JOINT
CYBERSECURITY
ADVISORY

Elaborado en conjunto por:

TLP:CLEAR

Identificación del producto: AA24-131A

10 de mayo de 2024

#StopRansomware: Black Basta

RESUMEN

***Nota**: Este aviso conjunto sobre ciberseguridad (CSA, por sus siglas en inglés) es parte de un esfuerzo continuo de #StopRansomware que consiste en publicar avisos para los defensores de la red que detallan diversas variantes de programas de chantaje, así como los agentes de amenazas de dichos programas. Estos avisos de #StopRansomware incluyen tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) e indicadores de compromiso (IOC, por sus siglas en inglés) observados recientemente y en el pasado para ayudar a las organizaciones a protegerse contra los programas de chantaje. Visite stopransomware.gov para ver todos los avisos de #StopRansomware y obtener más información sobre otras amenazas de programas de chantaje y recursos sin costo.*

La Oficina Federal de Investigación (FBI, por sus siglas en inglés), la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés), el Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) y el Centro de Análisis e Intercambio de Información de Varios Estados (MS-ISAC, por sus siglas en inglés) (en adelante, las organizaciones autoras) publican este CSA conjunto para facilitar información sobre Black Basta, una variante de programa de chantaje con la cual los agentes han cifrado y robado datos de al menos 12 de los 16 sectores de infraestructura crítica, incluido el sector de atención médica y salud pública (HPH, por sus siglas en inglés).

Medidas que las organizaciones de infraestructura crítica deben tomar en la actualidad para mitigar las amenazas cibernéticas de los programas de chantaje:

- Instalar las actualizaciones de sistemas operativos, software y firmware en cuanto se publiquen.
- Exigir la autenticación multifactor (MFA, por sus siglas en inglés) resistente a la suplantación de identidad para el mayor número posible de servicios.
- Capacitar a los usuarios para reconocer y denunciar los intentos de suplantación de identidad.

Para denunciar actividades sospechosas o delictivas relacionadas con la información contenida en este aviso conjunto sobre ciberseguridad, póngase en contacto con la oficina local de la FBI o con el Centro de Operaciones de la CISA, disponible las 24 horas, los 7 días de la semana, enviando un correo electrónico a Report@cisa.gov o llamando al (888) 282-0870. Cuando esté disponible, incluya la siguiente información sobre el incidente: fecha, hora y lugar del incidente; tipo de actividad; número de personas afectadas; tipo de equipo utilizado para la actividad; el nombre de la empresa u organización que presenta la denuncia; y un punto de contacto designado. Las organizaciones estatales, locales, tribales y territoriales (SLTT, por sus siglas en inglés) deben comunicar los incidentes al MS-ISAC (866-787-4722 o SOC@cisecurity.org).

Elaborado en conjunto por:




TLP:CLEAR
Identificación del producto: AA24-131A
10 de mayo de 2024

Este CSA conjunto presenta las TTP y los IOC obtenidos a partir de investigaciones de la FBI y de informes de terceros. Black Basta se considera una variante de programa de chantaje como servicio (RaaS, por sus siglas en inglés) y se identificó por primera vez en abril de 2022. Los afiliados a Black Basta han afectado a una gran variedad de empresas e infraestructura crítica en Norteamérica, Europa y Australia. Hasta mayo de 2024, los afiliados a Black Basta han afectado a más de 500 organizaciones de todo el mundo.

Los afiliados a Black Basta utilizan técnicas comunes de acceso inicial (como la suplantación de identidad y la explotación de vulnerabilidades conocidas) y, posteriormente, emplean un modelo de doble extorsión: cifran los sistemas y exfiltran los datos. Por lo general, las notas de rescate no incluyen una petición de rescate inicial ni instrucciones de pago.

En su lugar, las notas facilitan a las víctimas un código único y les indican que se pongan en contacto con el grupo del programa de chantaje a través de una dirección de localizador uniforme de recursos (URL, por sus siglas en inglés) `.onion` (accesible a través del navegador Tor). Normalmente, las notas de rescate conceden a las víctimas entre 10 y 12 días para pagar el rescate antes de que el grupo del programa de chantaje publique sus datos en el sitio de Black Basta en TOR, Basta News.

Las organizaciones de atención médica son objetivos atractivos para los agentes de los delitos cibernéticos por el tamaño, la dependencia tecnológica, el acceso a información médica personal y los impactos únicos de las interrupciones en la atención al paciente. Las organizaciones autoras recomiendan al sector de HPH y a todas las organizaciones de infraestructura crítica que apliquen las recomendaciones de la sección Medidas de mitigación de este CSA para reducir la probabilidad de compromiso por parte de Black Basta y otros ataques de programas de chantaje. Las víctimas de programas de chantaje deben denunciar el incidente a su oficina local de la FBI o a la CISA (consulte la sección Denuncias para obtener la información de contacto).

