CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Inteligencia de AMENAZAS

14TCA23-00015-01
Ransomware
BabLock

31 de octubre de 2023

Índice

Resumen ejecutivo

El presente informe detalla el análisis forense realizado sobre un binario detectado en el ataque informático a la infraestructura tecnológica de un proveedor chileno, al que nos referimos en el cuerpo del informe como “ISP” o “empresa”. El ataque fue detectado en la mañana del lunes 23 de octubre de 2023, y causó la caída de los sistemas de al menos 12 servicios públicos, algunos de ellos críticos.

En el informe, explicamos las funcionalidades observadas en el ransomware encontrado, mediante el uso de técnicas de ingeniería reversa sobre el archivo. Esto nos permite entender con mayor profundidad las acciones realizadas por el mismo y sus posibles repercusiones en la infraestructura y datos de los sistemas afectados. A pesar de que nuestros analistas no pudieron replicar la conducta del ransomware, y por tanto no pudieron confirmar la identidad del malware, todo lo observado sugiere fuertemente que se trata de BabLock, una familia de ransomware que tiene algunas similitudes con Babuk.

A pesar de que la empresa colaboró con el CSIRT, nuestros analistas no obtuvieron acceso físico a los servidores de la empresa; por tanto, todos los análisis presentados en el documento se realizaron sobre binarios recogidos por la empresa, en condiciones controladas por ésta.

El documento finaliza con una serie de recomendaciones para los encargados de ciberseguridad y administradores de infraestructura, con el objeto de evitar ser afectado por un ransomware como el detallado previamente.

Descripción de los hallazgos

IoC y contexto

Nombre Archivo	Descripción	SHA256
log.dll	Ransomware DLL	58c20b0602b2e0e6822d415b5e8b53c348727d8e145b1c096a6e46812c0f0cbc
TmDbgLog.dll	Ransomware DLL	5822b7c0b07385299ce72788fd058ccadc5ba926e6e9d73e297c1320feebe33f
u.exe	Vector de carga lateral de DLL (TrendMicro AirSupport versión 6.0.0.2045)	43a3fd549edbdf0acc6f00e5ceaa54c086ef048593bfbb9a5793f52a7cc57d1c
d.exe	Vector de carga lateral de DLL (BitDefender Update Downloader versión 4.0.22.44)	3476f0e0a4bd9f438761d9111bccff7a7d71afdc310f225bfebfb223e58731e6

Cabe destacar que los programas u.exe y d.exe detectados en las máquinas infectadas son aplicaciones legítimas de distintos antivirus. Sin embargo, el atacante aprovechó vulnerabilidades existentes en ellas para la carga lateral de las DLL maliciosas.

El atacante cargó a la máquina comprometida dos archivos ejecutables, por lo que no es necesario que la máquina afectada tenga estos programas instalados en ella.

Acciones realizadas

El lunes 23 de octubre, alrededor de las 18:00 horas, el ISP compartió con el CSIRT logs de seguridad perimetral relevantes.

El martes 24, alrededor de las 9:00 horas, la empresa compartió 4 binarios recogidos por la misma empresa: 2 archivos ejecutables y 2 librerías de linkeo dinámico (DLL). La información fue complementada con observaciones y archivos recogidos por personal de la empresa. El CSIRT se dedicó a recrear la línea de tiempo del ataque y a estudiar el comportamiento de los binarios, con y sin conexión a Internet. Se realizaron muchas pruebas y se observó el comportamiento de los binarios en diversas condiciones, pero no se logró replicar la encriptación de archivos en máquinas físicas o virtuales.

El miércoles 25 de octubre el ISP entregó archivos encriptados, una nota de rescate y nuevos logs de registros.

