CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

# Detalles del ransomware Conti que afectó al sistema de salud en Irlanda

Santiago, 18 de mayo de 2021

TLP: BLANCO

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

# Detalles de la alerta

Este resumen de ciberataques, vulnerabilidades e incidentes de seguridad cibernética tiene como propósito destacar algunos eventos de días pasados para que puedan ser interpretados y discutidos por las diferentes entidades que tengan acceso a su lectura. Este informe reúne los antecedentes conocidos hasta el día de su publicación. La información consignada en el presente documento es catalogada como TLP BLANCO.

## Los hechos

El 14 de mayo a las 2:28 AM, el servicio público de salud de Irlanda (Health Service Executive, HSE) reportó sufrir un ciberataque del tipo ransomware (secuestro y cifrado de los servidores y sistemas de la víctima, a la cual se exige un pago a cambio de la entrega de una clave para revertir la encriptación). Como respuesta, indicó el HSE en el mismo tweet, decidieron apagar todos sus sistemas informáticos para protegerlos del ataque y analizar la extensión del daño.

Durante el fin de semana, los servidores del Ministerio de Salud de Irlanda también fueron atacados, aunque solo se habrían visto comprometidos datos administrativos y no de los ciudadanos, según fuentes de Gobierno.

Los hospitales han seguido funcionando, usando sistemas basados en el papel, pero por las demoras que provocará este cambio se ha debido postergar la atención de muchos pacientes. Debieron suspenderse servicios de imagenología, radioterapia y procesos similares.


En la señal nacional de televisión irlandesa, RTÉ, el director ejecutivo del HSE, Paul Reid, confirmó posteriormente la información, calificando al ataque como “una operación criminal intencionalmente ejecutada”. Existía preocupación por los datos personales de los pacientes, e incluso potencialmente por detalles bancarios de los mismos.

Asimismo, el Primer Ministro Micheál Martin señaló que no se pagaría rescate alguno por los datos encriptados en esta irrupción. Mientras que el canciller Simon Coveney señaló que el HSE había montado una verdadera "sala de guerra" para enfrentar el ataque a sus sistemas informáticos y que está trabajando junto a la policía, las Fuerzas de Defensa, los Ministerios de Justicia, Defensa y Comunicaciones e Interpol y que está recibiendo toda la asesoría internacional posible.

Hoy, el ministro de Salud, Stephen Donnelly, aseguró que no ha habido evidencia de la publicación de ningún dato producto de este ataque.

## Se presume de un ataque ruso

Ayer, el ministro de Estado (subsecretario) para el Gobierno Electrónico, Ossian Smyth, indicó que el ataque pareciera provenir de Europa del Este, y que los responsables serían la banda criminal Wizard Spider (grupo basado en Rusia).

# Ransomware Conti

## Vector de entrada

Según lo trascendido, el ataque habría sido realizado con un ransomware llamado **Conti**, el que generalmente llega a los sistemas a través del sistema de correo electrónico. Los atacantes envían un e-mail con un archivo adjunto infectado, el que de ser abierto, infecta al sistema.

También se ha visto que algunos actores maliciosos pueden utilizar como puente otro tipo de infección, como por ejemplo la conocida como **IcedID**. En ese caso, se observó a un actor de amenazas pasar de una infección IcedID inicial a implementar Conti en todo el dominio en dos días y 11 horas. Los actores de amenazas permanecieron inactivos durante la mayor parte de este tiempo, antes de entrar en acción un sábado por la mañana temprano. La actividad duró dos horas y media. Utilizaron RDP, PsExec y Cobalt Strike para moverse lateralmente dentro del entorno antes de ejecutar Conti en la memoria en todos los sistemas activos.

## Método de descubrimiento de archivos

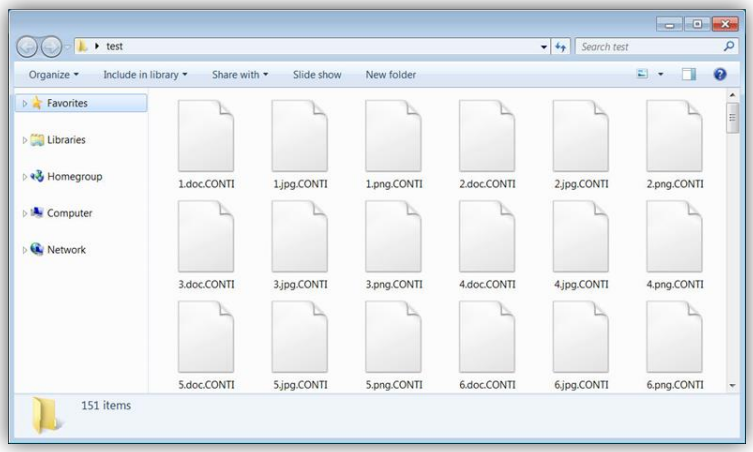
A diferencia de muchas familias de ransomware, Conti no apunta a una lista específica de archivos en función de su extensión. Realiza el método opuesto, en el que cifrará todos los archivos excepto aquellos con las extensiones: exe, dll, lnk y sys. El malware luego creará una lista de carpetas para ignorar mientras se encripta, como se indica en la siguiente figura. Si estos valores se encuentran en cualquier lugar del nombre del archivo o la ruta, omitirá el cifrado dentro de él.

| | |
|---|---|
| tmp | winnt |
| Datos de la aplicación | Datos de aplicación |
| temperatura | pulgar |
| $ Papelera de reciclaje | $ RECICLAJE BIN |
| Información del Volumen del Sistema | Archivos de programa |
| Archivos de programa (x86) | Bota |
| Ventanas | |

## Cifrado de los datos

Si bien Conti utiliza un método tradicional de cifrado, una característica única es cómo puede procesar el cifrado de archivos, lo que eleva su rendimiento y le permitió cifrar archivos decenas de veces más rápido que una aplicación de ransomware típica. Esto se posibilita mediante el uso de las API que utilizan los puertos de finalización de E/S de Windows.

Conti tiene un hilo de "trabajador" de cifrado que se centra en realizar el cifrado en un nombre de archivo determinado. El malware usa la llamada CreateIoCompletionPort () para crear 32 instancias de este hilo de trabajo en la memoria para esperar los datos. Una vez que se ha creado la lista de archivos, se envían a los subprocesos para su cifrado inmediato. El cifrado parece hacer referencia a los rastros de AES-256 y una variante de ChaCha.




## Otros elementos diferenciadores

Conti puede admitir operaciones de subprocesos múltiples como parte de su trabajo. Aunque esto no es único, ya que otros malware hacen lo mismo, este ransomware en particular gestiona una gran cantidad de subprocesos, 32 para ser precisos. Eso permite a Conti cifrar archivos más rápido en comparación con otras amenazas de este tipo.

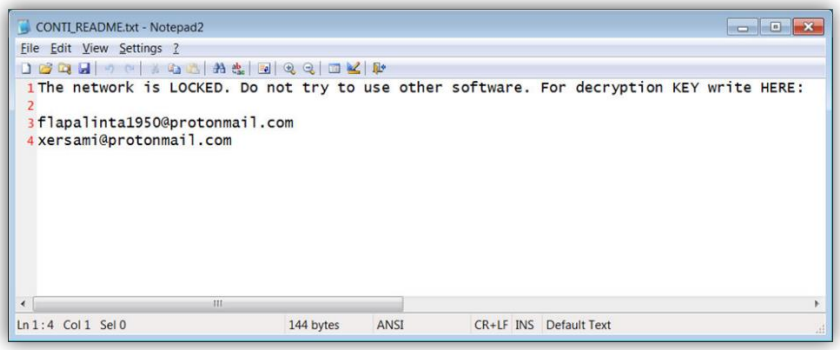
Más aún, detalle único en Conti es un control excepcional sobre los objetivos de cifrado mediante un cliente de línea de comandos. El ransomware se puede configurar para omitir el cifrado de unidades locales, con el objetivo de obtener datos en recursos compartidos SMB en red, mediante el uso de una lista de direcciones IP alimentadas a través de la línea de comando. Eso permite que la amenaza cause daños específicos en entornos infectados. El beneficio adicional de reducir el impacto general de un ataque le permite mostrar menos signos de infección en múltiples sistemas, ya que es posible que la infección no se vea por un tiempo a menos que un usuario acceda a los datos.

