CIBERBOLETÍN

MARZO 2021

TEMA DEL MES

El proceso de transformación de la inteligencia en defensas activas para las organizaciones.

VULNERABILIDADES

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

THREAT INTELLIGENCE

Ploutus-I, ciberataques contra cajeros automáticos. Análisis de su funcionamiento y modelado del ataque.

EN NUESTRA REGIÓN

Ciberataque al Servicio Público de Empleo Estatal Español SEPE. El ransomware Ryuk y su comportamiento en el último año.

CULTURA DE CIBERSEGURIDAD

La técnica Pass-The-Hash, qué es y cómo detectarla.

MNEMO

TEMA DEL MES

Convirtiendo nuestra inteligencia en defensa activa

A menudo la generación de inteligencia por parte de nuestros equipos termina en la entrega de un reporte contextualizado, basado en las evidencias obtenidas, con indicadores y comportamientos observados. Esto, en cierta medida es correcto desde el punto de vista de cyber threat intelligence, pero en muchas ocasiones las partes interesadas necesitan convertir toda esa inteligencia generada en **procesable** (conocido en inglés como actionable) y generar diferentes medidas internas de **defensa activa**.

Para que la inteligencia generada sea considerada procesable, debe de poder realizarse algún tipo de acción con ella, como la implementación de acciones defensivas.

También nos puede servir en cuatro grandes bloques para llevar a cabo diferentes acciones de actuación.

- Identificación
- Protección
- Detección
- Respuesta

Si la inteligencia generada nos permite realizar alguna de las cuatro acciones anteriores, es de vital importancia hacerlo para defender y minimizar el riesgo de la organización.

Analizar campañas, eventos, incidentes y aplicar diferentes modelos de trabajo y frameworks, permite ser granulares a su máximo exponente, permitiendo tener grandes capacidades de **correlación y generación de patrones y tendencias**.

Todos los indicadores obtenidos deben tener un rol diferente para ser accionables.

Direcciones IP, dominios, malware, artefactos, un comportamiento específico… Todos ellos pueden ser sometidos a diferentes acciones. Por ejemplo, una dirección IP puede ser bloqueada a nivel de comunicación o puede ser consultado su histórico en diferentes data sources para comprobar si tuvo interacción con algún equipo.

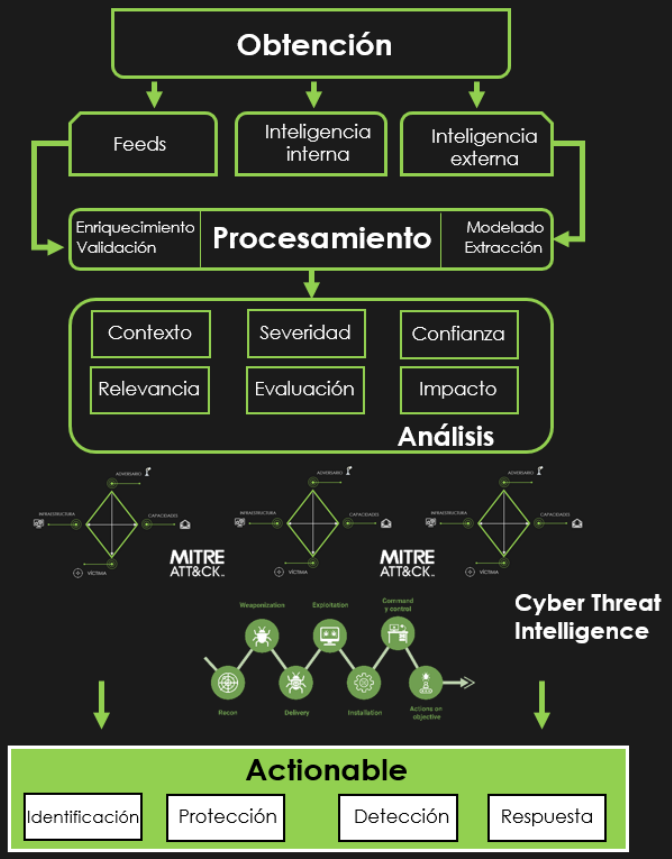
Ambas acciones podrían considerarse actividades accionables, con la pequeña diferencia de que una de ellas es activa (la primera) y la otra sería pasiva (la segunda).

Dependiendo del objetivo final y las circunstancias, se aplicará una acción activa o pasiva sobre los indicadores obtenidos del análisis.

Es importante remarcar que no sólo se pueden llevar acciones con los IOCs convencionales, sino que con patrones y comportamientos es totalmente aplicable esta metodología.

Existen diferentes flujogramas a aplicar con un final de convertir la inteligencia en accionable.

TEMA DEL MES



El anterior flujo de trabajo representa en cierta medida y a un alto nivel, las diferentes fases por donde deben de pasar los datos iniciales, que serán convertidos en información, para posteriormente generar inteligencia y por último, convertir dicha inteligencia en defensas accionables activas para poder protegernos de aquellos indicadores que pueden impactar contra nuestra organización.

La obtención partirá de lo que la organización disponga, esto puede ser reportes internos, reportes externos, feeds, etc…

Posteriormente, todos esos datos obtenidos tienen que pasar por una fase de procesamiento, la cual tiene como objetivo enriquecer y dar más sentido el objetivo de estudio durante la investigación.

La fase de análisis debe de ser capaz de convertir los datos iniciales en información para poder después generar inteligencia.

- **Contexto**: ¿Hay algo más alrededor que pueda ser interesante? ¿Esta información la he visto previamente?
- **Relevancia**: ¿Lo que estoy analizando es relevante para mi organización?
- **Severidad**: ¿Qué gravedad conllevaría que la amenaza tuviese lugar?
- **Confianza**: ¿La información que se está analizando proviene de una fuente de confianza?
- **Evaluación**: ¿Existe algún tipo de correlación con otros análisis realizados? ¿La información es de valor?
- **Impacto**: ¿Qué influencia tiene la amenaza en mi entorno?

Jose Luis Sánchez Martínez
Cyber Threat Intelligence Manager

La importancia de la defensa actionable radica en que da la posibilidad a las organizaciones de convertir todo su análisis e investigación en operaciones proactivas para poder interferir, denegar, engañar, etc… los pasos que dan los cibercriminales. Todos los analistas de CTI deben de poder ser capaces generar este tipo de producto basado en sus análisis.

TEMA DEL MES

La aplicación de diferentes metodologías como diamond model, cyber kill chain, extracción de TTPs mediante ATT&CK de MITRE, etc, puede ayudarnos a detectar esos valiosos patrones y tendencias para poder **centrar los esfuerzos de seguridad en lo que verdaderamente está siendo utilizado en diferentes campañas**.

En último lugar nos encontramos ante la fase que más valor tiene de todo el proceso, que es la conversión de todos los indicadores en defensas activas.

Para esto, existe un modelo muy conocido y ampliamente usado llamada **Course of Action Matrix**, el cual, combina las diferentes fases del cyber kill chain con siete acciones (7 Ds), cinco activas y dos pasivas. Estas siete acciones son las siguientes.

- Discover
- Deny
- Degrade
- Destroy
- Detect
- Disrupt
- Deceive

No siempre se podrán aplicar todas las acciones para todos los indicadores, por lo que habrá que hacer foco en aplicar las que más interesen. Por ejemplo, aplicando una acción de deny para una IP, bloquearíamos por completo una comunicación. Sin embargo, si estamos interesados en investigar dicha comunicación, quizás no es lógico ejecutar una acción de deny.

La columna de indicadores se debe de rellenar con aquellos que queremos llevar a cabo alguna acción. Sirvan los mostrados en la tabla como ejemplo.

