Identificador
[colCERT AD-0510-004]

16/05/2022

Advertencia de Seguridad Digital

[TLP: WHITE]

Ransomware Conti; doble extorsión para afectar a las entidades

El grupo Ruso Conti, ha venido realizando ataques a sedes gubernamentales de Perú y Costa Rica sustrayendo información y documentos de servidores, para luego exigir un rescate, Conti está relacionado con más de 1.000 ciberataques en el mundo.

La siguiente información da un contexto sobre el modus operandi y de manera específica, menciona indicadores de compromiso, para que sean tenidos en cuenta por los equipos técnicos y realizadas las acciones de mitigación correspondientes en las infraestructuras tecnológicas en cada entidad.

Contexto histórico.

Visto por primera vez entre octubre y diciembre del 2019, su línea de negocio es operar como ***RaaS (Ransomware as a service)***, básicamente consiste en divulgarse y ofertar sus servicios en foros clandestinos en donde otros aprendices y ciberdelincuentes adquieren un paquete de servicios, seguidamente por cada afectación, se recibe un porcentaje debido a los rescates cobrados. Conti con sede en Rusia ha desarrollado y propagado numerosas familias de malware y es considerado como el grupo más activo en campañas de ciberdelincuencia en el 2021.

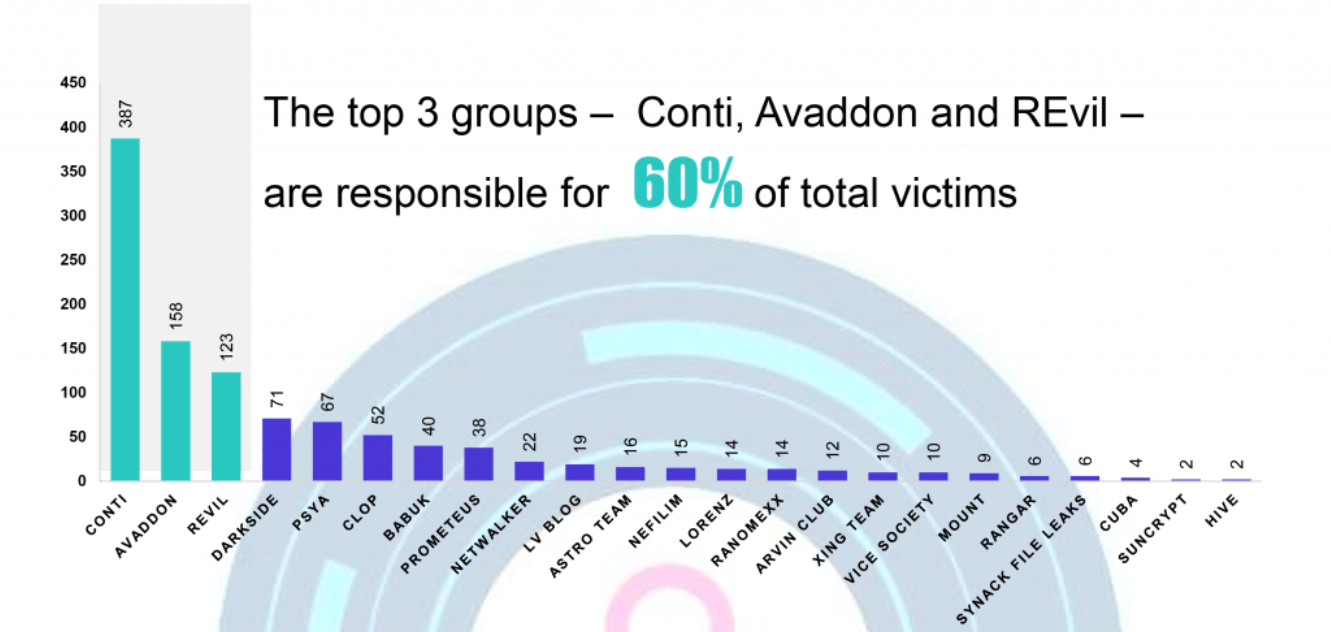

Figura No 1. *Afectaciones de Conti a nivel mundial.* ***Fuente:*** *Cognyte*

Para el año 2022 y según las investigaciones de los expertos, Conti perpetra un ataque a un objetivo cada 11 segundos, lo cual indica los mecanismos eficaces que lanzan en la afectación a las entidades.

Core de negocio

Dentro de los servicios perpetrados por Conti, se encuentran los siguientes:

- Desarrollo de criptomoneda.
- Ataque a la tendencia de la digitalización.
- Afiliación a cibercriminales.

Modo de operación

Hace uso del doxing o doble extorsión en donde, antes de cifrar la información de la entidad, procede a exfiltrarla para tener una garantía adicional de presión al advertir a la entidad que si no realiza el pago del rescate no solo pierde el acceso a la información, sino que también se verán expuestos sus datos sensibles, confidenciales y de continuidad de negocio de la organización afectada. La lista de los afectados va desde entidades privadas de todos los sectores económicos de un país hasta las organizaciones gubernamentales.

La extensión característica de Conti es .CONTI y los posibles nombres de notas de rescate son:

- CONTI.txt
- R3ADM3.txt
- readme.txt
- ONTI_README.txt

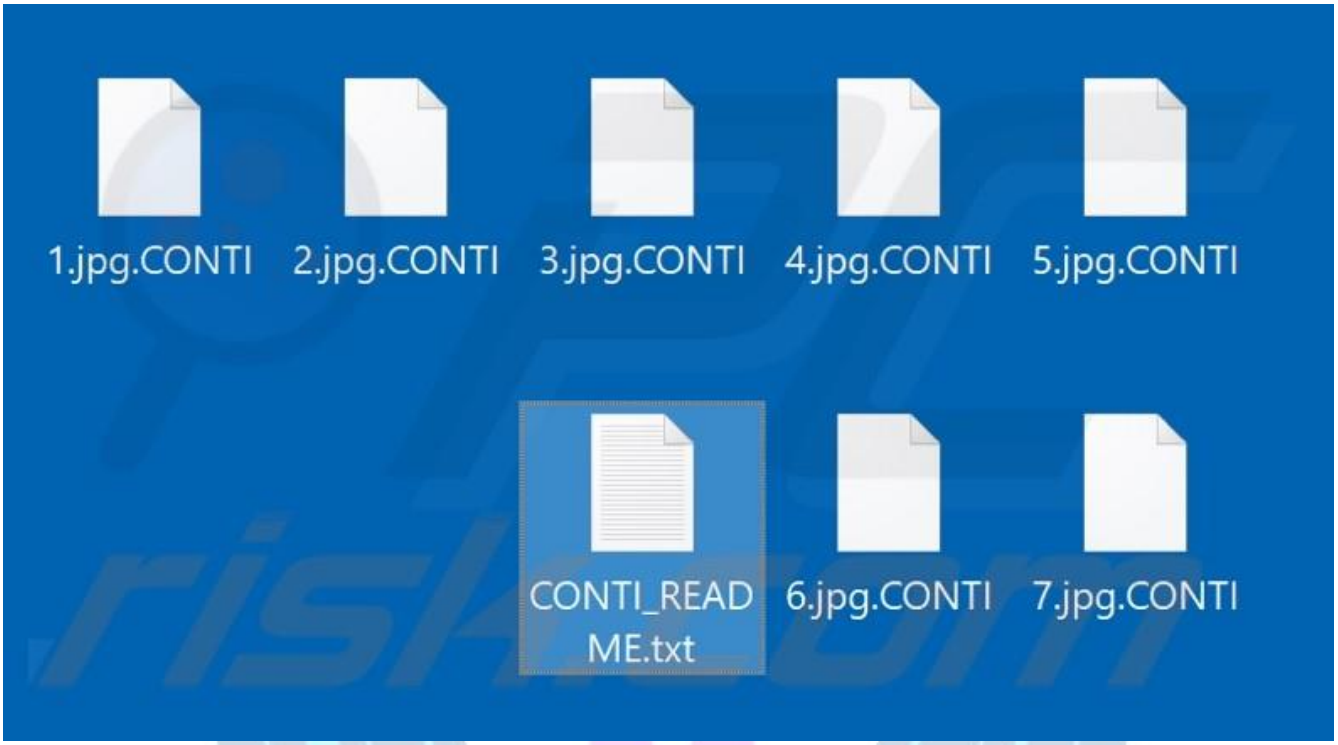

Figura No 2. *Archivos cifrados por Conti.* ***Fuente:*** *PCrisk.*

Posibles vectores de infección

- Envío de adjuntos y/o enlaces maliciosos como cebo para las víctimas, luego de que el usuario ejecute el adjunto, se llega a descargar un malware tipo Backdoor para luego desplegar el ransomware Conti, lo cual indica que actúa colaborativamente con otras APT.
- Explotación de vulnerabilidades del sistema, aplicativos o software.
- Ataque directamente sobre protocolos como RDP o Telnet.

