SENTRIA BY NETDATA

INVESTIGACIÓN

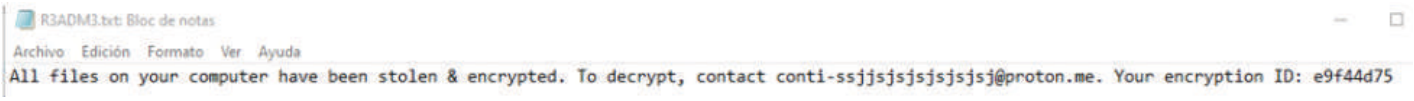
Ransomware As a Service

VARIANTE GRUPO CONTI

02/10/2023

SUMMARY

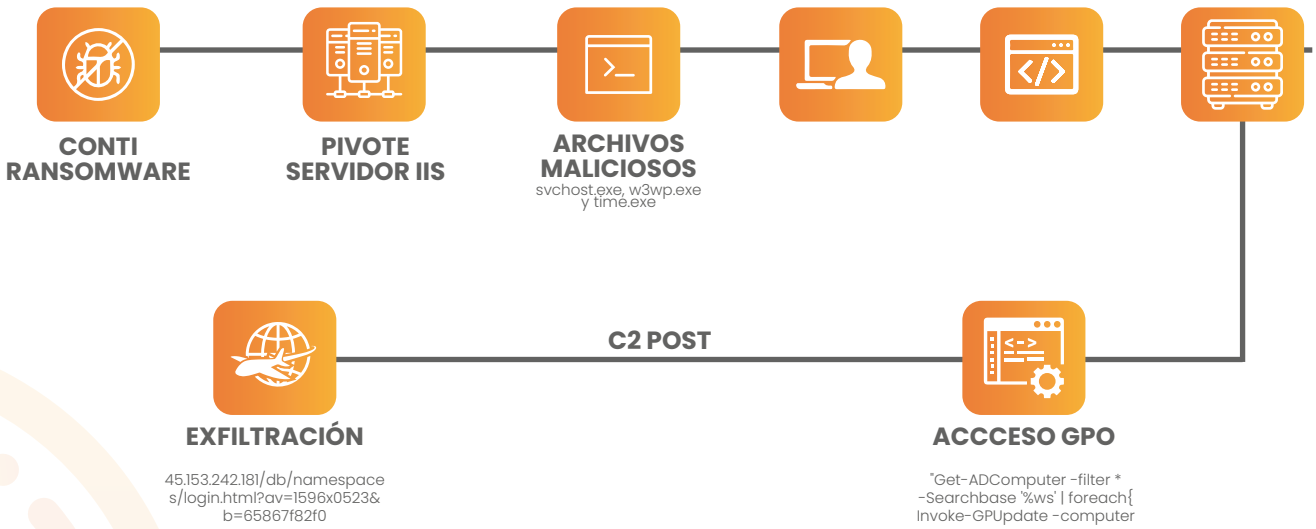
Como sabemos, el grupo Conti está vinculado al poderoso grupo Wizard Spider, que ha desarrollado un modelo de negocio basado en ataques de ransomware a través de un servicio conocido como Ransomware as a Service (RaaS). En este contexto, hemos identificado una variante del grupo Conti dentro de los servicios de Sentria 911.
Con el servicio de Sentria 911, hemos identificado un ataque que se atribuye a una variante del grupo Conti Ransomware. Esta atribución se basa en los indicadores recopilados durante nuestra investigación, así como en el mensaje de rescate encontrado durante el incidente.



Descripción general

Durante nuestra investigación, identificamos un patrón de comportamiento característico del grupo Conti Ransomware. El vector de ataque inicial se dirigió hacia los servidores IIS que estaban expuestos, que son uno de los objetivos preferidos de este grupo.
A partir de ahí, los atacantes realizaron movimientos laterales hacia el Directorio Activo, desde donde comenzaron a cifrar la información en todos los equipos de la red.

