



COMUNICADO PUBLICO

Cartagena, 14 de noviembre de 2022

La alcaldía de Cartagena se permite manifestar que a través de la Oficina Asesora de Informática (OAI), se confirmó un ataque cibernético a nuestra infraestructura tecnológica con un malware de tipo Ransomware que afectó uno de los esquemas de servidores de aplicaciones misionales.

Es importante señalar que los equipos afectados ya están siendo intervenidos para su restauración; adicionalmente informamos que serán suspendidos algunos sistemas de información de manera preventiva, medida que se mantendrá hasta nueva orden, lo anterior, con la finalidad de hacer una verificación interna exhaustiva del estado y sanitización efectiva de la infraestructura.

No obstante lo anterior, la alcaldía ha tomado medidas para la continuidad de sus labores y no afectar la prestación de los servicios al público, de esta forma, las solicitudes de la ciudadanía se podrán seguir realizando de manera presencial en las instalaciones de la alcaldía, así mismo, se recibirán las PQRS a través del buzón notificacionesvuac@cartagena.gov.co.

La OAI continuará su labor hasta eliminar definitivamente la amenaza, habilitando cada aplicativo validado, así como el uso de todos servicios para normalizar la atención a través de nuestra sede electrónica, de igual forma, se ha tomado contacto con las autoridades y se cuenta con el apoyo del Equipo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT para la resolución del incidente.

Se reitera al público en general, la importancia de no ingresar a sitios web sospechosos, no abrir archivos dudosos y tener cuidado con algunos correos que engañan para acceder a links que roban los datos personales o que llevan a descargar archivos que vienen infectados.

Atentamente,

Alcaldía Distrital de Cartagena



COMUNICACIÓN INTERNA:

Estimados Colaboradores, nos permitimos comunicar que la Oficina Asesora de Informática (OAI), confirmó un ataque cibernético a nuestra infraestructura tecnológica con un malware de tipo Ransomware que afectó uno de los esquemas de servidores de aplicaciones |misionales.

No obstante lo anterior, se puede hacer uso del correo electrónico institucional desde las instalaciones de la alcaldía, sus casas y dispositivos móviles, recomendando no abrir archivos y dar clic en enlaces que sean sospechosos para evitar nuevos incidentes

Las solicitudes de la ciudadanía se podrán seguir realizando mediante el correo notificacionesvuac@cartagena.gov.co, cada dependencia debe activar su plan de contingencia establecido para la continuidad de sus labores y no afectar la continuidad de los servicios prestados a la ciudadanía.

Se aclara, que este agente maligno ingresó por uno de los equipos utilizado para el trabajo diario. Por eso, se reitera que se debe hacer un uso adecuado de las herramientas dispuestas por el Distrito y no ingresar a sitios web sospechosos, no abrir archivos dudosos y tener cuidado con algunos emails que vienen cargados con código malicioso que engañan para acceder a links que roban los datos personales o que llevan a descargar archivos que vienen infectados.

La OAI continuará su labor hasta eliminar definitivamente la amenaza y habilitando cada aplicativo validado, así como el uso de todos servicios.

Atentamente,

Alcaldía Distrital de Cartagena

INCIDENTE DE SEGURIDAD

SERVIDOR SQL.41

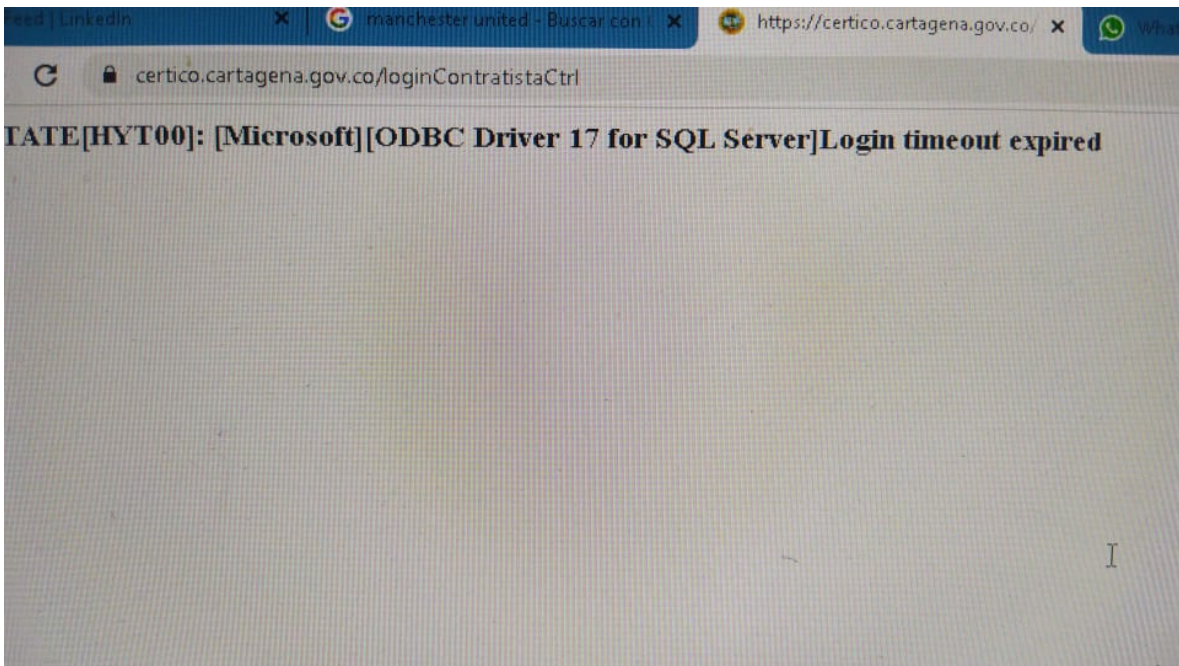
Tipo de incidente: Ataque de Malware tipo Ransomware Mallox

Fecha de inicio: 12 de noviembre del 2022.

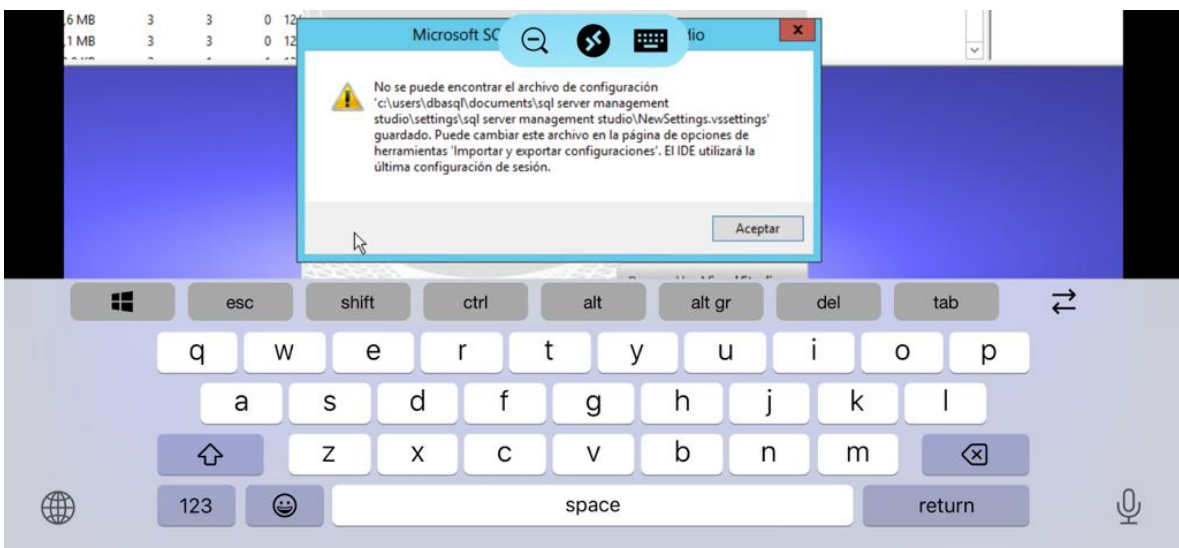
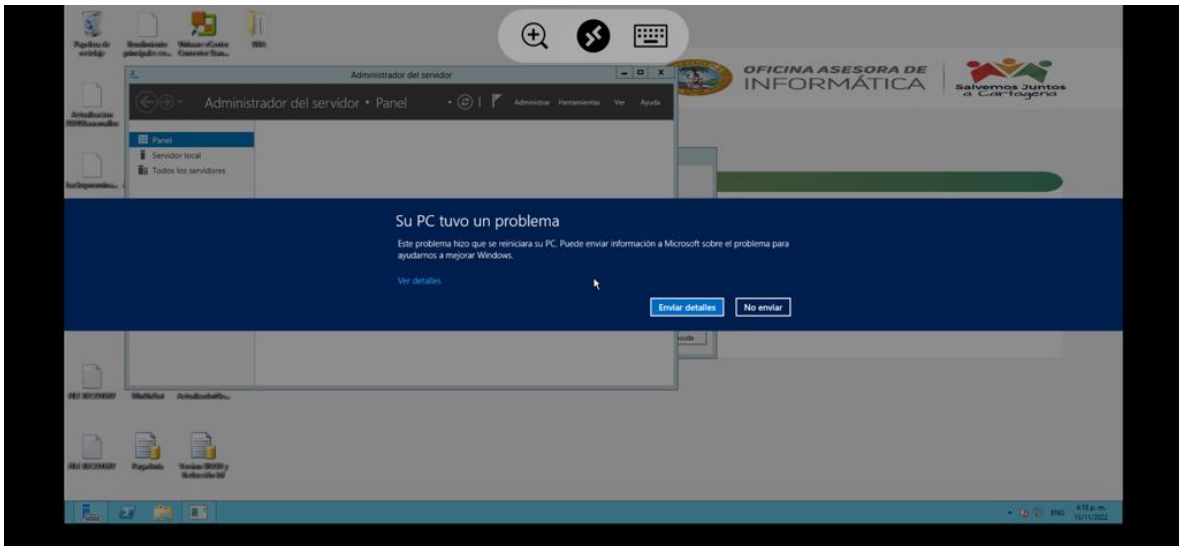
Hecho primero: El día 12 de noviembre alrededor de las 4:19 pm, se informa en el grupo de WhatsApp del equipo técnico AOI que no podía cargar el aplicativo SIGOB, Certico, mi cuenta, los cuales responde al ping pero no deja cargar la aplicación.