Principales afectaciones

- Movimiento lateral.
- Escalado de privilegios.
- Ejecución de malware.
- Exfiltración de datos.
- Realizar ataques de fuerza bruta sobre el protocolo SMB.
- Logra persistencia a través de servicios legítimos.
- Desactivación de Windows defender con el fin de evadir los filtros de seguridad del sistema.
- Enumeración de usuarios y servicios.
- Eliminación de copias e instantáneas.
- Uso de exploit como ZeroLogon.

Golpe contra Conti

En febrero del 2022 manifestó su apoyo total al gobierno Ruso en la actual guerra contra Ucrania, sin embargo ha sido compartido información del grupo parte por los mismos afiliados, quizá de origen ucraniano en un intento

de represalia por dicho apoyo. Los miembros han expuesto chats del grupo desde el año 2021 y también lo que en apariencia se observa como un conjunto de archivos llaves de descifrado, software interno y chats.

```
Greetings,

Here is a friendly heads-up that the Conti gang has just lost all their
shit. Please know this is true.
https://twitter.com/ContiLeaks/status/1498030708736073734

The link will take you to download an 1.tgz file that can be unpacked
running tar -xzvf 1.tgz command in your terminal . The contents of the first
dump contain the chat communications  (current, as of today and going to
the past) of the Conti Ransomware gang.  We promise it is very interesting.

There are more dumps coming , stay tuned.
You can help the world by writing this as your top story.

It is not malware or a joke.
This is being sent to many journalists and researchers.

Thank you for your support

Glory to Ukraine!
```

Figura No. 3. *Nota de afiliados ucranianos.* ***Fuente:*** *Twitter.*

Go Back

Directory: Conti/

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Documentation Leak.7z	234714	2022-03-01 05:29:38
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1160294	2022-03-02 13:10:39
Conti Locker Leak.7z	6852466	2022-03-05 04:29:03
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14

Figura No. 4. Directorio en apariencia de Conti. **Fuente:** Twitter.

Actualmente Conti cuenta con su tercera versión, se presume que, debido a la exposición de esta información del grupo, muy probablemente migren hacia una versión más actualizada y con nuevas capacidades.

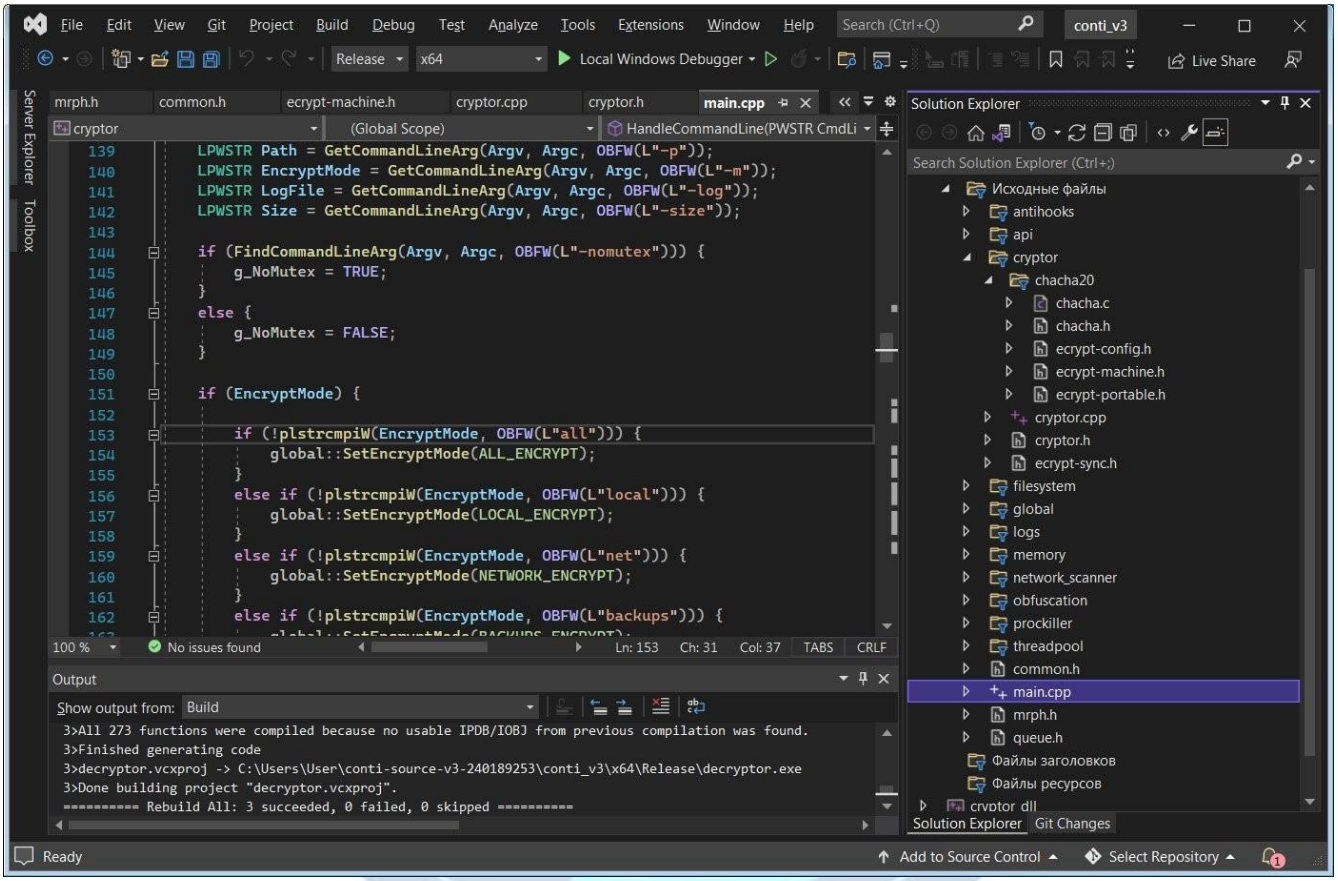

Figura No. 5. *Código V3 expuesto de Conti.* ***Fuente:*** *Diario informe.*

En la figura 6 se observan las TTP (tácticas, técnicas y procedimientos) ejecutados por el actor malicioso Conti, dentro de las cuales se destacan:

- La inyección de código para infectar procesos creados o modificar los legítimos, dentro de sus funcionalidades se encuentran las de elevar privilegios a través del acceso a la memoria, sistema, red y recursos.
- Uso del comando Shell para ejecutar comandos en donde se libere una carga útil de un malware.
- Abuso de funciones API en donde los atacantes intentan evadir las herramientas de protección al deshabilitarlas.
- Uso de cuentas validas a nivel de administrador para acceder de forma remota a un sistema de red a través de SMB para llamar archivos.