Cabe destacar que esta variante específica de Conti muestra un enfoque particularmente dirigido hacia los servicios de Directorio Activo y utiliza políticas de grupo (GPO) para cifrar la información en todos los equipos conectados a la red.
Durante el ataque, encontramos evidencia de que el grupo llevó a cabo actividades destinadas a eludir las defensas de seguridad. Esto incluyó la desactivación de las herramientas antivirus utilizadas por el atacante para facilitar el proceso de cifrado de datos. Además, identificamos que el grupo creó archivos específicos durante el ataque con el propósito de cifrar información dentro de la organización mediante las Políticas de Grupo (GPO) de los Directorios Activos.



DETALLE TÉCNICO

En el vector inicial encontramos que el atacante ingreso a la red a través de servicios publicados en sistemas IIS, sin embargo, lamentablemente al momento de ingresar a la red muchos de los logs estaban cifrados y no se logró recuperar información sobre qué tipo de técnicas usaron para ingresar a la red.

Tras infiltrarse en la red, el atacante procede a crear cuentas de usuario locales para asegurar su persistencia en el entorno. Además, lleva a cabo el robo de credenciales desde el Administrador de Credenciales de Windows, lo que le permite realizar movimientos laterales dentro de la infraestructura.

Durante la investigación de la variante se encontraron varios archivos maliciosos entre ellos encontramos un archivo nombrado por el atacante svchost.exe (174ada6f6ab5b456affb3a05a4549d18d1de9bc0507e0e398f2e2609bba93fd0), se realiza ingeniería reversa sobre este archivo y se encuentra lo siguiente:
Comparativa entre el proceso legítimo de Windows (Figura 1) y el proceso malicioso (Figura 2), donde podemos observar en la imagen List-1 que tienen diferencias en la información de Copyright, por lo que nos indica que el atacante está realizando una actividad de ocultar el malware y de evadir defensas y detecciones de antivirus.

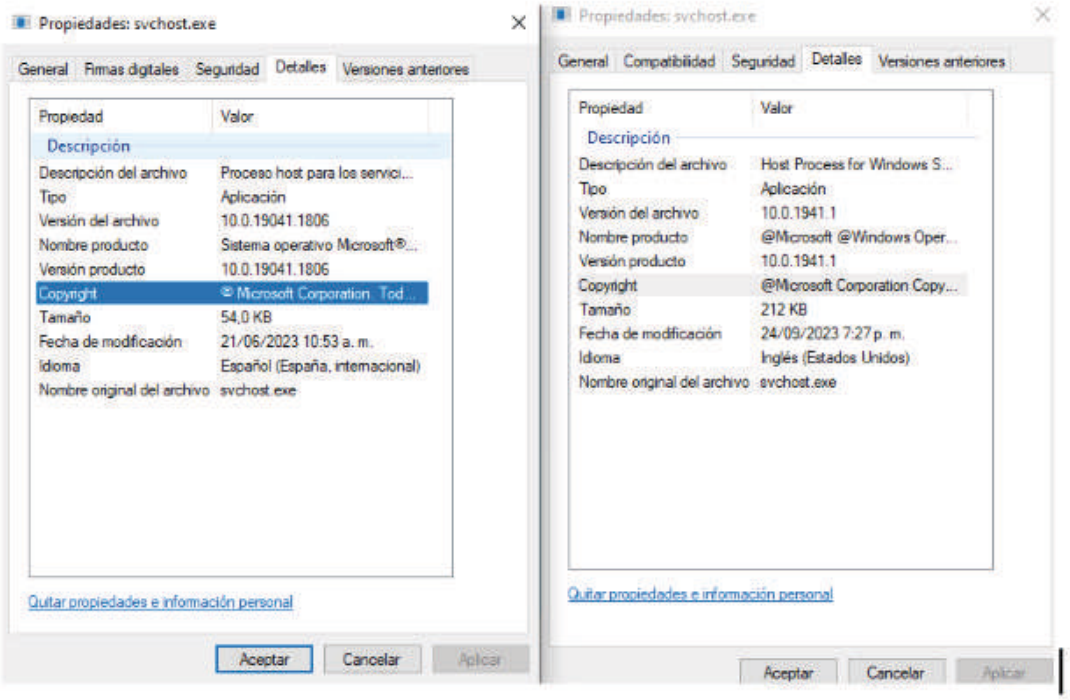


Figura List-1

DETECCIÓN

La ejecución inicia desde el directorio “temp” ejecutándose así mismo e intentando evadir defensas del sistema operativo.

```
"C:\Users\admin\AppData\Local\Temp\svchost.exe"
```

```
push    208h
push    eax
lea     eax, [esp+360h+Filename]
push    eax
call    sub_415270
add     esp, 0Ch
lea     eax, [esp+358h+Filename]
push    104h            ; nSize
push    eax             ; lpFilename
push    0               ; hModule
call    ds:GetModuleFileNameW
push    offset aKsvc_0  ; " -ksvc"
lea     eax, [esp+35Ch+Filename]
push    eax             ; lpString1
call    ds:lstrcatW
nop     dword ptr [eax]
```

Podemos observar en la figura List-2 que el malware ejecuta un comando con strings “-ksvc” que activa una secuencia de actividades, entre ellas actividades de espera para evadir sandboxing dentro de cada ejecución, como se observa en List-3

```
call    sub_404710
push    493E0h          ; dwMilliseconds
call    ebx ; Sleep
mov     esi, [esp+358h+lpParameter]
mov     ecx, esi        ; pszSrch
call    sub_404D30
push    493E0h          ; dwMilliseconds
call    ebx ; Sleep
lea     eax, [esp+358h+ThreadId]
mov     [esp+358h+ThreadId], 0
push    eax             ; lpThreadId
push    0               ; dwCreationFlags
push    esi             ; lpParameter
push    offset sub_4065F0 ; lpStartAddress
push    0               ; dwStackSize
push    0               ; lpThreadAttributes
call    ds:CreateThread
```

TABLA DE IMPORTACIONES

library (11)	duplicate (0)	flag (4)
NETAPI32.dll	-	x
USER32.dll	-	-
ole32.dll	-	-
OLEAUT32.dll	-	-
GPEDIT.DLL	-	x
ACTIVEDS.dll	-	x
SHLWAPI.dll	-	-
SHELL32.dll	-	-
WS2_32.dll	-	x
ADVAPI32.dll	-	-
KERNEL32.dll	-	-

Figura List-4

Se observa que el archivo malicioso no descarga dll pero usa las dll que provee el sistema para poder obtener mas poder dentro del S.O y hacer uso de las API de Windows para lograr mayor movilidad y camuflar su ataque como se observa en la figura List-4

NetShareGetInfo
NetShareEnum
NetShareSetInfo
NetApiBufferFree
NetGetDCName

Figura List-5

El inicio de la ejecución le permite realizar un descubrimiento del equipo usando la liberaría NETAPI32.dll usando las API. Enumera los recursos compartidos, información del equipo y obtiene el nombre de los directorios activos que puedan existir en la red como se logra observar en la Figura List-5.

9 (ADsOpenObject)	x
3 (ADsGetObject)	x
15 (FreeADsMem)	x

Figura List-6

Cuando accede a estas librerías ejecuta diferentes acciones dentro del sistema operativo, entre ellas, logra acceder al directorio activo usando la librería ACTIVEDS.dll , como se observa en Figura List-6

LDAP://%ws.%ws/DC=%ws,DC=%ws
LDAP://DC=%ws,DC=%ws
LDAP://CN=%ws,CN=Policies,CN=System,DC=%ws,DC=%ws

Figura List-7

Una vez logra descubrir el AD, usa la API de Windows CreateGPOlink para generar un vinculo con los objetos del AD y poder administrar las políticas de la GPO.