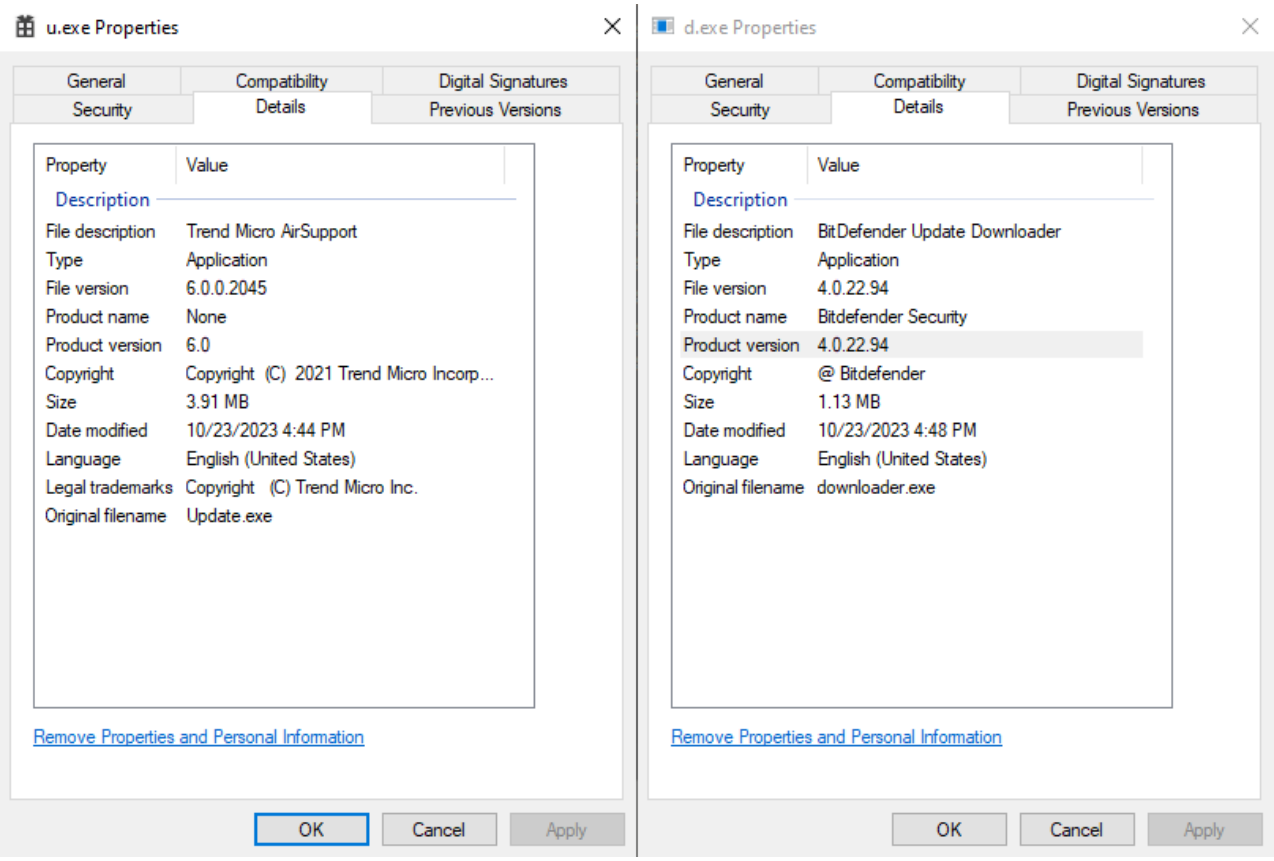
El viernes 27 el ISP avisó al CSIRT del hallazgo de un binario en un servidor encriptado que podría permitir replicar la encriptación de archivos. El ISP dio acceso al equipo del CSIRT a uno de sus data centers para observar, sin contacto físico, el servidor en cuestión. Entregó al CSIRT los registros de eventos de la máquina física, que se encontraba aislada de la red. No se logró obtener más información de la que ya se tenía.

Nuestro equipo ejecutó el binario encontrado en el servidor (d.exe) en varias condiciones posibles, sin obtener los resultados esperados (encriptación de los archivos de la máquina infectada). Sin embargo, en el proceso se observa el siguiente comportamiento:

1. Si el malware no tiene salida o conexión a Internet por medio de ping en modo oculto, éste no se ejecuta y no encripta el equipo víctima.
2. El malware requiere de la existencia de un archivo específico (config.ini), que es lanzado con notepad.exe y es eliminado una vez encriptada la máquina.
3. La ejecución del binario debe ser realizada incluyendo en la línea de comando una llave de sincronización. Esta llave es verificada por el malware. No sabemos si ésta es única para todas las infecciones, ni si es validada contra un servidor central.
4. Se observa también la búsqueda de existencia de un archivo de texto (isbwii.txt) cada dos segundos, sin el cual la DLL maliciosa no actúa.
5. Es muy probable que el malware posea módulos anti-VM y anti-debugging.