Para obtener una lista descargable de los IOC, consulte los siguientes recursos:

- AA24-131A (STIX XML, 238 KB)
- AA24-131A (STIX JSON, 181 KB)

INFORMACIÓN TÉCNICA

Nota: Este aviso utiliza el marco MITRE ATT&CK para entornos empresariales, versión 15. Consulte la sección Tácticas y técnicas de MITRE ATT&CK para ver la tabla de la actividad de los agentes de amenazas asignada a las tácticas y técnicas de MITRE ATT&CK®. Para obtener asistencia con la asignación de las actividades cibernéticas maliciosas al marco MITRE ATT&CK, consulte las prácticas recomendadas para la asignación de MITRE ATT&CK de la CISA y MITRE ATT&CK, y la herramienta Decider de la CISA.

Acceso inicial

Los afiliados a Black Basta utilizan principalmente la suplantación de identidad dirigida [T1566] para obtener acceso inicial. Según investigadores de ciberseguridad, los afiliados también utilizaron Qakbot durante el acceso inicial.[1]

A partir de febrero de 2024, los afiliados a Black Basta comenzaron a explotar la vulnerabilidad de ConnectWise CVE-2024-1709 [CWE-288] [T1190]. En algunos casos, se ha observado que los afiliados abusan de credenciales válidas [T1078].

Descubrimiento y ejecución

Los afiliados a Black Basta utilizan herramientas como el escáner de red SoftPerfect (`netscan.exe`) para escanear la red. Los investigadores de ciberseguridad han observado que los afiliados realizan trabajo de reconocimiento usando utilidades con nombres de archivos inofensivos, como `Intel` o `Dell`, que se dejan en la unidad raíz `C:\` [T1036].[1]

Movimiento lateral

Los afiliados a Black Basta utilizan herramientas como BITSAdmin y PsExec, junto con el protocolo de escritorio remoto (RDP, por sus siglas en inglés), para el movimiento lateral. Algunos afiliados también utilizan herramientas como Splashtop, Screen Connect y Cobalt Strike Beacon para facilitar el acceso remoto y el movimiento lateral.

Aumento de privilegios y movimiento lateral

Los afiliados a Black Basta utilizan herramientas de extracción de credenciales, como Mimikatz, para aumentar los privilegios. Según investigadores de ciberseguridad, los afiliados a Black Basta también han explotado las vulnerabilidades ZeroLogon (CVE-2020-1472, [CWE-330]), NoPac (CVE-2021-42278 [CWE-20] y CVE-2021-42287 [CWE-269]) y PrintNightmare (CVE-2021-34527, [CWE-269]) para el aumento de privilegios locales y del dominio de Windows Active [T1068].[1],[2]

Exfiltración y cifrado

Los afiliados a Black Basta utilizan RClone para facilitar la exfiltración de datos antes del cifrado. Antes de la exfiltración, los investigadores de ciberseguridad han observado que los afiliados a Black Basta utilizan PowerShell [T1059.001] para deshabilitar los productos antivirus y, en algunos casos, implementan una herramienta llamada Backstab, diseñada para deshabilitar las herramientas de detección y respuesta de puntos de conexión (EDR, por sus siglas en inglés) [T1562.001].[3] Una vez desconectados los programas antivirus, el algoritmo ChaCha20 con una clave pública RSA-4096 cifra los archivos por completo [T1486]. Se agrega una extensión de archivo `.basta` o aleatoria a los nombres de los archivos y se deja una nota de rescate titulada `readme.txt` en el sistema comprometido.[4] Para inhibir aún más la recuperación del sistema, los afiliados utilizan el programa `vssadmin.exe` para eliminar instantáneas de volumen [T1490].[5]

Herramientas utilizadas

Consulte la Tabla 1 para conocer las herramientas y aplicaciones disponibles públicamente que utilizan los afiliados a Black Basta. Esto incluye las herramientas legítimas reutilizadas para sus operaciones.

Tabla 1: Herramientas que utilizan los afiliados a Black Basta

Descargo de responsabilidad: El uso de estas herramientas y aplicaciones no debe atribuirse como malicioso sin pruebas analíticas que respalden el uso o control de los agentes de amenazas.

