Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RANSOMWARE LOCKBIT 3.0

19/Marzo/2023

CONTENIDO

INTRODUCCIÓN

LockBit 3.0, también conocido como “LockBit Black”, es más modular y evasivo que sus versiones anteriores y comparte similitudes con Blackmatter y Blackcat ransomware.

RANSOMWARE LOCKBIT 3.0

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_03_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/03/2023
Es día cero (0 day):	No

RESUMEN

LockBit 3.0 se configura durante la compilación con muchas opciones diferentes que determinan el comportamiento del ransomware. En la ejecución real del ransomware dentro del entorno de la víctima, se pueden suministrar varios argumentos para modificar aún más el comportamiento del ransomware. Por ejemplo, LockBit 3.0 acepta argumentos adicionales para operaciones específicas en el movimiento lateral y el reinicio en Modo seguro. Un argumento de contraseña es obligatorio durante la ejecución del ransomware. Los afiliados de LockBit 3.0 que no ingresen la contraseña correcta no podrán ejecutar el ransomware [T1480.001]. La contraseña es una clave criptográfica que descodifica el ejecutable de LockBit 3.0. Al proteger el código de esta manera, LockBit 3.0 dificulta la detección y el análisis de malware, ya que el código no se puede ejecutar ni leer en su forma cifrada. Las detecciones basadas en firmas pueden no detectar el ejecutable de LockBit 3.0 ya que la porción cifrada del ejecutable variará según la clave criptográfica utilizada y también generará un hash único. Cuando se proporciona la contraseña correcta, LockBit 3.0 descifrará el componente principal, continuará descifrando o descomprimiendo su código y ejecutará el ransomware.

LockBit 3.0 solo infectará máquinas que no tengan configuradas las opciones de idioma que coincidan con una lista de exclusión definida. Sin embargo, si se comprueba el idioma del sistema en tiempo de ejecución, lo determina una marca de configuración establecida originalmente en el momento de la compilación. Los idiomas en la lista de exclusión incluyen, pero no se limitan a, rumano (Moldavia), árabe (Siria) y tártaro (Rusia). Si se detecta un idioma de la lista de exclusión [T1614.001], LockBit 3.0 detendrá la ejecución sin infectar el sistema.

ACCESO INICIAL

Los afiliados que implementan ransomware LockBit 3.0 obtienen acceso inicial a las redes de las víctimas a través de la explotación del protocolo de escritorio remoto (RDP) [T1133], campañas de phishing [T1566].

PROCESO DE EJECUCIÓN E INFECCIÓN

Durante la rutina de malware, si los privilegios no son suficientes, LockBit 3.0 intenta escalar a los privilegios requeridos [TA0004]. LockBit 3.0 realiza funciones como:

- Enumerar información del sistema, como el nombre de host, la configuración del host, la información de dominio, la configuración de la unidad local, los recursos compartidos remotos y los dispositivos de almacenamiento externo [T1082]
- Terminación de procesos y servicios [T1489]
- Comandos de lanzamiento [TA0002]
- Habilitación del inicio de sesión automático para la persistencia y el escalamiento de privilegios [T1547]
- Eliminación de archivos de registro, archivos de la carpeta de la papelera de reciclaje y instantáneas que residen en el disco [T1485]

LockBit 3.0 intenta propagarse a través de una red víctima mediante el uso de una lista preconfigurada de credenciales codificadas en el momento de la compilación o una cuenta local comprometida con privilegios elevados [T1078]. Cuando se compila, LockBit 3.0 también puede habilitar opciones para la propagación a través de objetos de directiva de grupo y PsExec mediante el protocolo de bloque de mensajes del servidor (SMB). LockBit 3.0 intenta cifrar [T1486] datos guardados en cualquier dispositivo local o remoto, pero omite los archivos asociados con las funciones principales del sistema.
Después de cifrar los archivos, LockBit 3.0 deja caer una nota de rescate con el nuevo nombre de archivo . README.txt y cambia el fondo de pantalla y los iconos del host a la marca LockBit 3.0 [T1491.001]. Si es necesario, LockBit 3.0 enviará información cifrada de host y bot a un servidor de comando y control (C2) [T1027].
Una vez completado, LockBit 3.0 puede eliminarse del disco [T1070.004], así como cualquier actualización de directiva de grupo que se haya realizado, dependiendo de las opciones que se establecieron en el momento de la compilación.

EXFILTRACIÓN

Los afiliados de LockBit 3.0 usan Stealbit, una herramienta de exfiltración personalizada utilizada anteriormente con LockBit 2.0 [TA0010]; rclone, un administrador de almacenamiento en la nube de línea de comandos de código abierto [T1567.002]; y servicios de intercambio de archivos disponibles públicamente, como MEGA [T1567.002], para filtrar archivos de datos confidenciales de la empresa antes del cifrado. Si bien rclone y muchos servicios de intercambio de archivos disponibles públicamente se utilizan principalmente para fines legítimos, también pueden ser utilizados por actores de amenazas para ayudar a comprometer el sistema, explorar la red o la exfiltración de datos. Los afiliados de LockBit 3.0 a menudo utilizan otros servicios de intercambio de archivos disponibles públicamente para filtrar datos también [T1567].

Sitios de File Sharing
https://www.premiumize[.] .com
https://anonfiles[.] .com
https://www.sendspace[.] .com
https://fex[.] red
https://transfer[.] .sh
https://send.exploit[.] en

APROVECHAR EL SOFTWARE GRATUITO Y LAS HERRAMIENTAS DE CÓDIGO ABIERTO

Los afiliados de LockBit han sido observados usando varias herramientas gratuitas y de código abierto durante sus intrusiones. Estas herramientas se utilizan para una variedad de actividades como reconocimiento de red, acceso remoto, volcado de credenciales y exfiltración de archivos. El uso de PowerShell y scripts por lotes se observa en la mayoría de las intrusiones, que se centran en el descubrimiento del sistema, el reconocimiento, la búsqueda de contraseñas / credenciales y el escalamiento de privilegios. También se han observado artefactos de herramientas profesionales de prueba de penetración como Metasploit y Cobalt Strike.

Herramienta	Descripción	MITRE ATT&CK ID
Chocolatey	Administrador de paquetes de línea de comandos para Windows.	T1072
FileZilla	Aplicación de protocolo de transferencia de archivos (FTP) multiplataforma.	T1071.002
Impacket	Colección de clases de Python para trabajar con protocolos de red.	S0357
MEGA Ltd MegaSync	Herramienta de sincronización basada en la nube.	T1567.002
Microsoft Sysinternals ProcDump	Genera volcados de memoria. Se utiliza comúnmente para volcar el contenido del servicio de subsistema de autoridad de seguridad local, LSASS.exe.	T1003.001
Microsoft Sysinternals PsExec	Ejecutar un proceso de línea de comandos en un equipo remoto.	S0029
Mimikatz	Extrae credenciales del sistema.	S0002
Ngrok	Se abusa de la herramienta legítima de acceso remoto para eludir las protecciones de la red de las víctimas.	S0508
PuTTY Link (Plink)	Se puede utilizar para automatizar las acciones de Secure Shell (SSH) en Windows.	T1572
Rclone	Programa de línea de comandos para administrar archivos de almacenamiento en la nube	S1040
SoftPerfect Network Scanner	Realiza análisis de red.	T1046
Splashtop	Software de escritorio remoto.	T1021.001
WinSCP	Cliente de protocolo de transferencia de archivos SSH para Windows.	T1048

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20230320_02_LockBitRansomware3.0

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente