Investigación

CBR-Investigación Conti

Referencia del informe:	**CBR-INV03**
Clasificación de la información:	**RESTRINGIDA**

Tabla de contenido

1 Control de versiones

N.º Versión	Fecha	Cambio	Autor
1.0	20/07/2022	Creación	Rosa García López

2 Introducción

Conti es considerado como uno de los grupos ransomware más exitosos. Este grupo comenzó a operar en febrero de 2020, cuando archivos maliciosos con la extensión ".conti" fueron detectados por los investigadores de Group-IB. Sin embargo, la primera versión de prueba del malware data en noviembre de 2019.

Conti utiliza el modelo de negocio conocido como ransomware-as-a-service (RaaS). Los desarrolladores del ransomware venden o alquilan su tecnología a miembros afiliados, quienes la usan para llevar a cabo los ataques. Este grupo utiliza la extorsión y presión social para forzarles a pagar el rescate. Podrían vender los datos al mayor postor, esto se indica a las víctimas anunciando que si no se ha pagado lo pedido y no ven sus datos publicados es porque han sido vendidos.

3 Características

En los diferentes análisis de Conti se observan las siguientes características:

- Se puede ejecutar por la línea de comandos con diferentes argumentos:
  - -p "*carpeta*" – Cifra los archivos de una carpeta en particular.
  - -m local – Cifra la máquina víctima con múltiples hilos.
  - -m net – Cifra las carpetas compartidas con múltiples hilos.
  - -m all – Cifra todo el contenido de la víctima como también las carpetas compartidas con múltiples hilos.
  - -m backups – No implementado (podría estar relacionado con el borrado de archivos de backups).
  - -size chunk – Modo para cifrar archivos grandes.
  - -log logfile – No implementado (parece ser que crea un archivo que registra la actividad del malware mientras se ejecuta).
  - -nomutex – No crea un mutex.
- Elimina los archivos Shadow copies de la máquina víctima.
- Usa los algoritmos criptográficos ChaCha8 y RSA para el cifrado de los archivos.

- Posee código basura para complejizar el análisis, pero que no modifica la lógica principal del malware.
- Tanto las cadenas de caracteres como los nombres de las API de Windows se encuentran ofuscadas con distintos algoritmos, y las dos se ofuscan en tiempo de ejecución.
- A los archivos cifrados se les añade la extensión `.QTBHS`.
- No cifra un archivo si termina con alguna de las siguientes extensiones: `.exe`, `.dll`, `.lnk`, `.sys`, `.msi` y `.bat`
- No cifra los archivos que se llamen readme.txt o CONTI_LOG.txt.
- No cifra los archivos que se encuentren en las siguientes carpetas: tmp, winnt, temp, thumb, $Recycle.Bin, Boot, Windows, Trend Micro, perflogs, Sophos y HitmanPro

4 Firmas recientes

SHA256
3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb
e49fd2651d5f3d5ffd999104841edd3e6e6dbd342507df6d2201720bdca65a74
6c2b5abc372e31cd7f8da045400abc0b10149f4f7b7def48a6bf9d0071f805d2
95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7
7f6dbd9fa0cb7ba2487464c824b6d7e16ace9d4cd15e4452df4c9a9fd6bd1907
d8158db5cbae0845b9ced65cc4a6581bfe08ba5361b1294b2dfb6ef4c711fd15
fb737da1b74e8c84e6d8bd7f2d879603c27790e290c04a21e00fbde5ed86eee3
e1b147aa2efa6849743f570a3aca8390faf4b90aed490a5682816dd9ef10e473
980cc58338038f70184403a98f1166b17938ebe362f373f4f366be1aaeecc923
41324493142b10db127217274e21df37f6ccd13f01a8d29d2b23b7b1463423a7

5 Distribución de TTPs

5.1 Initial Access

El acceso inicial consiste en técnicas que usan varios vectores de entrada para obtener su acceso inicial dentro de la red.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1190 – Exploit Public-Facing Application**: Los atacantes pueden intentar acceder al sistema explotando vulnerabilidades o bugs, en cualquier aplicación que tenga sockets abiertos y accesibles a través de internet. Algunas de las vulnerabilidades que Conti ha explotado en Fortinet Fortios son: CVE-2018-13379 y CVE-2018-13374.
- **T1133 – External Remote Services**: Los servicios remotos abiertos al exterior son el vector de entrada más común y fácil que utilizan los grupos ransomware para ganar el acceso inicial en el sistema. Servicios remotos como VPNs, Windows Remote Management y otros mecanismos de acceso, permiten a los usuarios contectarse a la red interna de la empresa desde una localización externa.
  En varios análisis se ha determinado que Conti es uno de los grupos que utiliza esta táctica.
- **T1566.001 – Phishing: Spearphishing Attachment**: Esta táctica es una variante del *phishing* en la que el malware está adjuntado en un archivo del email y normalmente depende de la ejecución del usuario. Conti ha mandado correos de phishing clásicos en el que adjuntaba un archivo malicioso. Mayormente han sido archivos .doc o .xlsx con scripts incrustados y pidiendo al usuario que pinchara en “Permitir contenido”.
- **T1566.002 – Phishing: Spearphishing Link**: Este ransomware puede infectar a través de TrickBot, que ha sido enviado a través de links maliciosos en emails de phishing.
- **T1078 – Valid Accounts**: Los integrantes de Conti han sido observados ganando acceso sin autorizar a través de credenciales robadas de RDP.

5.2 Execution

Consiste en técnicas que resultan en código controlado por el atacante que es ejecutado en un sistema local o remoto.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1059.001 – Command and Scripting Interpreter**: Conti hace uso de las interfaces de comando para algunos de sus objetivos.
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell**: La interfaz de comandos de Windows (cmd) puede ser usada para controlar casi todos los aspectos del sistema. Conti ha utilizado opciones de la consola de comandos para controlar cómo escanea y encripta los archivos.

- **T1106 – Native API**: Las API nativas proporcionan un medio controlado para llamar a los servicios del sistema operativo de bajo nivel dentro del kernel. Conti hace llamadas a varias APIs durante su ejecución.

- **T1204.002 – User Execution: Malicious File**: El atacante depende de que el usuario abra un archivo malicioso, esto conllevará la ejecución de código. Conti utiliza una técnica clásica, en la que un documento con código malicioso incrustado llega a generar una shell de Windows cuando es ejecutado.