Hecho segundo: A las 6:12 pm se informa por el mismo medio que se enviaron las contraseñas reset al DBA, quien a la vez informa que a nivel de DB las BD de Sigob están bien.

Hecho tercero: El ingeniero Sysadmin siendo las 11:46 am del día 13 de noviembre, reporta caída de con Certico.



Hecho cuarto: siendo las 4:13 pm el DBA pregunta " Corrieron algún restore sobre la máquina ***.***.2**.41" y que está generando errores como:



Hecho Quinto: En el grupo se notifica por medio de mensaje que Tigo reporta que están en revisión del equipo TVM-PSQL-DTYCCI (servidor 40), dado que presenta ataque de ransomware, la dejan fuera de línea para las verificaciones respectivas; se solicita hacer la validación de las maquinas que están en contacto con el servidor en mención, para detectar la afectación que se haya con otros equipos.

4:53 19%



En Tigo Business sabemos que un acompañamiento constante es clave para brindarle a su empresa soluciones fundamentales, responder a sus necesidades y entregarle los mejores resultados.

Nos encontramos actualmente en proceso de revisión sobre el servidor TVM-PSQL-DTYCCI, este presenta evidencia de ataque del tipo Ransomware, actualmente esta máquina se encuentra fuera de línea por las revisiones que estamos ejecutando, por favor ejecutar las pruebas y revisiones que considere pertinente sobre su plataforma que tiene contacto con esta máquina, desde la cual pudo venir la infección o a la cual pudo extenderse. Estaremos brindando avances lo antes posible.



4:56 18%



Así mismo se recibió notificaciones de lo siguiente relacionado con seguridad.

Servidor: TVM-PSQL-DTYCCI

Apex Central (10.159.192.150) notification: Virus found action result.

The second virus scan action was successfully taken for the virus detected on \\CYDVM-PAPC01\Local Folder\OfficeScan\CYDVM-PAV03_OSCE\Clientes b2b\TVM-PSQL-DTYCCI.

Virus: Ransom.Win32.RANMSGHP.SMT.note

Action result: File deleted

Infected file: FILE RECOVERY.txt File path: D:\BK\ Scan engine: 21.600.1005 Virus pattern: 17.929.00 Event date/time: 11/12/2022 15:41:01

Apex Central (10.159.192.150) notification: Virus found action result.

The second virus scan action was successfully taken for the virus detected on \\CYDVM-PAPC01\Local Folder\OfficeScan\CYDVM-PAV03_OSCE\Clientes b2b\TVM-PSQL-DTYCCI.

Virus: Ransom.Win32.RANMSGHP.SMT.note

Action result: File deleted

Infected file: FILE RECOVERY.txt File path: H:\PRUEBAS\BACKUPS\db_a18848_accesscontrol_6_29_2022\

Scan engine: 21.600.1005

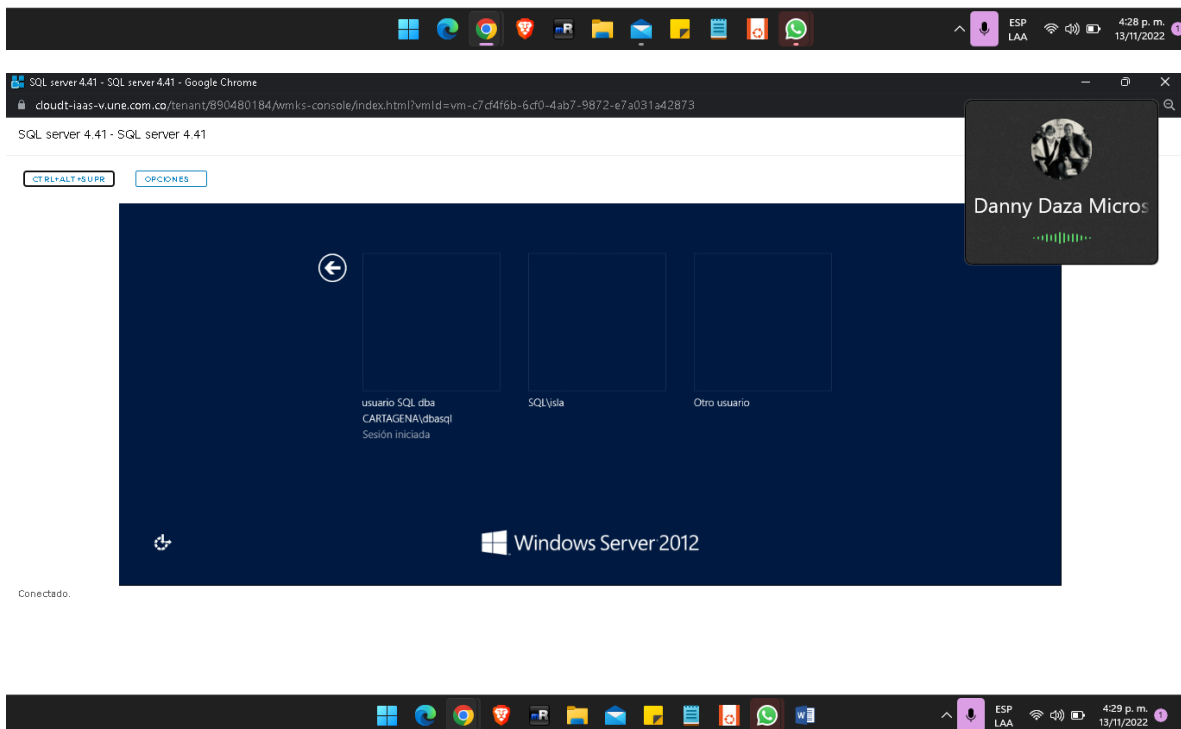
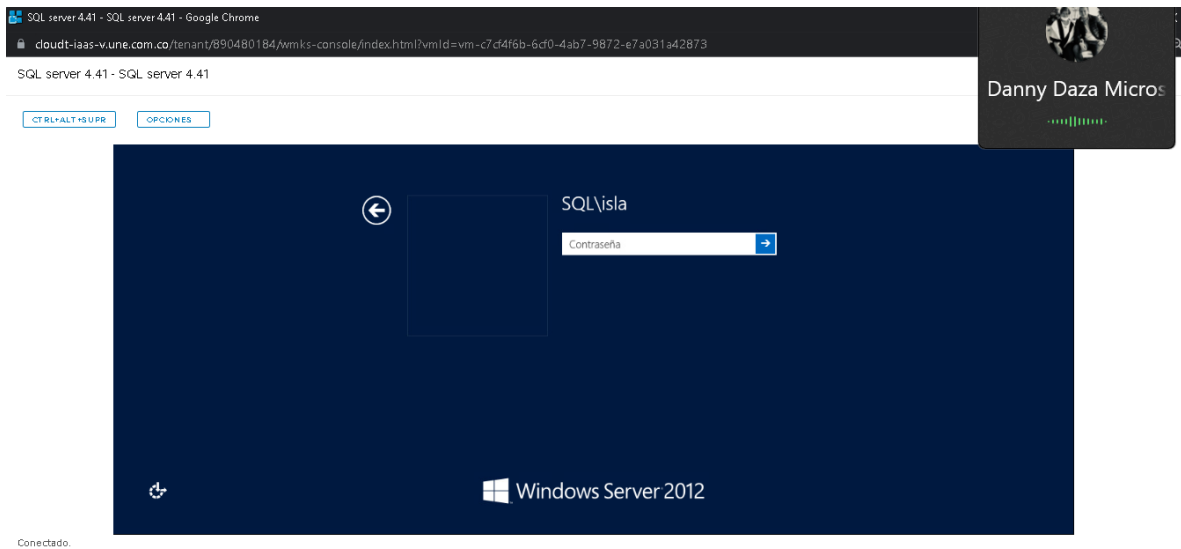
Virus pattern: 17.929.00

Event date/time: 11/12/2022 15:41:00



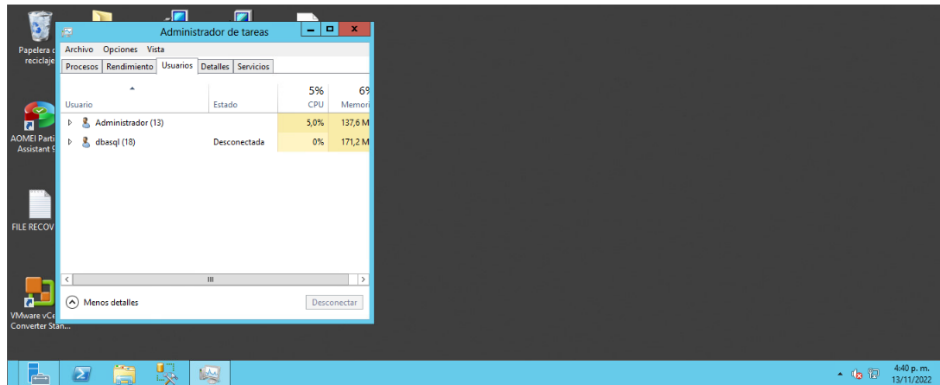
Hecho sexto: a las 4:57 pm el Sysadmin informa que esta el servidor 41 esta igual, y se está extendiendo porque el dc del 200.215, siendo las 5 pm se notifica que igual para el 200.216

Hecho Séptimo: Tanto el DBA como el Sysadmin inician una llamada grupal, para revisar el servidor 41 y sus DB; en las que se inicia a detectar discos llenos, detecta archivo FILE RECOVERY, Archivos encriptados, se encuentra un usuario llamado ISLA con perfil de administrador el cual levantó sospecha y se bloqueó



CTRL+ALT+SUPR

OPCIONES



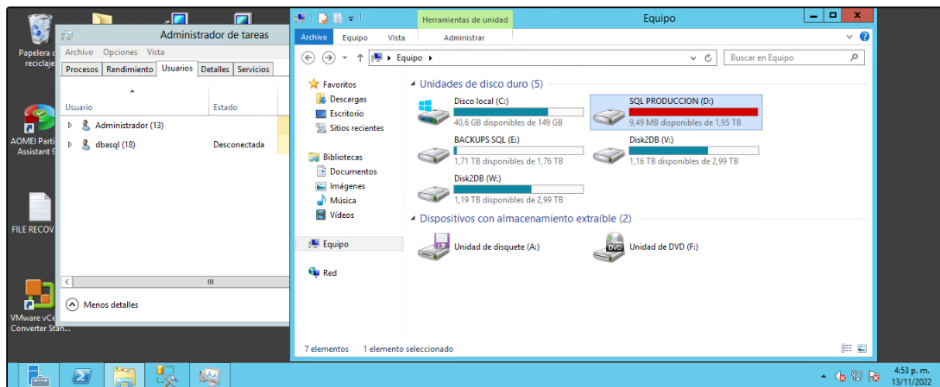
Conectado.



Disco duro lleno

CTRL+ALT+SUPR

OPCIONES



Conectado.



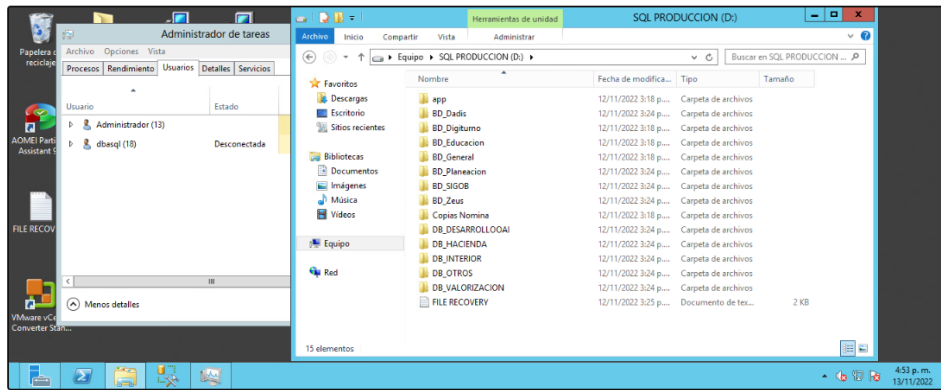
Carpetas de backup, se encuentra el archivo FILE RECOVERY

SQL server 4.41 - SQL server 4.41

PANTALLA COMPLETA

CTRL+ALT+SUPR

OPCIONES



Conectado.