El binario d.exe corresponde a una versión firmada pero caduca de Bitdefender versión 4.0.22.94; el otro (u.exe) corresponde también a una versión firmada pero caduca de Trend Micro AirSupport, versión 6.0.0.2045. Ambos archivos son utilizados por el atacante.

En la siguiente imagen observamos las propiedades de los dos binarios.



El malware utiliza la técnica de carga lateral de librerías dinámicas que apuntan al software vulnerable legítimo u.exe y d.exe. Durante la ejecución del ransomware, se detectan eventos registrados para el proceso C:\Program Files\Bitdefender\Endpoint Security\EPSecurityService.exe. ID: 4663.

En estos eventos, se hace referencia a programas de sistema tales como cmd.exe, find.exe, sc.exe y conhost.exe. Esto es ejecutado desde el proceso EPSecurityService.exe, como parte de la explotación de la vulnerabilidad CVE-2019-17099.

En la siguiente tabla se indican las técnicas y tácticas[1] observadas en el archivo log.dll:

ID	Descripción de técnica	Descripción de táctica
T1027.005	Archivos o información ofuscada	Evasión de defensas

[1] De acuerdo con el framework Mitre Att&ck (https://attack.mitre.org/).

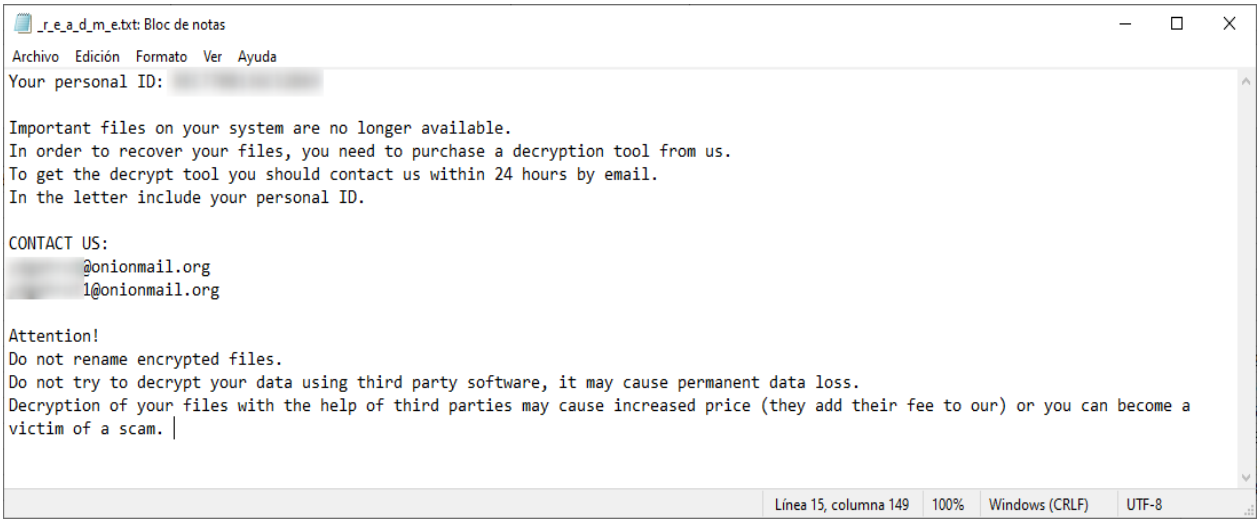
ID	Descripción de técnica	Descripción de táctica
T1083	Descubrimiento de archivos y carpetas	Descubrimiento
T1057	Descubrimiento de procesos	Descubrimiento
T1082	Descubrimiento de información de sistema	Descubrimiento
T1059	Intérprete de comandos y scripts	Ejecución
T1129	Módulos compartidos	Ejecución

En la tabla siguiente se observan las técnicas y tácticas observadas en el archivo TmDbLog.dll:

ID	Descripción de técnica	Descripción de táctica
T1027.005	Archivos o información ofuscada	Evasión de defensas
T1083	Descubrimiento de archivos y carpetas	Descubrimiento
T1082	Descubrimiento de información de sistema	Descubrimiento
T1129	Módulos compartidos	Ejecución

Nota de Secuestro

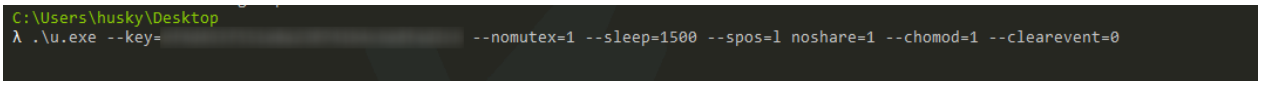
La nota de secuestro contiene el siguiente texto:



La extensión con la que quedan los archivos luego de ser encriptados es xzydr.

