CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Inteligencia de AMENAZAS

14TCA23-00017-01
Ransomware BlackSuit en el Sector Publico

7 de diciembre de 2023

Índice

Resumen ejecutivo

El siguiente informe detalla el análisis forense realizado sobre un binario detectado en un ataque informático a la infraestructura tecnológica de una institución pública. Este análisis fue realizado entre el 18 y 19 de octubre a partir de muestras extraídas directamente desde un servidor infectado ubicado físicamente en las dependencias de este servicio público.

Dentro de las características de este ransomware, conocido como BlackSuit, está el realizar escaneos de red para determinar su topología, el eliminar copias de respaldo contenidas dentro de la máquina infectada y la verificación de conectividad. Otra particularidad es que la ejecución de este binario requiere de una llave o ID de 32 caracteres, el que es asignado a cada víctima.

En el análisis dinámico de BlackSuit revela el uso de funciones de HeapApi relacionadas con la gestión de memoria asignada, y de funciones de WinBase para liberar objetos de memoria local e invalidar sus identificadores.

Finalmente presentamos una serie de recomendaciones para los administradores de infraestructura, con el objetivo de evitar ser afectados por este ransomware. Entre ellas, la de definir sus usuarios con el mínimo de privilegios necesario, minimizar la cantidad de puertos abiertos, monitorear las conexiones a IP y puertos no reconocidos, restringir el acceso a través de SSH, implementar herramientas de seguridad especializadas en sus servidores y realizar copias de seguridad regularmente.

Descripción de los hallazgos

IoC y contexto

SHA256	Nombre Archivo	Descripción
3166aeb7e9a37c25fe8a64455b0700d76aff7f64b953357a568beeaed125c353	aaaa.exe, locker_iZ.exe	Ransomware

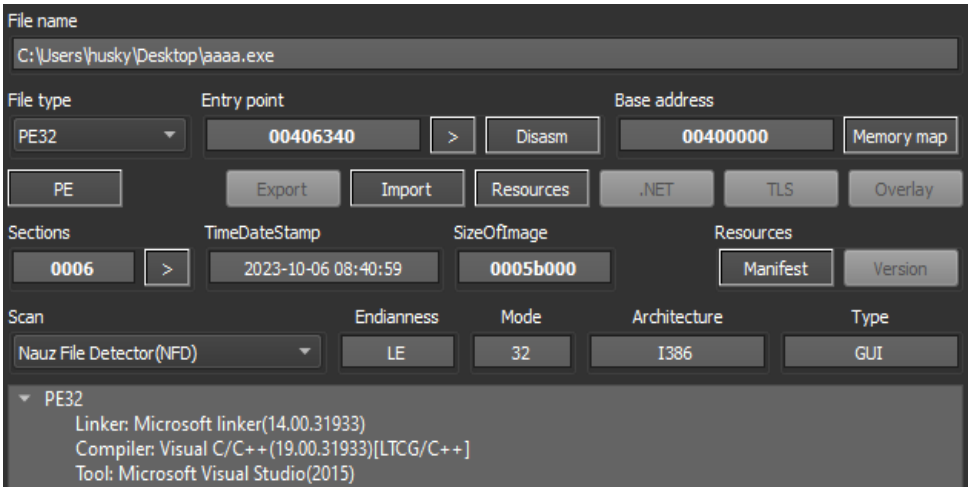
El archivo fue detectado en uno de los servidores afectados en la infraestructura.

Matriz Mitre ATT&CK:

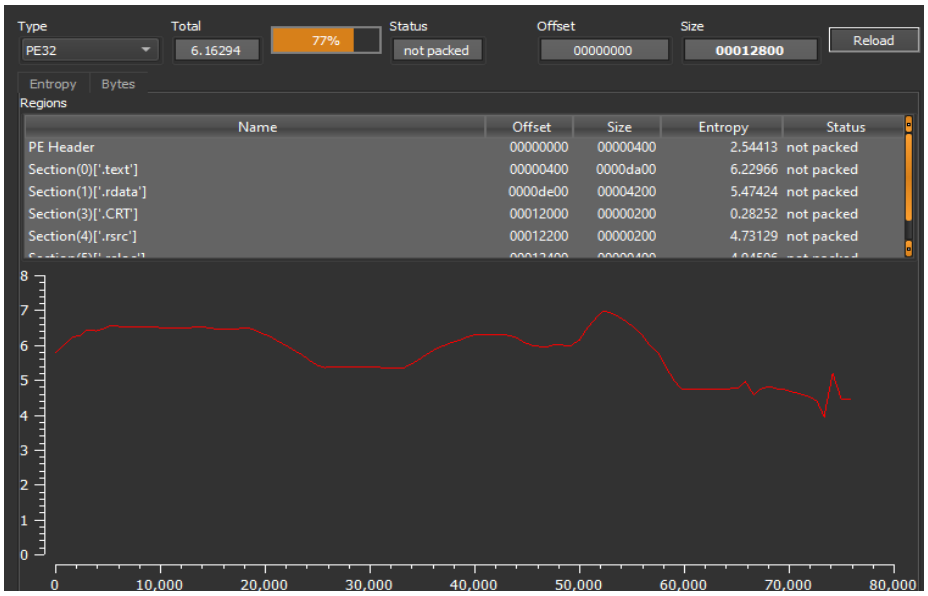
ID	Descripción de técnica	Descripción de táctica
T1129	Módulos compartidos	Ejecución
T1057	Proceso de descubrimiento	Descubrimiento
T1082	Descubrimiento de información del sistema	Descubrimiento
T1027	Archivos o información ofuscados	Evasión de Defensas
T1027.005	Extracción del indicador de las herramientas	Evasión de Defensas

Comportamiento dinámico inicial del archivo malicioso

El ransomware BlackSuit está compilado en C++. Este ransomware está siendo usado por el actor de amenazaa (ATA) para ser dirigido tanto a usuarios de sistemas operativos Windows como Linux.



Asimismo, observamos que la entropía del archivo ejecutable (medida de desorden de un software, que refleja su complejidad) es de 6.16, considerada como alta (el valor máximo es 8). A medida que se realizan modificaciones o se agrega código nuevo a un archivo, éste va perdiendo su estructura original, aumentando su entropía.



La creación del ransomware BlackSuit ocurrió el 06 de octubre de 2023 a las 08:40 AM.

compiler-stamp	0x65202A8B (Fri Oct 06 08:40:59 2023)
debugger-stamp	0x65202A8B (Fri Oct 06 08:40:59 2023)

Dentro del archivo ejecutable apreciamos un certificado, el cual cumple la función de Crypto Shell Extensions y genera la extensión en la fase de encriptación.

Name	Size	Packed Size	Virtual Size	Characteristics	Offset	Virtual Address
.rsrc	385	385				
.CRT	512	512	24	InitializedData ...	73 728	0x58000
.data	0	0	278 256	InitializedData ...	0	0x14000
.rdata	16 896	16 896	16 554	InitializedData ...	56 832	0xF000
.reloc	1 024	1 024	720	InitializedData ...	74 752	0x5A000
.text	55 808	55 808	55 786	Code Execute ...	1 024	0x1000

También se realizó una extracción de strings desde el binario de BlackSuit. A continuación, algunas funciones del heapapi.h.

- GetProcessHeap: Recupera un identificador del heap predeterminado del proceso de llamada. Luego, este identificador se puede utilizar en llamadas posteriores a las funciones del Heap.
- HeapAlloc: Asigna un bloque de memoria del heap. La memoria asignada no es extraíble. Si la función de HeapAlloc se realiza correctamente, asigna al menos la cantidad de memoria solicitada. Para asignar memoria desde el heap predeterminado del proceso, HeapAlloc usa el identificador devuelto por la función GetProcessHeap. Si se produce un error en la función, no llama a la función SetLastError. Una aplicación no puede llamar a GetLastError para obtener la información extendida.
- HeapFree: Libera un bloque de memoria asignado desde el heap con la función HeapAlloc o HeapReAlloc.
- GetLastError: Recupera el valor del último código de error del subproceso de llamada. El último código de error se mantiene en el subproceso. Varios subprocesos no sobrescriben el último código de error del otro.

Por otro lado, se observan funciones de winbase.h.

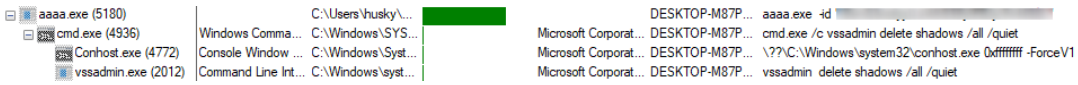
- LocalFree: Libera el objeto de memoria local especificado e invalida su identificador. Si la función se ejecuta correctamente, el valor devuelto es NULL. Si esto produce un error en la función, el valor de salida es igual a un identificador para el objeto de memoria local. Para obtener la información del error extendida, necesariamente se debe llamar a GetLastError.

```
MultiByteToWideChar
EnterCriticalSection
lstrlenW
WaitForMultipleObjects
LeaveCriticalSection
InitializeCriticalSection
FindClose
GetLastError
TerminateThread
WideCharToMultiByte
ExitProcess
lstrcatW
lstrcpyW
LocalFree
HeapFree
SetLastError
WriteConsoleA
HeapAlloc
GetProcessHeap
KERNEL32.dll
CharLowerW
USER32.dll
StrCpyNW
StrCmpNIW
```

Ejecución del Ransomware

Para su ejecución, BlackSuit es obligado incluir el parámetro "-id", que es un identificador de 32 caracteres distintos asignados a cada víctima.

- aaaa.exe -id "ID"
- cmd.exe /c vssadmin delete shadows /all /quiet
- \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- vssadmin delete shadows /all /quiet
- "C:\Windows\system32\cmd.exe" /C ping 1.1.1.1 -n 3 -w 5000 > Nul & Del /f /q "C:\Users\{Usuario}\Desktop\aaaa.exe"



Con el comando vssadmin delete shadows /all /quiet elimina todas las copias de los volúmenes, y luego comprueba por medio del comando ping si existe conexión a la IP 1.1.1.1 con un peso de 5000. Por último, el binario es eliminado del sistema.

Este malware también realiza un descubrimiento de la red en la que se ejecuta. Para esto, escanea desde la IP 10.0.0.0 hasta la 10.0.0.255.

```
231 214.513049900 PcsCompu_33:c5:ba    PcsCompu_51:c7:1d    ARP      60 Who has 10.0.0.3? Tell 10.0.0.4
244 237.263594430 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.0? Tell 10.0.0.4
245 237.263799704 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.1? Tell 10.0.0.4
246 237.263966668 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.2? Tell 10.0.0.4
249 237.264110921 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.5? Tell 10.0.0.4
250 237.264370901 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.6? Tell 10.0.0.4
251 237.264630805 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.7? Tell 10.0.0.4
252 237.264676358 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.8? Tell 10.0.0.4
253 237.264960872 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.9? Tell 10.0.0.4
254 237.265099668 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.10? Tell 10.0.0.4
255 237.265348615 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.11? Tell 10.0.0.4
256 237.265532670 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.12? Tell 10.0.0.4
257 237.265715422 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.13? Tell 10.0.0.4
258 237.265878899 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.14? Tell 10.0.0.4
259 237.266018133 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.15? Tell 10.0.0.4
260 237.266147748 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.16? Tell 10.0.0.4
261 237.266298309 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.17? Tell 10.0.0.4
262 237.266432951 PcsCompu_33:c5:ba    Broadcast            ARP      60 Who has 10.0.0.18? Tell 10.0.0.4
```

Por último, en el escaneo de la red infectada, el ransomware busca servicios SMB por el puerto 1452.

```
▸ Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_33:c5:ba (08:00:27:33:c5:ba), Dst: PcsCompu_51:c7:1d (08:00:27:51:c7:1d)
▸ Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
▾ Transmission Control Protocol, Src Port: 1452, Dst Port: 445, Seq: 0, Len: 0
    Source Port: 1452
    Destination Port: 445
    [Stream index: 0]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1122580662
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x002 (SYN)
```

Conclusión

Este análisis detallado del ransomware BlackSuit revela su peligrosa sofisticación y capacidad destructiva. El programa malicioso, compilado en C++, se dirige tanto a sistemas operativos Windows como Linux y se caracteriza por su complejidad, medida por una alta entropía en su archivo ejecutable.

Su fecha de creación, registrada el 6 de octubre de 2023, señala su reciente aparición en el panorama de ciberseguridad. Además, el uso de un certificado relacionado con Crypto Shell Extensions sugiere un enfoque meticuloso en la fase de encriptación.

La ejecución de BlackSuit implica la introducción de un identificador de víctima, seguido de la eliminación de copias de seguridad y comprobación de la conexión antes de su autodestrucción. El ransomware también muestra una capacidad de exploración de redes y búsqueda de servicios SMB en el puerto 1452.

En conjunto, BlackSuit representa una amenaza seria para la seguridad en línea y resalta la importancia de la ciberseguridad en la protección contra ataques cibernéticos avanzados.

Recomendaciones

A continuación, agrupamos las recomendaciones realizadas por el CSIRT en comunicados previos a los equipos de ciberseguridad y tecnología, con el objetivo de reducir el impacto de 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: 2023.12.11 15:19:38 -03'00'