| | | | |
|---|---|---|---|
| | EC-2021-033 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 17-febrero-2022 | **Ransomware Blackbyte** | V 1.1 |

## I. DATOS GENERALES:

**Clase de alerta:** Contenido dañino
**Tipo de incidente:** Malware
**Nivel de riesgo:** Alta

## II. ALERTA

Blackbyte es un Ranswomare que se encuentra operando desde el 2021, enfocado principalmente en víctimas corporativas a nivel mundial.

**Figura 1.** Ilustración asociada a Ransomware Blackbyte.

## III. INTRODUCCIÓN

Los actores maliciosos desarrollan diferentes herramientas para comprometer la información de las víctimas y obtener recursos económicos por esas acciones; en este sentido, el ransomware es un malware diseñado para cifrar archivos en un dispositivo, en donde los actores malintencionados exigen un rescate a cambio del descifrado.

| | | | |
|---|---|---|---|
| | EC-2021-033 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 17-febrero-2022 | **Ransomware Blackbyte** | V 1.1 |

Hoy en día se presentan diferentes ataques de ransomware tanto a nivel local como regional; existiendo múltiples variantes como BlackCat, Sugar, PYSA, Lockbit, Elbie (atacó reciente a una entidad en Ecuador) y Blackbyte; el mismo que hizo su aparición en julio del 2021.

BlackByte es una operación de ransomware como servicio (RaaS[1]) y según reportes del FBI y el Servicio Secreto de EE. UU, ha comprometido entidades en al menos tres sectores de infraestructura crítica de EE. UU; sin embargo, una falla en el Blackbyte permitió que la empresa de seguridad Trustwave lanzara una herramienta de descifrado que las víctimas podían usar de forma gratuita en lugar de pagarle al grupo para desbloquear sus archivos. Cabe señalar que este ransomware modificó nuevamente su sistema y realizó un nuevo ataque en días previos al Súper Bowl a la infraestructura del Equipo “San Francisco 49ers”.

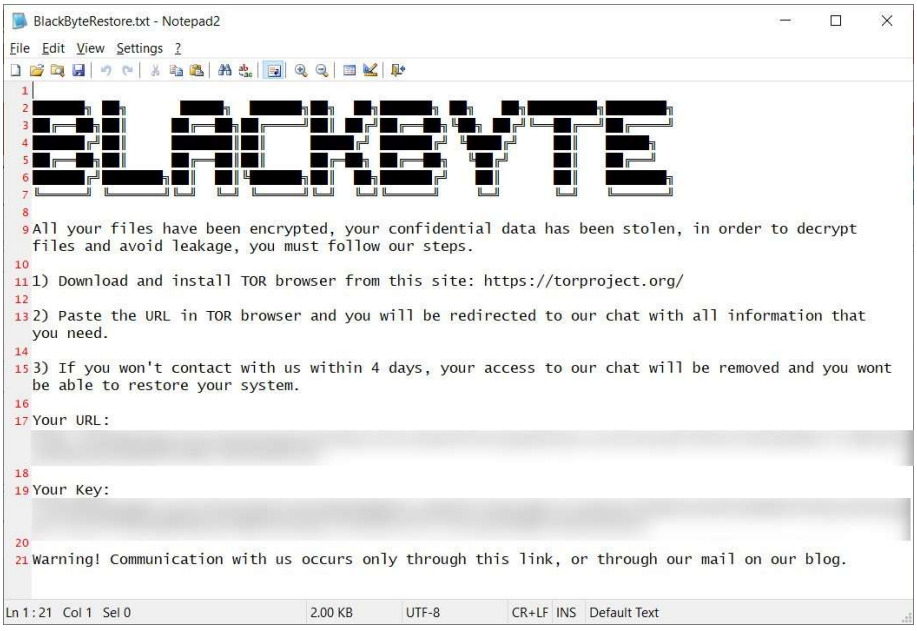


**Figura 2.** Nota de rescate de BlackByte
**Fuente:** BleepingComputer

[1] Permite a los afiliados usar su ransomware por un porcentaje de las ganancias.

| | | | |
|---|---|---|---|
| | EC-2021-033 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 17-febrero-2022 | **Ransomware Blackbyte** | V 1.1 |

## IV. VECTOR DE ATAQUE:

BlackByte obtiene acceso inicial explotando las vulnerabilidades de ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) presentes en el servidor de Microsoft Exchange del cliente.