Vectores de ejecución

La ejecución del binario u.exe entregado por el ISP no es compleja; sólo requiere de un parámetro: una llave de sincronización. En la imagen siguiente se muestra la ejecución; a continuación, se muestra el texto de la llamada en consola.



% u.exe --key={Key Sincronización} --nomutex=1 --sleep=1500 --spos=l --noshare=1 --chmod=1 --clearevent=1

El archivo u.exe es utilizado por el malware en DLL para la ejecución de su código. Al momento de la ejecución éste usa la librería dinámica llamada TmDbglog.dll, que se encuentra en el mismo directorio. Observamos un problema de buffer overflow, lo que no es un error pues el programa está solicitando datos cuya longitud se desconoce y para esto proporciona un buffer inicial. Al ser este tamaño de memoria demasiado pequeño, se devuelve un buffer overflow junto con el tamaño necesario y el programa puede remitir la petición con el tamaño de memoria correcto.

u.exe	1600	CreateFile	C:\Users\husky\Desktop\TmDbgLog.dll	SUCCESS
u.exe	1600	CloseFile	C:\Users\husky\Desktop\TmDbgLog.dll	SUCCESS
u.exe	1600	CloseFile	C:\Users\husky\Desktop\TmDbgLog.dll	SUCCESS
u.exe	1600	CreateFile	C:\Users\husky\Desktop\TmDbgLog.dll	SUCCESS
u.exe	1600	QuerySecurityFile	C:\Users\husky\Desktop\TmDbgLog.dll	BUFFER OVERFLOW
u.exe	1600	QuerySecurityFile	C:\Users\husky\Desktop\TmDbgLog.dll	SUCCESS
u.exe	1600	CloseFile	C:\Users\husky\Desktop\TmDbgLog.dll	SUCCESS

En la siguiente imagen el binario u.exe queda en una especie de bucle realizando llamadas, creando y cerrando archivos que están en el escritorio de la máquina de sandbox.

u.exe	1600	QueryDirectory	C:\Users\husky\Desktop*	SUCCESS
u.exe	1600	QueryDirectory	C:\Users\husky\Desktop	SUCCESS
u.exe	1600	QueryDirectory	C:\Users\husky\Desktop	NO MORE FILES
u.exe	1600	CloseFile	C:\Users\husky\Desktop	SUCCESS
u.exe	1600	CreateFile	C:\Users\husky\Desktop\README.txt	SUCCESS
u.exe	1600	QueryStandardI...	C:\Users\husky\Desktop\README.txt	SUCCESS
u.exe	1600	ReadFile	C:\Users\husky\Desktop\README.txt	SUCCESS
u.exe	1600	CloseFile	C:\Users\husky\Desktop\README.txt	SUCCESS
u.exe	1600	CreateFile	C:\Users\husky\Desktop\u.txt	SUCCESS
u.exe	1600	QueryStandardI...	C:\Users\husky\Desktop\u.txt	SUCCESS
u.exe	1600	ReadFile	C:\Users\husky\Desktop\u.txt	SUCCESS
u.exe	1600	CloseFile	C:\Users\husky\Desktop\u.txt	SUCCESS

Por otra parte, la ejecución del binario d.exe también es simple: requiere de un solo parámetro.

```
C:\Users\husky\Desktop
λ d.exe -k 6f4d455f551e0a230741b4c6e8fad2c6
```

% d.exe -k {Key de Sincronización}

El archivo d.exe es utilizado por el malware para la ejecución de su código. Al momento de la ejecución del binario malicioso éste usa una librería dinámica llamada log.dll, la cual es creada al momento de la ejecución del binario.

```
d.exe    6744  CreateFileMapping  C:\Users\husky\Desktop\log.dll                                                  SUCCESS
d.exe    6744  Load Image         C:\Users\husky\Desktop\log.dll                                                  SUCCESS
d.exe    6744  RegOpenKey         HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide                       SUCCESS
d.exe    6744  RegQueryValue      HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest NAME NOT FOUND
d.exe    6744  RegCloseKey        HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide                       SUCCESS
d.exe    6744  CreateFile         C:\Users\husky\Desktop\log.dll                                                  SUCCESS
d.exe    6744  CloseFile          C:\Users\husky\Desktop\log.dll                                                  SUCCESS
```