Descubre los usuarios del directorio activo con el comando y vuelve a inyectar código al proceso svchost.exe, como se puede observa Figura List-8

TABLA DE IMPORTACIONES

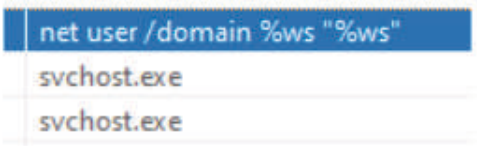


Figura List-8

El siguiente paso es descubrir los recursos compartidos enfoncando se el recurso sysvol de Windows para usarlo como distribuidor del cifrado mediante protocolo SMB.

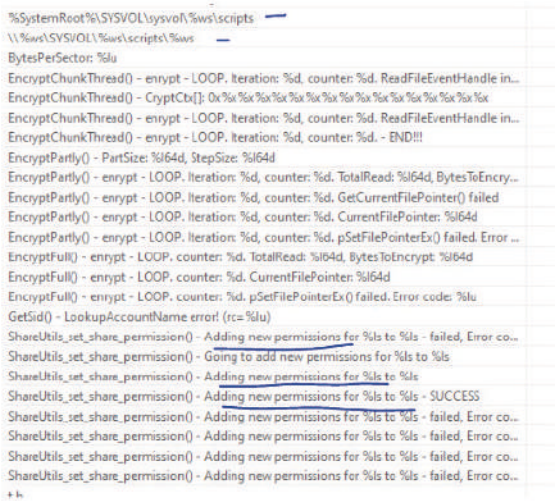


Figura List-9

En la Figura List-9, se puede observar cómo logra agregar nuevos permisos al usuario administrador en el directorio activo

Format = "powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%ws' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}""

```
002E4986  . 68 64B73000    PUSH svchost.0030B764          UNICODE "gpupdate.exe"
002E498B  . 897424 20      MOV DWORD PTR SS:[ESP+20],ESI
002E498F  . FFD7           CALL EDI
002E4991  . 68 80B73000    PUSH svchost.0030B780          UNICODE "/force"
002E4996  . 894424 28      MOV DWORD PTR SS:[ESP+28],EAX
002E499A  . FFD7           CALL EDI
002E499C  . 68 90B73000    PUSH svchost.0030B790          UNICODE "id_me"
002E49A1  . 894424 14      MOV DWORD PTR SS:[ESP+14],EAX
002E49A5  . FFD7           CALL EDI
002E49A7  . 68 9CB73000    PUSH svchost.0030B79C          UNICODE "gpupdate_now"
```

Figura List-10

TABLA DE IMPORTACIONES

Cuando logra acceder a los equipos mediante el recurso compartido sysvol de Windows, se ejecuta y tiene la capacidad de descubrir los servicios y procesos que se están ejecutando dentro del equipo victima para detenerlos y proceder al cifrado de los archivos, como se puede observar Figura Lis-11

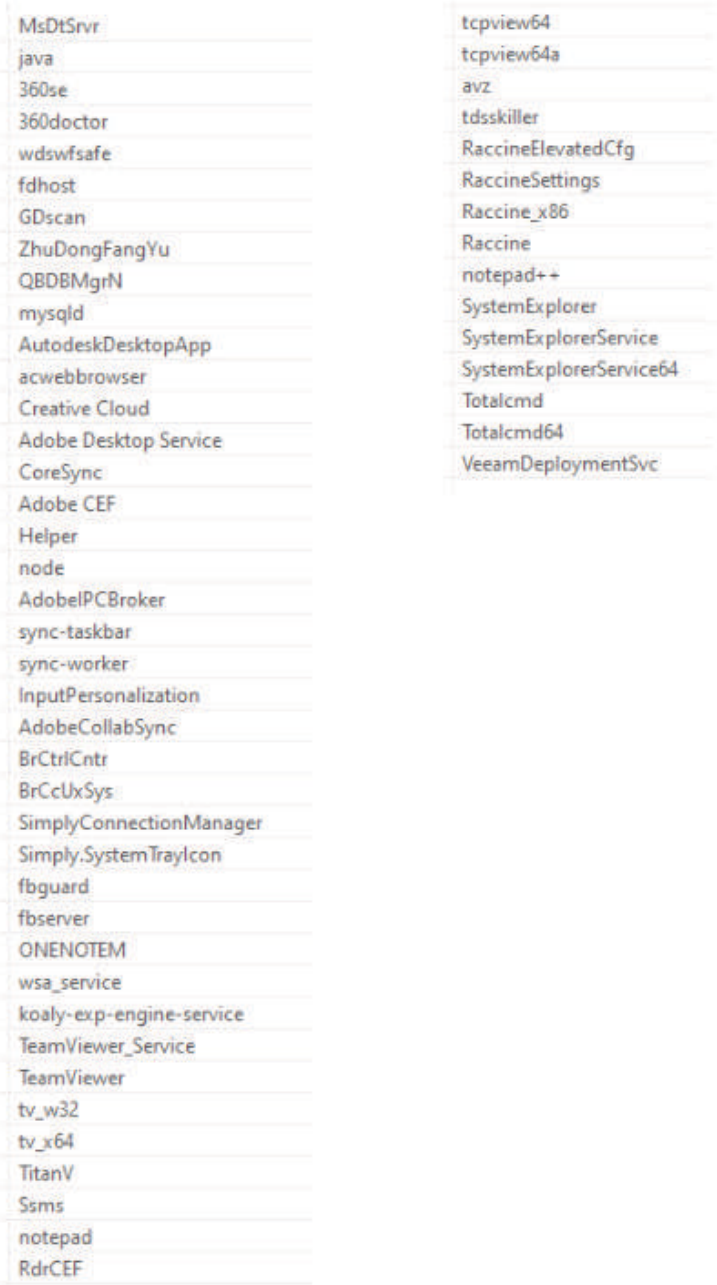
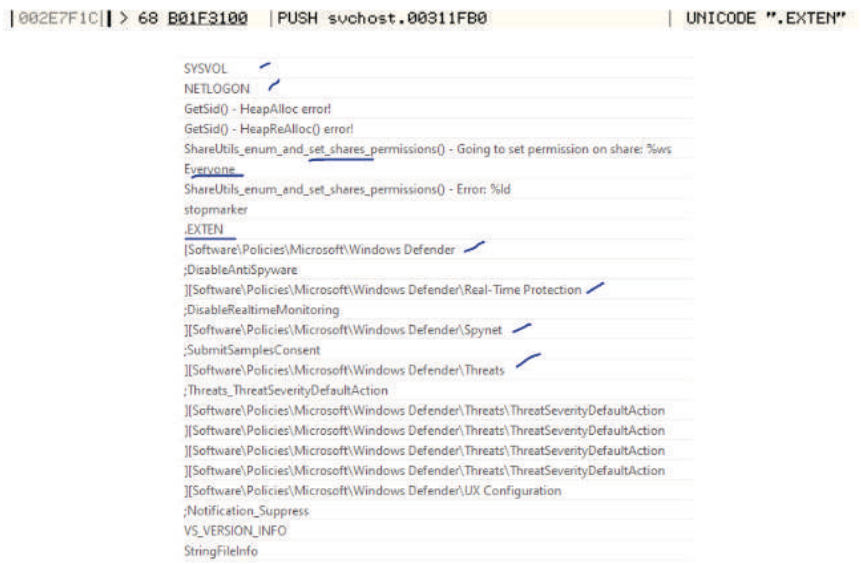


Figura List-11

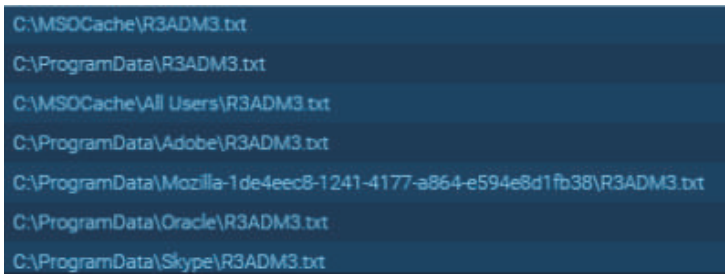
TABLA DE IMPORTACIONES

En este punto el malware logra cifrar los archivos dentro del equipo victima para secuestrarlos dejando la nota de rescate, como se puede observar en la Figura List-12

