BOLETÍN DE ALERTA

Boletín Nro.: 2023-29
Fecha de publicación: 06/06/2023

Tema: Aumento de infecciones por el *ransomware* Lockbit en la región

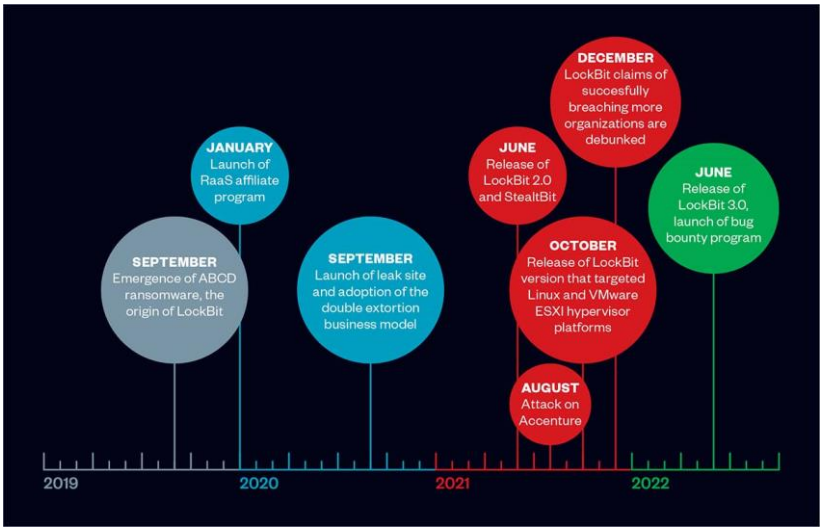
Descripción:

Los casos de ataques de secuestro de archivos por parte de un atacante, mejor conocidos como *ransomware* van alcanzando cada vez una mayor complejidad, así como una mayor cantidad de víctimas en toda la región y también en Paraguay, especialmente de Lockbit, sobre el cual han alertado múltiples agencias de ciberseguridad de todo el mundo.

LockBit es un grupo de *ransomware* que opera bajo el modelo de *Ransomware-as-a-Service* (*RaaS*) que se encuentra en actividad desde el año 2019. Desde su aparición y sus posteriores actualizaciones este grupo de ciberdelincuentes proporciona sus servicios a otros expertos y de esta manera propagan este tipo de ataques. A la actualidad LockBit lanzó la tercera versión de su *ransomware* (*LockBit 3.0*) también conocido como LockBit Black.

LockBit 3.0 trabaja principalmente a través de su propio DLS (*Data Leak Site*) que gestiona y trata las operaciones con las víctimas, así también este *ransomware* utiliza técnicas de anti-análisis para ocultarse y acepta argumentos especiales para operaciones específicas como movimiento lateral y reinicio en modo seguro.

La explotación de este *ransomware* permitiría a un atacante obtener acceso a las redes del dispositivo afectado, acceso remoto y *tunneling*, realizar escalamiento de privilegios, el volcado de credenciales y la exfiltración de archivos.



Cronología de actividades de LockBit

Fuente: https://www.trendmicro.com/vinfo/br/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

Ciberseguridad y Protección de la Información
Ministerio de Tecnologías de la Información y Comunicación (MITIC)
Gral. Santos y Concordia - Complejo Santos - Offic. E14
cert@cert.gov.py | +595 21 217 9000
Asunción - Paraguay | www.cert.gov.py

@CERTpy
/CERT-Py

Vectores de ataque:

- Los atacantes deben obtener acceso a las redes de las víctimas, la misma se realiza a través de la explotación de varias técnicas de ataques tales como: explotación del (*RDP*) especialmente debido a contraseñas débiles (locales o de dominio), , las campañas de , él y la explotación de vulnerabilidades de aplicaciones expuestas a Internet. En los últimos tiempos, y especialmente en Paraguay, las aplicaciones cuyas vulnerabilidades conocidas han sido explotadas con mayor frecuencia fueron casos con equipos Fortinet, Zimbra, Exchange Server siendo víctimas de ataques de ransomware como otro tipo de intrusiones.

Ejecución e infección:

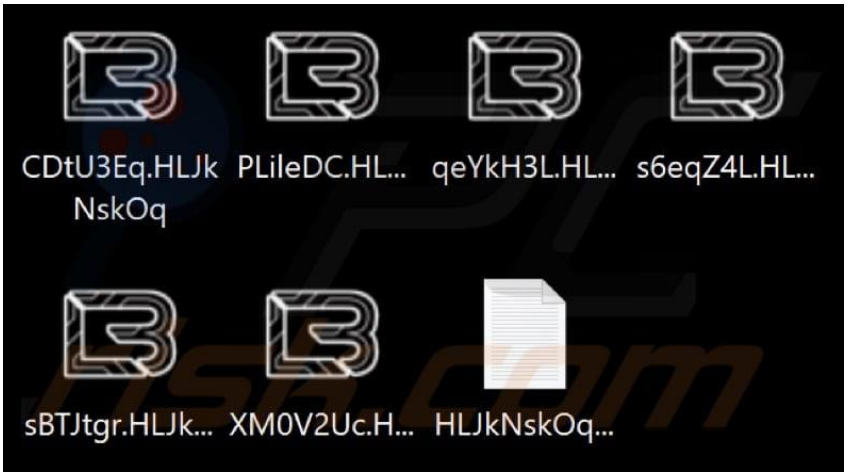
Durante el proceso de ataque del *ransomware*, si los privilegios no son suficientes, *LockBit 3.0* intenta escalar a los privilegios requeridos realizando las siguientes funciones:

- Enumeración de la información del sistema como el nombre del *host*, la configuración del *host*, la información del dominio, la configuración de la unidad local, los recursos compartidos remotos y los dispositivos de almacenamiento externo montados.
- Terminación de procesos y servicios.
- Comandos de lanzamiento.
- Habilitación de inicio de sesión automático para persistencia y escalamiento de privilegios.
- Eliminación de archivos de registro, archivos en la carpeta de la papelera de reciclaje e instantáneas que residen en el disco.

LockBit 3.0 trata de propagarse a través de la red de una 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. *LockBit 3.0* utiliza el software de escritorio remoto *Splashtop* para facilitar el movimiento lateral.

Cuando se compila, 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*), intenta cifrar los datos guardados en cualquier dispositivo local o remoto, pero omite los archivos asociados con las funciones principales del sistema. Cifra los archivos, modifica sus nombres, cambia el fondo de pantalla y añade un archivo de texto llamado [*random_string].README.txt* en el escritorio.

LockBit 3.0 sustituye los nombres de los archivos y sus extensiones por cadenas dinámicas aleatorias. Un ejemplo de cómo *LockBit 3.0* renombra los archivos: sustituye *1.jpg* por *CDtU3Eq.HLJkNskOq*, *2.png* por *PLikeDC.HLJkNskOq*, *3.exe* por *qwYkH3L.HLJkNskOq*, etc.



Fuente: https://www.pcrisk.es/guias-de-desinfeccion/11495-lockbit-3-0-ransomware

Una vez finalizado *LockBit 3.0* puede eliminarse a sí mismo del disco, así como cualquier actualización de directiva de grupo que se haya realizado, según las opciones que se hayan configurado en el momento de la compilación.

Exfiltración:

Los atacantes utilizan *StealBit*, una herramienta de exfiltración personalizada utilizada anteriormente con *LockBit 2.0*, también *rclone*, un administrador de almacenamiento en la nube de línea de comandos de código abierto y servicios de uso compartido de archivos disponibles públicamente, para filtrar archivos de datos confidenciales de la empresa antes del cifrado. Si bien *rclone* y muchos servicios de uso compartido de archivos disponibles públicamente se usan principalmente para fines legítimos, los actores de amenazas también pueden usarlos para ayudar en el compromiso del sistema, la exploración de la red o la filtración de datos. A menudo utilizan otros servicios de intercambio de archivos disponibles públicamente para filtrar datos. Adicionalmente, para más información acceder al siguiente enlace.

Existen varias vulnerabilidades que están siendo explotadas por el *ransomware LockBit*. Las principales se detallan a continuación:

- CVE-2018-13379, de severidad “Crítica”, con una puntuación asignada de 9.8. Esta vulnerabilidad del tipo *path traversal* se debe a una falla de limitación incorrecta en el portal web FortiOS *SSL VPN*. Esto permitiría a un atacante no autenticado a través de peticiones de recursos *HTTP* especialmente diseñadas, descargar archivos del sistema FortiOS.

- CVE-2021-22986, de severidad “Crítica”, con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla de seguridad en la interfaz *REST* de iControl en BIG-IP. Esto permitiría a un atacante a través de solicitudes especialmente diseñadas realizar ataques del tipo *server-side request forgery (SSRF*) y provocar ejecución remota de comandos arbitrarios en el sistema afectado.

- CVE-2021-20028, de severidad “Crítica”, con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla Esta vulnerabilidad se debe a la neutralización incorrecta de elementos especiales utilizados en un comando SQL (*SQLi*). Esto permitiría a un atacante realizar inyección de comandos SQL (*SQLi*) en los productos *Secure Remote Access* (*SRA*) que se encuentren en su *end-of-life* (*EoL*).

Se puede acceder al listado completo de las vulnerabilidades asociadas a *LockBit* aquí.

Mitigación:

Se recomienda que las organizaciones implementen las mitigaciones mencionadas a continuación para mejorar la seguridad ante el *ransomware LockBit 3.0*:

- Implementar un plan de recuperación para mantener y conservar múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación separada, segmentada y segura (p. ej., disco duro, dispositivo de almacenamiento, la nube).
- Mantener todos los sistemas operativos, *software* y *firmware* actualizados.
- Segmentar las redes para evitar la propagación de *ransomware*.
- Identificar, detectar e investigar cualquier actividad que sea considerada sospechosa a través del monitoreo de red.
- Instalar, actualizar periódicamente y habilitar la detección en tiempo real del software antivirus en todos los hosts.
- Revisar los controladores de dominio, los servidores, las estaciones de trabajo y los directorios activos en busca de cuentas nuevas o no reconocidas.
- Auditar cuentas de usuarios con privilegios administrativos y configurar controles de acceso según el principio de mínimo privilegio.
- Considerar agregar un banner o etiqueta de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.
- Deshabilitar las actividades y los permisos de línea de comandos y secuencias de comandos.
- Mantener copias de seguridad offline, que puedan ser utilizadas para la restauración de los datos.
- Verificar que todos los datos de respaldo estén encriptados, sean inmutables (es decir, no se puedan modificar ni eliminar) y cubran toda la infraestructura de datos de la organización.

- Implementar la autenticación multifactor (*MFA*) para prevenir en lo posible campañas de *phishing*, principalmente para correo web, redes privadas virtuales y cuentas que acceden a sistemas críticos.
- Utilizar soluciones de protección de correos electrónicos (ESG)
- Desarrollar y administrar políticas de contraseñas que cumplan con estándares internacionales conocidos como la NIST.
    - Utilizar contraseñas con un nivel alto de complejidad con al menos 8 caracteres y no más de 64 caracteres.
    - Almacenar en formato *hash* utilizando administradores de contraseñas reconocidos en la industria.
    - Agregar en la contraseña de usuario la técnica de *Salting* para las credenciales de inicio de sesión compartidas.
    - Evitar reutilizar contraseñas.
    - Implementar bloqueos de cuentas por intentos fallidos de inicio de sesión.
    - Deshabilitar las "sugerencias" de contraseña.
    - Solicitar cambios de contraseña con un determinado intervalo de tiempo, para prevenir patrones de contraseñas por parte de los usuarios y para dificultar el descifrado.
    - Requerir credenciales de administrador para instalar cualquier software.

Para más información acerca de las mitigaciones, acceder al siguiente enlace.

Adicionalmente, tener en cuenta las medidas de prevención indicadas en los siguientes enlaces que hemos publicado anteriormente:

- https://www.cert.gov.py/noticias/aumento-de-explotacion-masiva-de-vulnerabilidades-conocidas-por-parte-de-bandas-de-ransomware/
- https://www.cert.gov.py/noticias/principales-vulnerabilidades-criticas-explotadas-por-grupos-de-ransomware/

En el caso de un *ransomware*, en la gran mayoría de los casos no se pueden recuperar los archivos encriptados. Abonando el costo del rescate, estás colaborando a financiar esta actividad de ciber-delincuentes, no hay garantías de devolución, y además corren el riesgo de que pidan más dinero. Muy posiblemente no se vuelvan a contactar con ustedes para entregar las claves y no hay garantías que no vuelva a suceder.

Entonces nuestra tarea como CERT-PY en estos casos radica en encontrar el punto de entrada del *ransomware* para entender si es un caso aislado (y nuevo) o ya corresponde a una familia de *ransomware* conocida, que tal vez tenga una solución, además de entender su comportamiento para evitar su propagación y tomar las medidas correctivas necesarias.

Información adicional:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
- https://thehackernews.com/2023/03/lockbit-30-ransomware-inside.html
- https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/
- https://www.cert.gov.py/noticias/aumento-de-explotacion-masiva-de-vulnerabilidades-conocidas-por-parte-de-bandas-de-ransomware/
- https://www.cert.gov.py/noticias/principales-vulnerabilidades-criticas-explotadas-por-grupos-de-ransomware/
- https://www.trendmicro.com/vinfo/br/security/news/ransomware-spotlight/ransomware-spotlight-lockbit
- https://www.securin.io/all-about-lockbit-ransomware/
- https://nvd.nist.gov/vuln/detail/CVE-2018-13379
- https://www.fortiguard.com/psirt/FG-IR-18-384
- https://www.fortiguard.com/psirt/FG-IR-20-233
- https://nvd.nist.gov/vuln/detail/CVE-2021-22986
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017
- https://nvd.nist.gov/vuln/detail/CVE-2021-20028
- https://packetstormsecurity.com/files/162059/F5-iControl-Server-Side-Request-Forgery-Remote-Command-Execution.html
- https://www.securin.io/all-about-lockbit-ransomware/