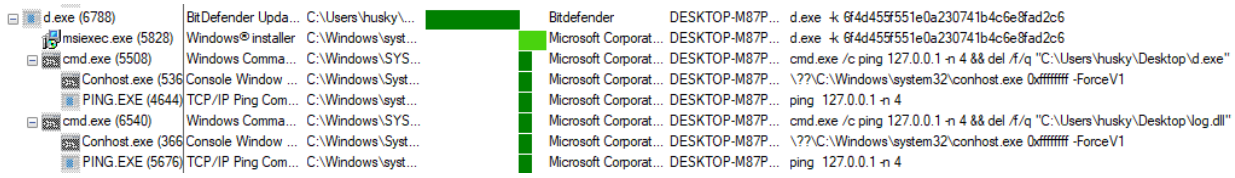
Luego queda en una especie de bucle, al igual que el binario anterior. En este caso busca un archivo de texto llamado isbwii.txt, lo que no permite la siguiente fase maliciosa del ransomware.

```
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  CreateFile     C:\Users\husky\Desktop\isbwii.txt    NAME NOT FOUND
d.exe    6744  Thread Exit                                         SUCCESS
d.exe    6744  Thread Exit                                         SUCCESS
d.exe    6744  Thread Create                                       SUCCESS
```

Una vez que creamos el archivo de texto que este binario intenta crear, el binario usa el archivo msiexec.exe, donde realiza una petición de información del volumen y otra petición de toda la información del archivo. Finalmente, el binario d.exe es eliminado del sistema junto con la librería dinámica (DLL).

```
d.exe    6788  CloseFile          C:\Users\husky\Desktop\isbwii.txt
d.exe    6788  CreateFile         C:\Windows\System32\msiexec.exe
d.exe    6788  QueryInformatio...C:\Windows\System32\msiexec.exe
d.exe    6788  QueryAllInforma...C:\Windows\System32\msiexec.exe
d.exe    6788  ReadFile           C:\Windows\System32\msiexec.exe
d.exe    6788  ReadFile           C:\Windows\System32\msiexec.exe
d.exe    6788  ReadFile           C:\Windows\System32\msiexec.exe
d.exe    6788  CloseFile          C:\Windows\System32\msiexec.exe
d.exe    6788  RegOpenKey         HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msiexec.exe
d.exe    6788  RegOpenKey         HKLM\Software\Microsoft\Wow64\x86\xtajit
d.exe    6788  CreateFile         C:\Windows\System32\msiexec.exe
d.exe    6788  CreateFileMapp...C:\Windows\System32\msiexec.exe
d.exe    6788  CreateFileMapp...C:\Windows\System32\msiexec.exe
```

En esta última imagen observamos los comandos usados en la ejecución del binario, seguida de su transcripción:



- d.exe -k 6f4d455f551e0a230741b4c6e8fad2c6
- cmd.exe /c ping 127.0.0.1 -n 4 && del /f/q "C:\Users\husky\Desktop\d.exe"
- \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- ping 127.0.0.1 -n 4
- cmd.exe /c ping 127.0.0.1 -n 4 && del /f/q "C:\Users\husky\Desktop\log.dll"
- \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- ping 127.0.0.1 -n 4

Recomendaciones

A continuación, agrupamos las recomendaciones realizadas por el CSIRT en comunicados previos a los equipos de ciberseguridad y tecnología. El objetivo de estas recomendaciones es mitigar el impacto que podría provocar una infección con un malware como el analizado en este reporte:

- Utilizar usuarios con privilegios mínimos.
- Minimizar la cantidad de puertos abiertos.
- Monitorear conexiones a IP y puertos no reconocidos.
- Restringir acceso a través de SSH.
- Implementar herramientas de seguridad especializadas en servidores tanto para máquinas virtuales y contenedores alojados en el servidor.
- Realizar copias de seguridad regularmente, las que deben ser almacenadas en diferentes lugares y medios, incluyendo una copia fuera de línea o de la institución.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.31 22:35:15 -03'00'