Figura List-12



Ejecuta una segunda corrida de su código para asegurarse que los archivos cifrados tengan la extensión .EXTEN, desactivar la protección de Windows mediante los siguientes comando, como se puede observar en la Figura List-13



Como se puede observar en la Figura List-14 luego de ello escribe los archivos para solicitar la recompensa en todas las carpetas del usuario que cifro información.

TABLA DE IMPORTACIONES

Una vez realizada exitosamente la actividad de cifrar la información, el malware establece una persistencia. Al realizar ingeniería reversa encontramos que el malware se instala en los registros de autorun para que se pueda ejecutar siempre que se reinicie la maquina o se inicie una sesión como se muestra en Figura List-15

```
push    0               ; lpdwDisposition
push    eax             ; phkResult
push    0               ; lpSecurityAttributes
push    2001Fh          ; samDesired
push    0               ; dwOptions
push    0               ; lpClass
push    0               ; Reserved
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe"...
push    80000002h       ; hKey
```

Figura List-15

Realizando un análisis de memoria, ya que, el valor de la lleve que se crea en la memoria encontramos que el value con el que se crea es con el id de la instancia que se ejecuta el malware, encontramos que el valor es " {41310010-0000-0100-0100-E9F44D75829E}" y la data del registro hace referencia donde se ejecuto el proceso y donde está alojado el malware como por ejemplo c:\windows\temp\svchost.exe .

Dentro de lo observado durante el ataque encontramos otro archivo nombrado por el atacante como time.exe (e8cf5633a560471fd926ce6d59ef3cbf6fbdc2b9bfcfc4ada3bac31d79a51353), donde se encuentra que es usado por el atacante como command and control y exfiltration de informaciónt.

Dentro de las peticiones observadas encontramos que el malware realizar una comunicación POST hacia las siguientes URLS:
45.153.242.181/db/namespaces/login.html?av=1596x0523&b=65867f82f0
45.153.242.181/authenticate/signin.html?ao=3j38i33731&r=qp78099352