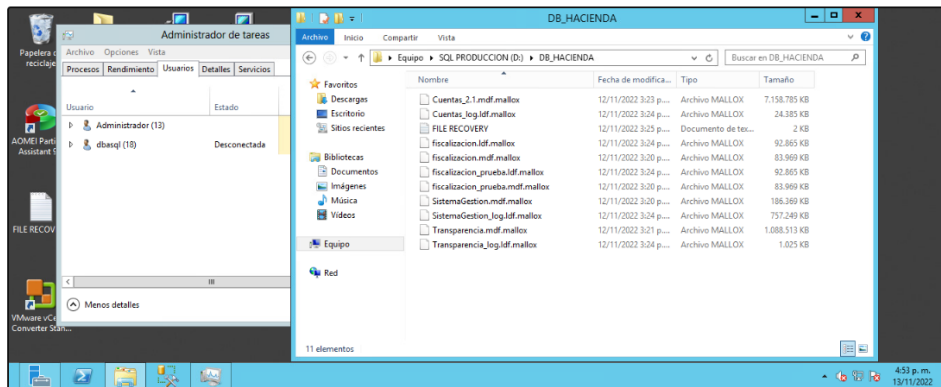
Archivos encriptados

SQL server 4.41 - SQL server 4.41

PANTALLA COMPLETA

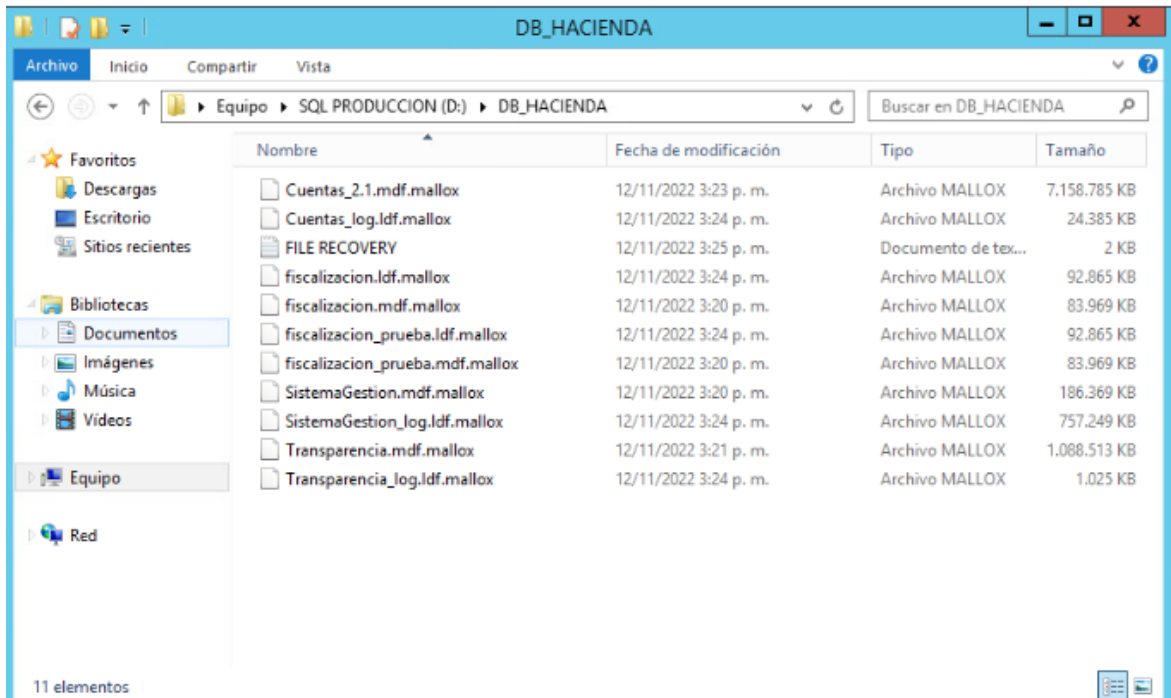
CTRL+ALT+SUPR

OPCIONES

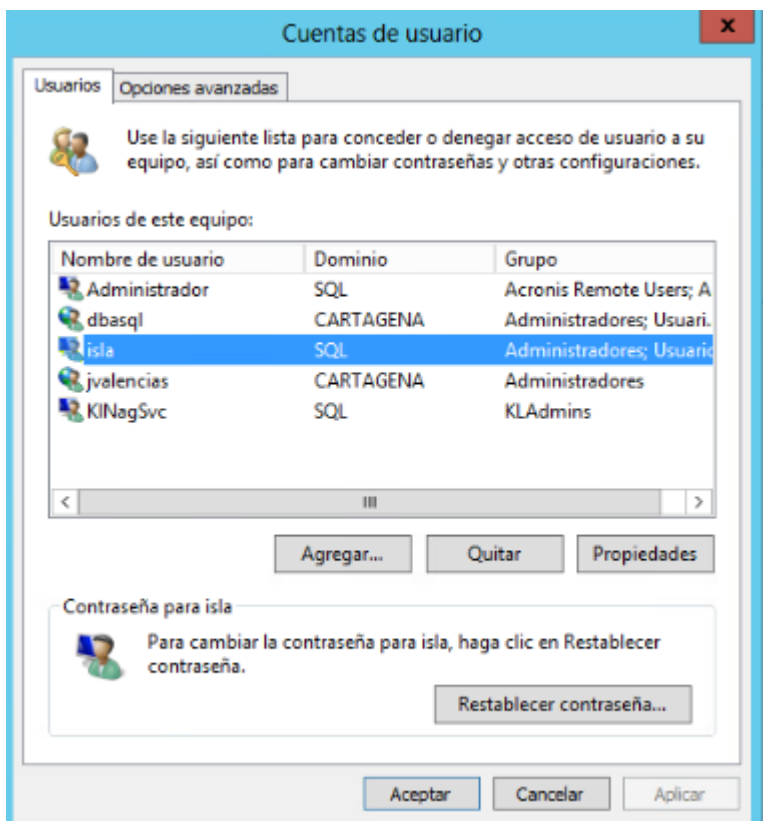


Conectado.



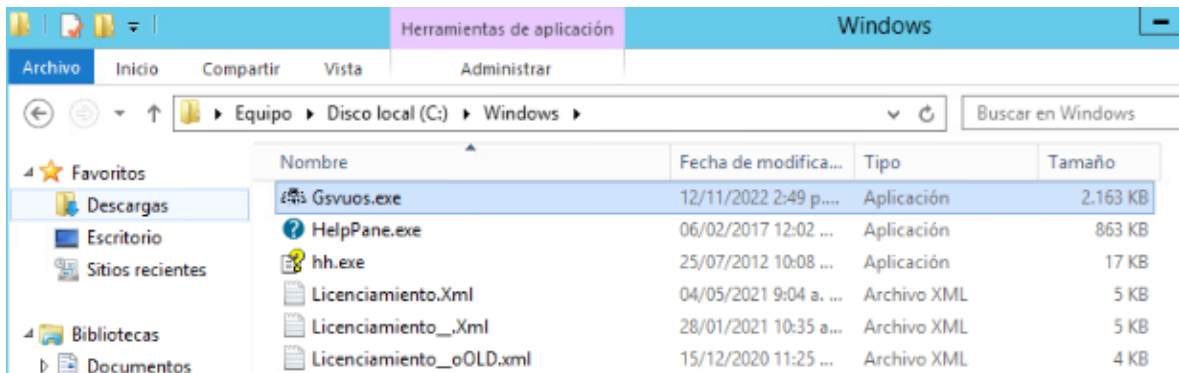


Usuarios locales encontrados en el servidor

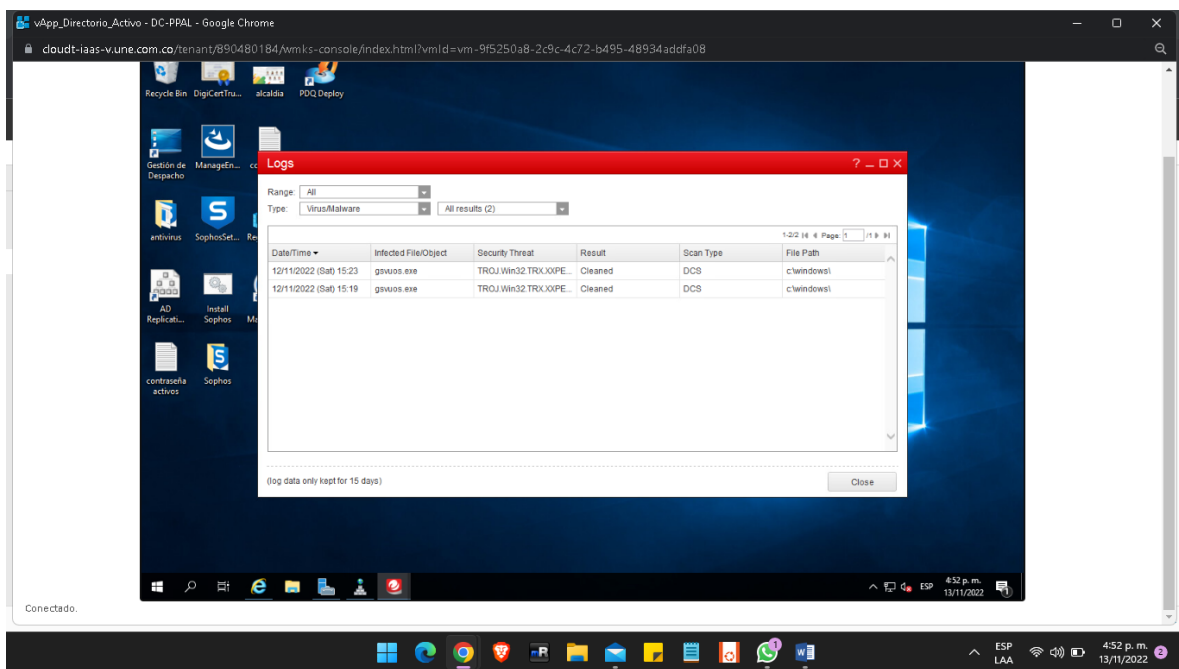


Hecho Octavo: se inicia la inspección sobre el **Servidor de dominio 200.215**, se identifica el virus