Una vez ejecutado, BlackByte elimina el Administrador de tareas (taskmgr) y el Monitor de recursos (resmon), posteriormente emite un comando ofuscado de PowerShell para detener el servicio de Windows Defender ( WinDefend)

A continuación, BlackByte realizó el reconocimiento de la red y la preparación del sistema antes del movimiento lateral dentro del entorno.

Antes de realizar el cifrado, BlackByte emite varios comandos:

- El primer comando **vssadmin resize shadowstorage,** cambia el tamaño de almacenamiento de instantáneas.
- El segundo comando busca eliminar instantáneas directamente a través de objetos

Usando WinRAR, BlackByte comprimió los datos locales de los puntos finales comprometidos y cargó los archivos en los sitios anónimos de intercambio de archivos **anonymfiles[.]com** y **file[.]io** Luego, los atacantes intentan extorsionar aún más al cliente amenazando con divulgar estos datos públicamente a través del sitio de fugas BlackByte Tor.

El ejecutable BlackByte deja una nota de rescate en todos los directorios donde se produce el cifrado. La nota de rescate incluye el sitio .onion que contiene instrucciones para pagar el rescate y recibir una clave de descifrado.

| | | | |
|---|---|---|---|
| | EC-2021-033 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:BLANCO | | |
| Fecha: | 17-febrero-2022 | **Ransomware Blackbyte** | V 1.1 |

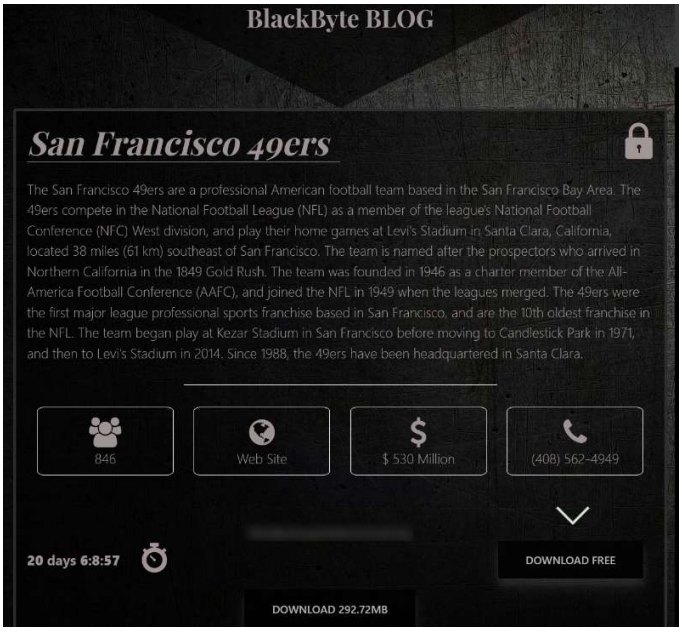


**Figura 3.** Nota de Rescate de BlackByte
**Fuente:** BleepingComputer

## V. INDICADORES DE COMPROMISO:

A continuación, se menciona indicadores de compromiso asociados a BlackByte:

| Propiedades Básicas | | |
|---|---|---|
| Archivos sospechosos descubiertos en las siguientes | Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary Files\root\e22c2559\92c7e946 | ASP.NET |
| | inetpub\wwwroot\aspnet_client | |
| | Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth | |

| | EC-2021-033 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 17-febrero-2022 | **Ransomware Blackbyte** | V 1.1 |

| Propiedades Básicas | | |
|---|---|---|
| ubicaciones: | Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current | |
| | Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes | |
| | Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts | |
| | Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts\premium | |
| Directorios | C:\Users\\complex.exe -single<br><br>C:\Windows\System32\cmd.exe /c for /l %x in (1,1,75) do start wordpad.exe /p C:\Users\tree.dll. | |
| MD5 | 4d2da36174633565f3dd5ed6dc5033c4<br>959a7df5c465fcd963a641d87c18a565<br>cd7034692d8f29f9146deb3641de7986<br>5f40e1859053b70df9c0753d327f2cee<br>d63a7756bfdcd2be6c755bf288a92c8b<br>df7befc8cdc3c5434ef27cc669fb1e4b<br>eed7357ab8d2fe31ea3dbcf3f9b7ec74<br>51f2cf541f004d3c1fa8b0f94c89914a<br>695e343b81a7b0208cbae33e11f7044c<br>d9e94f076d175ace80f211ea298fa46e<br>296c51eb03e70808304b5f0e050f4f94<br>8320d9ec2eab7f5ff49186b2e630a15f<br>0c7b8da133799dd72d0dbe3ea012031e<br>cea6be26d81a8ff3db0d9da666cd0f8f | 52b8ae74406e2f52fd81c8458647acd8<br>7139415fecd716bec6d38d2004176f5d<br>1785f4058c78ae3dd030808212ae3b04<br>c13bf39e2f8bf49c9754de7fb1396a33<br>b8e24e6436f6bed17757d011780e87b9<br>5c0a549ae45d9abe54ab662e53c484e2<br>8dfa48e56fc3a6a2272771e708cdb4d2<br>ad29212716d0b074d976ad7e33b8f35f<br>4ce0bdd2d4303bf77611b8b34c7d2883<br>d4aa276a7fbe8dcd858174eeacbb26ce<br>c010d1326689b95a3d8106f75003427c<br>9344afc63753cd5e2ee0ff9aed43dc56<br>ae6fbc60ba9c0f3a0fef72aeffcd3dc7<br>e2eb5b57a8765856be897b4f6dadca18 |

| | EC-2021-033 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 17-febrero-2022 | **Ransomware Blackbyte** | V 1.1 |

| Propiedades Básicas | | |
|---|---|---|
| | a77899602387665cddb6a0f021184a2b<br>31f818372fa07d1fd158c91510b6a077<br>1473c91e9c0588f92928bed0ebf5e0f4<br>d9e94f076d175ace80f211ea298fa46e<br>28b791746c97c0c04dcbfe0954e7173b<br>a9cf6dce244ad9afd8ca92820b9c11b9 | 405cb8b1e55bb2a50f2ef3e7c2b28496<br>58e8043876f2f302fbc98d00c270778b<br>11e35160fc4efabd0a3bd7a7c6afc91b<br>d2a15e76a4bfa7eb007a07fc8738edfb<br>659b77f88288b4874b5abe41ed36380d<br>e46bfbdf1031ea5a383040d0aa598d45<br>151c6f04aeff0e00c54929f25328f6f7 |

**Tabla 1.** IOC Ransomware Blackbyte
**Fuente:** Join Cybersecurity Advisory

## VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es **NO PAGAR** el rescate.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Implemente la segmentación de la red, de modo que todas las máquinas de su red no estén accesible desde cualquier otra máquina.
- No otorgue privilegios administrativos a todos los usuarios.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL y de origen no sospechoso.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.

| | EC-2021-033 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert |
|---|---|---|---|
| TLP: | TLP:BLANCO | | |
| Fecha: | 17-febrero-2022 | **Ransomware Blackbyte** | V 1.1 |

- Tener actualizado y utilizar un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de que la Organización/Institución se vea afectada por un ransomware, visita los siguientes enlaces; a fin de establecer un panorama de la situación: https://www.nomoreransom.org/es/decryption-tools.html#LockFile (herramientas de des encriptado en el caso de existir) / https://id-ransomware.malwarehunterteam.com/ (identificación de tipo de Ransomware y herramienta de des encriptado en el caso de existir una)
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

## VII. REFERENCIAS:

Abrams, L. (13 de 02 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/nfls-san-francisco-49ers-hit-by-blackbyte-ransomware-attack/

Advisory, J. C. (11 de 02 de 2022). *Join Cybersecurity Advisory*. Obtenido de Join Cybersecurity Advisory: https://www.ic3.gov/Media/News/2022/220211.pdf

Luna, M. (15 de 02 de 2022). *Engadget*. Obtenido de Engadget: https://www.engadget.com/fbi-blackbyte-ransomware-group-critical-us-infrastructure-132527900.html

VAN RIPER, H. (08 de 12 de 2021). *Redcanary*. Obtenido de Redcanary: https://redcanary.com/blog/blackbyte-ransomware/