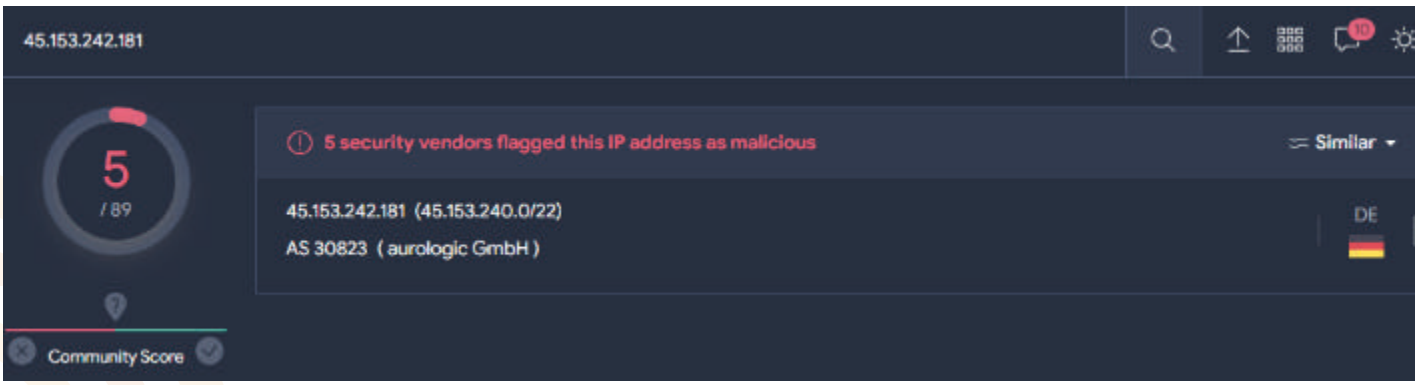
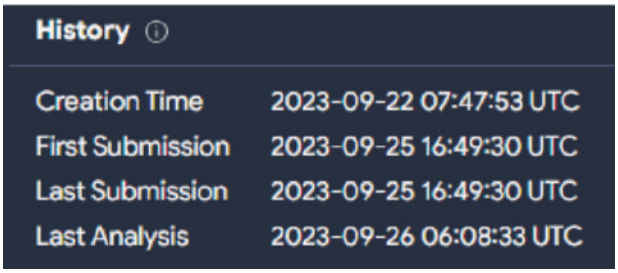
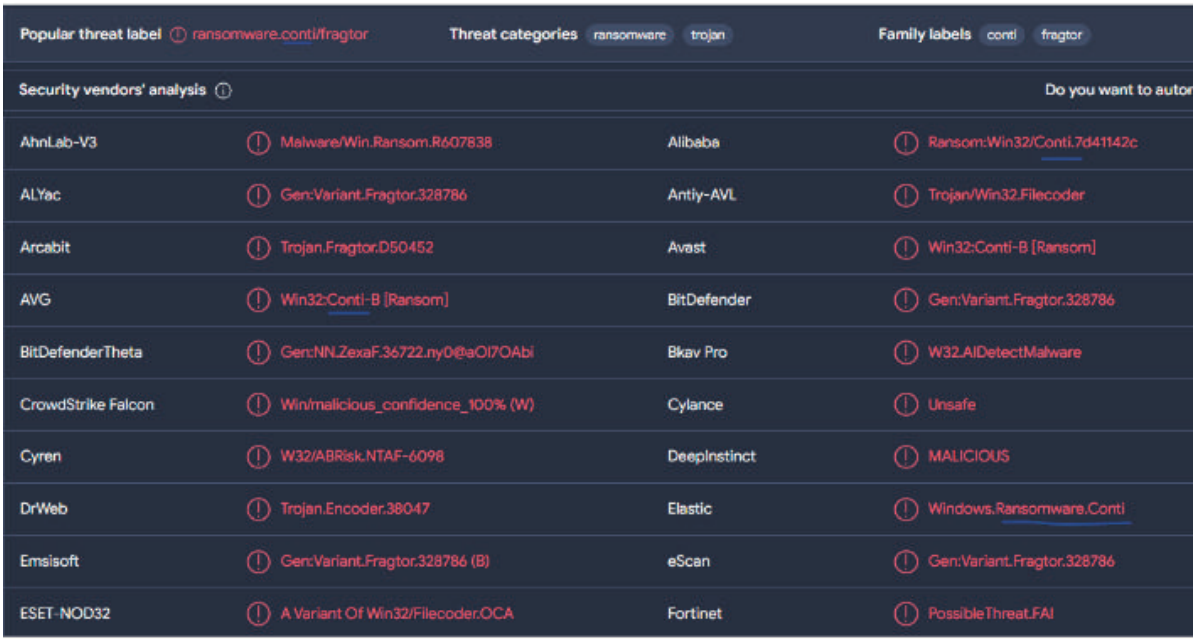


TABLA DE IMPORTACIONES

Se comprueba que es una variante de conti cuando nuestros investigadores hicieron un sandboxing el día 25/03/2023 en virus total, siendo el primer sample de este tipo analizado en dicha plataforma y que de acuerdo a la inteligencia se puede relacionar con el grupo de ransomware CONTI como se muestra en Figura List-16



History	
Creation Time	2023-09-22 07:47:53 UTC
First Submission	2023-09-25 16:49:30 UTC
Last Submission	2023-09-25 16:49:30 UTC
Last Analysis	2023-09-26 06:08:33 UTC