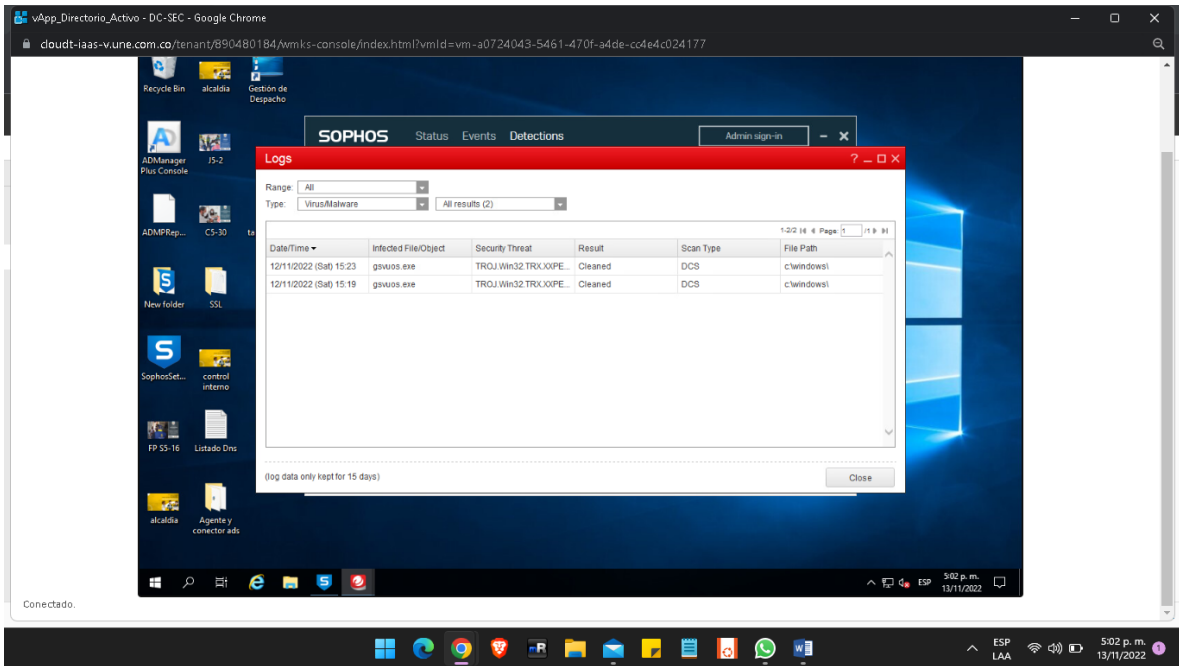
Virus identificado



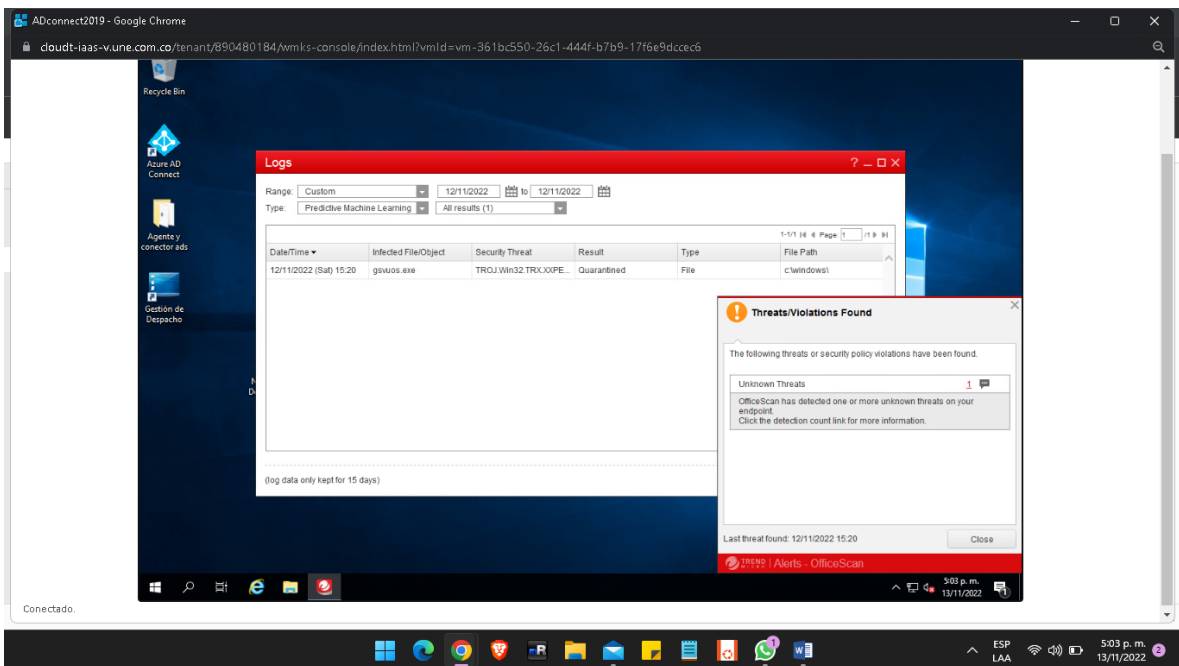
Virus detectado



Hecho Noveno: se inicia la inspección sobre el **Servidor 200.216**, encontrándose el ejecutable del virus

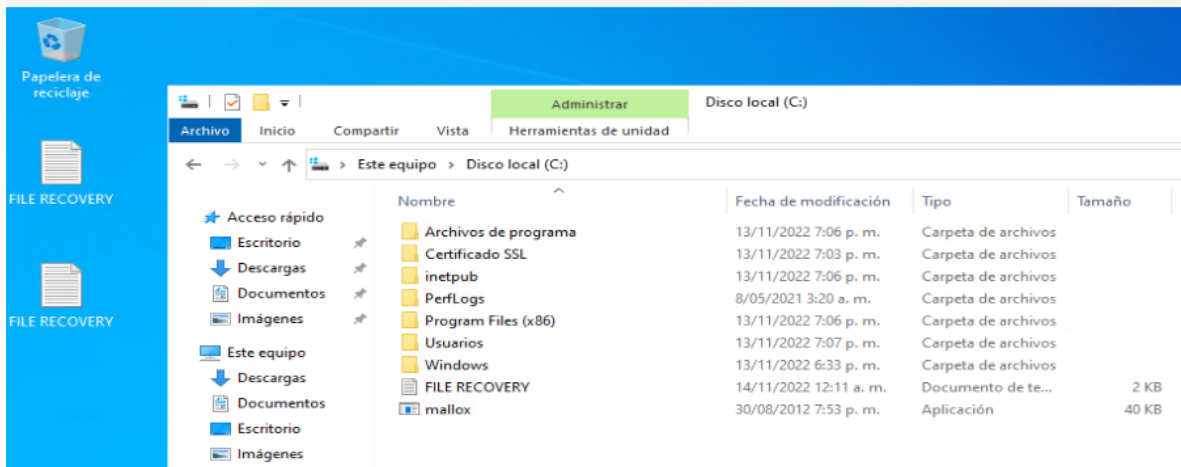


Adconnect2019 – conector office 365 con dc y conector sdwan con dc

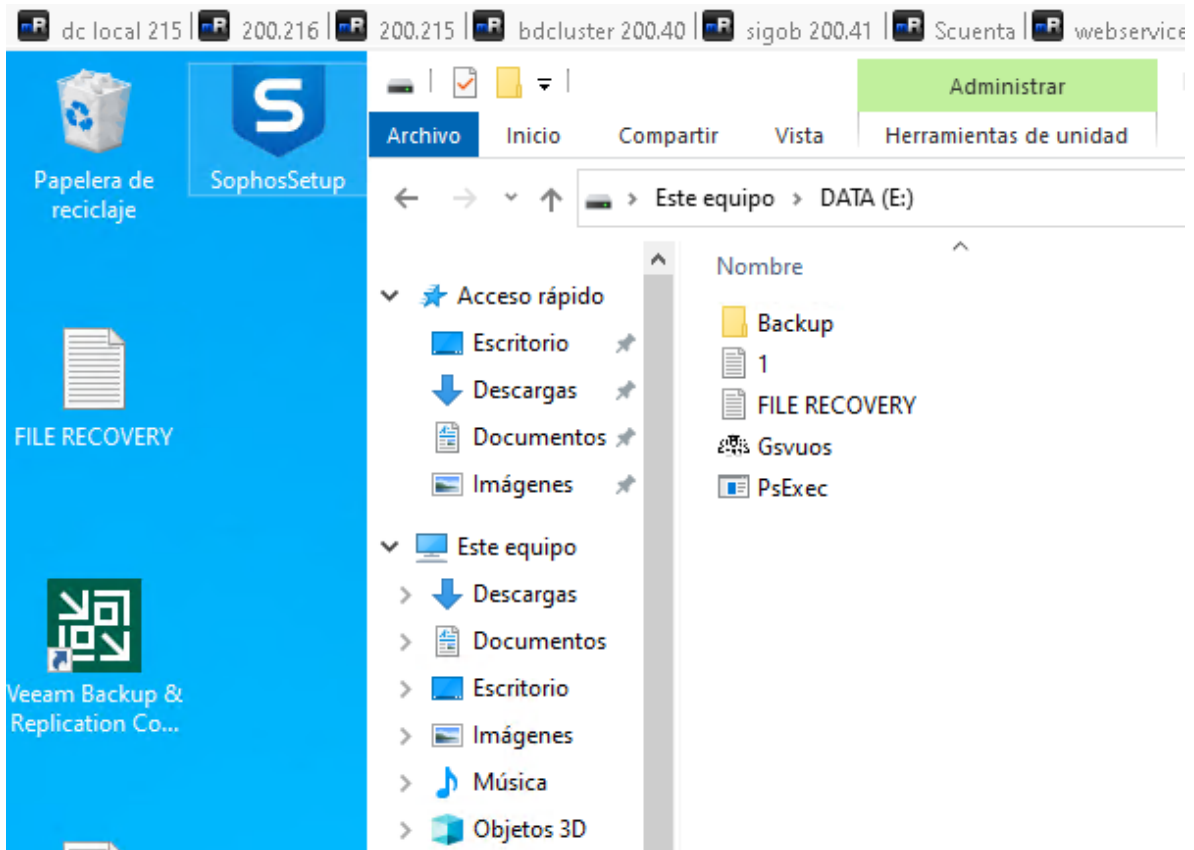


Hecho Noveno: Se toman instantáneas de los servidores 40 y 41

Servidor 10.20.200.217



Servidor veembackup ip 200.219



Hecho Décimo: se identifica que desde el servidor 10.20.200.41 se está propagando el virus, como se evidencia en los siguientes pantallazos

Date	Description
14/11/2022 9:01:27 a. m.	Your administrator isolated the computer
14/11/2022 3:03:16 a. m.	Process 10.20.200.41 unblocked automatically
13/11/2022 3:07:00 a. m.	Sophos Malicious Traffic Detection (64-bit) v1.16.2923 successfully installed

Posible causa o fuente de entrada

Date	Description
13/11/2022 6:29:48 p. m.	Threat acknowledged
19/09/2022 7:52:25 a. m.	Manual cleanup required: C:/sw/PSTools.zip/pskill64.exe
19/09/2022 7:52:21 a. m.	PsKill detected at C:\sw\PSTools.zip

Hecho Décimo Primero: en el día 14 de noviembre del 2022, se comienza el proceso de desinfección; procediendo de la siguiente manera: Se instala la herramienta *spy hunter 5 free*, el cual detecta 17 malwares en el servidor .41.

