entrada a nuevos ataques.

Actualmente las muestras detectadas no han explotado aún esta funcionalidad para comprometer el firmware. No obstante, se ha descubierto que el software malicioso ya cuenta con las funcionalidades de leer, escribir y borrar el firmware y podría dar paso a numerosos ataques en un futuro próximo por parte de este grupo de atacantes.

En la imagen siguiente se pueden observar, según la matriz de MITRE, las técnicas utilizadas por el Trickbot, resaltadas en verde.

Execution	Discovery	Collection	Command and Control	Exfiltration	Impact
Command and Scripting Interpreter	Account Discovery	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploitation for Client Execution	Application Window Discovery	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Inter-Process Communication	Browser Bookmark Discovery	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Native API	Cloud Infrastructure Discovery	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Scheduled Task/Job	Cloud Service Dashboard	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Shared Modules	Cloud Service Discovery	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Software Deployment Tools	Domain Trust Discovery	Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
System Services	File and Directory Discovery	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
User Execution	Network Service Scanning	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Windows Management Instrumentation	Network Share Discovery	Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
	Network Sniffing	Data Staged	Non-Standard Port		Resource Hijacking
	Password Policy Discovery	Email Collection	Protocol Tunneling		Service Stop
	Peripheral Device Discovery	Input Capture	Proxy		System Shutdown/Reboot
	Permission Groups Discovery	Man in the Browser	Remote Access Software		
	Process Discovery	Man-in-the-Middle	Traffic Signaling		
	Query Registry	Screen Capture	Web Service		
	Remote System Discovery	Video Capture			
	Software Discovery				
	System Information Discovery				
	System Network Configuration Discovery				
	System Network Connections Discovery				
	System Owner/User Discovery				
	System Service Discovery				
	System Time Discovery				
	Virtualization/Sandbox Evasion				

Imagen 17: Tácticas de ataque según la matriz de MITRE

Un compromiso en el firmware de la UEFI/BIOS podría suponer un alto impacto a nivel económico y reputacional, así como a nivel de disponibilidad de los sistemas. Debido a la persistencia que la funcionalidad 'Trickboot' puede adquirir y la peligrosidad del troyano Trickbot de implantar otro tipo de software malicioso, como pueden ser los ransomware Ryuk y Conti, hacen que el impacto que puede tener sea crítico.

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

- Comprobar que los sistemas no sean vulnerables y que el permiso de escritura en la BIOS esté restringido y las protecciones activadas.
- Comprobar que los sistemas no se hayan visto comprometidos ni se haya realizado ninguna conexión con los IOCs de TrickBot, para asegurar que ningún sistema haya podido ser infectado.
  https://bazaar.abuse.ch/browse/tag/trickboot/

  https://www.mcafee.com/enterprise/en-us/lp/insights-preview.html#threat-profile--conti-ransomware
- Comprobar los hashes del firmware con los hashes legítimos para comprobar su integridad y descartar que se hayan realizado modificaciones.
- Actualizar el firmware a las versiones que resuelvan las vulnerabilidades conocidas y tener la última versión instalada.
- Realizar exámenes forenses por parte del equipo de respuesta ante incidentes ante cualquier duda o sospecha de infección.
- Añadir reglas Yara a los sistemas de detección de intrusiones corporativos.

Ransomware Conti: nueva amenaza del año 2020

Conti[13] se trata de un ransomware que ha venido atacando empresas alrededor de todo el mundo en numerosos sectores. Este malware de tipo ransomware suele estar asociado con otras amenazas que también tienen afectación internacional.

Aunque Conti se detectó por primera vez en diciembre de 2019, se ha identificado un incremento en su actividad desde verano de este año, convirtiéndolo en una de las principales amenazas del 2020. Cuenta con algunas funcionalidades similares a las de la segunda versión de Ryuk lo que hace que se considere el sucesor más sofisticado de Ryuk. Es probable que los atacantes detrás de Ryuk y Conti pertenezcan al mismo grupo o se relacionen entre sí.

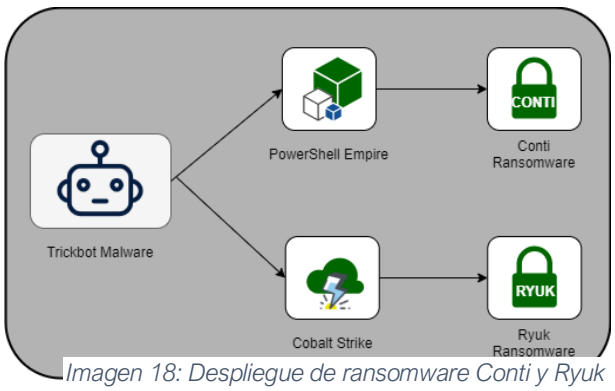


Imagen 18: Despliegue de ransomware Conti y Ryuk a través de Trickbot

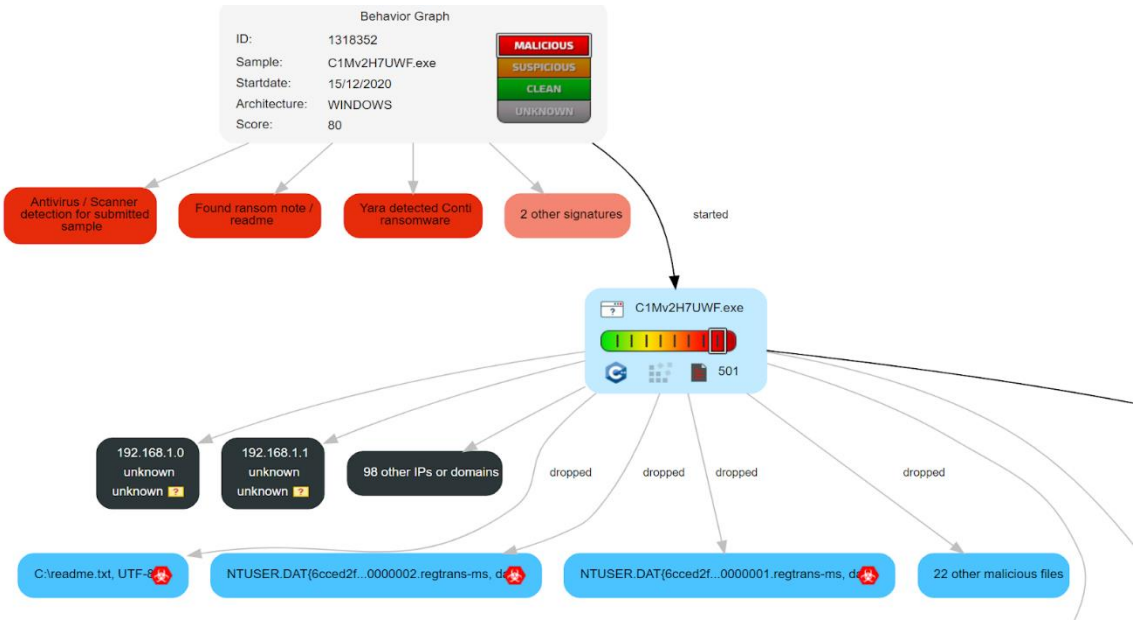
Las últimas campañas de difusión del Conti se han visto relacionadas con las campañas recientes de Trickbot, donde se ha utilizado este troyano como 'backdoor' para depositar el ransomware en última instancia de la cadena de ataque.

En uno de los ataques más grandes de Conti, el grupo exigía el pago de 750 Bitcoin para recuperar toda la información borrada y encriptada, aproximadamente 14 millones de dólares. En la página de leaks de Conti han sido publicadas más de 11 páginas de empresas a las que han conseguido infectar.

[13] https://threatpost.com/conti-iot-chip-advantech-ransom-demand/161691/

Conti[14] usa hasta 32 hilos en la CPU simultáneamente para encriptar los archivos, lo que lo hace mucho más rápido y eficaz a la hora de ejecutar el ransomware y comprometer el sistema. Tras el proceso de infección, este ransomware genera una nota denominada 'readme.txt'.

La siguiente imagen enseña el comportamiento de una muestra analizada. Se puede observar como en la ejecución se realizan varias actividades maliciosas entre las que la máquina infectada se trata de comunicar con múltiples IPs privadas de la red local.



Las conexiones con las IPs es otra de las acciones características del Conti y es que realiza un escaneo de la red local en búsqueda de equipos que tengan habilitado el puerto 445 perteneciente al protocolo SMB, utilizado por Windows para la compartición de recursos en red. El objetivo del Conti es encriptar todos aquellos datos que se encuentran compartidos a través del protocolo SMB.

Esto es especialmente peligroso si los atacantes conocen previamente la red y consiguen acceder mediante puertos vulnerables aprovechando el uso de esta funcionalidad, lo que podría ser combinado con técnicas de evasión, para eludir los sistemas de defensa y poder causar el mayor impacto posible.

En la siguiente imagen se observa un ejemplo del tráfico de red de la misma muestra analizada. Las peticiones corresponden con las peticiones que Conti realiza a todas las IPs del rango 198.168.1.0/24 por el puerto 445 (SMB), esperando recibir respuesta de todas las IPs que cuenten con el protocolo habilitado.

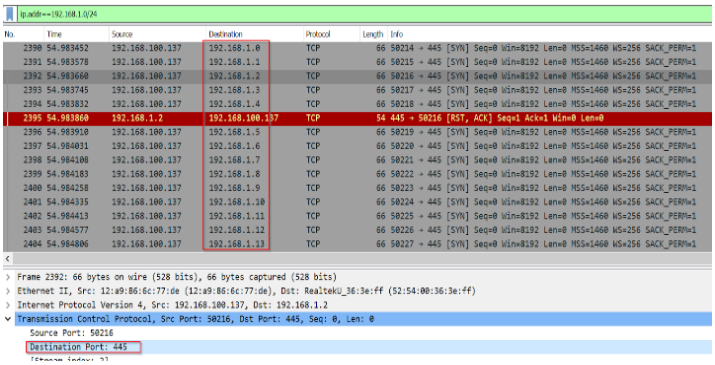


Imagen 20: tráfico de red de muestra maliciosa analizada

[14] https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/

Las muestras que se han analizado corresponden con la tercera versión del ransomware. La actividad detectada durante el mes de diciembre comenzó con difusiones de la segunda versión y, a partir de mitad de diciembre, parece que se ha difundido activamente Conti v3.

Entre las tácticas utilizadas por Conti podemos ver técnicas de evasión (como la ofuscación, evasión de sandboxes y análisis dinámicos o masquerading), técnicas de inyección de código y de creación de procesos, así como, técnicas de descubrimiento del sistema infectado y técnicas de encriptación.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 1 2	Masquerading 3	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1 1	LSASS Memory	Security Software Discovery 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Proxy 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Imagen 21: Tácticas en matriz MITRE

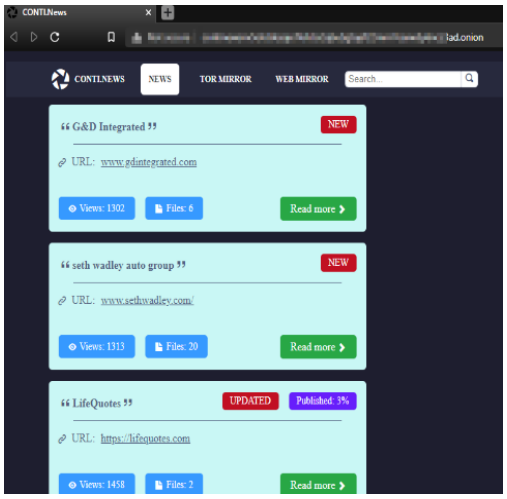


Imagen 22: página de noticias de Conti

El grupo de cibercriminales realiza publicaciones casi a diario de nuevas compañías afectadas por el ransomware. Esto prueba que el objetivo de estas campañas parece ser global.

El grupo detrás de esta página publica los archivos robados a las compañías afectadas en caso de no pagar la cantidad que se le exige por el rescate. Estos datos contienen información confidencial, datos personales, credenciales, datos bancarios, documentos internos, etc.

Mitigación de vulnerabilidades

Sabemos que existen, cómo mitigarlos y aún siguen siendo una ciberamenaza crítica

Los riesgos cibernéticos para la infraestructura de las compañías dependen de la sostenibilidad del sistema de seguridad. Esta tarea se hace cada vez más ardua por todo el trabajo conjunto y coordinado que las diferentes áreas deben asumir según sus responsabilidades.

En muchos ámbitos son mencionados los pilares de la seguridad como lo son la Confidencialidad, Integridad y Disponibilidad; pero añadido a esto, el desarrollo de un ambiente seguro es prioritario.

Para entender un poco el panorama real de las compañías en el momento de mantener su seguridad tecnológica, es necesario realizar un análisis por medio de las responsabilidades dentro del sistema de seguridad y de esta manera definir en dónde pueden existir mayores riesgos al respecto.

Descubrimiento de Vulnerabilidades

Los investigadores que apoyan la seguridad son quienes analizan y prueban desde diferentes frentes los fallos de seguridad dentro del desarrollo y aplicabilidad de las nuevas versiones de software, evitando que puedan ser aprovechadas para afectar los sistemas.

El proceso investigativo merece un reconocimiento con relación al análisis de las nuevas versiones de software, pero donde todo cambia radicalmente es la usabilidad de este; es donde aparece la línea que separa a los ciberdelincuentes de los profesionales de seguridad.

Una vez es descubierta la vulnerabilidad, esta puede ser publicada con su respectivo análisis dentro de un sistema controlado que no afecte a ninguna organización o persona y que apoye el avance tecnológico y seguridad cibernética. Este ciclo ya es conocido ampliamente, pero es mencionado como preámbulo a todo el análisis realizado a continuación.

La lucha en este punto es contra aquellos que realicen la misma labor contra el fabricante que genera sus boletines de seguridad publicando las brechas junto con los parches o nuevas versiones que las remedian.

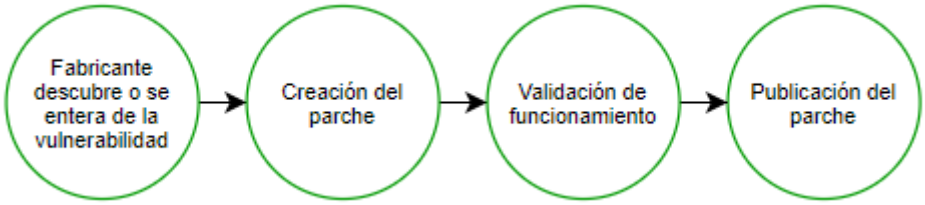
Pero dentro de este proceso existen variables con las que el tiempo de afectación se acelera y es cuando aparecen los exploits que aprovechan dichas vulnerabilidades y pueden ser utilizados para afectar sistemas expuestos.

En este momento existen varios estados en los cuales una organización se puede encontrar:

a. **Conocimiento**: Aquellas organizaciones que son conscientes de las brechas de seguridad, están atentos a los boletines de seguridad, alertas y proveedores que notifican al respecto de los nuevos riesgos a los cuales se ven expuestos.

b. **Desinterés**: Organizaciones donde no existen procesos que analicen, traten o mitiguen futuros riesgos tecnológicos a raíz de nuevas vulnerabilidades o exposiciones.
c. **Desconocimiento**: Es donde se encuentran todas las organizaciones frente a las vulnerabilidades de día cero, que son aquellas que no son de conocimiento general y podrían afectar una brecha la cual no está determinada ni tratada.

Las vulnerabilidades son el principal objetivo de los atacantes debido a que es el futuro triunfo a la hora de acceder a innumerables compañías.



Este proceso inicial de conocimiento de una nueva brecha de seguridad es imperceptible para las compañías a menos que mantengan al día sus procesos de investigación de alertas tempranas.

Los fabricantes cumplen con su labor de investigación según cada una de sus capacidades de investigación y su capacidad de contar con laboratorios que se dediquen a la mejora continua de sus productos.

Otras entidades no cuentan con tanta capacidad por lo que en el momento de una brecha de seguridad el nivel de respuesta o desarrollo de un parche de seguridad no es tan rápido, exponiendo la seguridad de sus usuarios. Estos últimos son aún más atractivos para atacantes ya que contarán con más tiempo para explotarlos.

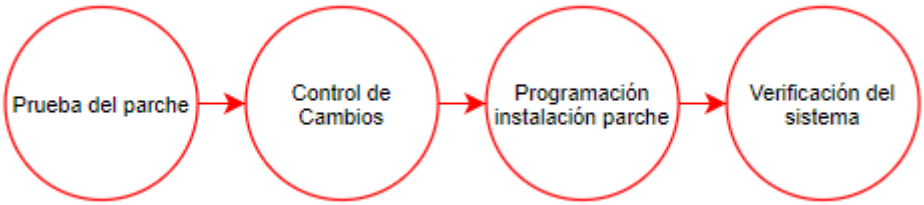
El papel de los fabricantes genera impacto positivo por medio de sus métodos de notificaciones de nuevos riesgos y publicación de nuevos parches que solucionen los problemas de seguridad detectados.

Existe la realidad cibernética donde las compañías deben protegerse debido a diferentes riesgos, que pueden ir desde **programas malignos** generados para aprovechar vulnerabilidades en general, **ataques dirigidos** para obtener información privilegiada o eventos que podrían desencadenar una **denegación de los servicios** corporativos.

A continuación, se muestra cómo se aborda tal responsabilidad según el rol interno y aporte a la sostenibilidad del sistema de seguridad.

El área de infraestructura cumple un rol muy importante dentro del aseguramiento y afinamiento de las plataformas donde se mantienen en reposo o en tránsito la información. En algunos casos son responsables de las estaciones de trabajo donde la información está en uso.

Con este preámbulo y en conocimiento que la información es lo más importante de las organizaciones, se puede definir que esta área es determinante en la sostenibilidad y aseguramiento de la seguridad corporativa.



Cuando se aborda al equipo de infraestructura para indicarles su apoyo puntual en el ciclo de aseguramiento con relación a la mitigación de nuevas vulnerabilidades, ellos deben tener en cuenta tareas de mitigación de estos riesgos por medio la implementación de parches, mejoras en la configuración o hardening de los sistemas que administran.

Los pasos mencionados son los que como mínimo deben abordar como parte de la solución, y el realizarlos de manera adecuada significa tener la responsabilidad de no afectar los servicios misionales de las compañías.

- **Prueba del parche:** En ocasiones los parches son la solución base de los problemas reportados, pero no todos; sin embargo, un parche nuevo podría afectar a la infraestructura modificando ítems que afecten configuraciones u otros software que se ejecuten sobre estos sistemas.

  Lo más común es contar con un sistema de pruebas donde se ejecuten dichas actualizaciones para valorar los riesgos antes de poner el sistema en producción con el nuevo parche, de esta manera no se afecta a los procesos que normalmente se ejecutan. Para todo esto será necesario contar con herramientas de virtualización en donde se podrían clonar los sistemas y probar los resultados.

- **Control de cambios**: cumplimiento normativo de seguridad de la información y calidad, donde se debe tener un proceso de control de cambios donde los integrantes de infraestructura deberían reportar la implementación de nuevos parches en sus sistemas. Esto implica pasar por una reunión de validación y por la generación de un plan de trabajo, plan de recuperación, programación y ejecución.

- **Programación de instalación del parche**: esta tarea se realiza por medio de sistemas de distribución de parches; esto aplica especialmente en estaciones de trabajo, porque en servidores no es común que se realice de manera automática por el riesgo que sugiere el no pasar por el proceso de pruebas y control de cambios.

  La mayoría de las compañías únicamente masifican parches de Microsoft porque otros softwares se ejecutan de manera automática. Cuando por privilegios de administrador no se logre, terminan quedando en la misma versión por mucho tiempo.

  En este punto la problemática se divide en el control estricto de implementación de nuevas versiones, parches o service pack de aplicaciones de servidores; y la masificación de parches en sistemas operativos clientes. Si es de manera masiva, se debe programar debido a la carga de red que puede suponer debido a la masificación.

- **Verificación del sistema:** infraestructura deberá realizar seguimiento del parche, tunning o cualquier actividad ejecutada para la mitigación de una vulnerabilidad, validando

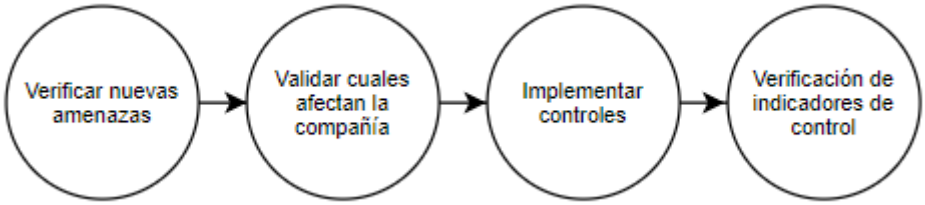
que las funcionalidades propias del servicio no se vean afectadas y reportando a las áreas de seguridad la instalación de este para sus validaciones.

Los procesos realizados por el área de infraestructura son los necesarios tanto dentro del proceso de mitigación del riesgo como dentro de la cadena de procedimientos que se deben llevar a cabo, pero no en todos los casos se pueden aplicar los parches o procedimientos recomendados.

Algunas ocasiones cuando estos afectan los servicios activos, se deben tomar decisiones de no uso para dar prioridad a la prestación del servicio; es por ello por lo que no es suficiente obviar esta responsabilidad sin tomar otras medidas que los apoyen el objetivo.

Debido a todos los pasos necesarios mencionados anteriormente, puede pasar hasta semanas antes de que se pueda aplicar un parche, por lo que implica su implementación y configuraciones específicas. Este tipo de análisis son claros para los ciberdelincuentes donde aprovechan este tiempo para buscar los sistemas expuestos en donde ni han notado los fallos de seguridad o están en el proceso de implementación de los controles.

Los **administradores de plataformas** tienen todo el protagonismo dentro de la lucha contra los atacantes que buscan explotar las vulnerabilidades de una organización.



Se mencionan de manera muy general diferentes etapas que se deberían cumplir al respecto dentro del ciclo de mitigación por parte de aquellos que administran las herramientas que están en la línea de defensa.

- **Verificar nuevas amenazas:** todas las plataformas pertenecen a un fabricante que cuenta con laboratorios que generan constantemente firmas que detectan nuevas amenazas. Es responsabilidad el mantener actualizados los sistemas de protección.

- **Validar cuales afectan a la compañía**: en varios casos las firmas liberadas no se aplican automáticamente, entonces es donde el administrador de la plataforma deberá verificar esas nuevas firmas para activarlas en protección donde sea necesario. La seguridad no puede darse de una manera estática ya que los ataques son dinámicos y por lo tanto las verificaciones que se deben realizar a diario deben cumplir con la misma ideología.

  Es común encontrar organizaciones donde sus soluciones de seguridad se configuran en el momento de la implementación y automatizan sus servicios de actualización de firmas, pero después no se hace ninguna tarea adicional que valide en nivel de detección con relación a los nuevos retos cibernéticos.

- **Implementar controles:** cada amenaza tiene un objetivo en específico y para ello existen soluciones de seguridad que permiten poner un escudo de protección para aquellas que son conocidas y en algunos casos poder generar acciones preventivas.

Pero las soluciones deben ser gestionadas adecuadamente bajo un monitoreo, aplicabilidad según eventos detectados y en especial con ajustes de prevención de indicadores de compromiso a los que puedan tener acceso bien sea por la misma industria de seguridad o gremios de seguridad cibernética.

Los controles también pueden ser implementados sobre activos intermedios, los cuales pueden proporcionar seguridad para aquellos que no tienen localmente las firmas o configuraciones de protección. Para este tipo de procesos es indispensable asegurar que sean el único canal de comunicación con los activos vulnerables y que sea viable la revisión de las conexiones que llegarán a ellos.

- **Verificación de indicadores de control:** Cuando se implementa un control de seguridad es importante validar si es funcional midiendo el nivel de exposición al cual estuvo expuesta la organización. De igual forma en el caso de las vulnerabilidades o exposiciones es importante realizar análisis de vulnerabilidades excluyendo los niveles de seguridad y al igual con estos implementados. Los datos comparativos reflejarán la realidad de protección de la organización.

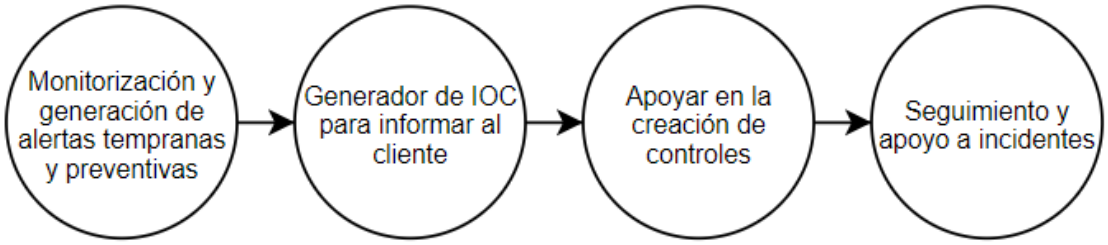
Las organizaciones deben contar con un plan de seguimiento del estado de seguridad de sus activos críticos que a su vez esté asociado con el impacto a sus objetivos misionales.

Perspectiva externa

La responsabilidad de atender los riesgos y brechas de seguridad de una compañía se encuentra en la estrategia de ciberseguridad organizacional. Las tareas resultantes de este plan de aseguramiento deben cubrir de manera consistente las necesidades de los procesos misionales de la organización y blindar sus intereses corporativos.

Otra manera de aportar al fortalecimiento de una estructura de seguridad está en la visión externa de la misma con la evaluación externa desde el punto de vista global, regional y gremial.

Los **proveedores de ciberseguridad** son figuras necesarias dentro del esquema de fortalecimiento cibernético de las organizaciones; son compañías donde su razón de ser es la ciberseguridad y, trabajan constantemente de manera independiente o con fabricantes de seguridad en estrategias para ofrecer a sus clientes soluciones y servicios que apoyen la mitigación de los riesgos.



La estrategia de seguridad debe contemplar escenarios globales que proporcionen herramientas de prevención a las compañías, permitiendo a las organizaciones tener una postura proactiva y no reactiva frente a los riesgos latentes.

La postura de los proveedores es importante en el éxito de la estrategia cibernética, al igual que la adopción de las medidas por parte de los clientes. A continuación, se mencionarán

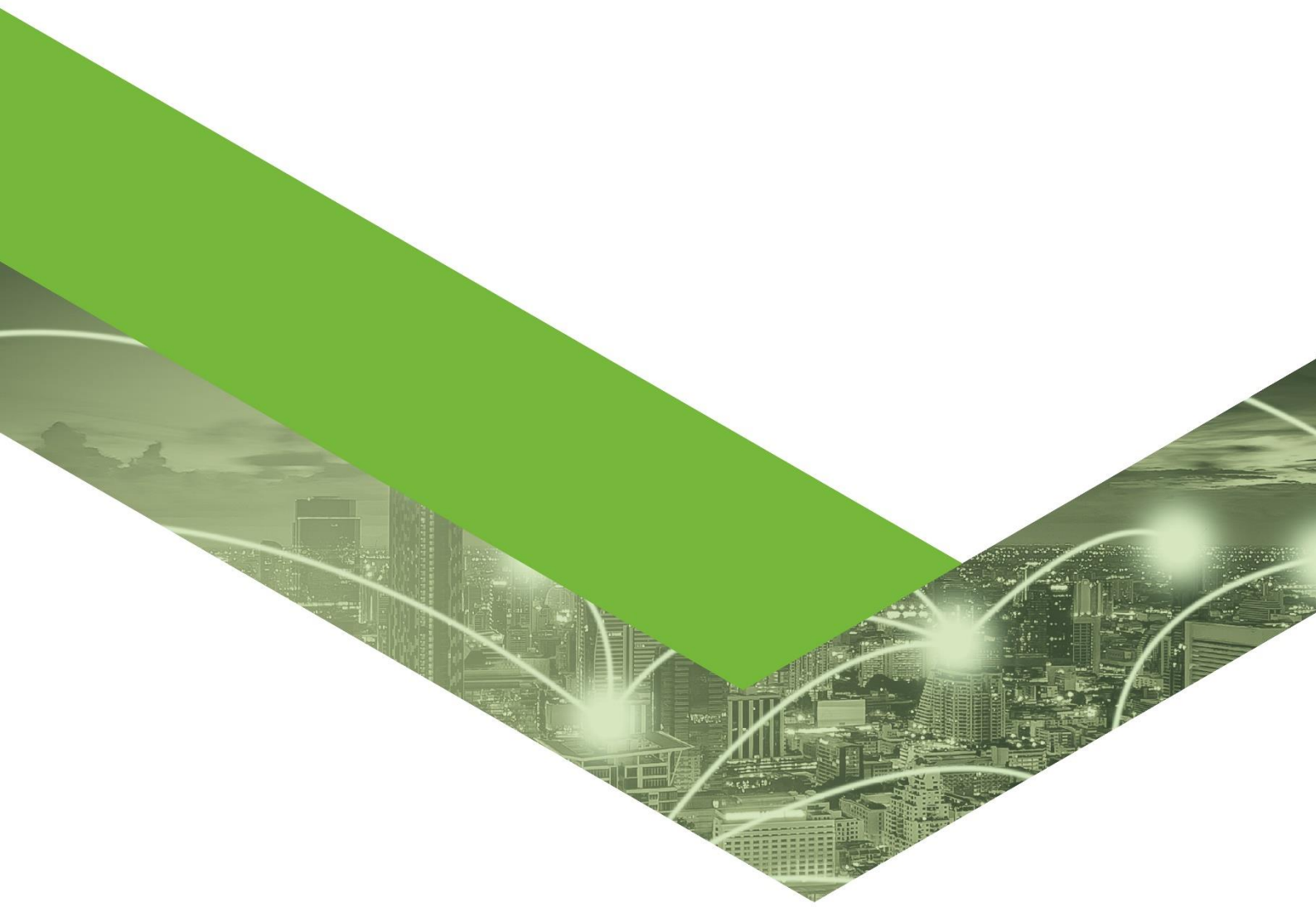
varios puntos globales donde se apoya activamente a las organizaciones desde una vista externa.

- **Monitorización y generación de alertas tempranas y preventivas**: analizar el comportamiento de los eventos de seguridad generados por los activos de seguridad de las organizaciones es importante para conocer el nivel de exposición y la efectividad de los controles implantados.
- **Generación de IOC**: Los indicadores de compromiso se pueden proporcionar por varias vías, dentro de las más comunes se encuentra la incorporación de firmas de seguridad propias de los fabricantes de las plataformas incorporadas. Un proveedor de seguridad que esté a la vanguardia de seguridad debe contar con alianzas fuertes en la comunidad cibernética que le permita tener acceso de primera mano a información de posibles ataques y que puedan proporcionar estos datos a los clientes antes que los fabricantes de seguridad los conozcan y generen firmas para estos.
- **Apoyo en la creación de controles**: La consultoría acerca de cómo implementar controles, políticas y siguientes pasos es tarea fundamental de los consultores externos, son quienes tienen la visión de cómo es el comportamiento de las amenazas en otros clientes o ambientes y por lo tanto compartirlas y asociarlas en aquellos que nos han sufrido dichos problemas.
- **Seguimiento y apoyo a incidentes**: En incidentes de ciberseguridad es donde las organizaciones necesitan todo el apoyo necesario por parte de sus socios estratégicos de servicios cibernéticos; debe existir un plan previo de atención a incidentes donde se tengan en cuenta todos los factores de riesgo y tener una respuesta clara ya sea de manera técnica o estratégica.

El trabajo de todos los actores involucrados en el proceso de mitigación de vulnerabilidades es vital para la sostenibilidad cibernética. No es un trabajo solamente de los administradores de los activos, sino de todos los que hacen parte de una u otra forma de los procesos de mitigación.

El trabajo colaborativo se debe extender más allá de los límites internos de la organización, siendo participe del trabajo coordinado con sus proveedores en la rama de seguridad tecnológica, planteando nuevos planes a futuros ataques y cómo disminuir las brechas que se puedan tener frente a los ataques actuales.

Los esfuerzos deberían centrarse en planear las estrategias de control y mitigación de ataques de día cero, los cuales son difíciles de prever. Además, se puede planear las acciones de reacción en caso de ser víctima de este tipo de ataques, donde los planes de continuidad funcionen de la manera más óptima.



MNEMO