El tercer método único utilizado por Conti incluye su abuso del Administrador de Reinicio de Windows. El Administrador permite el desbloqueo de archivos antes de que se reinicie el sistema operativo. La amenaza utiliza al Administrador para desbloquear y cerrar aplicaciones para que pueda cifrar sus datos. Eso es especialmente exitoso en los servidores de Windows, donde las bases de datos casi siempre están en funcionamiento.

```
rgsFileNames = Overlapped->Offset;
if ( !RmStartSession(&dwSessionHandle, 0, strSessionKey) )
{
  if ( !RmRegisterResources(dwSessionHandle, 1u, &rgsFileNames, 0, 0, 0, 0) )
  {
    dwRebootReasons = 0;
    pnProcInfoNeeded = 0;
    pnProcInfo = 0;
    if ( RmGetList(dwSessionHandle, &pnProcInfoNeeded, &pnProcInfo, 0, &dwRebootReasons) != ERROR_MORE_DATA
      || !pnProcInfoNeeded )
    {
      RmEndSession(dwSessionHandle);
      return 0;
    }
    error_msg_rm = RmShutdown(dwSessionHandle, RmForceShutdown, NULL) == 0;
  }
  RmEndSession(dwSessionHandle);
}
```

## La nota de rescate

A continuación, Conti deja caer una nota de rescate en el escritorio del usuario. El nombre de la nota de rescate es 'CONTI_README.txt'. A menudo, los autores de amenazas de ransomware usarían mayúsculas al dar un nombre a la nota de rescate, ya que aumenta las posibilidades de que el usuario detecte el mensaje de los atacantes. El mensaje de rescate es muy breve. Los atacantes no dicen cuál es la tarifa de rescate, sin embargo, exigen ser contactados por correo electrónico para lo cual proporcionan dos direcciones de email.



# Indicadores de compromiso (IoT) en previos ataques de Conti

Nombre de archivo de la nota de rescate: CONTI_README.txt

### Direcciones de email

| EMAIL | FUENTE | FECHA |
|---|---|---|
| flapalinta1950@protonmail.com | bleepingcomputer.com | 7/13/2020 |
| xersami@protonmail.com | bleepingcomputer.com | 7/13/2020 |
| carbedispgret1983@protonmail.com | Twitter | 12/2/2020 |
| flapalinta1950@protonmail.com | Twitter | 12/2/2020 |
| glocadboysun1978@protonmail.com | Twitter | 12/2/2020 |
| guifullcharti1970@protonmail.com | Twitter | 12/2/2020 |
| houkumlota1972@protonmail.com | Insikt Group | 12/2/2020 |
| phrasitliter1981@protonmail.com | Twitter | 12/2/2020 |
| snowacabad1981@protonmail.com | Insikt Group | 12/2/2020 |
| xersami@protonmail.com | Twitter | 12/2/2020 |
| mantiticvi1976[@]protonmail[.]com | www.pcrisk.e | 9/02/2020 |
| fahydremu1981[@]protonmail[.]com | www.pcrisk.e | 9/02/2020 |

### Dominios

| DOMINIO | FUENTE | FECHA |
|---|---|---|
| libsyn.com | Recorded Future | 7/13/2020 |
| intezer.com | Recorded Future | 7/13/2020 |
| thecyberwire.com | Recorded Future | 7/13/2020 |

### URL

| URL | FUENTE | FECHA |
|---|---|---|
| https://hwcdn.libsyn.com/p/b/d/0/bd0b1c9843002da4/CyberWire_Podcast_2020_07_10.mp3?c_id=77973305&cs_id=77973305&expiration=1594414460&hwt=326ad166bfac3ec5742d54b55b84c9ec | Recorded Future | 7/13/2020 |
| https://analyze.intezer.com/#/files/eae876886f19ba384f55778634a35a1d975414e83f22f6111e3e792f706301fe | Recorded Future | 7/13/2020 |
| https://thecyberwire.com/newsletters/daily-briefing/9/133 | Recorded Future | 7/13/2020 |

Hash

| HASH | TIPO | FUENTE | FECHA |
|---|---|---|---|
| accbcd0b6ddf54c303d08e1aabcfcf4c | Hash/MD5 | Insikt Group | 12/2/2020 |
| b5a255bfb7ade5b5ec85b6a6354d7bf9 | Hash/MD5 | Twitter | 12/2/2020 |
| b7b5e1253710d8927cbe07d52d2d2e10 | Hash/MD5 | Carbon Black | 12/2/2020 |
| bf6e754d56fe2896b13b0154eeb05d45 | Hash/MD5 | Twitter | 12/2/2020 |
| c3c8007af12c9bd0c3c53d67b51155b7 | Hash/MD5 | SavePearlHarbor | 12/2/2020 |
| 15864fbf8cacfddce9f76bb204376c468669b8cc | Hash/SHA-1 | AlienVault \| Pulses | 12/2/2020 |
| 596f1fdb5a3de40cccfe1d8183692928b94b8afb | Hash/SHA-1 | Carbon Black | 12/2/2020 |
| 8fa3841d36a7cd285a6045250e0b7801fb560d24 | Hash/SHA-1 | Insikt Group | 12/2/2020 |
| da778748ef41a4482da767de90e7ae2a8befa41e | Hash/SHA-1 | lmntrix.com | 12/2/2020 |
| 2579148e5f020145007ac0dc1be478190137d7915e6fbca2c787b55dbec1d370 | Hash/SHA-256 | Minervalabs Blog | 12/2/2020 |
| 61653b3cd1a290bbc531181edec807b20e263599aa6a2908dc259b867ec98297 | Hash/SHA-256 | Carbon Black | 12/2/2020 |
| 67f9404df22c6b1e82807f5c527805083f40b70b9dac6bc27c2583b70de17390 | Hash/SHA-256 | Carbon Black | 12/2/2020 |
| 68858814ebe2dcf21fd87ebb5fca829806307774060cb7f587f54de6625f2b02 | Hash/SHA-256 | Insikt Group | 12/2/2020 |
| 6b1b4bbff59456dfaa3307a20171fd7394f49a5f6d1b3cd59392ba41e4881878 | Hash/SHA-256 | Carbon Black | 12/2/2020 |
| 749c4c343978b9f236838034f868dac937fdfd9af31a6e5dd05b993a87d51276 | Hash/SHA-256 | Carbon Black | 12/2/2020 |
| 895007b045448dfa8f6c9ee22f76f416f3f18095a063f5e73a4137bcccc0dc9a | Hash/SHA-256 | Carbon Black | 12/2/2020 |
| 8c243545a991a9fae37757f987d7c9d45b34d8a0e7183782742131394fc8922d | Hash/SHA-256 | SavePearlHarbor | 12/2/2020 |
| d236d64b7bf9510ea1746d10a4c164a2ef2c724cc62b2bca91d72bdf24821e40 | Hash/SHA-256 | Twitter | 12/2/2020 |
| eae876886f19ba384f55778634a35a1d975414e83f22f6111e3e792f706301fe | Hash/SHA-256 | Carbon Black | 12/2/2020 |

Magic

Ejecutable PE32 (GUI) Intel 80386, para MS Windows

Tiempo compilado: Jue 4 de junio a las 00:02:10 2020 UTC.

Secciones de PE (5): Nombre Tamaño SHA256

- .text 94,720 67f9404df22c6b1e82807f5c527805083f40b70b9dac6bc27c2583b70de17390
- .rdata 1,024 749c4c343978b9f236838034f868dac937fdfd9af31a6e5dd05b993a87d51276
- .data 4,608 895007b045448dfa8f6c9ee22f76f416f3f18095a063f5e73a4137bcccc0dc9a
- .rsrc 1.024 61653b3cd1a290bbc531181edec807b20e263599aa6a2908dc259b867ec98297
- .reloc 1.024 6b1b4bbff59456dfaa3307a20171fd7394f49a5f6d1b3cd59392ba41e4881878

Lista de líneas de comando ejecutadas para detener los servicios de Windows e inhibir la recuperación:

| | |
|---|---|
| vssadmin Eliminar sombras / todo / silencio | net stop MSSQLServerADHelper100 / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = c: / on = c: / maxsize = 401MB | net stop MSSQLServerOLAPService / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = c: / on = c: / maxsize = unbounded | parada neta MySQL57 / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = d: / on = d: / maxsize = 401MB | net stop ntrtscan / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = d: / on = d: / maxsize = unbounded | net stop OracleClientCache80 / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = e: / on = e: / maxsize = 401MB | net stop PDVFSService / año |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = e: / on = e: / maxsize = unbounded | parada neta POP3Svc / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = f: / on = f: / maxsize = 401MB | Net stop ReportServer / año |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = f: / on = f: / maxsize = unbounded | Net stop ReportServer $ SQL_2008 / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = g: / on = g: / maxsize = 401MB | Net stop ReportServer $ SYSTEM_BGC / y |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = g: / on = g: / maxsize = unbounded | Net stop ReportServer $ TPS / año |
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = h: / on = h: / maxsize = 401MB | Net stop ReportServer $ TPSAMA / año |

| | |
|---|---|
| vssadmin cambiar el tamaño de almacenamiento de sombras / for = h: / on = h: / maxsize = unbounded | parada neta RESvc / año |
| vssadmin Eliminar sombras / todo / silencio | net stop sacsvr / y |
| net stop “Acronis VSS Provider” / año | parada neta SamSs / año |
| net stop "Enterprise Client Service" / año | net stop SAVAdminService / y |
| net stop "SQLsafe Backup Service" / año | net stop SAVService / año |
| net stop "Servicio de filtro SQLsafe" / año | parada neta SDRSVC / año |
| net stop "Veeam Backup Catalog Data Service" / año | net stop SepMasterService / año |
| parada neta AcronisAgent / y | parada neta ShMonitor / y |
| parada neta AcrSch2Svc / y | parada neta Smcinst / año |
| net stop Antivirus / año | net stop SmcService / y |
| parada neta ARSM / año | parada neta SMTPSvc / y |
| net stop BackupExecAgentAccelerator / y | parada neta SQLAgent $ BKUPEXEC / año |
| net stop BackupExecAgentBrowser / y | parada neta SQLAgent $ ECWDB2 / y |
| net stop BackupExecDeviceMediaService / y | parada neta SQLAgent $ PRACTTICEBGC / y |
| net stop BackupExecJobEngine / y | parada neta SQLAgent $ PRACTTICEMGT / y |
| net stop BackupExecManagementService / y | stop neto SQLAgent $ PROFXENGAGEMENT / año |
| net stop BackupExecRPCService / y | parada neta SQLAgent $ SBSMONITORING / año |
| net stop BackupExecVSSProvider / y | parada neta SQLAgent $ SHAREPOINT / y |
| net stop bedbg / año | parada neta SQLAgent $ SQL_2008 / y |
| parada neta DCAgent / a | parada neta SQLAgent $ SYSTEM_BGC / y |
| net stop EPSecurityService / año | parada neta SQLAgent $ TPS / año |
| net stop EPUpdateService / y | parada neta SQLAgent $ TPSAMA / año |
| net stop EraserSvc11710 / y | parada neta SQLAgent $ VEEAMSQL2008R2 / y |
| parada neta EsgShKernel / y | parada neta SQLAgent $ VEEAMSQL2012 / y |
| parada neta FA_Scheduler / y | net stop SQLBrowser / y |
| parada neta IISAdmin / año | net stop SQLSafeOLRService / y |
| parada neta IMAP4Svc / y | net stop SQLSERVERAGENT / y |
| parada neta McShield / año | net stop SQLTELEMETRY / y |
| parada neta McTaskManager / año | parada neta SQLTELEMETRY $ ECWDB2 / y |
| parada neta mfemms / año | net stop SQLWriter / y |
| parada neta mfevtp / y | net stop VeeamBackupSvc / y |
| parada neta MMS / año | parada neta VeeamBrokerSvc / y |
| net stop mozyprobackup / año | parada neta VeeamCatalogSvc / y |
| net stop MsDtsServer / y | parada neta VeeamCloudSvc / y |
| net stop MsDtsServer100 / y | net stop VeeamDeploymentService / y |
| net stop MsDtsServer110 / y | net stop VeeamDeploySvc / y |
| parada neta MSExchangeES / año | net stop VeeamEnterpriseManagerSvc / y |
| parada neta MSExchangeIS / año | parada neta VeeamMountSvc / y |
| parada neta MSExchangeMGMT / año | parada neta VeeamNFSSvc / y |
| parada neta MSExchangeMTA / año | parada neta VeeamRESTSvc / y |
| parada neta MSExchangeSA / año | parada neta VeeamTransportSvc / y |

| | |
|---|---|
| parada neta MSExchangeSRS / año | parada neta W3Svc / y |
| parada neta MSOLAP $ SQL_2008 / y | parada neta wbengine / y |
| parada neta MSOLAP $ SYSTEM_BGC / y | parada neta WRSVC / año |
| parada neta MSOLAP $ TPS / año | parada neta MSSQL $ VEEAMSQL2008R2 / y |
| parada neta MSOLAP $ TPSAMA / año | parada neta SQLAgent $ VEEAMSQL2008R2 / y |
| parada neta MSSQL $ BKUPEXEC / año | net stop VeeamHvIntegrationSvc / y |
| parada neta MSSQL $ ECWDB2 / y | net stop swi_update / y |
| parada neta MSSQL $ PRACTICEMGT / y | parada neta SQLAgent $ CXDB / y |
| parada neta MSSQL $ PRACTTICEBGC / y | parada neta SQLAgent $ CITRIX_METAFRAME / y |
| parada neta MSSQL $ PROFXENGAGEMENT / y | net stop "Copias de seguridad SQL" / año |
| net stop MSSQL $ SBSMONITORING / año | parada neta MSSQL $ PROD / año |
| parada neta MSSQL $ SHAREPOINT / y | parada neta "Servicio Zoolz 2" / año |
| parada neta MSSQL $ SQL_2008 / y | net stop MSSQLServerADHelper / y |
| parada neta MSSQL $ SYSTEM_BGC / y | parada neta SQLAgent $ PROD / año |
| parada neta MSSQL $ TPS / año | net stop msftesql $ PROD / y |
| parada neta MSSQL $ TPSAMA / año | net stop NetMsmqActivator / y |
| parada neta MSSQL $ VEEAMSQL2008R2 / y | parada neta EhttpSrv / y |
| parada neta MSSQL $ VEEAMSQL2012 / y | parada neta ekrn / y |
| net stop MSSQLFDLauncher / año | parada neta ESHASRV / año |
| net stop MSSQLFDLauncher $ PROFXENGAGEMENT / y | parada neta MSSQL $ SOPHOS / año |
| net stop MSSQLFDLauncher $ SBSMONITORING / año | parada neta SQLAgent $ SOPHOS / año |
| net stop MSSQLFDLauncher $ SHAREPOINT / y | parada neta AVP / y |
| parada neta MSSQLFDLauncher $ SQL_2008 / y | parada neta klnagent / y |
| net stop MSSQLFDLauncher $ SYSTEM_BGC / y | parada neta MSSQL $ SQLEXPRESS / y |
| net stop MSSQLFDLauncher $ TPS / año | parada neta SQLAgent $ SQLEXPRESS / y |
| net stop MSSQLFDLauncher $ TPSAMA / y | parada neta wbengine / y |
| net stop MSSQLSERVER / y | net stop mfefire / año |

## Recomendaciones

La CISA y el FBI recomiendan los siguientes pasos[1] para reducir el riesgo de ser comprometido por un ataque de ransomware.

- Exigir autenticación multifactor a quienes acceden de forma remota a las redes OT e IT.
- Activar fuertes filtros de spam para evitar que correos de phishing alcancen a los usuarios de la organización, y filtrar los emails que contengan archivos ejecutables.
- Implementar un programa de capacitación y ataques simulados de spearphishing, para desalentar que los usuarios visiten sitios maliciosos o abran adjuntos maliciosos, y reafirmar las respuestas apropiadas de los usuarios ante emails de spearphishing.
- Filtrar el tráfico de la red para prohibir la comunicación de acceso y salida con direcciones IP conocidamente maliciosas.
- Actualizar el software, incluyendo sistemas operativos, aplicaciones y firmware en los activos de la red IT, de forma oportuna. Considerar el uso de un sistema centralizado de administración de parches. Usar una estrategia de evaluación basada en el riesgo para determinar qué activos y zonas de la red OT deberían participar en el programa de administración de parches.
- Limitar el acceso a recursos desde la red, especialmente a través de restringir RDP. Si tras analizar riesgos RDP es considerado operacionalmente necesario, restringir las fuentes de origen y exigir autenticación multifactor.
- Programar antivirus/antimalware para que realice escaneos regulares de los activos de la red IT usando firmas actualizadas. Usar una estrategia de inventario basada en riesgo para determinar cómo se identifica a los activos de redes OT y cómo se evalúa la presencia en ellos de malware.
- Implementar la prevención de ejecución no autorizada a través de:
    - Deshabilitar los script de macros de los archivos de Microsoft Office compartidos a través de email. Considere usar software Office Viewer para abrir estos archivos en lugar de aplicaciones completas de Microsoft Office.
    - Implementar una lista permitida de aplicaciones (allowlisting), que solo permite a los sistemas ejecutar programas conocidos y aceptados por las políticas de seguridad. Implementar políticas de restricción de software (SRP) u otros controles para impedir que los programas ejecuten archivos de ubicaciones conocidas por su ransomware, como archivos temporales de populares navegadores de internet o programas de decompresión, incluyendo la carpeta AppData / LocalAppData.
- Monitorear o bloquear las conexiones entrantes de nodos de salida de Tor y otros servicios de anonimización a direcciones IP y puertos por los cuales no se esperan conecciones externas (por ejemplo, los que no son accesos VPN, de correo o web).
- Utilizar firmas para detectar o bloquear conecciones entrantes de servidores Cobalt Strike y otras herramientas de explotación para después de que la víctima ya ha sido comprometida.

[1] DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks| CISA https://us-cert.cisa.gov/ncas/alerts/aa21-131a

La CISA y el FBI recomiendan implementar las siguientes mitigaciones para reducir el riesgo de severa degradación de negocios o funcional si se cae en un ataque de ransomware.

- Implementar y asegurar segmentación robusta entre las redes IT y OT para limitar la capacidad de adversarios de pivotear a la red OT tras comprometer la red IT. Definir una zona desmilitarizada que elimine la comunicación no regulada entre las redes IT y OT.
- Organizar los activos OT en zonas lógicas tomando en cuenta lo criticidad, consecuencia y necesidad operacional de las cuentas. Definir vías de comunicación aceptables entre las zonas y desplegar controles de seguridad para filtrar el tráfico de las redes y monitorear la comunicación entre zonas. Prohibir a los protocolos de control de sistemas industriales (ICS) el atravesar la red IT.
- Identificar las interdependencias entre redes OT e IT y desarrollar soluciones alternativas o controles manuales para asegurar que las redes ICS pueden ser aisladas si las conexiones crean riesgos a la operación segura y confiable de los procesos OT. Testear regularmente planes de contingencia como controles manuales, con tal de que funciones críticas de seguridad puedan ser mantenidas durante un ciberincidente. Asegurar que la red OT puede operar a la capacidad necesaria incluso si la red IT es comprometida.
- Testear regularmente controles manuales para que las funciones críticas puedan ser mantenidas en funcionamiento si las redes ICS u OT deben ser desconectadas.
- Implementar procedimientos regulares de respaldo de datos en las redes IT y OT. Los procedimientos de respaldo deben ser realizados con frecuencia y regularidad, y contemplar las siguientes mejores prácticas:
    - Asegurar el testeo regular de los respaldos.
    - Resguardar los respaldos por separado, aislados de las conexiones de red que podrían permitir su infección por ransomware.
    - Mantener “imágenes doradas” regularmente actualizadas de los sistemas críticos por si se necesita reconstruirlos. Esto significa mantener “plantillas” que incluyan un sistema operativo preconfigurado y aplicaciones de software asociadas que puedan ser rápidamente desplegadas para reconstruir un sistema, como un servidor o máquina virtual.
    - Conserve el hardware de respaldo para reconstruir los sistemas en caso de que no se prefiera reconstruir el sistema primario. Hardware más viejo o más nuevo que el sistema primario puede resultar en problemas de instalación o compatibilidad al reconstruir desde imágenes.
    - Conservar código fuente o ejecutables. Es más eficiente reconstruir sobre imágenes de sistema, pero algunas imágenes no se instalarán correctamente en diferente hardware. Tener acceso separado al software que se necesita ayudará en estos casos.
- Asegurar que las cuentas de usuario y proceso son limitadas a través de las políticas de uso, control de las cuentas de usuario y administración de cuentas privilegiadas. Organizar los derechos de acceso según los principios del menor privilegio y la separación de tareas.

Si su organización es impactada por un incidente de ransomware, la CISA y el FBI recomiendan las siguientes acciones:

- Aislar el sistema infectado. Remover el sistema infectado de todas las redes y deshabilitar el wifi, Bluetooth y todas las potenciales capacidades de conexiones del computador. Asegurar que todos los discos compartidos y de red están desconectados, sean wifi o alámbricos.
- Apagar otros computadores y aparatos. Apagar y remover de la red los dispositivos que compartan una red con el aparato infectado y que no hayan sido totalmente encriptados por el ransomware. Si es posible, recolectar y asegurar todos los computadores infectados y potencialmente infectados en un lugar principal, asegurándose de claramente etiquetar cualquier equipo que haya sido cifrado. Apagar y segregar los computadores infectados, y otros que puedan no haber sido encriptados completamente puede ayudar a la recuperación total o parcial de archivos por especialistas.
- Asegurar los respaldos. Asegurarse de que los datos de respaldo estén desconectados de las redes y seguros. Si es posible, escanee sus datos de respaldo con un programa antivirus para asegurarse de que esté libre de malware.

# Referencias

Carbon Black | TAU Threat Discovery: Conti Ransomware: https://www.carbonblack.com/blog/tau-threat-discovery-CONTI-ransomware/

The DFIR Report | Conti Ransomware: https://thedfirreport.com/2021/05/12/conti-ransomware/

CISA | Ransomware: https://www.cisa.gov/ransomware

CISA | DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks https://us-cert.cisa.gov/ncas/alerts/aa21-131a