SpuHunter 5 Free | ¡Se ha completado el análisis!
17 Problemas de seguridad encontrados | 17 / 673694 | COMPRAR

Home | Análisis en ejecución | Análisis de malware/PC | Herramientas avanzadas | Protector del sistema | Configuración | Servicio de asistencia técnica | Acerca de

Malware: 17 | Permisos: 513

A continuación, se muestra una lista de objetos de malware detectados en este ordenador. La categoría malware incluye spyware, adware, trojanos, ransomware, gusanos, virus y rootkits. El malware suele representar una amenaza para la seguridad del equipo y debe erradicarse lo antes posible. Cada uno de los objetos presentados a continuación aparece marcado para su eliminación. En caso de que quieras conservar alguno de los objetos, ahora tienes la oportunidad de desmarcarlo.

- Gravedad: 80% (Alta)** Trojan.MSIL.Krypt.GB (1 objeto)
MSIL.Krypt.GB is a Trojan that stealthily installs itself, most often by exploiting system vulnerabilities and security flaws, through software downloads from malicious websites or via email attachments from untrusted sources (usually .exe, .pdf, .avi, and even .jpg files). MSIL.Krypt.GB runs silently in the background and performs malicious functions. MSIL.Krypt.GB may allow hackers to gain complete control over your system after installation. MSIL.Krypt.GB may covertly delete files, install additional malware, steal passwords and banking information, modify your system security settings, and monitor and transmit your computer activity and other highly sensitive personal data to a remote attacker.
- [F] SqlDecryptor.exe
- Gravedad: 20% (Baja)** Adware.Linkury.O (1 objeto)
Linkury.O is an adware program that can automatically display or download advertisements to a computer. These advertisements may appear in a pop-up window, web browser, toolbar or within an ad-supported program. Adware often comes bundled with freeware such as games, emoticons, file-sharing software, or screensavers. Linkury.O may track your web browsing habits, sites visited, ad usage information, and transmit that data to third parties to deliver targeted advertisements to you or for other advertising and marketing purposes. In addition, the data collected by adware like Linkury.O is generally non-identifiable; in other words, you are not personally identified during the collection of the information. Although Linkury.O may not pose a serious threat to your privacy or security, it may have some side effects like slow computer performance and annoying pop-up ads.
- [F] ZeusImpKey.XmlSerializers.dll
- Gravedad: 50% (Media)** Malware.Generic (1 objeto)
Malware may include spyware, adware, trojans, ransomware, worms, viruses, and rootkits. Malware generally represents a security threat and should be removed from your system as soon as possible.
- [F] Gwgcnc.exe
- Gravedad: 80% (Alta)** Trojan.Mimikatz (6 objetos)
Mimikatz is a Trojan that installs itself secretly and quietly onto your computer, most often by exploiting system vulnerabilities and security flaws, through a software download from a malicious website or downloading email attachments from untrusted sources (usually .exe, .pdf, .avi, and even .jpg files). Mimikatz does not replicate but hides in the background and performs malicious functions. Mimikatz may allow hackers to gain complete control over your system after installation. With this level of control, Mimikatz may delete files, install additional malware, steal passwords, change your system settings, and monitor your computer activity.
- [F] mimidrv.sys

Próximo

8:13 a. m. 14/11/2022

SpuHunter 5 Free | ¡Se ha completado el análisis!
17 Problemas de seguridad encontrados | 17 / 673694 | COMPRAR

Home | Análisis en ejecución | Análisis de malware/PC | Herramientas avanzadas | Protector del sistema | Configuración | Servicio de asistencia técnica | Acerca de

Malware: 17 | Permisos: 513

A continuación, se muestra una lista de objetos de malware detectados en este ordenador. La categoría malware incluye spyware, adware, trojanos, ransomware, gusanos, virus y rootkits. El malware suele representar una amenaza para la seguridad del equipo y debe erradicarse lo antes posible. Cada uno de los objetos presentados a continuación aparece marcado para su eliminación. En caso de que quieras conservar alguno de los objetos, ahora tienes la oportunidad de desmarcarlo.

- [F] mimidrv.sys
- [F] mimispool.dll
- [F] mimilove.exe
- [F] mimilib.dll
- Rutas: C:\Users\Isla\Desktop\mimikatz\Win32\mimilib.dll
MD5: 46a598798b05e4c72e796edc2317b52
Tamaño: 31744 bytes
- [F] mimispool.dll
- [F] kiwi.exe
- Gravedad: 80% (Alta)** Trojan.Injector.KPU (1 objeto)
Injector.KPU is a Trojan that stealthily installs itself, most often by exploiting system vulnerabilities and security flaws, through software downloads from malicious websites or via email attachments from untrusted sources (usually .exe, .pdf, .avi, and even .jpg files). Injector.KPU runs silently in the background and performs malicious functions. Injector.KPU may allow hackers to gain complete control over your system after installation. Injector.KPU may covertly delete files, install additional malware, steal passwords and banking information, modify your system security settings, and monitor and transmit your computer activity and other highly sensitive personal data to a remote attacker.
- [F] kiwi.exe
- Gravedad: 80% (Alta)** Trojan.FakeMS (2 objetos)
FakeMS is a Trojan that installs itself secretly and quietly onto your computer, most often by exploiting system vulnerabilities and security flaws, through a software download from a malicious website or downloading email attachments from untrusted sources (usually .exe, .pdf, .avi, and even .jpg files). FakeMS does not replicate but hides in the background and performs malicious functions. FakeMS may allow hackers to gain complete control over your system after installation. With this level of control, FakeMS may delete files, install additional malware, steal passwords, change your system settings, and monitor your computer activity.

Próximo

8:16 a. m. 14/11/2022

SpuHunter 5 Free | ¡Se ha completado el análisis!
17 Problemas de seguridad encontrados | 17 / 673694 | COMPRAR

Home | Análisis en ejecución | Análisis de malware/PC | Herramientas avanzadas | Protector del sistema | Configuración | Servicio de asistencia técnica | Acerca de

Malware: 17 | Permisos: 513

A continuación, se muestra una lista de objetos de malware detectados en este ordenador. La categoría malware incluye spyware, adware, trojanos, ransomware, gusanos, virus y rootkits. El malware suele representar una amenaza para la seguridad del equipo y debe erradicarse lo antes posible. Cada uno de los objetos presentados a continuación aparece marcado para su eliminación. En caso de que quieras conservar alguno de los objetos, ahora tienes la oportunidad de desmarcarlo.

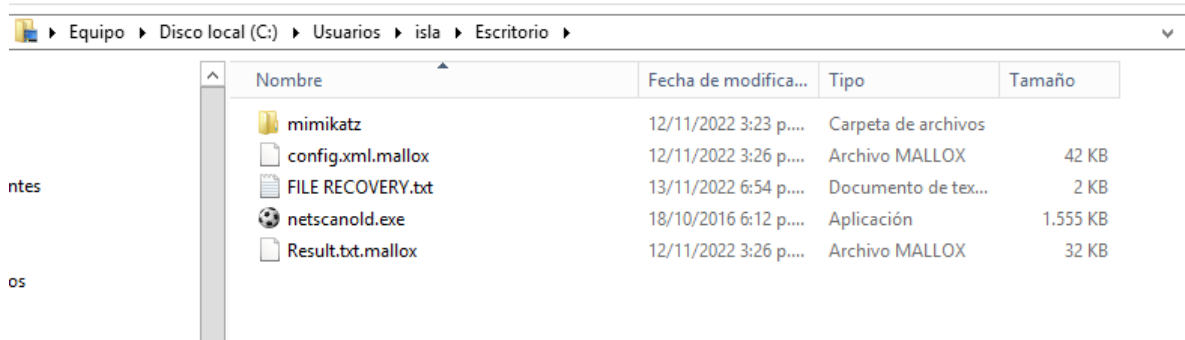
- Instal additional malware, steal passwords, change your system settings, and monitor your computer activity.
- [F] Klav (New Parser).exe
- [F] Klav (New Parser).exe
- Gravedad: 50% (Media)** Malware.Generic (3 objetos)
Malware may include spyware, adware, trojans, ransomware, worms, viruses, and rootkits. Malware generally represents a security threat and should be removed from your system as soon as possible.
- [F] NS6JR57.exe
- [F] Mtdowvuo0e.exe
- [D] C:\Users\MSSQLSERVER\AppData\Roaming\Tvpocbk
- Gravedad: 80% (Alta)** Trojan.MSIL.Inject.HD (2 objetos)
MSIL.Inject.HD is a Trojan that stealthily installs itself, most often by exploiting system vulnerabilities and security flaws, through software downloads from malicious websites or via email attachments from untrusted sources (usually .exe, .pdf, .avi, and even .jpg files). MSIL.Inject.HD runs silently in the background and performs malicious functions. MSIL.Inject.HD may allow hackers to gain complete control over your system after installation. MSIL.Inject.HD may covertly delete files, install additional malware, steal passwords and banking information, modify your system security settings, and monitor and transmit your computer activity and other highly sensitive personal data to a remote attacker.
- [F] 7HLWRRHU.exe
- Rutas: C:\Users\MSSQLSERVER\AppData\Local\Temp\7HLWRRHU.exe
MD5: da899a21b9afdf66e049ced1b361d7
Tamaño: 709632 bytes
- [F] SKXUGYT.exe