Popular threat label: ransomware.conti/fragtor	Threat categories: ransomware, trojan	Family labels: conti, fragtor	
Security vendors' analysis			Do you want to autor
AhnLab-V3	Malware/Win.Ransom.R607838	Alibaba	Ransom:Win32/Conti.7d41142c
ALYac	Gen:Variant.Fragtor.328786	Antiy-AVL	Trojan/Win32.Filecoder
Arcabit	Trojan.Fragtor.D50452	Avast	Win32:Conti-B [Ransom]
AVG	Win32:Conti-B [Ransom]	BitDefender	Gen:Variant.Fragtor.328786
BitDefenderTheta	Gen:NN.ZexaF.36722.ny0@aOI7OAbi	Bkav Pro	W32.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cyren	W32/ABRisk.NTAF-6098	DeepInstinct	MALICIOUS
DrWeb	Trojan.Encoder.38047	Elastic	Windows.Ransomware.Conti
Emsisoft	Gen:Variant.Fragtor.328786 (B)	eScan	Gen:Variant.Fragtor.328786
ESET-NOD32	A Variant Of Win32/Filecoder.OCA	Fortinet	PossibleThreat.FAI

Dentro de la investigación encontramos otro archivo nombrado por el atacante w3wp.exe (77c90f9bda9929274adcf2871cfa250334a531855577858a8ff78140a616f74a), este archivo realiza mucha de las funciones del archivo svchost.exe con la variante de que este archivo no realiza persistencia, ni directivas hacia objetos de AD usando remote thread para cifrar remotamente a los equipos.

IOCs

45.153.242.181
w3wp.exe (77c90f9bda9929274adcf2871cfa250334a531855577858a8ff78140a616f74a)
svchost.exe
(174ada6f6ab5b456affb3a05a4549d18d1de9bc0507e0e398f2e2609bba93fd0)
time.exe (e8cf5633a560471fd926ce6d59ef3cbf6fbdc2b9bfcfc4ada3bac31d79a51353)
TTPs:

Tactics	Tecniques
Initial Access	Exploit Public Facin Aplication
Execution	Native API User Execution
Persistence	Boot or Logon Autostart Execution Create account
Privilege escalation	Valid accounts Access token Manipulation
Defense evasion	Process Injection Domain Policy modification Group Policy modification
Credential Access	Credentials from password stores
Discovery	Network Service Discovery
Lateral movement	Remote Services
Command and control	Data encoding Encrypted channels
Exfiltration	Automated Exfiltration
Impact	Data encrypted for impact
Conti Ransomware	https://attack.mitre.org/software/S0575/

Dentro de la investigación encontramos otro archivo nombrado por el atacante w3wp.exe (77c90f9bda9929274adcf2871cfa250334a531855577858a8ff78140a616f74a), este archivo realiza mucha de las funciones del archivo svchost.exe con la variante de que este archivo no realiza persistencia, ni directivas hacia objetos de AD usando remote thread para cifrar remotamente a los equipos.

RECOMENDACIONES

- Aplicar filtrado de aplicaciones con respecto a los servicios publicados, como por ejemplo Aplicar WAF para recibir todas las peticiones.
- Aplicar NEXT generation Firewalls como los de Palo Alto Networks a nivel perimetral para agregar una capa de protección basados en las ultimas firmas de ataques a los servicios que están expuestos hacia internet.
- Aplicar un modelo zero trust con ayuda de los Next Generation Firewall Palo Alto para proteger el tráfico este-oeste.
- Tener herramientas XDR que ayuden a correlacionar y aplicar machine learning/Inteligencia artificial varias fuentes de información para aumentar eficacia y rapidez para detectar y responder los nuevos ataques, como lo puede hacer Cortex XDR.
- Monitoreo 24/7 de los incidentes generados en las herramientas XDR con equipos especializados ante detección y respuestas de incidentes de ciberseguridad. Desde SENTRIA te podemos ayudar a suplir esta necesidad
- Realiza cacería de amenazas proactiva de indicadores de compromiso y/o comportamientos de ataques. Desde SENTRIA te podemos ayudar a suplir esta necesidad

CYBER SQUAD 911

SENTRIA