- **T1047 – Windows Management Instrumentation**: WMI es una herramienta de administración que proporciona un entorno uniforme para acceder los componentes del sistema Windows. Conti ha usado esta característica para esparcir un beacon de CobaltStrike con el comando:

```
wmic /node:<IP _ address> /user:"<domain>\<user>"
/password:"<password>" process call create "cmd /c <cobaltstrike _
path>"
```

5.3 Persistence

Consiste en técnicas usadas por los atacantes para mantener acceso al sistema, aunque este sea reiniciado, cambien las credenciales, o se produzcan otras interrupciones que puedan finalizar su acceso.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1098 – Account Manipulation**: La manipulación de cuentas incluye cambiar las contraseñas de cuentas comprometidas, añadir cuentas a grupos con más permisos, modificar las políticas de contraseñas y cualquier acción que preserve el acceso del atacante a la cuenta. Conti ejecuta comandos para crear cuentas y añadirlas al grupo de administradores.

- **T1197 – BITS Jobs**: Proveen un mecanismo de persistencia al ejecutar payloads. También pueden ser útiles a la hora de evitar ser detectado, pues se ejecutan en segundo plano. Conti lo utiliza para moverse lateralmente ejecutando:

```
Bitsadmin /transfer debjob /download
\\[localuser]\C$\Windows\[Conti].dll C:\Windows\[conti].dll
```

- **T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder**: Los atacantes usan esta técnica para mantener la persistencia en el entorno de la víctima. Instalar el ransomware como Registry Run Key o añadirlo a la carpeta StartUp es muy común.

- **T1543.003 – Create or Modify System Process: Windows Service**: Consiste en crear o modificar servicios de Windows para ejecutar repetidamente payloads como parte de resistencia, ya que se ejecutan en segundo plano. Conti utiliza el framework CobalStrike, cuyos beacons son instalados como servicios.

- **T1053.005 – Scheduled Task/Job: Scheduled Task**: Los atacantes abusan del programador de tareas de Windows para programar tareas de ejecución inicial o recurrente de código malicioso. Conti usa TrickBot RAT para crear tareas programadas.

5.4 Privilege Escalation

Consiste en técnicas que usan los adversarios para ganar permisos de mayor nivel en un sistema o red.

La técnica que utiliza, o ha utilizado, Conti de esta táctica es:

- **T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control**: Para escalar privilegios, Conti hace uso generalmente de los frameworks Cobalt Strike o PowerShell Empire.
- **T1134 – Access Token Manipulation**: Los atacantes modifican tokens de acceso para operar como otro usuario y traspasar los controles de seguridad. Conti emplea esta técnica ajustando los privilegios del token de acceso a través de la función AdjustTokenPrivileges() de WinAPI.
- **T1055.001 – Process Injection: Dynamic-link Library Injection**: Conti ha cargado un DLL encriptado en la memoria y luego lo ha ejecutado.
- **T1068 – Exploitation for Privilege Escalation**: Los atacantes pueden obtener permisos de alto nivel al explotar servidores web de cara al público para el acceso inicial. Conti ha explotado vulnerabilidades de Log4j, PrintNightmare o Zerologon para escalar privilegios.

5.5 Defense Evasion

Consiste en técnicas usadas por los atacantes para evitar ser detectados tras comprometer a la víctima.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1140 – Deobfuscate/Decode Files or Information**: Los atacantes pueden usar archivos ofuscados o información para esconder los artefactos usados en una intrusión de un análisis. Conti utiliza un cargado de escenario ofuscado en base 64, “CompareForFor.hta”.
- **T1562.001 – Impair Defenses: Disable or Modify Tools**: El ransomware deshabilita las características de seguridad para asegurarse de que la ejecución de su muestra y la encriptación de archivos no será bloqueada. Conti utiliza PowerShell para desactivar las características de Windows Defender:

```
>> powershell New-ItemProperty -Path
HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender -Name
DisableAntiSpyware -Value 1 -PropertyType DWORD -Force

>> powershell Set-MpPreference -DisableRealTimeMonitoring $true

>> powershell Uninstall-WindowsFeature -Name Windows-Defender
```

- **T1562.004 – Impair Defenses: Disable or Modify System Firewall**: Conti modifica el firewall del sistema para conseguir sobrepasar las restricciones de seguridad de la red. Conti activa la aplicación de Escritorio Remoto a través de *netsh*:

```
netsh advfirewall firewall set rule group=”Remote Desktop” new
enable=yes
```

- **T1070.001 – Indicator Removal on Host: Clear Windows Event Logs**: Los atacantes limpian los logs para ocultar evidencia de su intrusión. Esto hace el trabajo del equipo de respuesta ante incidentes más difícil.
- **T1036 – Masquerading**: Los atacantes intentan manipular las características de sus herramientas para hacerlas parecer legítimas o benignas. Conti trata de pasar por un programa estándar del sistema o software legítimo.
- **T1055 – Process Injection**: Los atacantes inyectan código en procesos siendo ejecutados con el fin de evadir las defensas basadas en procesos, y también para elevar privilegios. Conti crea un proceso en un estado suspendido, la memoria es desmapeada y reemplazada con código malicioso; esto se conoce como *process hollowing*.
- **T1218 – System Binary Proxy Execution**: Los atacantes pueden sobrepasar las defensas basadas en procesos y/o firmas mediante la delegación de ejecución de su contenido malicioso en archivos binarios firmados o confiables. Conti usa archivos firmados por Microsoft: mshta.exe y regsvr.exe.

5.6 Credential Access

Consiste en técnicas para robar credenciales como nombres de cuentas y contraseñas.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1110 – Brute Force**: Los atacantes pueden usar técnicas de fuerza bruta para obtener acceso a cuentas cuando no conocen la contraseña o han obtenido los hashes de las contraseñas.
- **T1003.001 - OS Credential Dumping: LSASS Memory**: Los atacantes intentan acceder a material con credenciales guardado en el proceso de memoria del Local Security Authority Subsystem Service (LSASS). Conti usa esta técnica a través de los servicios DLL que tiene Windows.
- **T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting**: Contib ha usado los ataques de Kerberos para intentar obtener el hash del usuario administrador.

5.7 Discovery

Consiste en técnicas que permiten al atacante obtener conocimiento sobre nuestro sistema y red interna.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1087 – Account Discovery**: Los atacantes tratan de obtener un listado de cuentas en un sistema o entorno. Un comando comúnmente usado es:

```
whoami /groups
```

- **T1083 – File and Directory Discovery**: Se trata de una técnica que implica enumerar archivos y directorios para determinar si ciertos objetos deberían ser encriptados/robados o no. Los troyanos de ransomware generalmente hacen una búsqueda automática de archivos con determinadas extensiones o nombres.