Próximo

8:16 a. m. 14/11/2022

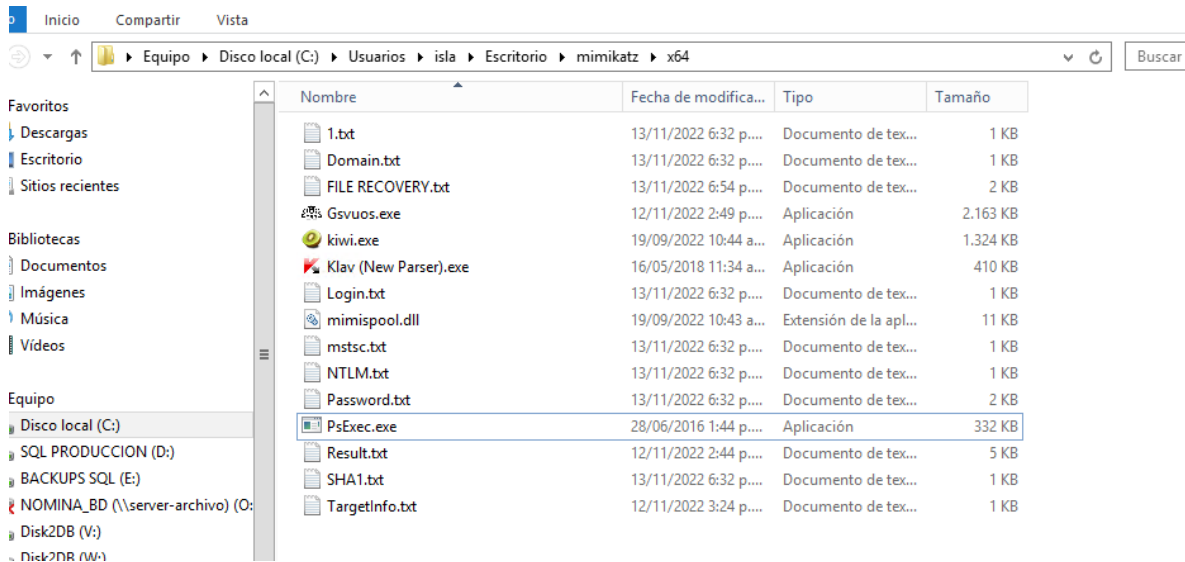
Hecho Décimo Segundo: Por medio de la herramienta libre RakhniDecryptor de karspesky utilizada para desencriptar los archivos, se inicia a correrla; pero esta no reconoce la encriptación, dándose como acción fallida el proceso de desencriptar.

Hecho Décimo tercero: A través de la inspección del usuario local ISLA, se encuentran archivos sospechosos en el escritorio y en imágenes, archivos con extensión mallox, archivo FILE RECOVERY, GSPUOS.EXE, como se evidencia a continuación:



Equipo > Disco local (C:) > Usuarios > isla > Escritorio

Nombre	Fecha de modifica...	Tipo	Tamaño
mimikatz	12/11/2022 3:23 p...	Carpeta de archivos	
config.xml.mallox	12/11/2022 3:26 p...	Archivo MALLOX	42 KB
FILE RECOVERY.txt	13/11/2022 6:54 p...	Documento de tex...	2 KB
netscanold.exe	18/10/2016 6:12 p...	Aplicación	1.555 KB
Result.txt.mallox	12/11/2022 3:26 p...	Archivo MALLOX	32 KB



Inicio Compartir Vista

Equipo > Disco local (C:) > Usuarios > isla > Escritorio > mimikatz > x64

Nombre	Fecha de modifica...	Tipo	Tamaño
1.txt	13/11/2022 6:32 p...	Documento de tex...	1 KB
Domain.txt	13/11/2022 6:32 p...	Documento de tex...	1 KB
FILE RECOVERY.txt	13/11/2022 6:54 p...	Documento de tex...	2 KB
Gsvuos.exe	12/11/2022 2:49 p...	Aplicación	2.163 KB
kiwi.exe	19/09/2022 10:44 a...	Aplicación	1.324 KB
Klav (New Parser).exe	16/05/2018 11:34 a...	Aplicación	410 KB
Login.txt	13/11/2022 6:32 p...	Documento de tex...	1 KB
mimispool.dll	19/09/2022 10:43 a...	Extensión de la apl...	11 KB
mstsc.txt	13/11/2022 6:32 p...	Documento de tex...	1 KB
NTLM.txt	13/11/2022 6:32 p...	Documento de tex...	1 KB
Password.txt	13/11/2022 6:32 p...	Documento de tex...	2 KB
PSEXEC.exe	28/06/2016 1:44 p...	Aplicación	332 KB
Result.txt	12/11/2022 2:44 p...	Documento de tex...	5 KB
SHA1.txt	13/11/2022 6:32 p...	Documento de tex...	1 KB
TargetInfo.txt	12/11/2022 3:24 p...	Documento de tex...	1 KB

Usuarios | Opciones avanzadas

Use la siguiente lista para conceder o denegar acceso de usuario a su equipo, así como para cambiar contraseñas y otras configuraciones

Usuarios de este equipo:

Nombre de usuario	Dominio	Grupo
Administrador	SQL	Acronis Remote U...
isla	SQL	Administradores; ...
KINagSvc	SQL	KLAdmins

Hecho Décimo cuarto: se detecta que el Usuario isla se había agregado al DC, Al igual que el KlnaGsc y este tiene grupo admins del karpesky

KLAdmins Properties

Multiple Names Found

More than one object matches the following object name: "isla". Select an object from this list or, to reenter the name, click Cancel.

Matching names:

Name	Logon Name (pr...	E-Mail Address	Description	In Folder
isla	isla			cartagena.gov.c...
Islandi Navaro	Inavaro			cartagena.gov.c...

KlnaGsc y este tiene grupo admins del karpesky

Perfiles de usuario

Los perfiles del usuario contienen la configuración de escritorio y otro tipo de información relacionada con su cuenta de usuario. Se puede crear un perfil diferente en cada equipo que use o bien seleccionar un perfil móvil para usarlo en cualquier equipo.

Perfiles almacenados en este equipo:

Nombre	Tamaño	Tipo	Estado	Modificado	
APPPPOOL\,.NET v4.5	3,75 MB	Local	Local	12/11/2022	^
APPPPOOL\,.NET v4.5 ...	3,75 MB	Local	Local	12/11/2022	
Perfil predeterminado	?	Local	Local		
Administrador	6,37 GB	Local	Local	14/11/2022	
isla	76,8 MB	Local	Local	12/11/2022	≡
WINagSvc	3,77 MB	Local	Local	12/11/2022	∨

[Haga clic aquí para crear cuentas de usuario.](#)

isla Properties

Sessions Remote control Remote Desktop Services Profile COM

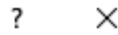
General Address Account Profile Telephones Organizatic

Member Of Password Replication Dial-in Environment

Member of:

Name	Active Directory Domain Services Fo
Administradores	cartagena.gov.co/Builtin
Enterprise Domain Controllers de ...	cartagena.gov.co/Users
Usuarios de escritorio remoto	cartagena.gov.co/Builtin
Usuarios del dominio	cartagena.gov.co/Users

isla Properties



Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile	COM+	Attribute Editor			
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of	Password Replication	Dial-in	Object	

Canonical name of object:

Object class: User

Created: 12/11/2022 3:10:20 p. m.

Modified: 14/11/2022 12:20:12 p. m.

Update Sequence Numbers (USNs):

Current: 16105758

Original: 15923849

Protect object from accidental deletion

KLAdmins Properties



General	Members	Member Of	Managed By
Object	Security	Attribute Editor	

Canonical name of object:

Object class: Group

Created: 2/02/2016 1:24:21 p. m.