Nombre de la herramienta	Descripción
BITSAdmin	Una utilidad de línea de comandos que gestiona las descargas y cargas entre un cliente y un servidor utilizando el servicio de transferencia inteligente en segundo plano (BITS, por sus siglas en inglés) para efectuar transferencias asíncronas de archivos.
Cobalt Strike	Herramienta de pruebas de penetración que se utiliza en las profesiones de seguridad para comprobar la seguridad de redes y sistemas. Los afiliados a Black Basta la han utilizado para facilitar el movimiento lateral y la ejecución de archivos.

Nombre de la herramienta	Descripción
Mimikatz	Una herramienta que permite a los usuarios ver y guardar credenciales de autenticación, como tickets de Kerberos. Los afiliados a Black Basta la han utilizado para facilitar el aumento de privilegios.
PSExec	Una herramienta diseñada para ejecutar programas y comandos en sistemas remotos.
PowerShell	Una solución de automatización de tareas multiplataforma compuesta por una shell de línea de comandos, un lenguaje de scripting y un marco de gestión de la configuración, que funciona en Windows, Linux y macOS.
RClone	Un programa de línea de comandos utilizado para sincronizar archivos con servicios de almacenamiento en la nube, como Mega.
SoftPerfect	Un escáner de red (`netscan.exe`) utilizado para hacer ping en computadoras, escanear puertos, descubrir carpetas compartidas y recuperar información sobre dispositivos de red a través del Instrumental de administración de Windows (WMI, por sus siglas en inglés), del protocolo simple de administración de redes (SNMP, por sus siglas en inglés), del protocolo de transferencia de hipertexto (HTTP, por sus siglas en inglés), del Shell seguro (SSH, por sus siglas en inglés) y de PowerShell. También realiza análisis en búsqueda de servicios remotos, registros, archivos y contadores de desempeño.
ScreenConnect	Software de asistencia remota, acceso y reuniones que permite a los usuarios controlar dispositivos a distancia a través de Internet.
Splashtop	Software de escritorio remoto que permite acceder a distancia a dispositivos para ofrecer asistencia, acceso y colaboración.
WinSCP	Windows Secure Copy es un cliente gratuito y de código abierto de protocolo de transferencia de archivos de SSH, protocolo de transferencia de archivos, WebDAV, Amazon S3 y protocolo de copia segura. Los afiliados a Black Basta lo han utilizado para transferir datos desde una red comprometida a cuentas controladas por agentes.

TÁCTICAS Y TÉCNICAS DE MITRE ATT&CK

Consulte las tablas 2-6 para conocer todas las tácticas y técnicas de agentes de amenazas a las que se hace referencia en este aviso.

Tabla 2: Técnicas de ATT&CK para el acceso inicial con Black Basta

Título de la técnica	Identificación	Uso
Suplantación de identidad	T1566	Los afiliados a Black Basta han utilizado correos electrónicos de suplantación de identidad dirigida para obtener acceso inicial.
Explotación de aplicaciones públicas	T1190	Los afiliados a Black Basta han explotado la vulnerabilidad de ConnectWise CVE-2024-1709 para obtener acceso inicial.

Tabla 3: Técnicas de ATT&CK para el aumento de privilegios con Black Basta

Título de la técnica	Identificación	Uso
Explotación para aumentar privilegios	T1068	Los afiliados a Black Basta han utilizado herramientas de extracción de credenciales, como Mimikatz, Zerologon, NoPac y PrintNightmare, para aumentar los privilegios.

Tabla 4: Técnicas de ATT&CK para la evasión de la defensa con Black Basta

Título de la técnica	Identificación	Uso
Enmascaramiento	T1036	Los afiliados a Black Basta han realizado trabajo de reconocimiento usando utilidades con nombres de archivos inofensivos, como `Intel` o `Dell`, para evadir la detección.
Deterioro de las defensas: desactivar o modificar herramientas	T1562.001	Los afiliados a Black Basta han implementado una herramienta llamada Backstab para deshabilitar las herramientas de detección y respuesta de puntos de conexión (EDR). Los afiliados a Black Basta han utilizado PowerShell para desactivar productos antivirus.

Tabla 5: Técnicas de ATT&CK para la ejecución con Black Basta

Título de la técnica	Identificación	Uso
Intérprete de comandos y scripting: PowerShell	T1059.001	Los afiliados a Black Basta han utilizado PowerShell para desactivar productos antivirus.

Tabla 6: Técnicas de ATT&CK para el impacto con Black Basta

Título de la técnica	Identificación	Uso
Inhibición de la recuperación del sistema	T1490	Los afiliados a Black Basta han utilizado el programa `vssadmin.exe` para eliminar instantáneas.
Cifrado de datos para lograr impacto	T1486	Los afiliados a Black Basta han utilizado una clave pública para cifrar los archivos por completo.