Por último, habrá que rellenar las celdas en base a la tecnología o actividad que se realizará. En la fase de C&C, si queremos engañar al cibercriminal, podemos realizar un sinkhole del dominio y emular las respuestas, pero si queremos bloquear las comunicaciones, con una regla en la tecnología perimetral que se disponga se podrá cortar la comunicación

		Pasivo		Activo				
MNEMO	Indicadores	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconocimiento	Obtención de correos electrónicos							
Preparación								
Distribución	Emails enviados con links Cuentas de origen							
Explotación	Ejecución EXE							
Instalación	Persistencia mediante archivo en StartUp y claves de registro Run							
Comando y Control (C&C)	Comunicación con servidor C&C puerto 8921							
Acciones sobre los objetivos	Exfiltración de información en .zip							

VULNERABILIDADES

Principales vulnerabilidades Marzo 2021

Microsoft Exchange Server, BIG-IP y VMware View Planner

Titulo	Identificador	CVSS	Descripción
Falla de seguridad presente en **Microsoft Exchange Server**	CVE-2021-26855	CVSS v3.1: 9.8	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 **BIG-IP**	CVE-2021-22987	CVSS v3.1: 9.9	Vulnerabilidad presente en algunas versiones de **BIG-IP**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **VMware**	CVE-2021-21978	CVSS v3.1: 9.8	Vulnerabilidad que afecta a **VMware View Planner 4.x anteriores a 4.6**, la cual puede permitir a un actor malicioso ejecutar código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **Cisco**	CVE-2021-1411	CVSS v3.1: 9.9	Vulnerabilidad presente en algunas versiones de **Cisco Jabber**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **Cisco**	CVE-2021-1451	CVSS v3.1: 9.8	Vulnerabilidad que afecta a **Cisco IOS XE**, la cual puede permitir a un actor malicioso ejecutar código en el sistema vulnerable.
Falla de seguridad presente en productos de **SAP**	CVE-2021-21480	CVSS v3.1: 9.9	Vulnerabilidad que afecta a **SAP Manufacturing Integration and Intelligence**, la cual puede permitir a un actor malicioso ejecutar código y escalar privilegios en el sistema vulnerable.
Falla de seguridad presente en **Java Xstream**	CVE-2021-21345	CVSS v3.1: 9.9	Vulnerabilidad presente en **XStream anterior a la versión 1.4.16**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado, solo manipulando el flujo de entrada.
Falla de seguridad presente en productos de **Dell**	CVE-2021-21513	CVSS v3.1: 9.8	Vulnerabilidad que afecta a **Dell EMC versión 9.5**, la cual puede permitir a un actor malicioso ejecutar código de manera remota en el dispositivo afectado.
Falla de seguridad presente en **Apache OFBiz**	CVE-2021-26295	CVSS v3.1: 9.8	Vulnerabilidad presente en las versiones anteriores a **17.12.06 de Apache OFBiz**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado.
Falla de seguridad presente en productos de **SAP**	CVE-2021-21481	CVSS v3.1: 9.6	Vulnerabilidad presente en varias versiones de **SAP NetWeaver**, la cual puede ocasionar que un atacante ejecute código de manera remota en el dispositivo afectado.

VULNERABILIDADES

MNEMO-CERT presenta las 10 vulnerabilidades más representativas que fueron identificadas en el mes de marzo 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 Microsoft corrigió como parte de las actualizaciones de emergencia "out-of-band", la cual afecta a **Exchange Server** 2013, 2016 y 2019. CVE-2021-26855 es una falla de "falsificación de solicitud del lado del servidor" (SSRF), la cual permite a un actor malicioso ejecutar un código de manera arbitraria en la instancia afectada.

Además, más de 10 grupos maliciosos han aprovechado esta falla, como el grupo "Hafnium" quien ha dirigido sus ataques a organizaciones en Estados Unidos, y actores maliciosos como "Tick", "LuckyMouse", "Calypso", "Websiic", "CactusPete", "Mikroceen APT", entre otros. En adición, se ha identificado que las familias de ransomware "DearCry" y "Black Kingdom" han realizado campañas aprovechando esta falla. **MNEMO-CERT** publicó varios avisos referentes a esta vulnerabilidad los cuales se pueden consultar en las siguientes URL:

- Información referente a CVE-2021-26855
    - https://mailchi.mp/mnemo.com/aviso-de-seguridad-microsoft-publica-actualizaciones-para-corregir-fallas-de-seguridad-presentes-en-exchange-server
    - https://mailchi.mp/mnemo.com/aviso-de-seguridad-recomendaciones-de-seguridad-departamento-de-seguridad-de-estados-unidos-emite-alerta-referente-a-vulnerabilidades-en-exchange
- Campañas que aprovechan CVE-2021-26855
    - https://mailchi.mp/mnemo.com/aviso-de-seguridadnuevos-indicadores-relacionados-con-campaa-que-aprovecha-vulnerabilidades-en-exchange-server
    - https://mailchi.mp/mnemo.com/aviso-de-seguridad-apt-grupos-maliciosos-aprovechan-fallas-de-seguridad-presentes-en-exchange-server
- Grupos de ransomware que utilizan CVE-2021-26855
    - https://mailchi.mp/mnemo.com/aviso-de-seguridadransomware-dearcry-afecta-a-servidores-microsoft-exchange
    - https://mailchi.mp/mnemo.com/aviso-de-seguridadransomware-black-kingdom-afecta-a-servidores-microsoft-exchange

En la siguiente posición está la vulnerabilidad presente en **BIG-IP**, la cual ha sido aprovechada por actores maliciosos. La falla está presente en la interfaz REST de iControl; puede permitir a un atacante no autenticado con acceso a la interfaz ejecutar comandos arbitrarios en el sistema, conduciendo a un compromiso total, o actividad de movimiento lateral e intercepción del tráfico de la aplicación. **MNEMO-CERT** publicó dos avisos referentes a esta falla los cuales se pueden consultar en las siguientes URL:

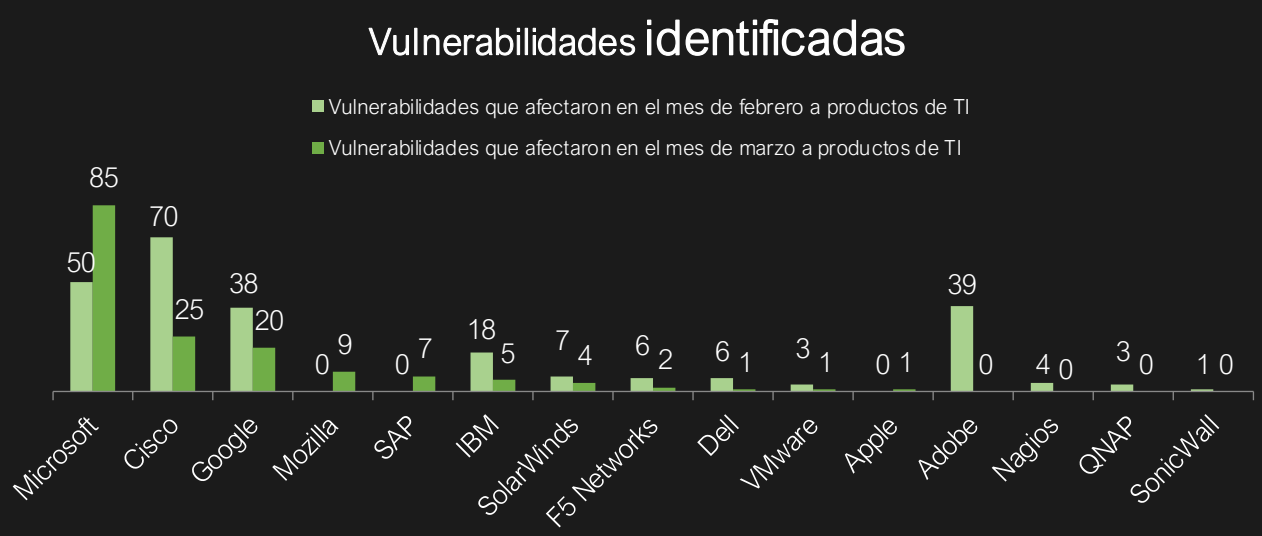
VULNERABILIDADES

- https://mailchi.mp/mnemo.com/aviso-de-seguridad-f5-corrige-vulnerabilidades-presentes-en-dispositivos-big-ip-y-big-iq
- https://mailchi.mp/mnemo.com/aviso-de-seguridadactores-maliciosos-comienzan-a-aprovechar-vulnerabilidad-presente-en-productos-de-f5-networks

La vulnerabilidad presente en **VMware View Planner** es causada por una validación incorrecta de entrada, la cual puede ocasionar que un atacante remoto ejecute código de manera arbitraria en la aplicación Web. En adición, **MNEMO-CERT** ha identificado algunas Pruebas de Concepto referentes a esta vulnerabilidad, las cuales se pueden consultar en las siguientes URL:

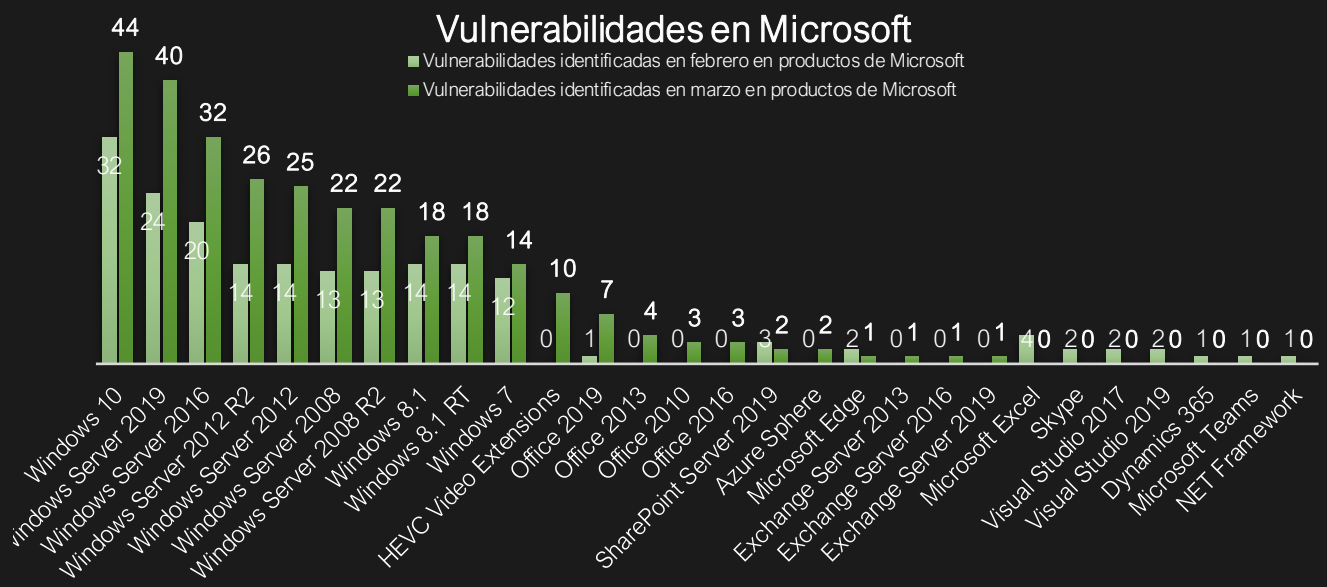
- https://github.com/GreyOrder/CVE-2021-21978
- https://github.com/me1ons/CVE-2021-21978
- https://github.com/skytina/CVE-2021-21978

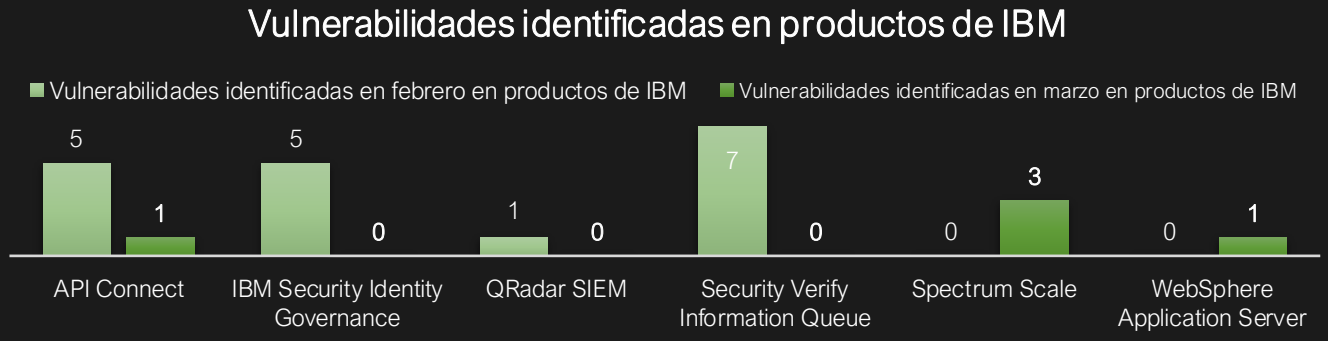
Asimismo, cabe señalar que durante este mes varios fabricantes corrigieron diversos fallos en sus diferentes productos, siendo los más destacados de las compañías "Microsoft", "Cisco" y "Google", a comparación de que el mes pasado, las más sobresalientes fueron "Cisco", "Microsoft" y "Adobe".



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 marzo de 2021 y un comparativo con el mes de febrero del mismo año.

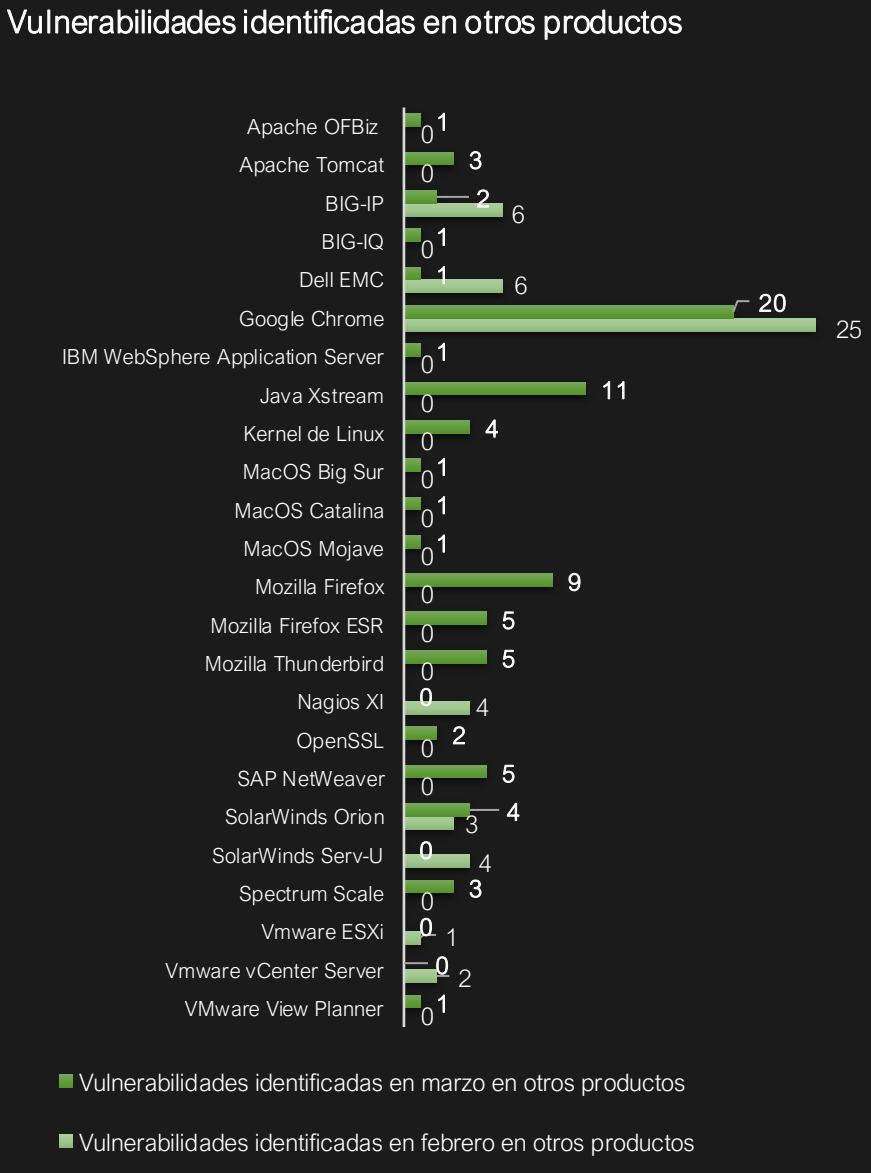
VULNERABILIDADES





MNEMO

VULNERABILIDADES



THREAT INTELLIGENCE

Actividad cibercriminal contra cajeros automáticos

La cantidad de familias de malware dirigido contra dispositivos ATM es reducida, ya que para desarrollar un malware de este tipo es necesario tener conocimientos sobre el comportamiento de estos dispositivos, incluso en ocasiones, puede ser necesario disponer de un ATM propio para realizar pruebas.