- **T1135 - Network Share Discovery**: Con el objetivo de encriptar máquinas cercanas y tener más víctimas, los atacantes buscan carpetas y discos compartidos en sistemas remotos.
- **T1057 – Process Discovery**: Conti hace uso de métodos que enumeran procesos activos para formar los siguientes pasos del ataque.
- **T1018 – Remote System Discovery**: Consiste en enumerar los dispositivos remotos que pertenecen a la red comprometida. Algunos de los comandos usados son:

```
>> net view /all
>> net view /all /domain
>> dsquery subnet -limit 0
>> nltest /domain _ trusts
>> nltest /dclist
```

- **T1049 – System Network Connections Discovery**: Para ganar acceso al sistema, los atacantes normalmente buscan conexiones activas en el sistema en las que se puedan mover y encriptar. Típicamente usan los comandos:

```
>> net session
>> net use
>> netstat -ano
>> query session
```

5.8 Lateral Movement

Consiste en técnicas que utilizan los atacantes para entrar y controlar sistemas remotos en una red.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1570 – Lateral Tool Transfer**: Conti hace uso de RDP para propagar el ransomware o las herramientas usadas, dentro de la red. Se les ha visto utilizar bitsadmin con el comando:

```
Bitsadmin /transfer debjob /download
\\[localuser]\C$\Windows\[Conti].dll C:\Windows\[Conti].dll
```

- **T1021.001 – Remote Services: Remote Desktop Protocol**: Tras acceder al sistema, el grupo puede continuar moviéndose en la red con el uso de conexiones de escritorio remoto. Conti activa el protocolo de escritorio remoto en el Registro de Windows y en la configuración del cortafuegos:

```
>> reg add “HKLM\System\CurrentControlSet\Control\Terminal Server” /v
“fDenyTSConnections” /t REG_DWORD /d 0 /f
>> netsh advfirewall firewall set rule group=”Remote Desktop” new
enable=yes
```

- **T1021.002 – Remote Services: SMB/Windows Admin Shares**: Conti tiene una opción en la línea de comandos que encripta servicios remotos a través de SMB.

5.9 Command and Control

Consiste en técnicas que usan los atacantes para comunicarse con sistemas bajo su control dentro de la red de la víctima.

La técnica que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1071.001 - Application Layer Protocol: Web Protocols**: Conti ha descargado QBot a través de un documento de Excel que estaba adjunto en un email de phishing.

```
Image_path: $programfiles\Microsoft Office\Office14\EXCEL.EXE
URL: hxxp://101.99.95[.]143/44657.5824381944.dat
```

5.10 Exfiltration

Consiste en técnicas cuya finalidad es robar datos de tu red.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1041 – Exfiltration Over C2 Channel**: Para realizar la doble extorsión, Conti envía la información robada a través de su canal primario C2.
- **T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage**: Exfiltrar datos a un servidor en la nube puede verse como algo legítimo, por lo que es una ventaja para los atacantes. Conti utiliza “rclone”, un programa de código abierto, para mandar los archivos a la nube.

5.11 Impact

Consiste en técnicas que alteran la disponibilidad o comprometan la integridad mediante la manipulación de los procesos comerciales y operacionales.

Las técnicas que utiliza, o ha utilizado, Conti de esta táctica son:

- **T1486 – Data encrypted for impact**: Conti puede usar *CreateIoCompletionPort()*, *PostQueuedCompletionStatus()* y *GetQueuedCompletionPort()* para encriptar archivos rápidamente, excluyendo los que tengan extensión .exe, .dll y .lnk. Ha utilizado una llave AES-256 diferente para cada archivo incluyendo una llave publica RAS-4096 única para cada víctima.
- **T1490 – Inhibit System Recovery**: En esta técnica los atacantes hacen todo lo posible para que no se pueda recuperar la información si no es negociando con ellos. Para conseguirlo, eliminan copias de seguridad, las copias shadow y desactivan las características de reparación y recuperación automáticas.
- **T1489 – Service Stop**: Conti ha sido observado parando servicios con “taskkill.exe”. Algunos comandos son:

```
>> taskkill /f /im vee
```

```
>> taskkill /f /im postg
```

6 Información filtrada

6.1 Manual

El 5 de agosto de 2021. El usuario conocido como *m1Geelka* en un foro, compartió un link con documentos relacionados con Conti. Esta acción fue causa de, según el usuario, un pago más bajo del esperado por su trabajo.

Entre estos documentos se encuentra un manual, titulado "CobaltStrike Manuals_V2 Active Directory", en el que los integrantes de Conti recogen una guía, bastante detallada, con las posibles acciones para llevar a cabo un ataque. Este manual podría ser seguido por afiliados al grupo aún teniendo un bajo nivel.

Además, también dio a conocer las direcciones IP de los canales C2 que estaba usando Conti en ese momento:

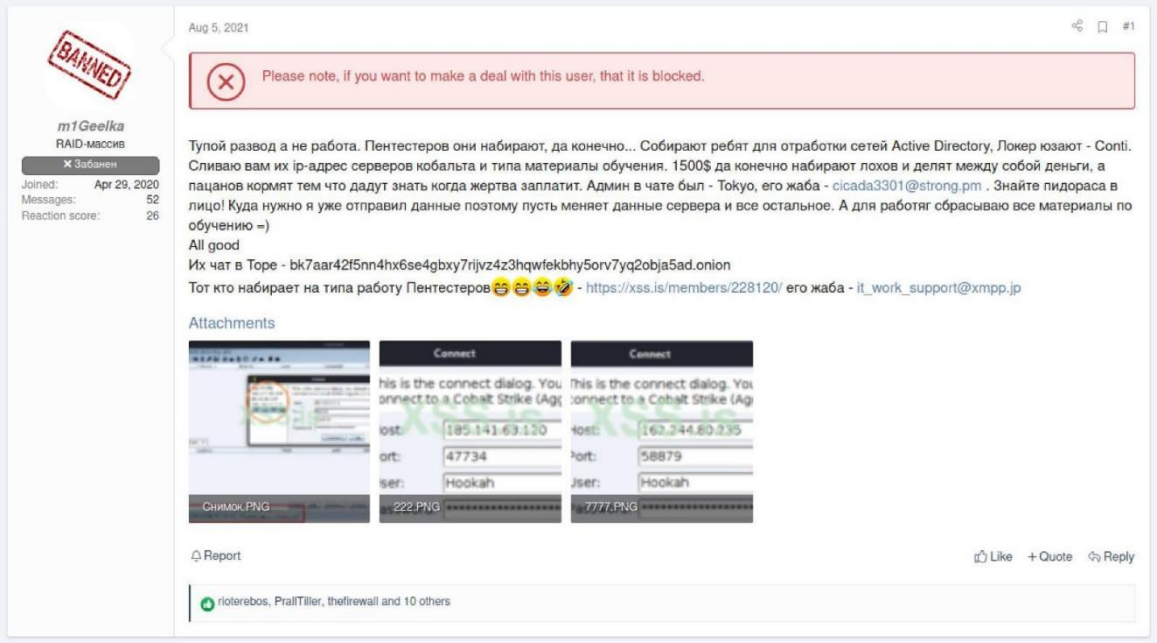

Ilustración 1 - Post con los documentos filtrados

Un mes después de esta noticia, un equipo de Cisco Talos publicó los documentos completamente traducidos, incluyendo el manual en formato PDF y un ZIP con todos los archivos, proporcionando información de gran valor para los expertos en ciberseguridad.

6.2 Código fuente y chats

El 27 de febrero de 2022, un usuario conocido como *@ContiLeaks* en Twitter filtró 393 archivos JSON que contienen aproximadamente 60.000 mensajes internos de los chats privados de Conti y

Ryuk, a raíz del desacuerdo con un mensaje que mostraba el apoyo de Conti hacia Rusia en la guerra.

Estas conversaciones van desde el 21 de enero de 2021 hasta el 27 de febrero de 2022. Se encuentra información de gran valor, como direcciones de carteras para criptomonedas, la organización de la banda, la evasión de las fuerzas de la ley, cómo llevan a cabo sus ataques y mucho más.

Al día siguiente, el mismo usuario compartió más archivos entre los que se encontraban el código fuente del panel administrativo, capturas de pantalla de los servidores de almacenamiento, etc. La parte del código estaba protegida por contraseña, que no fue compartida por el usuario, pero sí crackeada por un investigador más tarde.

El código proporcionó un gran conocimiento sobre el funcionamiento del malware y afecta positivamente para los investigadores de seguridad. Sin embargo, también proporciona a otros grupos la posibilidad de copiarlo e iniciar más ataques.

6.3 Versión 3 de Conti

El mismo usuario, *@ContiLeaks*, filtró el 20 de marzo de 2022 una copia de la versión 3 del código fuente de Conti; que crea los ejecutables para encriptar y desencriptar los archivos.

Tras analizar el código, han concluido que existe muy poca mejora respecto a la anterior versión y es un paso hacia atrás en cuanto a la calidad del código. Lo más probable es que los cambios que se hayan introducido fueran hechos por otra persona distinta del programador original.

Esta información permite a los profesionales poder detectar una brecha o infección más rápido y, así, poder frenar la propagación del ransomware.

7 Cese de actividad

El 19 de mayo de 2022, el panel de administración de la página oficial de Conti, *Conti News*, fue cerrado. El servicio de negociaciones también fue cerrado, mientras que el resto de la infraestructura; chats, servidores, correos, etc., sufrieron un reinicio masivo.

Aunque esto parezca una decisión repentina, realmente ha sido un acto calculado por parte de la banda para, según expertos, volver con una nueva marca. Debido a las alegaciones públicas del grupo en favor de Rusia los primeros días de la invasión a Ucrania, Conti no podía recibir ingresos. Desde febrero de 2022 Conti no recibió casi ningún pago, mientras que el ransomware era cada vez detectado con más facilidad y desplegado con menos frecuencia. La única opción posible seria optar por renovar su imagen.

Como acto final de la banda Conti tenía que dar un espectáculo, y ese fue el ataque masivo al gobierno de Costa Rica el 8 de mayo de 2022; que fue declarado como una emergencia nacional por el presidente Rodrigo Chaves.

Sin embargo, esto no significa que la organización se haya disuelto. Los miembros han pasado ha formar parte de otros grupos que están afiliados de algún modo con Conti, algunos de ellos son: Hive, AlphV/BlackCat, HelloKitty/FiveHands y AvosLocker.

8 Limpieza

Actualmente no existe una herramienta de desencriptación fiable que se capaz de recuperar los archivos cifrados. Esto nos deja con las opciones de recuperar la información a través de una copia de seguridad.

Para estar seguros de que nuestro sistema está libre de ransomware o para simplemente detectarlo, podemos usar alguna de las siguientes herramientas: Kaspersky Anti-Ransomware, GridinSoft, Bitdefender Antivirus, etc.

9 Mitigación

Existe una vulnerabilidad en el ransomware de Conti que permite parar la ejecución antes de que encripte los archivos.

Se trata de una vulnerabilidad DLL Hijacking, en la que debemos poner el archivo DLL en una carpeta desde la que creamos que podría ejecutarse el ransomware. Esta mitigación solo funcionaria en los sistemas de Windows, y es posible gracias a que, para ser ejecutado, el ransomware busca y carga en memoria los archivos DLL necesarios.

El exploit se encuentra publicado en Malvuln y también hay un vídeo en el que se muestra un ejemplo de su uso con Conti. Además de Conti, esta vulnerabilidad afecta a los grupos REvil, BlackBasta, LockBit y AvosLocker.

10 IOCs

10.1 Servicios que para

Conti hace uso del comando `cmd.exe /c net stop %s /y`, sustituyendo %s por el nombre del servicio, para parar los servicios de la siguiente lista:

“Acronis VSS Provider”, “Enterprise Client Service”, “Sophos Agent”, “Sophos AutoUpdate Service”, “Sophos Clean Service”, “Sophos Device Control Service”, “Sophos File Scanner Service”, “Sophos Health Service”, “Sophos MCS Agent”, “Sophos MCS Client”, “Sophos Message Router”, “Sophos Safestore Service”, “Sophos System Protection Service”, “Sophos Web Control Service”, “SQL Backups”, “SQLsafe Backup Service”, “SQLsafe Filter Service”, “Symantec System Recovery”, “Veeam Backup Catalog Data Service”, “Zoolz 2 Service”, AcronisAgent, AcrSch2Svc, Antivirus, ARSM, AVP, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDeviceMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, bedbg, DCAgent, EhttpSrv, ekrn, EPSecurityService, EPUpdateService, EraserSvc11710, EsgShKernel, ESHASRV, FA_Scheduler,

ISAdmin, IMAP4Svc, KAVFS, KAVFSGT, kavfsslp, klnagent, macmnsvc, masvc, MBAMService, MBEndpointAgent, McAfeeEngineService, McAfeeFramework, McAfeeFrameworkMcAfeeFramework, McShield, McTaskManager, mfemms, mfevtp, MMS, mozyprobackup, MsDtsServer, MsDtsServer100, MsDtsServer110, MSExchangeES, MSExchangeIS, MSExchangeMGMT, MSExchangeMTA, MSExchangeSA, MSExchangeSRS, msftesql$PROD, MSOLAP$SQL_2008, MSOLAP$SYSTEM_BGC, MSOLAP$TPS, MSOLAP$TPSAMA, MSSQL$BKUPEXEC, MSSQL$ECWDB2, MSSQL$PRACTICEMGT, MSSQL$PRACTTICEBGC, MSSQL$PROD, MSSQL$PROFXENGAGEMENT, MSSQL$SBSMONITORING, MSSQL$SHAREPOINT, MSSQL$SOPHOS, MSSQL$SQL_2008, MSSQL$SQLEXPRESS, MSSQL$SYSTEM_BGC, MSSQL$TPS, MSSQL$TPSAMA, MSSQL$VEEAMSQL2008R2, MSSQL$VEEAMSQL2008R2, MSSQL$VEEAMSQL2012, MSSQLFDLauncher, MSSQLFDLauncher$PROFXENGAGEMENT, MSSQLFDLauncher$SBSMONITORING, MSSQLFDLauncher$SHAREPOINT, MSSQLFDLauncher$SQL_2008, MSSQLFDLauncher$SYSTEM_BGC, MSSQLFDLauncher$TPS, MSSQLFDLauncher$TPSAMA, MSSQLSERVER, MSSQLServerADHelper, MSSQLServerADHelper100, MSSQLServerOLAPService, MySQL57, NetMsmqActivator, ntrtscan, OracleClientCache80, PDVFSService, POP3Svc, ReportServer, ReportServer$SQL_2008, ReportServer$SYSTEM_BGC, ReportServer$TPS, ReportServer$TPSAMA, RESvc, sacsvr, SamSs, SAVAdminService, SAVService, SDRSVC, SepMasterService, ShMonitor, Smcinst, SmcService, SMTPSvc, SNAC, SntpService, sophossps, SQLAgent$BKUPEXEC, SQLAgent$CITRIX_METAFRAME, SQLAgent$CXDB, SQLAgent$ECWDB2, SQLAgent$PRACTTICEBGC, SQLAgent$PRACTTICEMGT, SQLAgent$PROD, SQLAgent$PROFXENGAGEMENT, SQLAgent$SBSMONITORING, SQLAgent$SHAREPOINT, SQLAgent$SOPHOS, SQLAgent$SQL_2008, SQLAgent$SQLEXPRESS, SQLAgent$SYSTEM_BGC, SQLAgent$TPS, SQLAgent$TPSAMA, SQLAgent$VEEAMSQL2008R2, SQLAgent$VEEAMSQL2008R2, SQLAgent$VEEAMSQL2012, SQLBrowser, SQLSafeOLRService, SQLSERVERAGENT, SQLTELEMETRY, SQLTELEMETRY$ECWDB2, SQLWriter, SstpSvc, svcGenericHost, swi_filter, swi_service, swi_update, swi_update_64, TmCCSF, tmlisten, TrueKey, TrueKeyScheduler, TrueKeyServiceHelper, UI0Detect, VeeamBackupSvc, VeeamBrokerSvc, VeeamCatalogSvc, VeeamCloudSvc, VeeamDeploymentService, VeeamDeploySvc, VeeamEnterpriseManagerSvc, VeeamHvIntegrationSvc, VeeamMountSvc, VeeamNFSSvc, VeeamRESTSvc, VeeamTransportSvc, W3Svc, wbengine, WRSVC.

10.2 IPs maliciosas

- 85.93.88.165
- 82.118.21.1
- 185.141.63.120
- 162.244.80.235
- 23.106.160.174
- 23.82.140.137

10.3 Dominios

badiwaw[.]com	fipoleb[.]com	kipitep[.]com	pihafi[.]com	tiyuzub[.]com
balacif[.]com	fofudir[.]com	kirute[.]com	pilagop[.]com	tubaho[.]com
barovur[.]com	fulujam[.]com	kogasiv[.]com	pipipub[.]com	vafici[.]com

basisem[.]com	ganobaz[.]com	kozoheh[.]com	pofifa[.]com	vegubu[.]com
bimafu[.]com	gerepa[.]com	kuxizi[.]com	radezig[.]com	vigave[.]com
bujoke[.]com	gucunug[.]com	kuyeguh[.]com	raferif[.]com	vipeced[.]com
buloxo[.]com	guvafe[.]com	lipozi[.]com	ragojel[.]com	vizosi[.]com
bumoyez[.]com	hakakor[.]com	lujecuk[.]com	rexagi[.]com	vojefe[.]com
bupula[.]com	hejalij[.]com	masaxoc[.]com	rimurik[.]com	vonavu[.]com
cajeti[.]com	hepide[.]com	mebonux[.]com	rinutov[.]com	wezeriw[.]com
cilomum[.]com	hesovaw[.]com	mihojip[.]com	rusoti[.]com	wideri[.]com
codasal[.]com	hewecas[.]com	modasum[.]com	sazoya[.]com	wudepen[.]com
comecal[.]com	hidusi[.]com	moduwoj[.]com	sidevot[.]com	wuluxo[.]com
dawasab[.]com	hireja[.]com	movufa[.]com	solobiv[.]com	wuvehus[.]com
derotin[.]com	hoguyum[.]com	nagahox[.]com	sufebul[.]com	wuvici[.]com
dihata[.]com	jecubat[.]com	nawusem[.]com	suhuhow[.]com	wuvidi[.]com
dirupun[.]com	jegufe[.]com	nerapo[.]com	sujaxa[.]com	xegogiv[.]com
dohigu[.]com	joxinu[.]com	newiro[.]com	tafobi[.]com	xekezix[.]com
dubacaj[.]com	kelowuh[.]com	paxobuy[.]com	tepiwo[.]com	docns[.]com
fecotis[.]com	kidukes[.]com	pazovet[.]com	tifiru[.]com	tapavi[.]com

10.4 Herramientas y archivos

Muchas de las herramientas que utiliza Conti son legítimas, por lo que es recomendable monitorizar su uso.

Herramienta	Archivos	SHA256
AdFind	СНЯТИЕ-AD.rar AdFind.exe backup.bat script.sh p.bat	b21599f39223409e059cd2066a80832f305854e7d12b5ed3401d47a32ac962eb b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682 794a5621fda2106fcb94cbd91b6ab9567fb8383caa7f62febafcf701175f2b91 085e87a6694edafd9a614a1f1143eb85233c04afbe9f84c89ebe5aebcd14546f 047c2d5a6cf769c33e019c0b576aef702cae77f3418f0aeba0706467be5ba681
Antivirus Removal Tools	Bitdefender_2019_Uninstall_Tool.exe trendmicro pass AV remove.bat sophos remvDIEsophos.bat sophos remvremovesophos.bat	269bea10e27d697a849b28ed0b688b8a2b5c85d65341bde1383c14876291d7c5

	sophos remvuninstallSophos.bat gmer.exe PCHunter32.exe PCHunter64.exe PowerTool.exe PowerTool64.exe 3 # AV.7z	
Cobalt Strike	agscript BaseArtifactUtils.class c2lint cobaltstrike cobaltstrike.auth cobaltstrike.jar cobaltstrike.store cs.jar hook.jar icon.jpg license.pdf ListenerConfig.class Peclone readme.txt start.bat start.sh teamserver update update.jar /third-party/README.winvnc.txt /third-party/winvnc.x64.dll	5ea267958786999986413bd982227f77716acb1f09d02ea56571631269dbdf95 75584d0477d5340b898d2fc1eb369516b76478359e7603eba9fcb615a75247af 78d82b72aae1d847c64745a932bce927823337de58852833e8cafca168eb4366 3a3725bf0cca3fc3d641aed0a1280b7d957aa5c872223f1b6320f315bdea457d 27aa9643628a7494ad3daa969c287b4119bbfdfffa943acfe2c866e1b9d965ea 1cdfa75b103f4b3218a9f6ddec137a5438c5e6571151d0979c60d96dfbbf9231 e25f83836e90fe17ed5d57516219373f0c4dcf0210638501223b63091d1fc6c3 3c4eb1e68c36e1287f0ed9c9a4470b95cf8f25b901d502fd9f5ccedec7d2ef54 6b098b82a0ff28c9bc0f812856eb5e2a861285d9ce12f3c7374542dc3d3acfbd c20d8ce3809123923b8897c97f251a766b5b56b61bd89134cb986ff10c2a309e 47060339e9d434f361ea750916a3980bd308995c4980c91e069d0b7a664a91af 340e3250b9d4717ca09543e34db19f5614b3bb84e93f3b6e0b467856455d2735

	/third-party/winvnc.x86.dll enhancement-chain.7z enhancement_chain.cna README.md	a29b4969c1f6c7759d6f94780145e126a8d67812fa388239a595472f1a9f3b13 19bc4b2b9704a5b4aa2edef5477219cd97052833f2fc2112ec6ecf9a9027ea35 e9b33a2f96b60f710e14d29cb38371b587094cfc4378276eebb9701d74cd3f71 1a0296704d9c3af491b8910ca7461d50e913c85b40c6620650ee24160849a625 3481ec6c99e3b78793538a3a5b818384355af4eefc9624ec2d66ab96e1357aac 92320d2f875e02f3c5f989926b1af60f20caea0034a4728d2f898ba8bafada3f 3f164991219c1804afa1fb75ee79d5cbfc0100ea71a90840cbad7352838a637b 627719d254c8168c56c8fbd40c88fbb65ebe141995b8c65763103aa07e117d47 13feaa32e4b03ede8799e5bee6f8d54c3af715a6488ad32f6287d8f504c7078b c50183eed715ec2392249e334940acf66315797a740a8fe782934352fed144c6 6a659500d1a672ad2d57cc0b004ea40b1479ab4b968858ba873e4def851d62bd 760664d7f0770ab440c8f24cd48c132372fbebfe6338c59801000613a0f4b4fe d440e4494adcfd94004e9ead2adcaaaf22696c71fc51246b881d628567ce1111
Empire Kerberoast	Kerber-ATTACK.rar command.txt Invoke-Kerberoast.ps1	abbe373077c72125901669d1b9f74b9eecd95eeda2c3b794197a20ea49cd25c0 495da9bb972019fae2c8a4d38846e15b9c364ef7189377f2c93b86791a1b210d 4729c83292e034642fd1081ddd4d0329bc9f57b9be989b647a025ffacdd55036
Proxifier	ProxifierPE.zip Helper64.exe	68e1b13bbe2a1de32c41a2db53999b9207ee7dbdc042e19cabd83cab5ef785a6

	Proxifier.exe ProxyChecker.exe PrxDrvPE64.dll PrxDrvPE.dll	167ecba4e15f0310770f265b0fbb00aaf3c4f04ee17e1c0cc26304152e8a1f4f 271fcf35f2da45bd6ea567f86cd1ec5179905f2bdd70c392aad76433890a525b 5527dc7eac16fbc16e55829245f0d0fcb3f8d44b962d314fb5a934a804802143 1664da61de30fa7103ee5ef09c9f59a117aa0437ee35f800e722097f38ca27c9 8dc3afb39efabc780f2272b33cb0f8b42504991edbfe5f32ecce6abe10d0afe7
Rclone	2load.txt rclone.conf rclone.exe rclonemanager.ps1 рклон.txt рклон.zip	861bc2cf05107d91b03406231e1e04839c7ed7e0e325f95d68b28f61a202fbc8 d47e2b72f71a35a201156f6611a934b391d52629a378587fb67bbb351dd50269 9b5d1f6a94ce122671a5956b2016e879428c74964174739b68397b6384f6ee8b 1f7b6fc3326be16f1847517d53bbf44f024b3cc8bccf69c59e107073db82ae02 1da5ea82ddc736eefb5e014ab55ba1ee340c71474af11067666de9cfb8c1579b ba110536613c50460ff5be6413d2f58bbe80ba3fee809ff6a27a2c7d13a47e91
Router Scan	Routerscan.7z auth_basic.txt auth_digest.txt auth_form.txt config.ini exclusions.txt filter.txt libeay32.dll librouter.dll msvcr100.dll	b875051a6d584b37810ea48923af45e20d1367adfa94266bfe47a1a35d76b03a 1729fa47ede6a8b5046fef6c538431d4e8bb9020d9124e20c872e01495f91fb6 86db3629d98f47ea078ee41b54f2833bfbd5f632d0fce3b342e099aad368421d 91ae5e6459a40c8084be102693a8c09d5179a3e78b8a11860cce6e69ca533623 307b3453bff0e5c2a7f5a677b6c1a64a455850d6d18952d5061a3649fbe09666 e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

	ports.txt ranges.txt RouterScan.exe RouterScan.log ssleay32.dll wlanpass.txt /pixiewps/LICENSE.md /pixiewps/pixiewps.exe /pixiewps/pthreadGC2.dll pixiewps/README.md /src/demoapp/demo.dpr /src/demoapp/demo.exe	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 7dd77348867a776967eb573c31c4b32211d3950bb3392187c30860f52538cab2 740e97254ae4104a588557e9d5abbe3a75896efe87e291201f49eb64c81dfc45 60c06e0fa4449314da3a0a87c1a9d9577df99226f943637e06f61188e5862efa 62440c93be34b792656b3c66ada73a17aea6d8260590f1cd75bf338e7893414b a521b9bfd7b469d84a7910efdc8b385f087d85f3874ebe37c0c7059e0a23b7ba 18229920a45130f00539405fecab500d8010ef93856e1c5bcabf5aa5532b3311 7d06d988198e18dadf31816ba834dba9c0c333009bd14b8cdea3fcb2fcabc519 9c2aaf899342146ef6912e337bf893bc2f6835e66a8bcce431df5c134c4ba887 2988be6f3413a90106932f3fc8d32d62b459289846150b75cf5e0831c980cf6b 2893b648d0e972e6c5dede0919ab35ad13e9a244c0685822601f93310e73724e b91166d5623d4077003ae8527e9169092994f5c189c8a3820b32e204b4230578 3b59889ee4189c7e2077e35c3f9884d09cd6bc50b7007622bb3e6a4def882c5e 9940cec1ad427946a67ec5b3b15f022cc64acea99da179457a117d706ec14207 0b1401a84b1fe4b7e6676c5c300643c025dfdf89e57b0bde2c67fca2d0ef4ab7 3653d87909a0315231d2adcbf3316be0d088cfd72abab00911a3afa42444e1ad

11 Matriz del MITRE ATT&CK pintada

about

Conti

Capa con las tácticas y técnicas que usa el ransomware Conti.

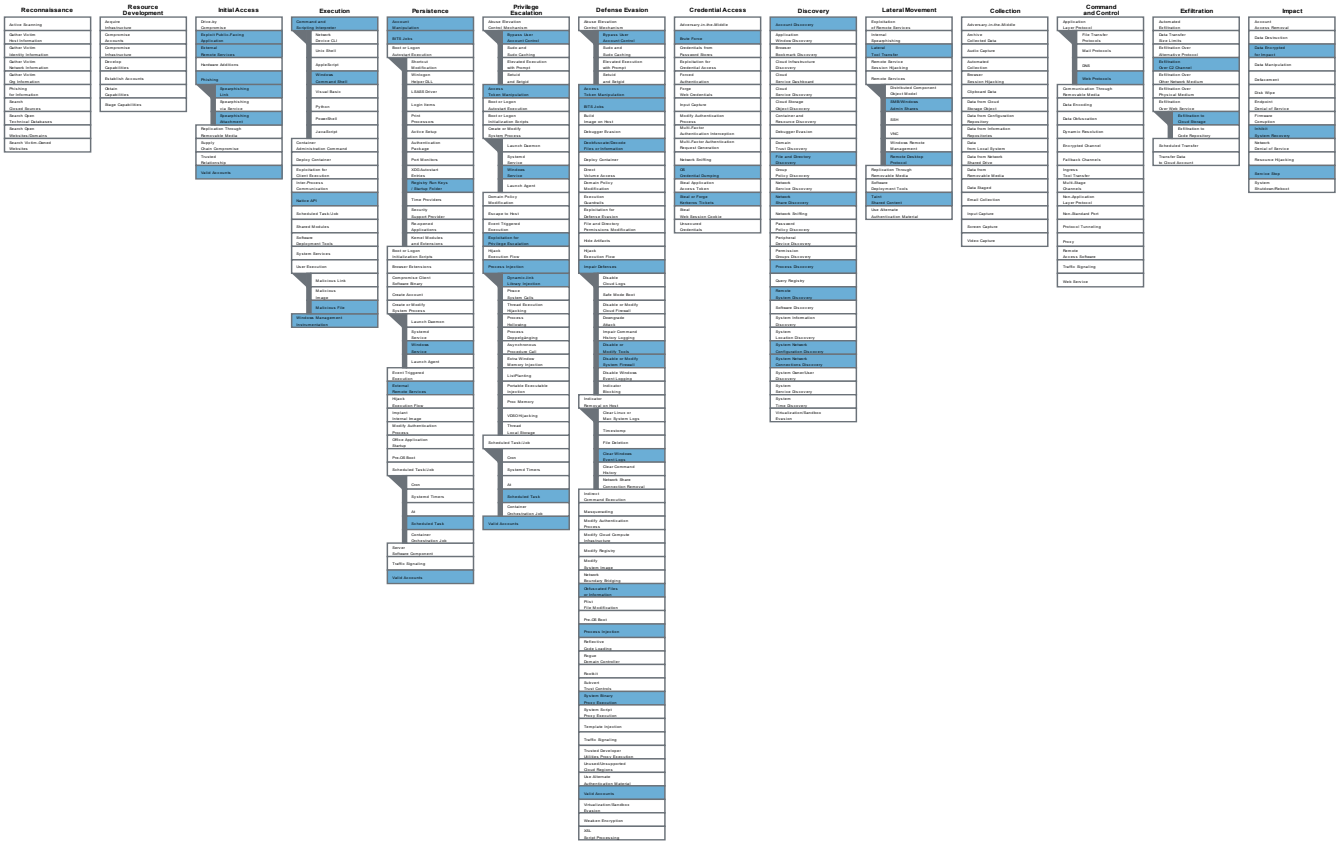

Ilustración 2 – Matriz pintada con los TTPs de Conti

12 Reglas YARA

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-05-09
Identifier: 3584
Reference: https://thedfirreport.com
*/

/* Rule Set ----------------------------------------------------------------
------ */

import "pe"
```

```
rule icedid_rate_x32 {
meta:
description = "files - file rate_x32.dat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 =
"eb79168391e64160883b1b3839ed4045b4fd40da14d6eec5a93cfa9365503586"
strings:
$s1 = "UAWAVAUATVWSH" fullword ascii
$s2 = "UAWAVVWSPH" fullword ascii
$s3 = "AWAVAUATVWUSH" fullword ascii
$s4 = "update" fullword ascii /* Goodware String - occured 207 times */
$s5 = "?klopW@@YAHXZ" fullword ascii
$s6 = "?jutre@@YAHXZ" fullword ascii
$s7 = "PluginInit" fullword ascii
$s8 = "[]_^A\\A]A^A_" fullword ascii
$s9 = "e8[_^A\\A]A^A_]" fullword ascii
$s10 = "[_^A\\A]A^A_]" fullword ascii
$s11 = "Kts=R,4iu" fullword ascii
$s12 = "mqr55c" fullword ascii
$s13 = "R,4i=Bj" fullword ascii
$s14 = "Ktw=R,4iu" fullword ascii
$s15 = "Ktu=R,4iu" fullword ascii
$s16 = "Kt{=R,4iu" fullword ascii
$s17 = "KVL.Mp" fullword ascii
$s18 = "Kt|=R,4iu" fullword ascii
$s19 = "=8c[Vt8=" fullword ascii
$s20 = "Ktx=R,4iu" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 700KB and
( pe.imphash() == "15787e97e92f1f138de37f6f972eb43c" and (
pe.exports("?jutre@@YAHXZ") and pe.exports("?klopW@@YAHXZ") and
pe.exports("PluginInit") and pe.exports("update") ) or 8 of them )
}

rule conti_cobaltstrike_192145 {
meta:
description = "files - file 192145.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 =
"29bc338e63a62c24c301c04961084013816733dad446a29c20d4413c5c818af9"
strings:
$x1 = "cmd.exe /c echo NGAtoDgLpvgJwPLEPFdj>\"%s\"&exit" fullword ascii
$s2 = "veniamatquiest90.dll" fullword ascii
```

```
$s3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde
temporibus mollitia illum" fullword ascii
$s4 = "Quaerat tempora culpa provident" fullword ascii
$s5 = "Velit consequuntur quisquam tempora error" fullword ascii
$s6 = "Quo omnis repellat ut expedita temporibus eius fuga error"
fullword ascii
$s7 = "Dolores ullam tempora error distinctio ut natus facere
quibusdam" fullword ascii
$s8 = "Corporis minima omnis qui est temporibus sint quo error magnam"
fullword ascii
$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et
quidem fugit" fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque
tempora ut neque nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut
doloremque" fullword ascii
$s15 = "Dolorum eum ipsum tempora non et" fullword ascii
$s16 = "Quas alias illum laborum tempora sit est rerum temporibus dicta
et" fullword ascii
$s17 = "Et quia aut temporibus enim repellat dolores totam recusandae
repudiandae" fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus"
fullword ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui
fugiat et accusantium" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "5cf3cdfe8585c01d2673249153057181" and
pe.exports("StartW") or ( 1 of ($x*) or 4 of them ) )
}

rule conti_cobaltstrike_icju1 {
meta:
description = "files - file icju1.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 =
"e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06"
strings:
$x1 = "cmd.exe /c echo NGAtoDgLpvgJwPLEPFdj>\"%s\"&exit" fullword ascii
$s2 = "veniamatquiest90.dll" fullword ascii
$s3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde
temporibus mollitia illum" fullword ascii
```

```
$s4 = "Quaerat tempora culpa provident" fullword ascii
$s5 = "Velit consequuntur quisquam tempora error" fullword ascii
$s6 = "Quo omnis repellat ut expedita temporibus eius fuga error"
fullword ascii
$s7 = "Dolores ullam tempora error distinctio ut natus facere
quibusdam" fullword ascii
$s8 = "Corporis minima omnis qui est temporibus sint quo error magnam"
fullword ascii
$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et
quidem fugit" fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque
tempora ut neque nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut
doloremque" fullword ascii
$s15 = "Dolorum eum ipsum tempora non et" fullword ascii
$s16 = "Quas alias illum laborum tempora sit est rerum temporibus dicta
et" fullword ascii
$s17 = "Et quia aut temporibus enim repellat dolores totam recusandae
repudiandae" fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus"
fullword ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui
fugiat et accusantium" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "a6d9b7f182ef1cfe180f692d89ecc759" or ( 1 of ($x*) or
4 of them ) )
}

rule conti_v3 {

meta:
description = "conti_yara - file conti_v3.dll"
author = "pigerlin"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 =
"8391dc3e087a5cecba74a638d50b771915831340ae3e027f0bb8217ad7ba4682"

strings:
$s1 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s2 = "conti_v3.dll" fullword ascii
$s3 = " <requestedExecutionLevel level='asInvoker' uiAccess='false' />"
fullword ascii
```

```
$s4 = " Type Descriptor'" fullword ascii
$s5 = "operator co_await" fullword ascii
$s6 = " <trustInfo xmlns=\"urn:schemas-microsoft-com:asm.v3\">"
fullword ascii
$s7 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s8 = " Base Class Descriptor at (" fullword ascii
$s9 = " Class Hierarchy Descriptor'" fullword ascii
$s10 = " Complete Object Locator'" fullword ascii
$s11 = " delete[]" fullword ascii
$s12 = " </trustInfo>" fullword ascii
$s13 = "__swift_1" fullword ascii
$s15 = "__swift_2" fullword ascii
$s19 = " delete" fullword ascii

condition:
uint16(0) == 0x5a4d and filesize < 700KB and
all of them

}


rule conti_cobaltstrike_192145_icju1_0 {
meta:
description = "files - from files 192145.dll, icju1.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 =
"29bc338e63a62c24c301c04961084013816733dad446a29c20d4413c5c818af9"
hash2 =
"e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06"
strings:
$x1 = "cmd.exe /c echo NGAtoDgLpvgJwPLEPFdj>\"%s\"&exit" fullword ascii
$s2 = "veniamatquiest90.dll" fullword ascii
$s3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde
temporibus mollitia illum" fullword ascii
$s4 = "Quaerat tempora culpa provident" fullword ascii
$s5 = "Dolores ullam tempora error distinctio ut natus facere
quibusdam" fullword ascii
$s6 = "Velit consequuntur quisquam tempora error" fullword ascii
$s7 = "Corporis minima omnis qui est temporibus sint quo error magnam"
fullword ascii
$s8 = "Quo omnis repellat ut expedita temporibus eius fuga error"
fullword ascii
$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et
quidem fugit" fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
```

```
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque
tempora ut neque nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut
doloremque" fullword ascii
$s15 = "Et quia aut temporibus enim repellat dolores totam recusandae
repudiandae" fullword ascii
$s16 = "Dolorum eum ipsum tempora non et" fullword ascii
$s17 = "Quas alias illum laborum tempora sit est rerum temporibus dicta
et" fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus"
fullword ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui
fugiat et accusantium" fullword ascii
condition:
( uint16(0) == 0x5a4d and filesize < 2000KB and ( 1 of ($x*) and 4 of
them )
) or ( all of them )
}
```

13 Referencias

https://attack.mitre.org/

https://assets.sentinelone.com/sentinellabs/conti-ransomware-unpacked

https://bazaar.abuse.ch/browse/signature/Conti/

https://www.researchgate.net/publication/354505924_Analysis_of_Conti_Ransomware_Attack_on_Computer_Network_with_Live_Forensic_Method

https://blog.qualys.com/vulnerabilities-threat-research/2021/11/18/conti-ransomware

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5759-ccn-cert-id-02-21-conti-v3-ransomware-1/file.html

https://www.group-ib.com/media/conti-armada-report/

https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521.pdf

https://thedfirreport.com/2021/05/12/conti-ransomware/

https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/

https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/

https://www.bleepingcomputer.com/news/security/translated-conti-ransomware-playbook-gives-insight-into-attacks/

https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html

https://www.socinvestigation.com/conti-ransomware-ioc-cybersecurity-infrastructure-security-agency-updates-nearly-100-domain-names/

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

https://www.bleepingcomputer.com/news/security/conti-revil-lockbit-ransomware-bugs-exploited-to-block-encryption/

https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/

https://cyberint.com/blog/research/iocs-identified-to-hunt-conti-ransomware/