INDICADORES DE COMPROMISO

Consulte la Tabla 7 para conocer los IOC obtenidos a partir de investigaciones de la FBI.

Tabla 7: Archivos maliciosos asociados con el programa de chantaje Black Basta

Hash	Descripción
0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298	rclone.exe
d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e	Winscp.exe
88c8b472108e0d79d16a1634499c1b45048a10a38ee799054414613cc9dccccc	DLL
58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd	DLL
39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead	DLL
5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221	DLL
51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e	DLL
d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1	DLL
5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43	DLL
05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431	DLL
a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6	DLL
86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737	DLL
07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799	DLL
96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be	ELF
1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779	ELF
360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98	ELF
0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a	EXE
9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc	EXE
62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087	EXE
7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59	EXE
350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd	EXE
90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7	EXE
fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08	EXE

Hash	Descripción
acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f	EXE
d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d	EXE
f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4	EXE
723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224	EXE
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	EXE
fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f	EXE
df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415	EXE
462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7	EXE
3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a	EXE
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	EXE
37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004	EXE
3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35	EXE
17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20	EXE
42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78	EXE
882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3	EXE
e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757	EXE
0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e	EXE
69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944	EXE
3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a	EXE
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	EXE
b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9	EXE

Consulte las tablas 8-11 para conocer los IOC obtenidos a partir de informes de terceros confiables.

Tabla 8: Indicadores de red

Descargo de responsabilidad: Las organizaciones autoras recomiendan a los defensores de la red que investiguen las direcciones de protocolo de Internet (IP, por sus siglas en inglés) antes de tomar medidas, como el bloqueo, ya que se sabe que muchos agentes cibernéticos cambian las direcciones IP, a menudo diariamente, y algunas direcciones IP pueden alojar dominios válidos.

Dirección IP	Descripción
66.249.66[.]18	0gpw.588027fa.dns.realbumblebee[.]net, dns.trailshop[.]net, dns.artspathgroupe[.]net

Dirección IP	Descripción
66.249.66[.]18	my.2a91c002002.588027fa.dns.realbumblebee[.]net
66.249.66[.]18	fy9.39d9030e5d3a8e2352daae2f4cd3c417b36f64c6644a783b9629147a1.afd8b8a4615358e0313bad8c544a1af0d8efcec0e8056c2c8eee96c7.b06d1825c0247387e38851b06be0272b0bd619b7c9636bc17b09aa70.a46890f27.588027fa.dns.realbumblebee[.]net
95.181.173[.]227	adslsdfdsfmo[.]world
	fy9.36c44903529fa273afff3c9b7ef323432e223d22ae1d625c4a3957d57.015c16eff32356bf566c4fd3590c6ff9b2f6e8c587444ecbfc4bcae7.f71995aff9e6f22f8daffe9d2ad9050abc928b8f93bb0d42682fd3c3.445de2118.588027fa.dns.realbumblebee[.]net
207.126.152[.]242	xkpal.d6597fa.dns.blocktoday.net nuher.3577125d2a75f6a277fc5714ff536c5c6af5283d928a66daad6825b9a.7aaf8bba88534e88ec89251c57b01b322c7f52c7f1a5338930ae2a50.cbb47411f60fe58f76cf79d300c03bdecfb9e83379f59d80b8494951.e10c20f77.7fcc0eb6.dns.blocktoday[.]net
72.14.196[.]50	.rasapool[.]net, dns.trailshop[.]net
72.14.196[.]192	.rasapool[.]net
72.14.196[.]2	.rasapool[.]net
72.14.196[.]226	.rasapool[.]net
46.161.27[.]151	
207.126.152[.]242	nuher.1d67bbcf4.456d87aa6.2d84dfba.dns.specialdrills[.]com
185.219.221[.]136	
64.176.219[.]106	
5.78.115[.]67	your-server[.]de
207.126.152[.]242	xkpal.1a4a64b6.dns.blocktoday[.]net
46.8.16[.]77	
185.7.214[.]79	Servidor de red privada virtual (VPN, por sus siglas en inglés)
185.220.100[.]240	Salida de Tor
107.189.30[.]69	Salida de Tor
5.183.130[.]92	
185.220.101[.]149	Salida de Tor
188.130.218[.]39	

Dirección IP	Descripción
188.130.137[.]181	
46.8.10[.]134	
155.138.246[.]122	
80.239.207[.]200	winklen[.]ch
183.181.86[.]147	Xserver[.]jp
34.149.120[.]3	
104.21.40[.]72	
34.250.161[.]149	
88.198.198[.]90	your-server[.]de; literoved[.]ru
151.101.130[.]159	
35.244.153[.]44	
35.212.86[.]55	
34.251.163[.]236	
34.160.81[.]203	
34.149.36[.]179	
104.21.26[.]145	
83.243.40[.]10	
35.227.194[.]51	
35.190.31[.]54	
34.120.190[.]48	
116.203.186[.]178	
34.160.17[.]71	

Tabla 9: Indicadores de archivos

Nombre del archivo	Hash
C:\Users\Public\Audio\Jun.exe	b6a4f4097367d9c124f51154d8750ea036a812d5b adde0baf9c5f183bb53dd24
C:\Users\Public\Audio\esx.zip	
C:\Users\Public\Audio\7zG.exe	f21240e0bf9f0a391d514e34d4fa24ecb997d93937 9d2260ebce7c693e55f061

Nombre del archivo	Hash
C:\Users\Public\Audio\Jun.exe	b6a4f4097367d9c124f51154d8750ea036a812d5b adde0baf9c5f183bb53dd24
C:\Users\Public\Audio\7z.dll	
C:\Users\Public\db_Usr.sql	8501e14ee6ee142122746333b936c9ab0fc541328 f37b5612b6804e6cdc2c2c6
C:\Users\Public\Audio\db_Usr.sql	
C:\Users\Public\Audio\hv2.ps1	
C:\Users\Public\7zG.exe	
C:\Users\Public\7z.dll	
C:\Users\Public\BitLogic.dll	
C:\Users\Public\NetApp.exe	4c897334e6391e7a2fa3cbcbf773d5a4
C:\Users\Public\DataSoft.exe	2642ec377c0cee3235571832cb472870
C:\Users\Public\BitData.exe	b3fe23dd4701ed00d79c03043b0b952e
C:\Users\Public\DigitalText.dll	
C:\Users\Public\GeniusMesh.exe	
\Device\Mup\{redacted}\C$\Users\Public\Musi c\PROCEXP.sys	
\Device\Mup\{redacted}\C$\Users\Public\Musi c\DumpNParse86.exe	
\Device\Mup\{redacted}\C$\Users\Public\Musi c\POSTDump.exe	
\Device\Mup\{redacted}\C$\Users\Public\Musi c\DumpNParse.exe	
C:\Users\Public\socksps.ps1	
C:\Users\Public\Thief.exe	034b5fe047920b2ae9493451623633b14a85176f5 eea0c7aadc110ea1730ee79
C:\Users\All Users\{redacted}\GWT.ps1 C:\Program Files\MonitorIT\GWT.ps1	8C68B2A794BA3D148CAE91BDF9C8D35728975 2A94118B5558418A36D95A5A45F
Winx86.exe Comentario: alias de cmd.exe	

Nombre del archivo	Hash
C:\Users\Public\Audio\Jun.exe	b6a4f4097367d9c124f51154d8750ea036a812d5b adde0baf9c5f183bb53dd24
C:\Users\Public\eucr.exe	3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e 3629f34afc338058680407
C:\Windows\DS_c1.dll	808c96cb90b7de7792a827c6946ff481238029596 35a23bf9d98478ae6a259f9
C:\Windows\DS_c1.dll	3a8fc07cadc08eeb8be342452636a754158403c3d 4ebff379a4ae66f8298d9a6
C:\Windows\DS_c1.dll	4ac69411ed124da06ad66ee8bfbcea2f593b5b199 a2c38496e1ee24f9d04f34a
C:\Windows\DS_c1.dll	819cb9bcf62be7666db5666a693524070b0df589c 58309b067191b30480b0c3a
C:\Windows\DS_c1.dll	c26a5cb62a78c467cc6b6867c7093fbb7b1a96d92 121d4d6c3f0557ef9c881e0
C:\Windows\DS_c1.dll	d503090431fdd99c9df3451d9b73c5737c79eda6e b80c148b8dc71e84623401f
*\instructions_read_me.txt	

Tabla 10: Dominios conocidos de Cobalt Strike de Black Basta

Dominio	Fecha/Hora (UTC)
trailshop[.]net	5/8/2024 6:37
realbumblebee[.]net	5/8/2024 6:37
recentbee[.]net	5/8/2024 6:37
investrealtydom[.]net	5/8/2024 6:37
webnubee[.]com	5/8/2024 6:37
artspathgroup[.]net	5/8/2024 6:37
buyblocknow[.]com	5/8/2024 6:37
currentbee[.]net	5/8/2024 6:37
modernbeem[.]net	5/8/2024 6:37
startupbusiness24[.]net	5/8/2024 6:37
magentoengineers[.]com	5/8/2024 6:37

Dominio	Fecha/Hora (UTC)
childrensdolls[.]com	5/8/2024 6:37
myfinancialexperts[.]com	5/8/2024 6:37
limitedtoday[.]com	5/8/2024 6:37
kekeoamigo[.]com	5/8/2024 6:37
nebraska-lawyers[.]com	5/8/2024 6:37
tomlawcenter[.]com	5/8/2024 6:37
thesmartcloudusa[.]com	5/8/2024 6:37
rasapool[.]net	5/8/2024 6:37
artspathgroupe[.]net	5/8/2024 6:37
specialdrills[.]com	5/8/2024 6:37
thetrailbig[.]net	5/8/2024 6:37
consulheartinc[.]com	3/22/2024 15:35
otxcosmeticscare[.]com	3/15/2024 10:14
otxcarecosmetics[.]com	3/15/2024 10:14
artstrailman[.]com	3/15/2024 10:14
ontexcare[.]com	3/15/2024 10:14
trackgroup[.]net	3/15/2024 10:14
businessprofessionalllc[.]com	3/15/2024 10:14
securecloudmanage[.]com	3/7/2024 10:42
oneblackwood[.]com	3/7/2024 10:42
buygreenstudio[.]com	3/7/2024 10:42
startupbuss[.]com	3/7/2024 10:42
onedogsclub[.]com	3/4/2024 18:26
wipresolutions[.]com	3/4/2024 18:26
recentbeelive[.]com	3/4/2024 18:26
trailcocompany[.]com	3/4/2024 18:26
trailcosolutions[.]com	3/4/2024 18:26
artstrailreviews[.]com	3/4/2024 18:26
usaglobalnews[.]com	2/15/2024 5:56

Dominio	Fecha/Hora (UTC)
topglobaltv[.]com	2/15/2024 5:56
startupmartec[.]net	2/15/2024 5:56
technologgies[.]com	1/2/2024 18:16
jenshol[.]com	1/2/2024 18:16
simorten[.]com	1/2/2024 18:16
investmentgblog[.]net	1/2/2024 18:16
protectionek[.]com	1/2/2024 18:16

Tabla 11: Posibles dominios de Black Basta

airbusco[.]net
allcompanycenter[.]com
animalsfast[.]net
audsystemecll[.]net
auuditoe[.]com
bluenetworking[.]net
brendonline[.]com
businesforhome[.]com
caspercan[.]com
clearsystemwo[.]net
cloudworldst[.]net
constrtionfirst[.]com
erihudeg[.]com
garbagemoval[.]com
gartenlofti[.]com
getfnewsolutions[.]com
getfnewssolutions[.]com
investmendvisor[.]net
investmentrealtyhp[.]net
ionoslaba[.]com

jessvisser[.]com
karmafisker[.]com
kolinileas[.]com
maluisepaul[.]com
masterunix[.]net
monitor-websystem[.]net
monitorsystem[.]net
mytrailinvest[.]net
prettyanimals[.]net
reelsysmoona[.]net
seohomee[.]com
septcntr[.]com
softradar[.]net
startupbizaud[.]net
startuptechnologyw[.]net
steamteamdev[.]net
stockinvestlab[.]net
taskthebox[.]net
trailgroupl[.]net
treeauwin[.]net
unitedfrom[.]com
unougn[.]com
wardeli[.]com
welausystem[.]net
wellsystemte[.]net
withclier[.]com

MEDIDAS DE MITIGACIÓN

Las organizaciones autoras recomiendan que todas las organizaciones de infraestructura crítica implementen las siguientes medidas de mitigación para mejorar la postura de ciberseguridad de su organización, en función de la actividad de Black Basta. Estas medidas de mitigación coinciden con los objetivos de desempeño en ciberseguridad (CPG, por sus siglas en inglés) intersectoriales que desarrollaron la CISA y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés). Los CPG proporcionan un conjunto mínimo de prácticas y protecciones que la CISA y el NIST recomiendan que todas las organizaciones implementen. La CISA y el NIST basaron los CPG en marcos y orientación de ciberseguridad establecidos para brindar protección contra las amenazas, las tácticas, las técnicas y los procedimientos más comunes e impactantes. Consulte los objetivos de desempeño en ciberseguridad intersectoriales de la CISA para obtener más información sobre los CPG y las protecciones de referencia recomendadas.

- **Instale las actualizaciones de sistemas operativos, software y firmware en cuanto se publiquen** [CPG 1.E]. Priorice la actualización de las vulnerabilidades explotadas conocidas (KEV, por sus siglas en inglés).
- **Exija la autenticación multifactor (MFA) resistente a la suplantación de identidad** [CPG 2.H] para el mayor número posible de servicios.
- **Implemente las recomendaciones, que incluyen la capacitación de los usuarios para reconocer y denunciar los intentos de suplantación de identidad** [CPG 2.I], del documento conjunto Orientación sobre la suplantación de identidad: detener el ciclo de ataque en la fase uno.
- **Asegure el software de acceso remoto** implementando las medidas de mitigación del documento conjunto Guía para asegurar el software de acceso remoto.
- **Realice copias de seguridad de sistemas críticos y configuraciones de dispositivos** [CPG 2.R] para permitir la reparación y restauración de dispositivos.
- **Aplique las medidas de mitigación del documento conjunto Guía de #StopRansomware**.

Las organizaciones autoras también recomiendan a los defensores de la red del sector de HPH y otras organizaciones de infraestructura crítica que consulten el documento de la CISA Guía de mitigación: sector de atención médica y salud pública (HPH), y los objetivos de desempeño en ciberseguridad de HPH del HHS, que brindan las prácticas recomendadas para combatir las amenazas cibernéticas generalizadas contra las organizaciones. Las recomendaciones incluyen lo siguiente:

- **Gestión de activos y seguridad**: Los profesionales de la ciberseguridad deben identificar y comprender todas las relaciones o interdependencias, la funcionalidad de cada activo, lo que expone y qué software se está ejecutando para garantizar que los datos y sistemas críticos estén protegidos de manera adecuada. Las organizaciones del sector de HPH deben garantizar que la información médica protegida electrónica (ePHI, por sus siglas en inglés) esté asegurada y cumpla con la Ley de Responsabilidad y Portabilidad de Seguros Médicos (HIPAA, por sus siglas en inglés). Las organizaciones pueden completar inventarios de activos mediante análisis activos, procesos pasivos o una combinación de ambas técnicas.

- **Seguridad del correo electrónico y prevención de la suplantación de identidad**: Las organizaciones deben instalar software moderno contra programas malignos y actualizar las firmas automáticamente cuando sea posible. Para obtener orientación adicional, consulte la Guía para mejorar la seguridad web y del correo electrónico de la CISA.
    - **Compruebe si hay hipervínculos incrustados o falsificados**: Valide que la URL del enlace coincida con el texto del enlace en sí. Para hacerlo, pase el cursor sobre el enlace para ver la URL del sitio web al que desea acceder.
- **Gestión de acceso**: La MFA resistente a la suplantación de identidad completa el mismo proceso, pero quita a las "personas" de la operación para ayudar a frustrar las estafas de ingeniería social y los ataques de suplantación de identidad dirigidos que podrían haber tenido éxito con una MFA tradicional. Las dos formas principales de MFA resistente a la suplantación de identidad son la autenticación FIDO/Web Authentication (WebAuthn) y la autenticación basada en infraestructura de clave pública (PKI, por sus siglas en inglés). Priorice el uso de MFA resistente a la suplantación de identidad en las cuentas con mayor riesgo, como las cuentas administrativas privilegiadas de activos clave. Para obtener información adicional sobre la MFA resistente a la suplantación de identidad, consulte la Guía de implementación de MFA resistente a la suplantación de identidad de la CISA.
- **Gestión y evaluación de vulnerabilidades**: Una vez que se identifiquen las vulnerabilidades en su entorno, evalúelas y priorícelas para abordar adecuadamente los riesgos planteados de acuerdo con la estrategia de riesgos de su organización. Para ayudar con la priorización, es esencial que haga lo siguiente:
    - **Asigne sus activos a funciones críticas para la empresa.** Para la corrección de vulnerabilidades, priorice los activos que son más críticos para las operaciones en curso o que, si resultan afectados, podrían impactar en la continuidad del negocio, la seguridad de la información de identificación personal (PII, por sus siglas en inglés) (o información médica protegida [PHI, por sus siglas en inglés]) confidencial, la reputación o la posición financiera de su organización.
    - **Utilice información de inteligencia sobre amenazas.** Para la corrección, priorice las vulnerabilidades que los agentes de amenazas explotan de forma activa. Para ayudar, aproveche el catálogo de KEV de la CISA y otras fuentes de inteligencia sobre amenazas.
    - **Aproveche las metodologías, calificaciones y puntuaciones de priorización**. El Sistema de Puntuación de Vulnerabilidades Comunes (CVSS, por sus siglas en inglés) evalúa la gravedad técnica de las vulnerabilidades. El Sistema de Puntuación de Predicción de Explotación (EPSS, por sus siglas en inglés) mide la probabilidad de explotación y puede ayudar a decidir qué vulnerabilidades priorizar. La metodología de categorización de vulnerabilidades específica de las partes interesadas (SSVC, por sus siglas en inglés) de la CISA aprovecha los árboles de decisiones para priorizar las vulnerabilidades relevantes en cuatro decisiones: Supervisar, Supervisar*, Asistir y Actuar en función del estado de explotación, del impacto técnico, de la prevalencia de la misión y de los impactos en la seguridad y el bienestar público.

VALIDAR LOS CONTROLES DE SEGURIDAD

Además de aplicar las medidas de mitigación, las organizaciones autoras recomiendan ejecutar, probar y validar el programa de seguridad de su organización frente a los comportamientos de amenazas asignados al marco MITRE ATT&CK para entornos empresariales que figuran en este aviso. Las organizaciones autoras recomiendan que pruebe su inventario establecido de controles de seguridad para evaluar cómo se desempeñan frente a las técnicas de ATT&CK descritas en este aviso.

Para empezar:

1. Seleccione una de las técnicas de ATT&CK descritas en este aviso (consulte las tablas 2-6).
2. Alinee sus tecnologías de seguridad con la técnica.
3. Pruebe sus tecnologías con la técnica.
4. Analice el desempeño de sus tecnologías de detección y prevención.
5. Repita el proceso para todas las tecnologías de seguridad a fin de obtener un conjunto de datos completos sobre el desempeño.
6. Ajuste su programa de seguridad (esto incluye a las personas, los procesos y las tecnologías) en función de los datos que se generaron en este proceso.

Las organizaciones autoras recomiendan probar su programa de seguridad de forma continua, a escala, en un entorno de producción para garantizar un desempeño óptimo frente a las técnicas de MITRE ATT&CK identificadas en este aviso.

REFERENCIAS

[1] SentinelOne: Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor
[2] Trend Micro: Ransomware Spotlight - Black Basta
[3] Kroll: Black Basta - Technical Analysis
[4] Who Is Black Basta? (blackberry.com)
[5] Palo Alto Networks: Threat Assessment - Black Basta Ransomware

DENUNCIAS

Su organización no tiene la obligación de responder ni facilitar información a la FBI en respuesta a este CSA conjunto. Si, después de revisar la información presentada, su organización decide facilitar información a la FBI, debe hacerlo en conformidad con las leyes estatales y federales aplicables.

La FBI está interesada en recibir toda la información que se pueda compartir para incluir registros de límites que muestren la comunicación hacia y desde direcciones IP extranjeras, una nota de rescate de muestra, comunicaciones con agentes de amenazas, información de billeteras Bitcoin, archivos de descifrado o una muestra inofensiva de un archivo cifrado.

Otra información de interés es la siguiente: el punto de contacto de una empresa atacada, el estado y el alcance de la infección, las pérdidas estimadas, el impacto operativo, la identificación de las

transacciones, la fecha de la infección, la fecha de detección, el vector de ataque inicial y los indicadores basados en el host y la red.

La FBI, la CISA y el HHS no recomiendan el pago de rescates, ya que el pago no garantiza que se recuperen los archivos de las víctimas. Además, el pago también puede incentivar a los adversarios a atacar a otras organizaciones, alentar a otros delincuentes a participar en la distribución del programa de chantaje o financiar actividades ilícitas. Independientemente de si usted o su organización han decidido pagar el rescate, la FBI y la CISA le instan a denunciar de inmediato los incidentes con programas de chantaje al Centro de Denuncias de Delitos en Internet (IC3, por sus siglas en inglés) de la FBI, a una oficina local de la FBI o a la CISA mediante su sistema de denuncia de incidentes o su Centro de Operaciones, disponible las 24 horas del día, los 7 días de la semana (enviando un correo electrónico a report@cisa.gov o llamando al 1-844-Say-CISA [1-844-729-2472]).

DESCARGO DE RESPONSABILIDAD

La información presentada en este informe se proporciona “tal como está” solo con fines informativos. La FBI, la CISA, el HHS y el MS-ISAC no promocionan a ninguna entidad comercial, producto, empresa o servicio, incluidas las entidades, los productos o los servicios vinculados en este documento. Cualquier referencia a entidades comerciales, productos, procesos o servicios específicos mediante marcas de servicio, marcas registradas, fabricantes, o de otro modo, no constituye ni implica la promoción, la recomendación ni el favoritismo por parte de la FBI, la CISA, el HHS o el MS-ISAC.

HISTORIAL DE VERSIONES

10 de mayo de 2024: versión inicial.