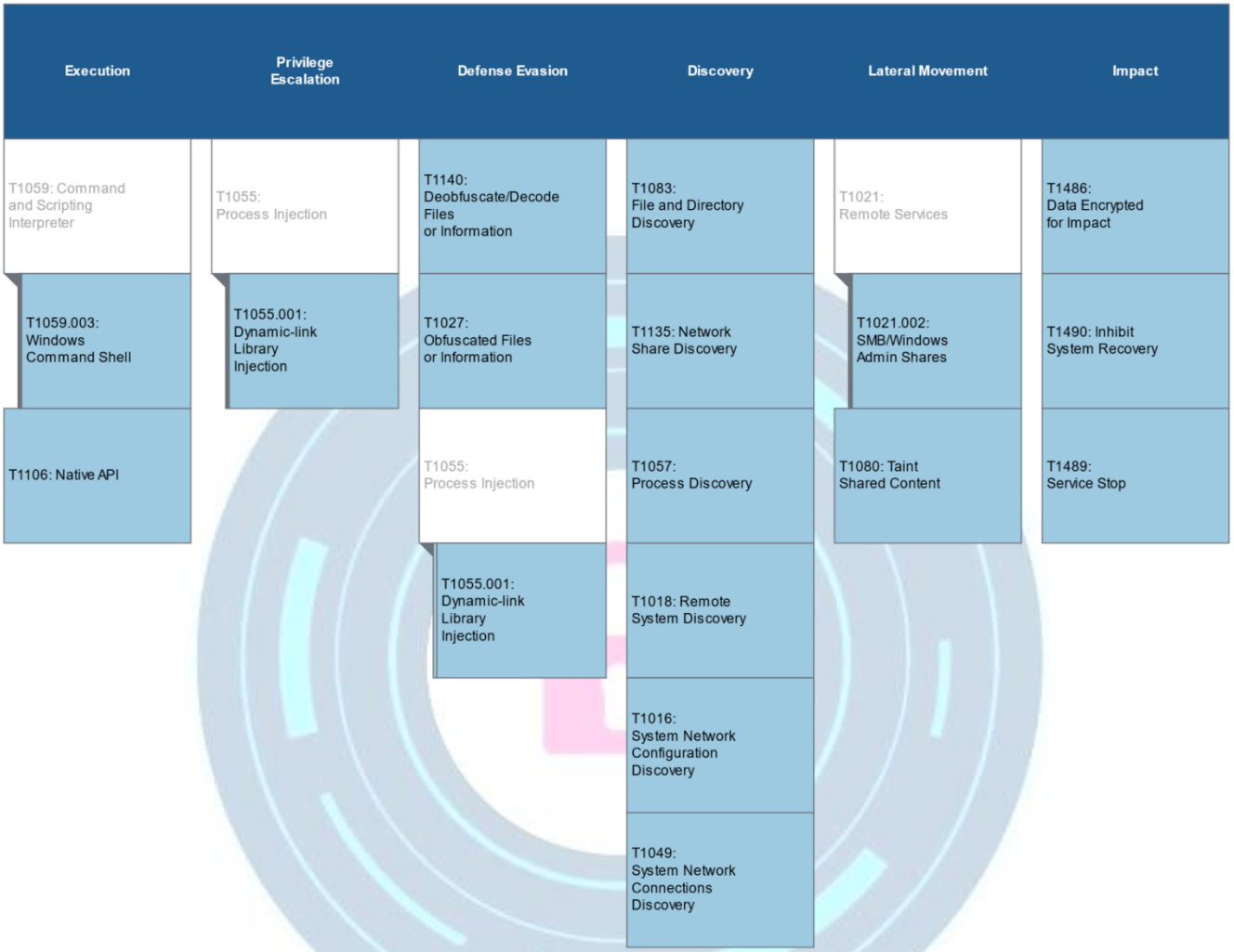

Figura No. 6. *TTP de Conti.* ***Fuente:*** *MITRE ATT&CK.*

Indicadores de compromiso

A continuación, se presentan algunos de los servidores comando y control del grupo Conti, desde donde se siguen instrucciones y hacia donde se migra la información exfiltrada de la entidad afectada.

162[.]244[.]80[.]235
85[.]93[.]88[.]165
185[.]141[.]63[.]120
82[.]118[.]21[.]1

Vulnerabilidades explotadas por Conti

- Log4Shell
- Spring4Shell
- REST F5
- Printnightmare
- Vulnerabilidades asociadas a SMB

Recomendaciones:

- Implementar políticas y procedimientos de backups para la entidad/organización.
- Implemente seguridad en los hosts como, Por ejemplo, en Windows 10, las reglas de reducción de superficie de ataque (ASR) que pueden evitar que las aplicaciones de Office inyecten código
- Implemente módulos de kernel para controlar el acceso a procesos, tal es el caso de SELinux, grsecurity y AppArmor.
- Supervise los metadatos de los archivos firmas, encabezados o datos, usuarios, permisos.
- Identifique archivos DLL o PE que sean anómalos o desconocidos.
- Supervise procesos que puede abusar del Shell de comandos de Windows y restrinja permisos elevados solo a personal administrativo.
- Restrinja las comunicaciones de uso compartido de archivos como SMB.
- Utilice contraseñas robustas, largas y complejas, al igual que cámbielas periódicamente, establezca políticas de acceso y contraseñas.

Referencias

- Twitter.
- MITRE ATT&CK.

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con ColCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT