22/02/2022

Alerta de Seguridad Digital

[TLP: WHITE]
[PAP: GREEN]

IoC - Ransomware BlackByte.

El auge de los ataques cibernéticos de tipo Ransomware a infraestructuras tecnológicas de entidades gubernamentales y empresas privadas viene en aumento, impactando considerablemente los servicios, aplicaciones y la operación en general, los cuales en su dinámica de operación vienen mutando, generando nuevas variantes, que no son detectados por los equipos y plataformas de seguridad.

A continuación, se recrea el entorno de ataque y se describe el modo de operación, indicadores de compromiso y recursos impactados por el Ransomware BlackByte.

Características más predominantes de BlackByte:

- Tiene funcionalidad de gusano en donde realiza consulta de otros posibles equipos objetivo, al conocer el alcance de infección, procede a propagarse a través de la red.
- Paquete Wake-on-LAN en donde se puede controlar de manera remota los equipos afectados al encenderlos cuando están apagados, hibernando o suspendidos.

En la figura No.1 se describen las fases de infección del Ransomware; la primera etapa es un Script principal ofuscado que al ejecutarlo desencadena un script de segunda fase que despliega un archivo DLL en la memoria, dando lugar a la tercera fase. El archivo DLL evade herramientas antimalware y antiransomware del sistema Windows, carga los archivos necesarios para la infección y propagación, finaliza procesos y aplicativos que obstaculizan el cifrado y genera un paquete Wake On LAN que da paso al cifrado de equipos inclusive si estos se encuentras apagados.

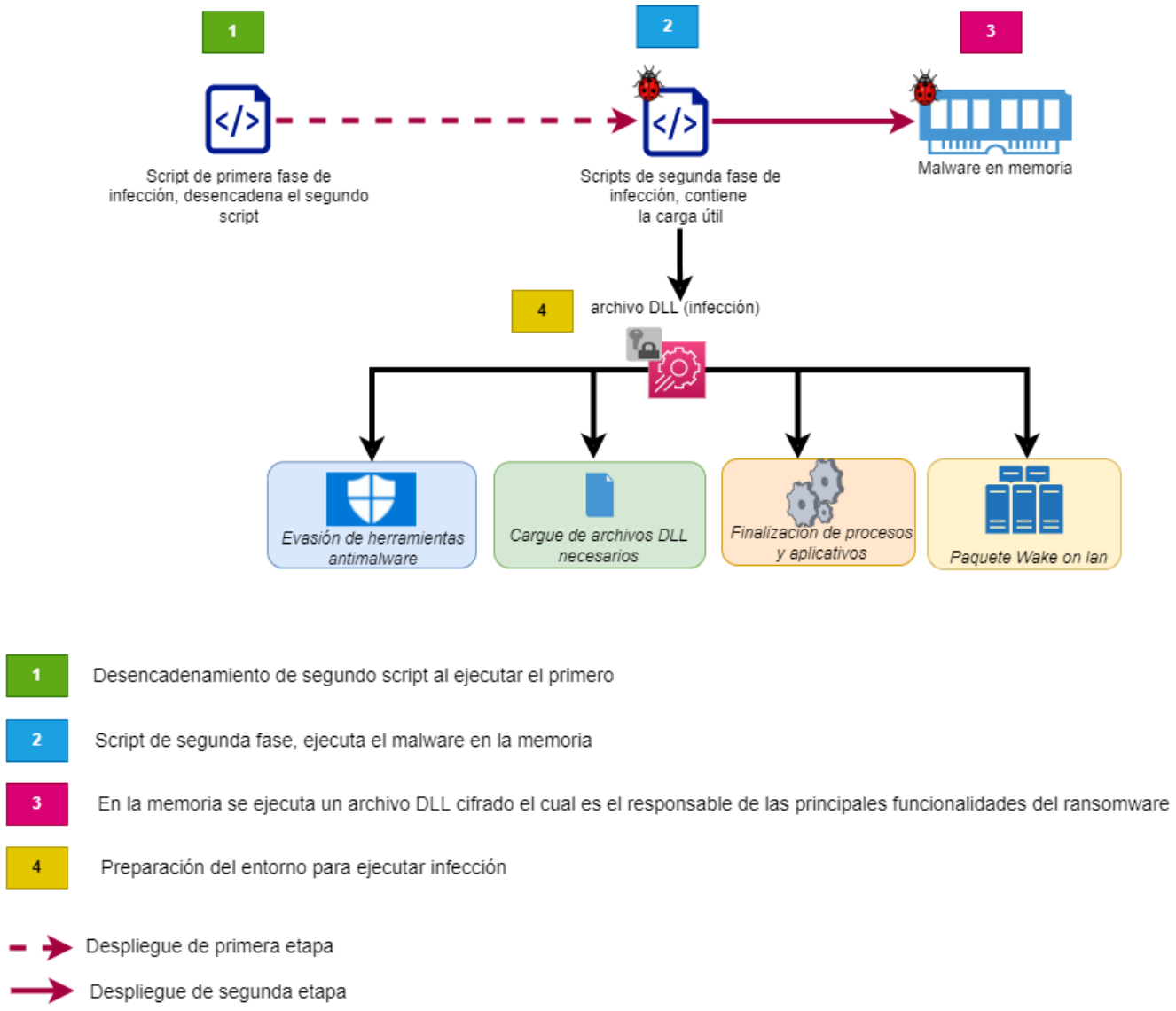

Figura No. 1. *Fases de infección de BlackByte. Fuente: CSIRT Gobierno.*

El primer Script el cual se encuentra ofuscado, decodifica el payload para ejecutarlo en memoria, el archivo DLL prepara el entorno a vulnerar de la siguiente manera:

- Evade herramientas como Windows Defender.
- Carga los DLL necesarios para la ejecución e infección.
- Generación del ID de la víctima de la siguiente forma; ID del procesador infectado y número de sesión del volumen, todo esto en MD5, al existir un ID es porque ya se ejecuta el Ransomware en la red.
- Eliminación de procesos y aplicativos que dificultan el cifrado de los archivos.
- Eliminación de las siguientes subclaves:

    - **vssadmin.exe**: backups existentes, shadow copies.
    - **wbadmin.exe**: permite realizar copias de seguridad y restauración de sistemas operativos, carpetas y aplicaciones.

- **Bcdedit.exe**: configuración de aplicaciones de arranque.
- **Powershell.exe**: realiza automatización de tareas a través de una shell de línea de comandos.
- **Diskshadow.exe**: realizar operaciones de instantáneas de volumen.
- **Net.exe**: configuración de ajustes de red.
- **Taskkill.exe**: ejecuta la herramienta de eliminación de tareas.
- **Wmic.exe**: ejecutable en el disco duro del equipo y que contiene el código máquina.

- Ejecución de SetThreadExecutionState para evitar que el equipo entre en suspensión o se apague la pantalla con el finde eliminar procesos.
- Finalización y evasión de Raccine (antiransomware de Windows).
- Eliminación de instantáneas en todos los volúmenes.
- Eliminación de puntos de restauración.
- Otorga acceso completo a unidades de destino.
- Eliminación de papelera de reciclaje.
- Blackbyte se copia a sí mismo en una ruta para crear una tarea programada en un host remoto para ejecutar el Script de primera fase.

Se observa a continuación la nota de rescate del grupo, en donde se informa acerca del cifrado de los datos y se listan los pasos para descifrarlos al contactar al grupo atacante.

```
All your files have been encrypted, your confidential data has been stolen,
in order to decrypt files and avoid leakage, you must follow our steps.

1) Download and install TOR Browser from this site: https://torproject.org/

2) Paste the URL in TOR Browser and you will be redirected to our chat with all information that you need.

3) If you do not contact us within 4 days, your chat access key won't be valid.
   Also, your company will be posted on our blog, darknet and hacker forums,
   which will attract unnecessary attention from journalists and not only them.
   You are given 4 days to think over the situation, and take reasonable actions on your part.

Warning! Communication with us occurs only through this link, or through our mail on our blog.
We also strongly DO NOT recommend using third-party tools to decrypt files,
as this will simply kill them completely without the possibility of recovery.
I repeat, in this case, no one can help you!
```

Figura No 2. *Nota de rescate con instrucciones de BlackByte. Fuente: CSIRT Gobierno.*

En la figura No. 3 y No. 4, se visualiza el blog oficial de BlackByte en donde se exponen algunas de las entidades objetivo; así como el correo de contacto del grupo.

Figura No. 3. *Blog oficial de BlackByte. Fuente: monitoreo en la Darkweb.*

Figura No 4. *Blog oficial de BlackByte. Fuente: monitoreo en la Darkweb.*

En la figura No 5, se detalla la llave de acceso proporcionada a la entidad vulnerada, la cual se especifica en la nota de rescate.

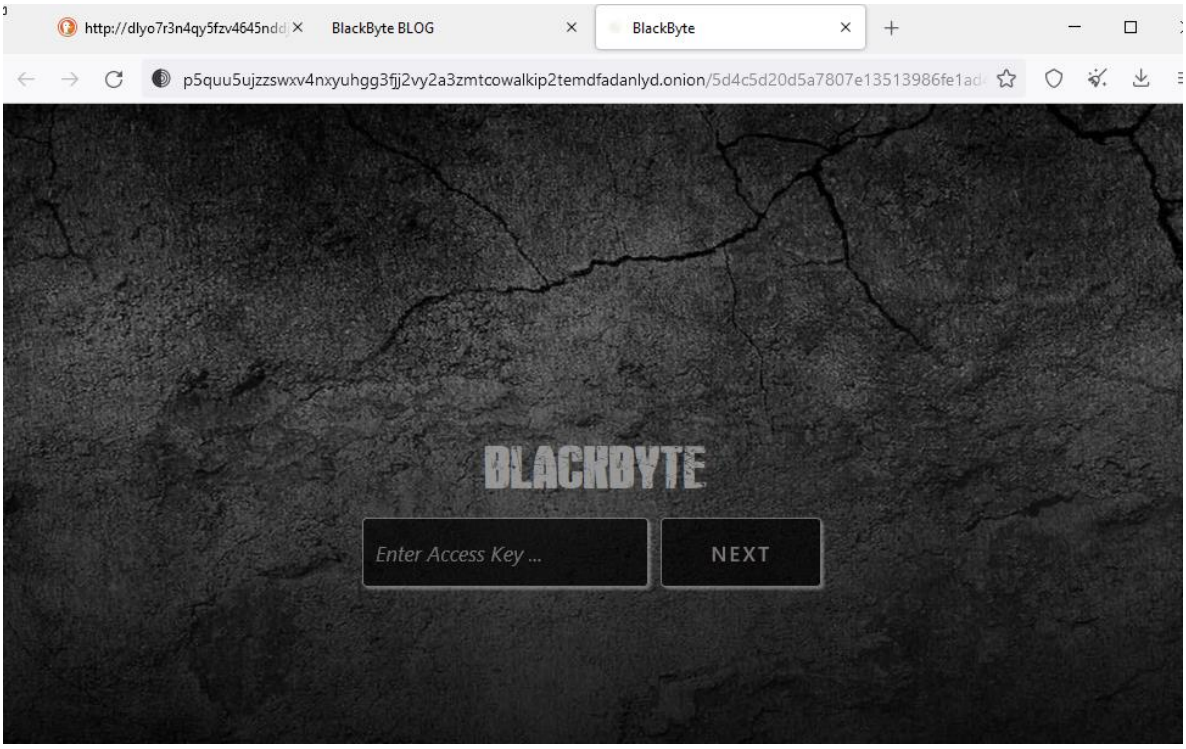

Figura No. 5. *Llave de acceso para comunicarse con el atacante. Fuente: monitoreo en la Darkweb.*

En la figura No. 6, se observa el precio del rescate de los datos cifrados e instrucciones específicas de cómo crear una billetera de Bitcoins, realizar el envío de 160 BTC para recibir a cambio un descifrador, información presentada luego de insertar la llave de acceso.

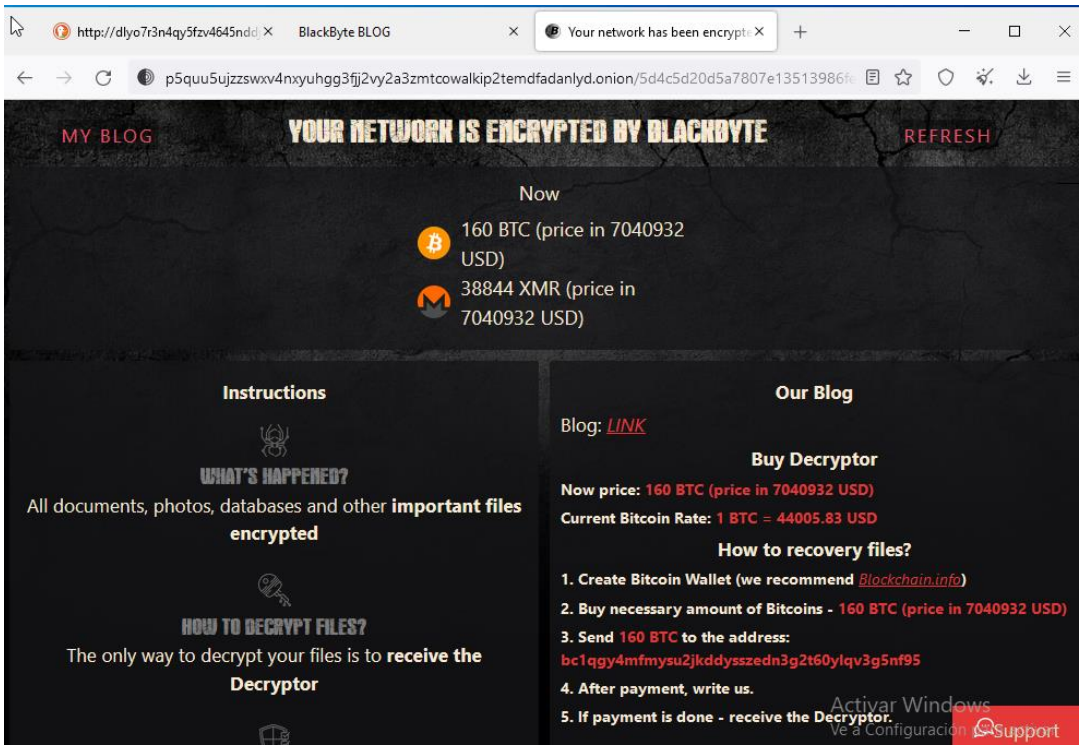

Figura No. 6. *Contacto con grupo atacante. Fuente: monitoreo en la Darkweb.*

A continuación, se especifican los indicadores de compromiso (IoC):

RUTAS	HASH EN MD5	TAREAS PROGRAMADAS
Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946	4d2da36174633565f3dd5ed6dc5033c4	C:\Users\\complex.exe -single .
inetpub\wwwroot\aspnet_client	cd7034692d8f29f9146deb3641de7986	C:\Windows\System32\cmd.exe /c for /l %x in (1,1,75) do start wordpad.exe /p C:\Users\tree.dll.
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth	eed7357ab8d2fe31ea3dbcf3f9b7ec74	
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current	d63a7756bfdcd2be6c755bf288a92c8b	
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes	695e343b81a7b0208cbae33e11f7044c	
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts	296c51eb03e70808304b5f0e050f4f94	
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts\premium	0c7b8da133799dd72d0dbe3ea012031e	
% AppData%\BB.ico	a77899602387665cddb6a0f021184a2b	
%AppData%\BlackByteRestore.txt	1473c91e9c0588f92928bed0ebf5e0f4	
%AppData%\dummy	28b791746c97c0c04dcbfe0954e7173b	
%HOMEPATH%\complex.exe	52b8ae74406e2f52fd81c8458647acd8	
Users\tree.dll	1785f4058c78ae3dd030808212ae3b04	
	b8e24e6436f6bed17757d011780e87b9	
	8dfa48e56fc3a6a2272771e708cdb4d2	
	4ce0bdd2d4303bf77611b8b34c7d2883	

c010d1326689b95a3d8106f75003427c
ae6fbc60ba9c0f3a0fef72aeffcd3dc7
405cb8b1e55bb2a50f2ef3e7c2b28496
11e35160fc4efabd0a3bd7a7c6afc91b
659b77f88288b4874b5abe41ed36380d
151c6f04aeff0e00c54929f25328f6f7
959a7df5c465fcd963a641d87c18a565
5f40e1859053b70df9c0753d327f2cee
df7befc8cdc3c5434ef27cc669fb1e4b
51f2cf541f004d3c1fa8b0f94c89914a
d9e94f076d175ace80f211ea298fa46e
8320d9ec2eab7f5ff49186b2e630a15f
cea6be26d81a8ff3db0d9da666cd0f8f
31f818372fa07d1fd158c91510b6a077
d9e94f076d175ace80f211ea298fa46e
a9cf6dce244ad9afd8ca92820b9c11b9
7139415fecd716bec6d38d2004176f5d
c13bf39e2f8bf49c9754de7fb1396a33
5c0a549ae45d9abe54ab662e53c484e2
ad29212716d0b074d976ad7e33b8f35f
d4aa276a7fbe8dcd858174eeacbb26ce
9344afc63753cd5e2ee0ff9aed43dc56

e2eb5b57a8765856be897b4f6dadca18
58e8043876f2f302fbc98d00c270778b
d2a15e76a4bfa7eb007a07fc8738edfb
e46bfbdf1031ea5a383040d0aa598d45

Tabla No 1. *Indicadores de compromiso asociados a BlackByte*.

Recomendaciones:

- Asegúrese de que todos los IoC identificados se introduzcan las firmas en los dispositivos perimetrales para su supervisión y alerta continuas, contacte a su proveedor de seguridad para que actualicen su plataformas.
- Implemente procedimientos para la generación de copias de seguridad, que garanticen la disponibilidad sobre la última versión de los datos de manera íntegra, salvaguarde dichas copias de modo que no puedan ser modificadas o manipuladas.
- Implemente la segmentación de red, de manera que no se pueda acceder a los equipos de red desde todos los equipos.
- Instale actualizaciones de software y firmware de los aplicativos usados tan pronto como se publiquen.
- Monitorice los controladores de dominio, servidores, host y Active Directory en busca de cuentas de usuario desconocidas. Audite las cuentas de usuario con privilegios administrativos y configure el control de acceso teniendo en cuenta el principio del menor privilegio.
- Deshabilite los puertos de acceso remoto no utilizados o el Protocolo de escritorio remoto (RDP) y supervise el acceso remoto y los registros RDP en busca de actividad inusual.
- Haga uso del doble factor de autenticación al iniciar sesión en una cuenta o servicio.
- Realice jornadas de capacitación y concienciación de los usuarios, funcionarios y colaboradores, en donde se puedan observar las últimas campañas de los ciberdelincuentes junto con vectores de infección más populares.
- Establezca una directriz en donde se ordene a los funcionarios y contratistas cambiar continuamente las contraseñas de las plataformas a las cuales acceden junto con características de dichas contraseñas.
- Valide continuamente los funcionarios y contratistas que han cambiado de cargo o han sido desvinculados de la entidad y elimine dicho perfil.
- Cambien el nombre de la SSID o de la red inalámbrica y no lo proporcione a público que no le compete, use WPA2/WPA3 para proteger las redes inalámbricas. Evite que se conecten a la red corporativa, dispositivos desconocidos, por el contrario permita el filtrado de direcciones por la dirección MAC de los equipos dentro de la entidad.
- Realice un sondeo del sitio web a fin de identificar servicios que estén abiertos, que no se usen, obsoletos o sean considerados una amenaza de la seguridad (telnet y RDP).

- Aplique parches de seguridad y actualización según la versión de sistema operativo, antivirus y programas con las últimas actualizaciones, NO use bajo ningún motivo aplicaciones obsoletas que ya no cuenten con soporte técnico.

Referencias:

[1] Github, “BlackByte Decryptor” [Online] https://github.com/SpiderLabs/BlackByteDecryptor

Contáctanos

Si tienes alguna consulta técnica comunicarse con el colCERT y CSIRT Gobierno a través de los siguientes canales:


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


@colCERT