Es por eso que no es común encontrarse habitualmente con malware de ATM operando en la naturaleza, llevando un tiempo prolongado realizar actualizaciones de estos malware antes de lanzar una nueva campaña. Por esta razón, cada vez que se detecta una muestra de ATM operando, se genera una gran inquietud entre las entidades de seguridad y el sector financiero.

Durante el mes de marzo de 2021, se ha descubierto la actividad del malware Ploutus, el cual ha sufrido una actualización desde su última versión. Esta nueva variante ha sido llamada Ploutus-I y ha estado afectando, principalmente, a cajeros automáticos de entidades bancarias localizadas en América Latina. Los dispositivos afectados pertenecen al proveedor brasileño Itautec, del que se tiene conocimiento de alianzas con otros fabricantes como OKI y NCR. El equipo de Cyber Threat Intelligence ha llevado a cabo el análisis de dicha muestra.

Ploutus-I se ha aprovechado de los cajeros con vulnerabilidades del middleware ATM XFS y, el impacto que ha tenido sobre éstos, ha sido el vaciado de cajeros automáticos de la entidad bancaria objetivo, inutilización de máquinas ATM y denegando el efectivo a los clientes de la entidad.

Al igual que ocurre con la mayoría de malware contra ATM, la distribución y operación de Ploutus-I requiere de la presencia física en el cajero automático que se pretende vulnerar. En este caso, una mula accede a la unidad de disco duro del cajero automático, soltando en el directorio C:\itautec los archivos necesarios para vulnerarlo.

Este directorio es reconocido como legítimo por los sistemas Antivirus/Antimalware, que lo tienen contemplado en una lista blanca. Los archivos que son solados en el sistema para que el malware se ejecute de manera correcta son los que se encuentran en la siguiente tabla:

Path del archivo	Descripción	Hash MD5
C:\itautec\exe\Itautec.exe	Variante de Ploutus-I	a0dee20dd90b557bf411df318740ddc2
C:\itautec\exe\log.dll	Utilidad para Logging	CAE007EF56306F7A8F07FF6678C15837
C:\itautec\exe\GG.exe	Controla el XFS Middleware	33E849EF4604B89BDD905CEAAC9C4E9E
C:\itautec\exe\XFSGG.dll	Controla el XFS Middleware	EAB939B1F5E310400A7DE60F62622B04
C:\itautec\exe\msxfs.dll	XFS APIs	3BDA1500AF49F91045D4BB93272F7352

El orden de ejecución de estos archivos comienza con la ejecución del binario **Itautec.exe**, el cual simula ser un "**Agente de protección de Itautec**", probablemente para proporcionar una capa más de evasión, y se encuentra escrito en **.NET**, lo que dificulta aún más la protección basada en firmas.

Property	Value
FileDescription	Itautec Protection Agent
FileVersion	0.0.0.1
InternalName	Diebold.exe
LegalCopyright	Copyright © 2017
OriginalFilename	Diebold.exe
ProductName	Itautec Protection Agent
ProductVersion	0.0.0.1

*Imagen 1. Metadatos de **Itautec.exe**.*

Este archivo se encarga de generar persistencia en el sistema. Para ello agrega una clave de registro dentro de la ruta **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon**, cuyo valor de clave es el directorio donde se encuentra el propio ejecutable de Ploutus-I, con nombre Itautec.exe.

Cuando el malware se encuentra en ejecución llama a la función principal **Launcher.Keyboard::RealStart()**, ya que es la encargada de ejecutar el resto de acciones. Este malware tiene una función de **KeyLogger**, que a diferencia de otros malware que utilizan esta función para capturar credenciales, este lo utiliza para capturar las pulsaciones introducidas por el cibercriminal a través del teclado enchufado al cajero automático.

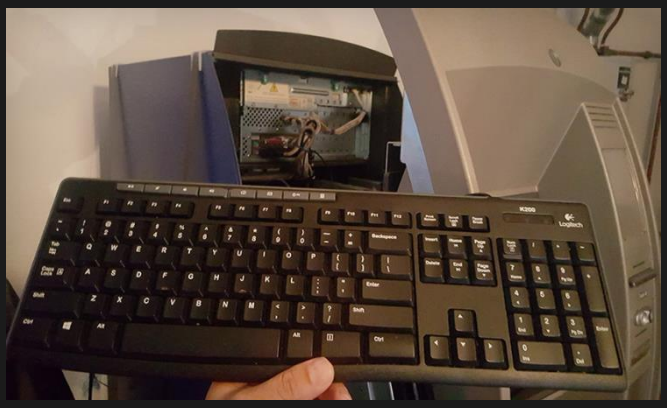


Imagen 2. Teclado enchufado al cajero automático en una campaña antigua de Ploutus. Fuente: Fireye.

El flujo natural del evento tras activarse el KeyLogger, es la introducción de la instrucción **F8F1F2F3F4**, la cual llama a la función **Launch.LaunchClient()**. Esta función es la encargada de llamar al archivo GG.exe, que se trata de un controlador del XFS Middleware del cajero automático.

Este binario se hace pasar por una herramienta legítima de Itautec, utilizada para probar la funcionalidad del dispensador. En este caso, observando los metadatos del archivo, se ha observado que este archivo malicioso simula ser un producto llamado **JIG NMD**, el cual se trata de una herramienta utilizada para probar la funcionalidad de los dispensadores de los cajeros automáticos del fabricante.

El objetivo que tiene este archivo es abrir una sesión en el dispensador utilizando el nombre **NDC_CASH_DISPENSER**. Cuando esta sesión es abierta, envía el código 310, que sirve para llamar a la acción WFS_INF_CDM_CONF, la cual sirve para obtener información del periférico. Tras esto, se asegura de que el dispensador tenga efectivo alojado y el Cassette en el que se encuentra, utilizando la función WFS_CMD_CDM_READ_DATA.

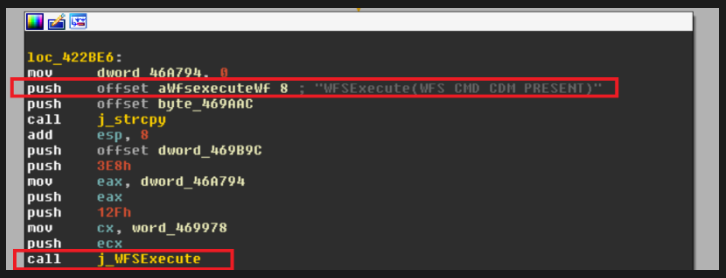


Imagen 3. Función de dispensación de efectivo del dispensador.

Para la extracción de efectivo, este malware limita el número de veces al día que se puede realizar la acción. Si este número no se ha superado, se utiliza la instrucción **WFS_CMD_CDM_PRESENT** para retirar el efectivo del cajero.

Los cibercriminales tienen un perfecto conocimiento del sistema que están atacando, además de sus capacidades físicas como el número total de billetes que pueden pasar por la escotilla en una sola transacción. Este número también es configurado dentro del propio malware y varía dependiendo del cajero.

```
Activacion Correcta Codigo:
WFSExecute Result[-351] Data Leng [1] Cassete 1: 0 Cassete 2: 0 Cassete 3: 0 Cassete 4: 70 Cassete 5: 0
WFS_CMD_CDM_PRESENT Result[0]
WFSExecute Result[-351] Data Leng [1] Cassete 1: 0 Cassete 2: 0 Cassete 3: 0 Cassete 4: 70 Cassete 5: 0
WFS_CMD_CDM_PRESENT Result[0]
```

Imagen 4. Archivo de Logs que muestra el Cassete y número de billetes dispensados. Fuente: Metabase Q.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
XFS_SUPP.dll	2	00051F84	00000000	00000000	00051FD0	0004C3B8
XFSGG.dll	7	00051F20	00000000	00000000	0005203C	0004C354
log.dll	6	00051F90	00000000	00000000	000520F2	0004C3C4
Innova.dll	5	00051BEC	00000000	00000000	00052140	0004C020
MFC42.DLL	140	00051C3C	00000000	00000000	0005214C	0004C070
MSVCRT.dll	43	00051E70	00000000	00000000	00052260	0004C2A4
KERNEL32.dll	13	00051C04	00000000	00000000	0005244C	0004C038
USER32.dll	16	00051F40	00000000	00000000	00052540	0004C374
GDI32.dll	2	00051BE0	00000000	00000000	0005256E	0004C014
ADVAPI32.dll	4	00051BCC	00000000	00000000	000525B8	0004C000
XFSGG.dll	1	00097102	00000000	00000000	000970F0	000970FA

Imagen 5.Tabla de importación de GG.exe.

Analizando su tabla de importación, se verifica también que este archivo contiene dependencias con otras librerías soltadas junto al mismo y que no se han comentado hasta el momento. Estas librerías son **XFSGG.dll** y **log.dll**, cuyos hashes se encuentra al principio de este apartado.

Adicional a esto, al analizar la tabla de Strings del archivo, se pueden ver numerosas cadenas de texto escritas en portugués, lo que sugiere que la procedencia de los cibercriminales que han desarrollado el archivo es altamente probable que sea en Brasil.

```
dd offset aNotaEnviadaARe ; "Nota enviada a rej. simples no empilhad"...
dd offset aFalhaDeComu_13 ; "Falha de comunicacao com K7 de rejeicao"...
dd offset aNaoImplement_0 ; "Nao implementado                       "...
dd offset aSemK7          ; "Sem K7                                 "...
dd offset aIntervencaoNec ; "Intervencao necessaria no K7           "...
dd offset aNivelBaixoNoK7 ; "Nivel baixo no K7                      "...
dd offset aK7VazioK7Baixo ; "K7 vazio (K7 baixo nao detectado)      "...
dd offset aK7Vazio        ; "K7 vazio                               "...
dd offset aK7VazioAliment ; "K7 vazio-Alimentacao continua em outro "...
dd offset aK7MarcadoComoV ; "K7 marcado como vazio                  "...
dd offset aOFeederNaoCons ; "O feeder nao consegue alimentar as nota"...
dd offset aAliment_Interr ; "Aliment. interrompida-Nota entre feeder"...
dd offset aFalhaDeSensorN ; "Falha de sensor ( NF ou NFC )          "...
dd offset aAliment_Inte_0 ; "Aliment. interrompida-Rejeicao simples "...
dd offset aRej_PacoteAbor ; "Rej. pacote,abortado nova alimentacao n"...
```

Imagen 6. Strings en portugués alojados en GG.exe.

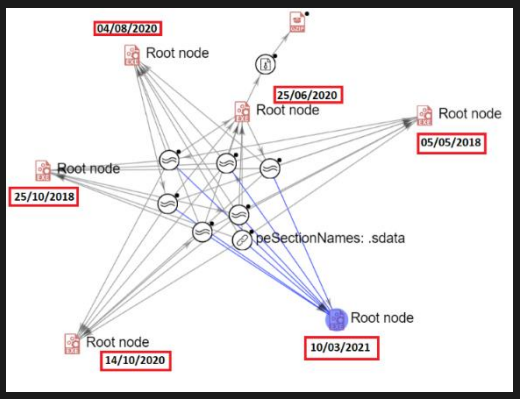
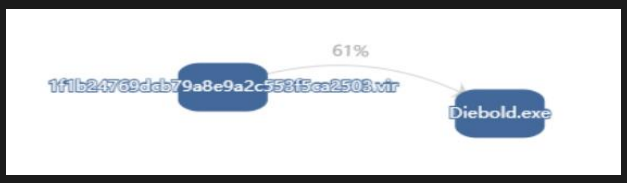


Imagen 7. Muestras similares y fecha de su última detección.

La muestra utilizada en esta última campaña que ha sido analizada por el equipo de Cyber Threat Intelligence, ha mostrado correlación con 6 muestras, las cuales han sido vistas por última vez entre un rango de fecha que va desde mayo de 2018 hasta Marzo de 2021.

La fecha de creación que figura sobre todos estos archivos varía entre 2017 y 2018, compartiendo en todos los casos la información que se refleja en sus metadatos, la cual aparece en la **Imagen 1** de este apartado.

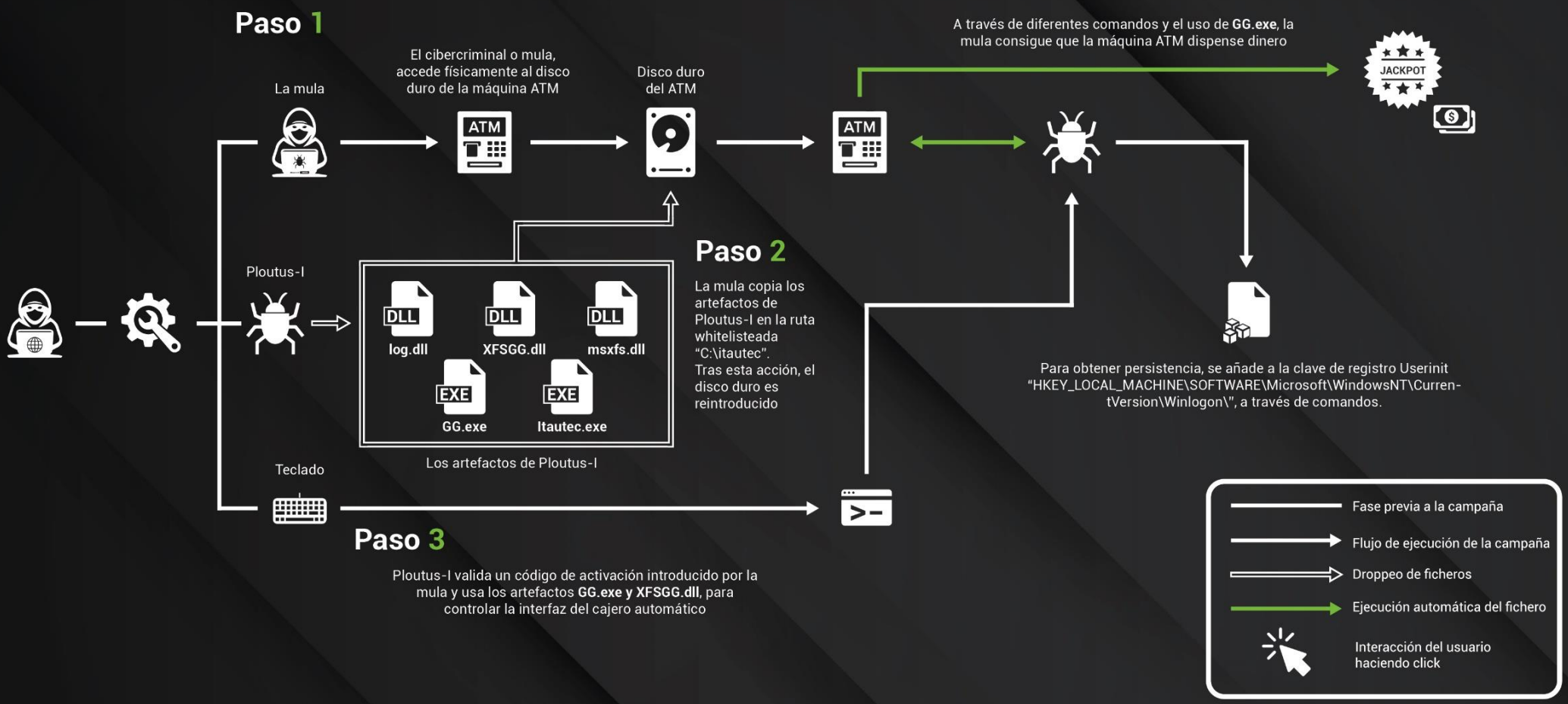
En cuanto a similitud de código se refiere, de las muestras representadas en el gráfico solo comparten parte del código dos de ellas, como se puede ver en la siguiente imagen:



Esto es debido al tipo de codificación que se utiliza para cada muestra con el objetivo de evadir sistemas de detección basados en firmas.

Como se ha podido comprobar, el desarrollo de un nuevo malware contra dispositivos ATM es un trabajo complejo, por lo que en numerosas ocasionas deriva de la actualización de un malware ya existente, al que se le añaden funcionalidades en base a las necesidades de los cibercriminales por saltarse nuevas medidas de seguridad implementadas en los cajeros automáticos.

Conocer el mayor número posible de este tipo de malware permite a los investigadores anteponerse al desarrollo de una actualización de los mismos, generando medidas preventivas que ayuden a detectar con antelación una posible infección.



Recon/Weapon

- Los cibercriminales realizan una búsqueda de cajeros automáticos del proveedor brasileño, Itautec, para comprometerlos
- Por un lado, estos atacantes obtienen material que les pueda servir para acceder al disco duro del cajero automático, así como un teclado.
- Por otro lado, desarrollan la variante Ploutus-I para infectar cajeros automáticos Itautec.

Delivery

- En esta fase, el ciberdelincuente o mula, abre una parte blanda del cajero automático para extraer el disco duro.

Exploitation / Installation

- Todos los artefactos empleados en la infección de Ploutus-I son copiados en una carpeta que se encuentra en una whitelist.
- Ploutus-I valida el código de activación, introducido a través de un teclado.
- Tras reintroducir el disco duro infectado en la máquina ATM comprometida, la mula activa el malware a través de un teclado. El binario GG.exe y la librería XFSGG.dll son usadas para interactuar con el software Itautec/OKI XFS Middleware, para poder dispensar el dinero.
- La persistencia es obtenida al añadir la ruta del malware a la clave de registro Userinit "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\".

C2 / Actions on objetives

- La fase C2 no aplica, dado que este malware no se comunica con ninguna infraestructura C2.
- La mula realiza una combinación de comandos para que la máquina ATM comience a dispensar dinero. Esta técnica se conoce como jackpotting.

EN NUESTRA REGIÓN

RYUK sobre el Servicio Público de Empleo Estatal Español SEPE

El pasado 9 de marzo el Servicio Público de Empleo Estatal (SEPE) fue víctima de un ciberataque que dejó sus sistemas y portales inaccesibles. Durante ese día, la Dirección General del SEPE manifestó que se trabajaba para restaurar los servicios, aunque inicialmente los resultados no fueron positivos. El impacto del ataque generó días de indisponibilidad y un funcionamiento parcial de sus servicios online.

Las primeras evidencias del ataque permitieron identificar que habían sido víctimas de una de las variantes del ransomware Ryuk, el cual fue observado por primera vez en agosto de 2018. Esta es una variante del ransomware Hermes 2.1, vendido en el foro exploit.in desde febrero de 2017 por el grupo ciberdelincuente CryptoTech.

Esta familia de ransomware se ha estado viendo involucrada en despliegues masivos en redes internas de empresas, lo que supone una importante amenaza.

Ryuk habitualmente se descarga y ejecuta desde un equipo, tras su infección mediante un troyano. Se estima que el 83% de los ataques de Ryuk son realizados por el grupo de cibercriminales denominado UNC1878, del cual se sospecha que es de origen ruso. Aunque sus principales objetivos se centran alrededor del sistema sanitario de Estados Unidos, existen víctimas a nivel global.

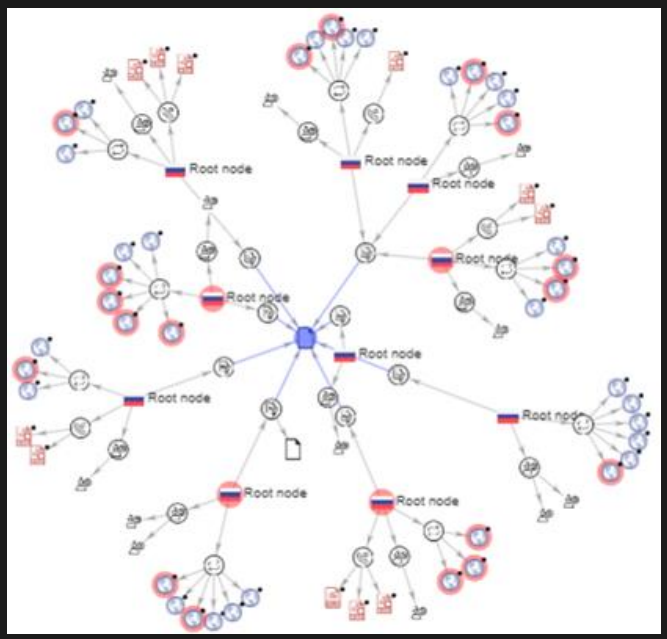


Imagen 8. Árbol de Indicadores de VirusTotal Ryuk

Durante un estudio de incidentes en el 2020, se detectó que TrickBot era el principal responsable de la distribución de Ryuk. TrickBot se puede distribuir en sentido ascendente a través del malware como servicio Emotet. Por lo tanto, las cadenas de infección Emotet-TrickBot-Ryuk y TrickBot-Ryuk se han encontrado con frecuencia y persisten al menos hasta septiembre de 2020.

EN NUESTRA REGIÓN

Sin embargo, desde mediados de septiembre de 2020, la cadena de infección BazarLoader-Ryuk parece reemplazar a las que involucran a TrickBot; BazarLoader se distribuye generalmente mediante campañas de phishing de forma semejante a la utilizada anteriormente por Emotet y TRickbot.

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2021-02-05 08:22	e4c2da8ed10ce0758e3fb...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	b4305df7cc0c86b820c87...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	a0fe497c852a15e9753a1...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	27888502631594404939...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	64300298ab9c2ae8a492...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	71050bf4044c88e14f826f...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	607ba56767e941ca233e...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	0263be9e306789eb88f8c...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	08c11bf41602c9375004d...	exe	BazaLoader	BazaLoader BazarLoader signed	@JAMESWT_MHT	
2021-02-05 08:22	2fba2768e2d97e2521e68...	exe	BazaLoader	BazaLoader BazarLoader	@JAMESWT_MHT	
2021-02-03 16:54	52bbe09c7150ea66269c...	exe	BazaLoader	BazaLoader exe signed	@James_inthe_box	
2021-01-29 18:36	66af4bca3df1ee98ec1fdb...	exe		exe	@James_inthe_box	
2021-01-29 15:13	de307ecbfecca217a680c...	exe	BazaLoader	BazaLoader Foreground signed	@JAMESWT_MHT	
2021-01-29 15:13	bc6fa495ed90d846d087...	exe	BazaLoader	BazaLoader Foreground signed	@JAMESWT_MHT	
2021-01-29 15:13	889e728a55b58b3a124d...	exe	BazaLoader	BazaLoader Foreground signed	@JAMESWT_MHT	
2021-01-29 15:13	3c91963b604f32bb0fb91...	exe	BazaLoader	BazaLoader Foreground signed	@JAMESWT_MHT	

Imagen 9. BazaLoader (Certum Trusted Network CA)

Para el envío de los emails maliciosos, los atacantes utilizan su propia infraestructura o comprometen servidores de correo. Estos emails contienen enlaces a ficheros ejecutables, firmados con certificados revocados. Dichos ficheros son descargados de plataformas legítimas como Google Drive. Estas características permiten al malware su ejecución en el sistema sin ser detectado por los sistemas de seguridad.

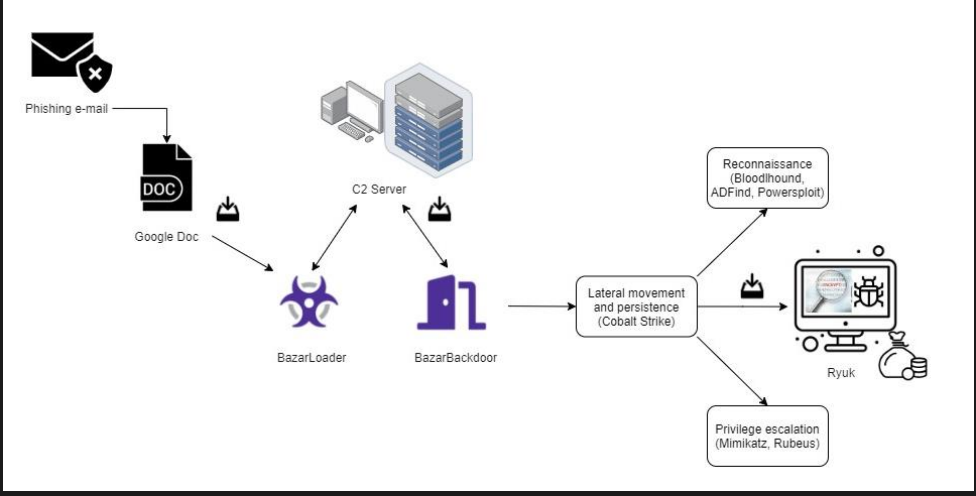


Imagen 10. Secuencia simplificada de la cadena de infección Bazar-Ryuk

El programa se copia a sí mismo con el sufijo "REP.exe" o "LAN.exe" entre equipos, estos procesos serán los responsables de arrancar máquinas apagadas mediante el protocolo Wake-on-Lan y de replicarse a través de recursos compartidos y tareas programadas. Para ello, realiza un escaneo de red enviando un ping para identificar posibles destinos donde replicarse.

EN NUESTRA REGIÓN

Tras esto, lista las IPs contenidas en la caché ARP del equipo y les envía un paquete Wake-on-LAN para encenderlos. Por cada máquina identificada comenzará a realizar peticiones SMB intentando acceder de forma iterativa a las unidades $ del equipo; si se comprueba que hay acceso a una máquina, la instancia de Ryuk que se está ejecutando con el argumento "REP" intentará replicarse en la misma. Para ello, realizará una copia de Ryuk, que remitirá vía SMB, en el directorio "c:\Users\Public\"de dicho equipo.

Para realizar la propagación utiliza una cuenta privilegiada de dominio.

Si se bloquea la cuenta de dominio utilizada por Ryuk, o se cambia contraseña, la propagación continuará hasta que el ticket de kerberos asociado a la autenticación expire.

De forma paralela, el binario principal importará la clave RSA que participará en el proceso de cifrado de los ficheros, identificará las unidades locales montadas, y por cada una de ellas, cambiará sus permisos mediante la herramienta de Windows icacls para otorgar total acceso a los mismos.

Por último, Ryuk elimina las "Volume Shadow Copies", para evitar la recuperación de los datos. El objetivo final de Ryuk es realizar el cifrado de los ficheros locales y remotos, pidiendo un rescate para su descifrado. Las instrucciones del rescate se almacenan en el fichero ryukreadme.html, que probablemente contenga un enlace a una página de TOR (.onion) para la negociación.

En la siguiente imagen, se pueden observar, según la matriz de MITRE, las técnicas utilizadas por Ryuk, resaltadas en azul. Podemos destacar el uso de API Nativas como, por ejemplo, el uso de la API ZwQueryInformationProcess junto con diversos flags ProcessDebugPort, ProcessDebugFlags, ProcessDebugObjectHandle) que permitirán determinar si hay un debugger presente para implementar técnicas anti-debug.

También se destacan la recopilación de información del sistema, modificación de llaves de registro, la evasión de los sistemas de defensa, el descubrimiento de directorios y ficheros, la detención de servicios y por último el cifrado de datos.

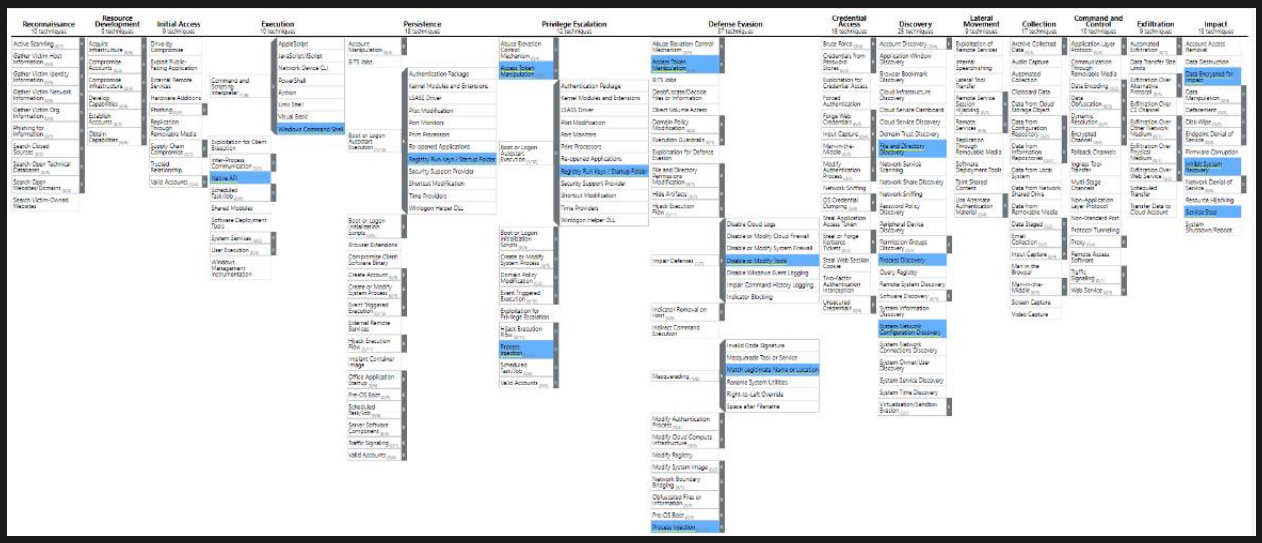


Imagen 11. Tácticas de ataque según la matriz de MITRE usadas por Ryuk

EN NUESTRA REGIÓN

Con lo que respecta a SEPE, según declaraciones de su director, no se solicitó un rescate por parte de los atacantes, pero aceptó que el impacto del ataque paralizó el servicio en 710 oficinas presenciales y 52 telemáticas, lo que ha llevado a la entidad a replantear las medidas de seguridad y prevención que tenían instauradas antes de este evento.

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

- Implementar los indicadores de compromiso a los sistemas antimalware corporativos.
- 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 indicados a continuación en las reglas de los firewalls.
- 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'.
- Añadir la regla Yara creada por el CCN-CERT publicada en su Informe en el siguiente enlace: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5768-ccn-cert-id-03-21-ryuk-ransomware/file.html

La técnica Pass-The-Hash

En diversos ataques avanzados persistentes (Advanced Persistent Threat) que se han analizado en los últimos años, se han detectado algunos patrones de técnicas y herramientas utilizadas. Uno de estos patrones recurrentes, que se observan posterior a que el atacante haya logrado ingresar al primer sistema objetivo, es la técnica de **Pass-the-Hash (PtH).**

Este ataque tiene el objetivo de obtener credenciales de acceso para poder realizar movimientos laterales y comprometer otros equipos o componentes del sistema; tiene como meta principal acceder al controlador de dominio y, de esta manera, asegurar el control de la mayoría de los **sistemas de información en entornos Microsoft Windows.**

Para poder aprovechar esta técnica **Pass-the-Hash (PtH)** se usa el protocolo NTLM, que Windows utiliza para que después de la autenticación inicial, el usuario no tenga que introducir su contraseña una y otra vez, ya que Windows recopila la contraseña ingresada por el usuario, de la cual se obtiene un hash y **se almacena en el archivo SAM** para una futura autenticación.

Este hash es conocido como **hash NTLM**, el cual se obtiene a partir de la contraseña del usuario, donde cada uno de los caracteres, se convierte a formato Unicode Little Endian. Después se crea una cadena con todos los caracteres y se toma un hash MD4 lo que nos da como resultado un **código de 128 bits**. El actor malicioso obtiene este hash NTLM para posteriormente inyectarlo en el proceso lsass.exe para que se logre la autenticación.

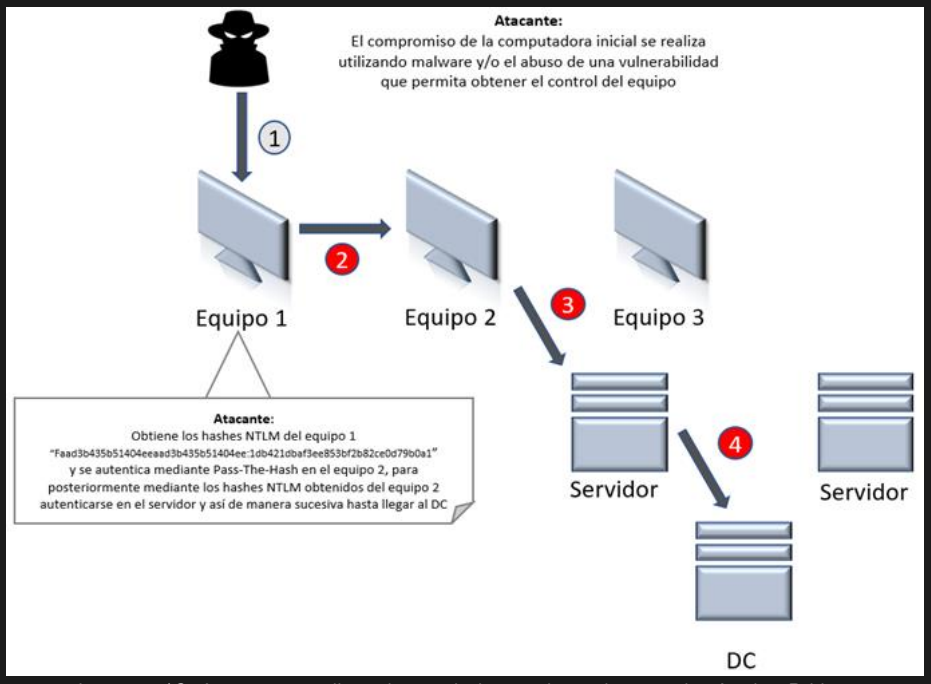


Imagen 12. Atacante realizando movimientos laterales con la técnica PtH

El hash NTLM es una mejora del hash LM, que era utilizado anteriormente en el protocolo de contraseñas de Microsoft. Esta mejora se llevó a cabo debido a que **el hash LM tiene una serie de características que permitían a los atacantes utilizar fuerza bruta para obtener la contraseña,** sin necesidad de emplear demasiado esfuerzo o tiempo.

El hash LM **convertía todo a mayúsculas,** permitiendo a los programas de fuerza bruta atacar directamente utilizando mayúsculas y reduciendo así el tiempo de cálculo. Además, el hecho de **dividir la contraseña en dos** permite actuar en paralelo sobre ambos segmentos.

Por lo mencionado anteriormente, cuando **un atacante accede con éxito a un sistema o equipo, realiza un volcado de credenciales ya sea en texto plano o en hash** para, posteriormente, utilizarlas e intentar acceder a otra parte del sistema que esté interconectado, ya que es común que en un entorno empresarial se reutilicen contraseñas de un usuario para acceder a diversos equipos con privilegios elevados.

Esto también es **aplicable para cuentas de usuario administrador en entornos de Directorio Activo**. De esta forma se realizan movimientos laterales para llegar hasta el controlador de dominio, desde el cual se puede acceder a todos los recursos e información, así como tener el control de las políticas aplicadas a todos los sistemas.

Para la obtención de hashes NTLM existen diversas herramientas que acceden al archivo SAM en búsqueda de las credenciales, por ejemplo, **mimikatz, lazagne, Rubeus, crackmapexec,** por mencionar algunas, incluso el uso de **frameworks** de ataque como **Cobalt Strike, Empire, Kodiac, PowerSploit o metasploit**.

Una vez obtenidos los hashes, se utilizan diversas herramientas que permiten la autenticación mediante el protocolo NTLM con los equipos, proporcionando únicamente, el hash NTLM y el nombre de usuario correspondiente. Por otra parte, también se pueden acceder a los servicios que se encuentren activos en caso de que utilicen Single-Sign-On (SSO) como por ejemplo cuando se utiliza Kerberos.

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c81c8295ec4bfa3c9b90dcd6c64727e2:::
Frank Castle:1001:aad3b435b51404eeaad3b435b51404ee:1db421dbaf3ee853bf2b82ce0d79b0a1:::
```

Imagen 13. Ejemplo de hashes NTLM de un equipo

Microsoft por su parte ha intentado solucionar estos tipos de ataques de PtH a través de diversos cambios:

- Reemplazo del cifrado RC4 a AES
- Implementación de Credential Guard
- Políticas enfocadas a Logon Cache
- JEA – Just Enough Administration
- APP Locker
- EMET
- Filtrado de ejecución de medios de administración en sistemas operativos Microsoft Windows (PowerShell, cmd, WMIC, reg32dll, etc.)
- Listas blancas/negras de aplicaciones

Sin embargo, todos estos cambios solo hicieron que el ataque fuera más complicado de llevar a cabo, pero no resolvió el problema.

Una forma de detectar y generar alertas de ataques PtH es mediante el registro de eventos de Windows, más específicamente los **eventos con ID 4624 ("Una cuenta inicio sesión correctamente")**, analizando los detalles de estos eventos **se deben considerar las siguientes características para detectar un posible ataque PtH** en el equipo:

- **Logon Type: 3** (Un usuario o equipo inició sesión en este equipo desde la red).
- **Logon Process:** NtLmSsP
- **Security ID:** Null SID (Esta característica es opcional y no obligatoria, sin embargo, hasta el momento no hay evidencias de ataques PtH que no usen Null SID).
- **Key Length: 0** (Esta característica es una de las más importantes a revisar para detectar un Pass the Hash en la red).

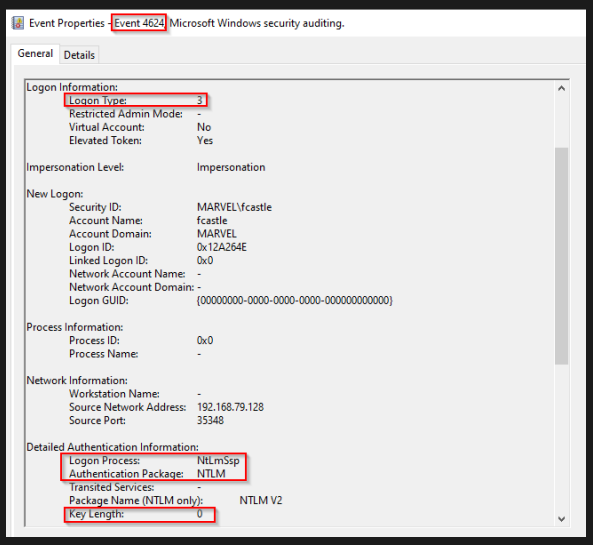


Imagen 15. Registro de evento 4624 de una autenticación por PtH

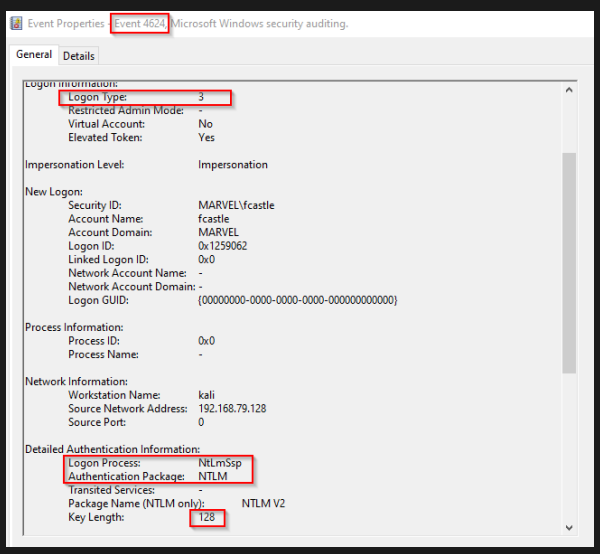


Imagen 14. Registro de evento 4624 de una autenticación legitima (RDP)

Un dato adicional que el registro de **evento 4624 contiene es la dirección IP de origen para la autenticación**, por lo cual se deben validar cuales son los inicios de conexiones válidas y de esta forma se pueda identificar rápidamente **el origen del Pass the Hash dentro de la red**.

Además, es importante detallar que de manera adicional para distinguir un inicio de sesión legítimo de una autenticación utilizando PtH, se deben registrar eventos de sesión interactivos previos a la conexión, esto permitirá reducir los falsos positivos.

Algunos eventos que indican inicios de sesión interactivos son los siguiente:

- **4768: Se solicitó un ticket de autenticación de Kerberos (TGT).**
- **4769: Se solicitó un ticket de servicio Kerberos (TGS).**
- **4648: Se intentó un inicio de sesión utilizando credenciales explícitas.**

Es necesario resaltar que, en la actualidad, diversas empresas hacen grandes esfuerzos en ciberseguridad enfocados al área de monitoreo en búsqueda de posibles amenazas, sin embargo, muchas veces es necesario la involucración de diversas áreas como sistemas, infraestructura, etc. en conjunto con el área de monitoreo para poder detectar **a tiempo** estas amenazas.

El objetivo será emitir las alertas correspondientes logrando que se disminuya el riesgo e impacto que se pueda llegar a tener ante un posible ataque, ya que mediante el trabajo colectivo se conoce el funcionamiento y actividad interna de la empresa lo que permite detectar con mayor facilidad actividad que sea anormal o sospechosa.


MNEMO