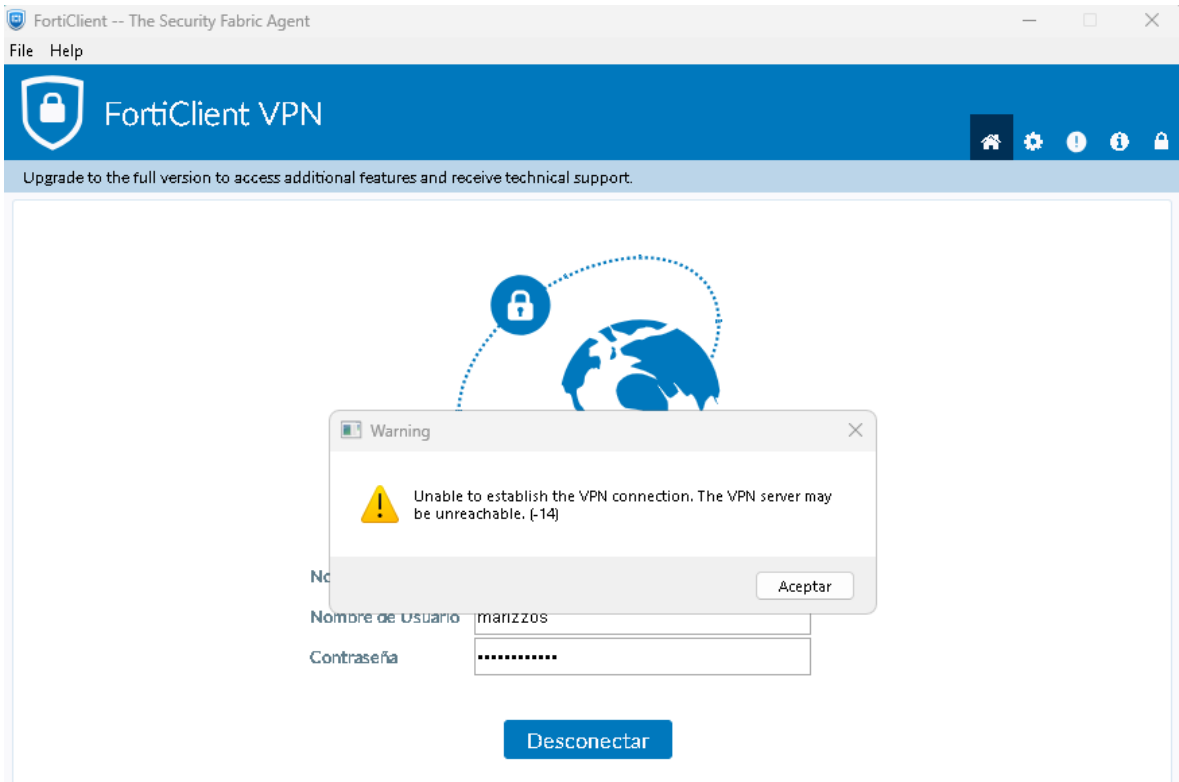
Modified: 23/11/2021 11:43:38 a. m.

Update Sequence Numbers (USNs):

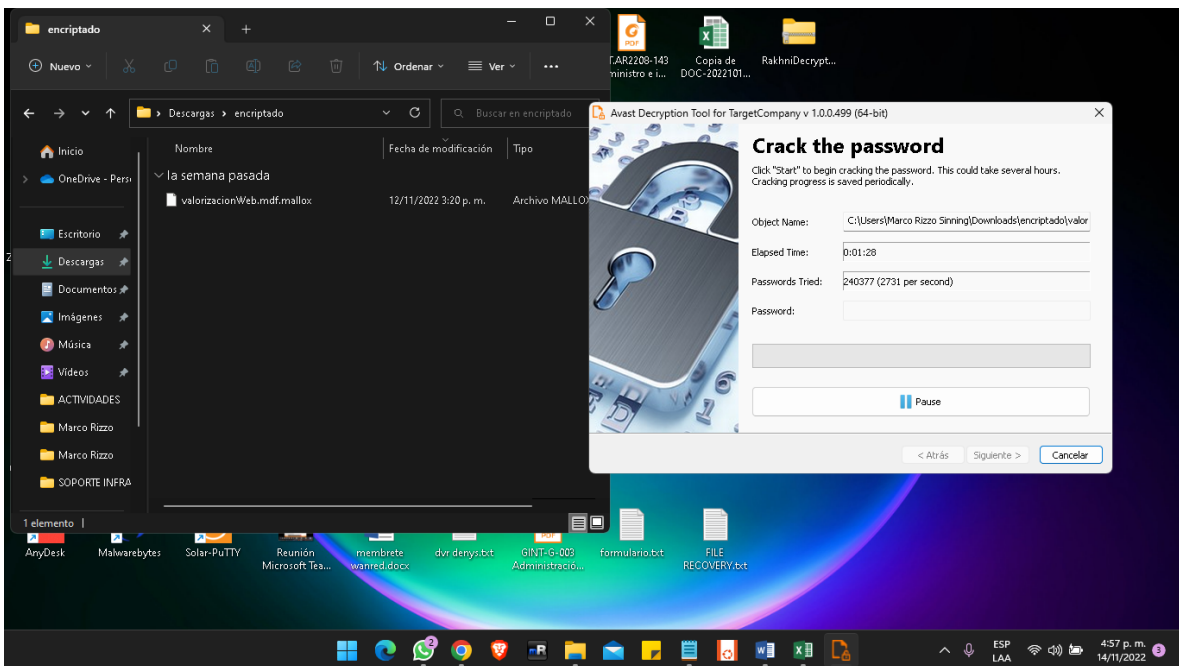
Current: 16696

Original: 16696

Protect object from accidental deletion



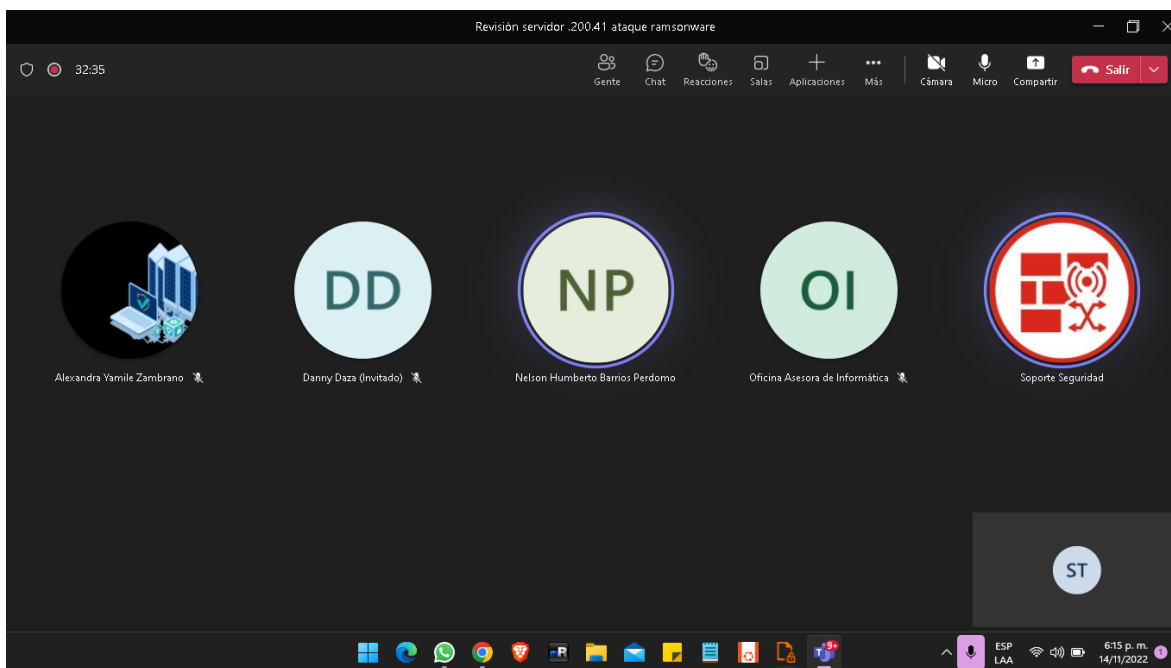
Hecho Décimo cuarto: se corre otra nueva Herramienta de recuperación, Crack the password; pero tampoco se pudo recuperar la información.



Hecho Décimo quinto: Se genera por medio de una llamada telefónica la activación de la respuesta a incidentes de seguridad por medio del COLCERT, quienes por medio del

ingeniero Nelson Barrios se lleva el levantamiento del incidente informándoles toda la situación del ataque, afectación.

Hecho Décimo sexto: Posterior a la llamada se genera mesa de trabajo con el equipo se la OAI y el COLCERT, en donde se indaga de manera más exhaustiva los pasos dado para la detección y validación de los pasos dados desde la OAI para contener el ataque. Se orienta desde el COLCERT, las actuaciones a seguir y la disponibilidad de su parte en colaborar con el incidente que presenta la alcaldía distrital de Cartagena de indias.



Atentamente;

Alexandra Yamile Zambrano Jojoa

C.C. 25.280188

Asesora en Seguridad de Cartagena de Indias.