Alerta de Seguridad Informática (2CMV-00016-001)

Nivel de Riesgo: Alto

Tipo: Informe de Ransomware

Fecha de lanzamiento original: 06 de Julio de 2019 | Última revisión 06 de Julio de 2019

Notificación

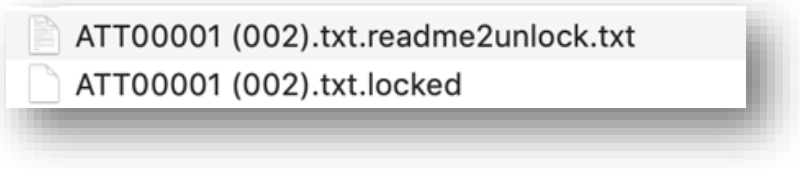
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

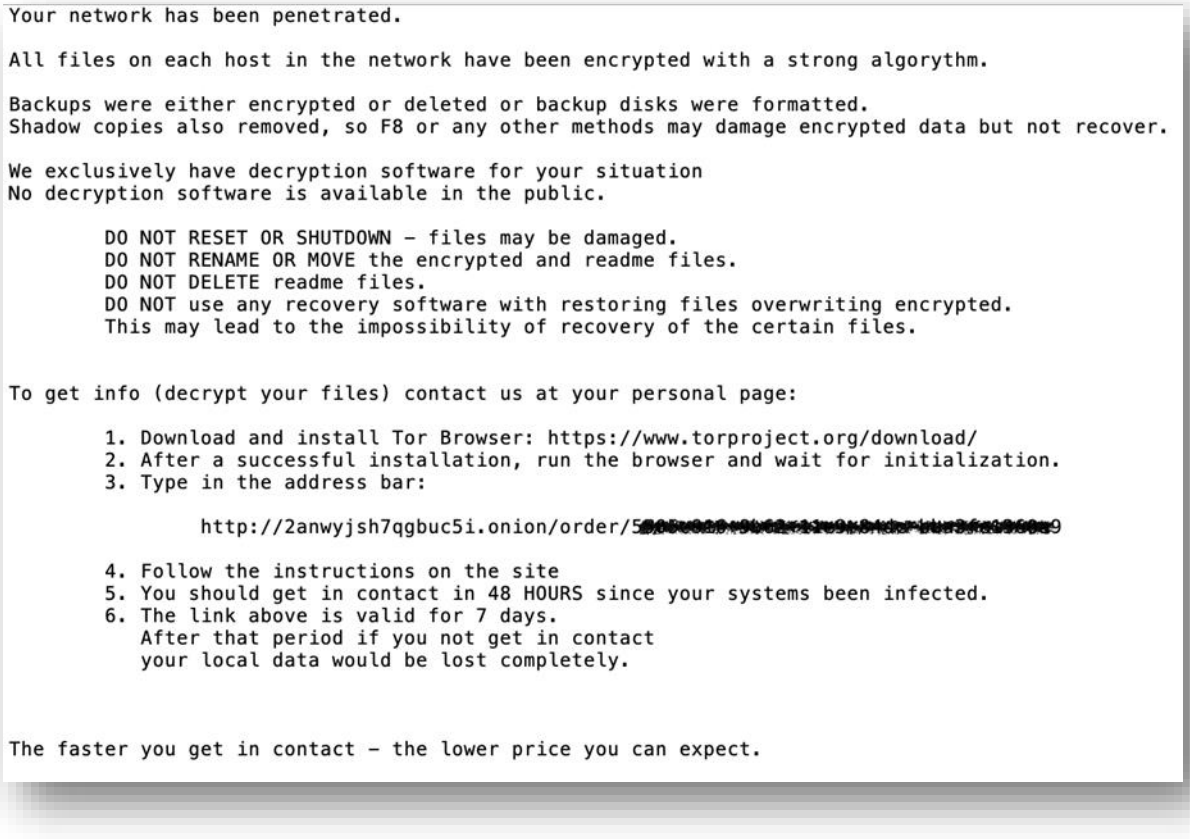
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha detectado muestras de Ransomware coincidentes con una nueva variante de BitPaymer, que afecta sistemas operativos de la familia Windows de Microsoft.

Dentro de los efectos producidos por el Ransomware, están los de cifrar archivos de extensiones conocidas, modificándolas a ".locked", junto con la creación de un nuevo archivo el cual mantiene el nombre original seguido de la extensión txt.

En su interior se explican las instrucciones para la recuperación de la data original.



Ejemplos de Archivos Cifrados



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: https://www.torproject.org/download/
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

                http://2anwyjsh7qgbuc5i.onion/order/5[redacted]9

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 7 days.
           After that period if you not get in contact
           your local data would be lost completely.


The faster you get in contact - the lower price you can expect.
```

Contenido de Archivo Txt

Dentro de las instrucciones se requiere visitar un enlace “.onion” siendo necesario acceder a la red Tor.

http[:]//2anwyjsh7qgbuc5i[.]onion/order/

Detalles técnicos

Se detectó comportamiento anómalo con el archivo asociado al hash que se indica más adelante.

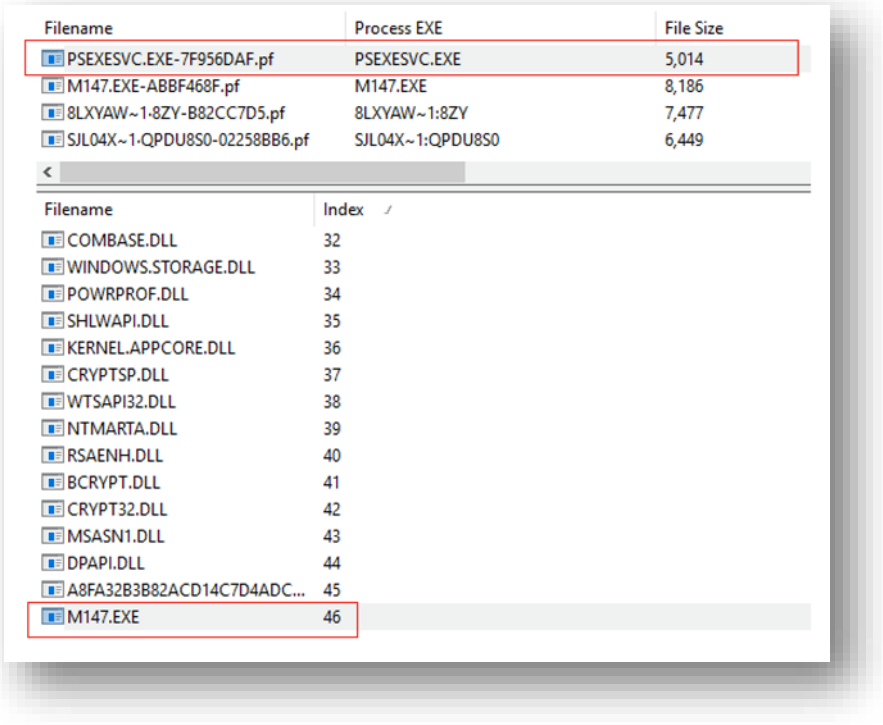
Herramientas de sandboxing tradicional muestran la existencia de mecanismos de cifrado dentro de su actividad. Sin embargo, para la ejecución del mismo se requieren librerías adicionales que no están presentes en esta muestra.

Además, existe la utilización de mecanismos de ocultación dentro del sistema operativo por medio del empleo de ADS (Alternate Data Stream).

Evidencias

El registro de archivos ejecutados muestra el historial de librerías y procesos levantados a través de PSEXESVC.EXE

A su vez, M147.EXE carga elementos ocultos mediante ADS tal como se ilustra en la siguiente imagen

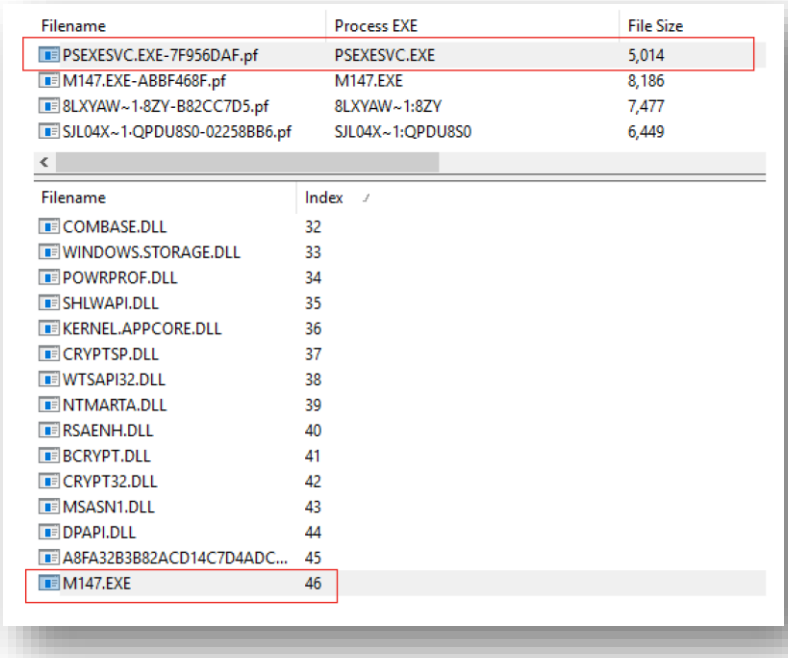


Filename	Process EXE	File Size
PSEXESVC.EXE-7F956DAF.pf	PSEXESVC.EXE	5,014
M147.EXE-ABBF468F.pf	M147.EXE	8,186
8LXYAW~1-8ZY-B82CC7D5.pf	8LXYAW~1:8ZY	7,477
SJL04X~1-QPDU8S0-02258BB6.pf	SJL04X~1:QPDU8S0	6,449

Filename	Index
COMBASE.DLL	32
WINDOWS.STORAGE.DLL	33
POWRPROF.DLL	34
SHLWAPI.DLL	35
KERNEL.APPCORE.DLL	36
CRYPTSP.DLL	37
WTSAPI32.DLL	38
NTMARTA.DLL	39
RSAENH.DLL	40
BCRYPT.DLL	41
CRYPT32.DLL	42
MSASN1.DLL	43
DPAPI.DLL	44
A8FA32B3B82ACD14C7D4ADC...	45
M147.EXE	46

Se establece que la ejecución queda registrada en System log de Windows, el cual coincide con los horarios consignados por el prefetch del sistema operativo

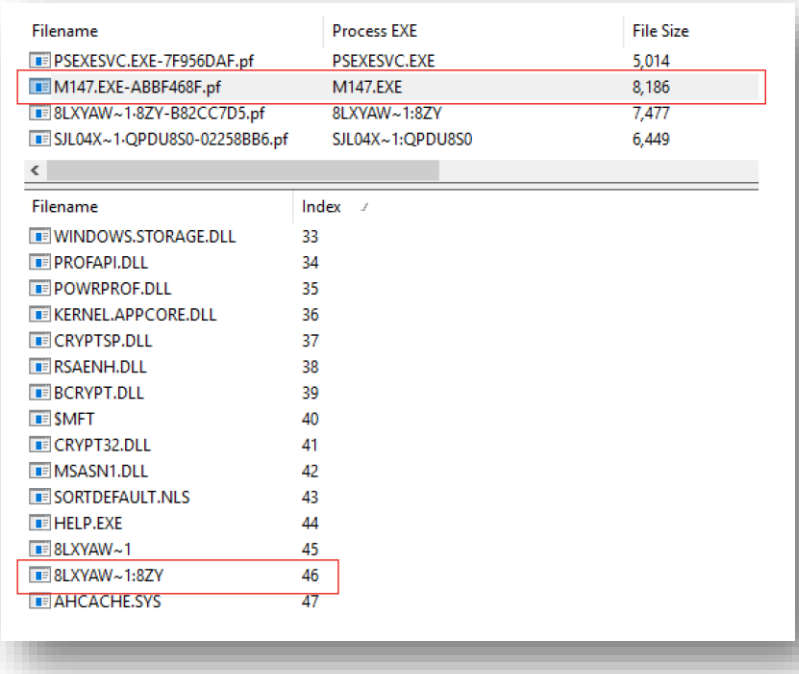
El registro de archivos ejecutados muestra el historial de librerías y procesos levantados a través de PSEXESVC.EXE



Filename	Process EXE	File Size
PSEXESVC.EXE-7F956DAF.pf	PSEXESVC.EXE	5,014
M147.EXE-ABBF468F.pf	M147.EXE	8,186
8LXYAW~1·8ZY-B82CC7D5.pf	8LXYAW~1:8ZY	7,477
SJL04X~1·QPDU8S0-02258BB6.pf	SJL04X~1:QPDU8S0	6,449

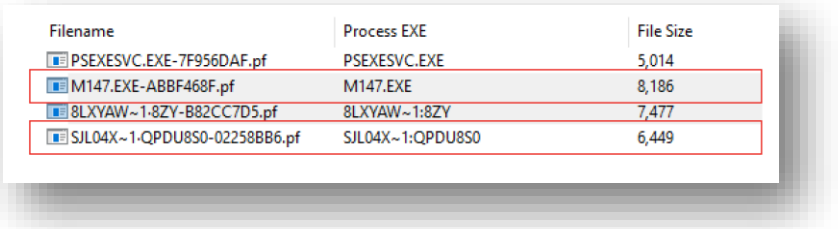
Filename	Index
COMBASE.DLL	32
WINDOWS.STORAGE.DLL	33
POWRPROF.DLL	34
SHLWAPI.DLL	35
KERNEL.APPCORE.DLL	36
CRYPTSP.DLL	37
WTSAPI32.DLL	38
NTMARTA.DLL	39
RSAENH.DLL	40
BCRYPT.DLL	41
CRYPT32.DLL	42
MSASN1.DLL	43
DPAPI.DLL	44
A8FA32B3B82ACD14C7D4ADC...	45
M147.EXE	46

A su vez, M147.EXE carga elementos ocultos mediante ADS tal como se ilustra en la siguiente imagen



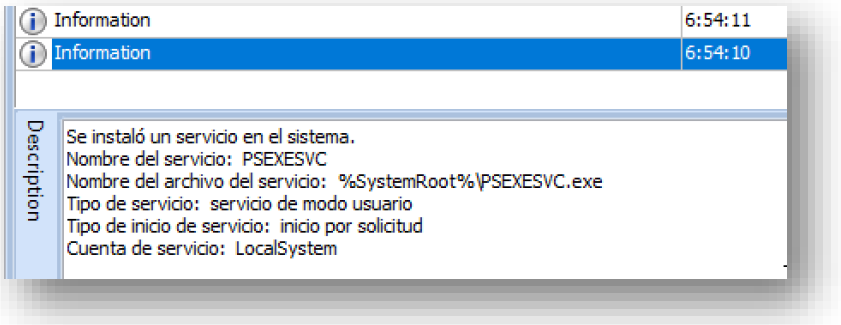
Filename	Process EXE	File Size
PSEXESVC.EXE-7F956DAF.pf	PSEXESVC.EXE	5,014
M147.EXE-ABBF468F.pf	M147.EXE	8,186
8LXYAW~1·8ZY-B82CC7D5.pf	8LXYAW~1:8ZY	7,477
SJL04X~1·QPDU8S0-02258BB6.pf	SJL04X~1:QPDU8S0	6,449

Filename	Index
WINDOWS.STORAGE.DLL	33
PROFAPI.DLL	34
POWRPROF.DLL	35
KERNEL.APPCORE.DLL	36
CRYPTSP.DLL	37
RSAENH.DLL	38
BCRYPT.DLL	39
$MFT	40
CRYPT32.DLL	41
MSASN1.DLL	42
SORTDEFAULT.NLS	43
HELP.EXE	44
8LXYAW~1	45
8LXYAW~1:8ZY	46
AHCACHE.SYS	47



Filename	Process EXE	File Size
PSEXESVC.EXE-7F956DAF.pf	PSEXESVC.EXE	5,014
M147.EXE-ABBF468F.pf	M147.EXE	8,186
8LXYAW~1-8ZY-B82CC7D5.pf	8LXYAW~1:8ZY	7,477
SJL04X~1-QPDU8S0-02258BB6.pf	SJL04X~1:QPDU8S0	6,449

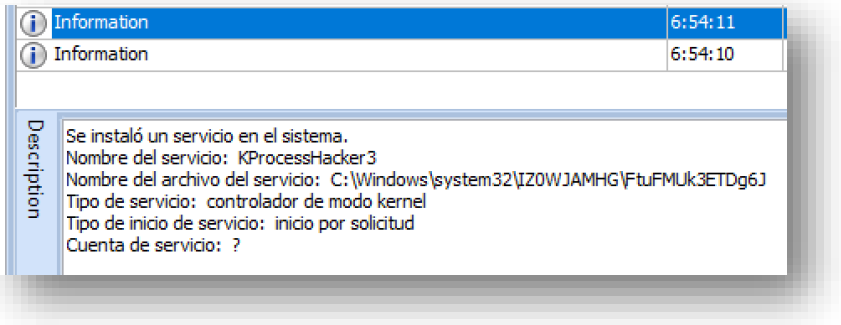
Se establece que la ejecución queda registrada en System log de Windows, el cual coincide con los horarios consignados por el prefetch del sistema operativo



Information	6:54:11
Information	6:54:10

Description

Se instaló un servicio en el sistema.
Nombre del servicio: PSEXESVC
Nombre del archivo del servicio: %SystemRoot%\PSEXESVC.exe
Tipo de servicio: servicio de modo usuario
Tipo de inicio de servicio: inicio por solicitud
Cuenta de servicio: LocalSystem



Information	6:54:11
Information	6:54:10

Description

Se instaló un servicio en el sistema.
Nombre del servicio: KProcessHacker3
Nombre del archivo del servicio: C:\Windows\system32\IZ0WJAMHG\FtuFMUk3ETDg6J
Tipo de servicio: controlador de modo kernel
Tipo de inicio de servicio: inicio por solicitud
Cuenta de servicio: ?

Indicadores de Compromiso

Payload de BitPaymer

Filename (el malware genera nombres aleatorios)

WASpotLife.DLL

SHA-256

801b04a1504f167c25f568f8d7cbac13bdde6440a609d0dcd64ebe225c197f9b

Para despliegue en la red

Filename
PSEXESVC.EXE

SHA-256
3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Actualizar los antivirus a sus últimas versiones y base de datos de protección
- No desactivar funciones de seguridad de antivirus u otro sistema de protección

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob