TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
ACTUALIZACIÓN DE INDICADORES DE COMPROMISO Y COMPORTAMIENTO DE RANSOMWARE LOCKBIT BLACK QUE AFECTÓ AL PODER JUDICIAL

1. Antecedentes generales.

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, compartió ayer, lunes 26 de septiembre de 2022, indicadores de compromiso y una descripción del comportamiento del ransomware LockBit Black, el que afectó al Poder Judicial.

2. Nuevas variaciones en el comportamiento del ransomware LockBit Black.

El análisis de la muestra de LockBit Black permitió esclarecer cómo se produce la infección del ransomware.

El archivo bat 123.cmd realiza una llamada al archivo ejecutable externo injector.exe. Este archivo contiene dos parámetros: el parámetro -e, que realiza la llamada a un archivo de sistema denominada rdpclip.exe; y el parámetro -d, el cual convoca a una biblioteca de enlaces dinámicos llamada lbb.dll. La biblioteca lbb.dll realiza la llamada a otras bibliotecas de enlaces dinámicos con el propósito de hacer las cargas dentro del sistema para la realización de la encriptación.

El análisis realizado a la muestra permitió encontrar el ransomware dentro la biblioteca lbb.dll y no en el ejecutable injector.exe, el cual en este caso solo fue un vector de lanzamiento para la inyección de la biblioteca.

```
injector.exe -e "rdpclip.exe" -d "lbb.dll"
```

El ransomware utiliza el objeto “rootDSE” para establecer una conexión con el active directory. Al obtener el atributo puede enlazar al dominio infectado para así autoreplicarse.

3. Indicadores de Compromiso

Las muestras obtenidas por el CSIRT de Gobierno permitieron obtener los siguientes Indicadores de Compromiso:

- 123.cmd
  SHA256: 385D4FBD3A3AAB0CFE109F0EB2626863B91EC02CEAA4C3E4C104F63CA6DC0C93

- injector.exe
  SHA256: 0DA8CFBA645951768B16DB7707ED2C75BBBB2E396E7DA6DA71A9DCA6EF35DF17

- lbb.dll
  SHA256: 5EF365469867CB30F5094D668E596819BF7163411E2A92CC1D7BD117FCD11BFE

4. Recomendaciones

El CSIRT de gobierno quiere alertar a la comunidad del Estado y entidades en convenio de colaboración para que pongan especial atención sobre esta amenaza y sigan, al menos, las siguientes recomendaciones:

- Asegurar que todos los componentes de sus sistemas (PC y servidores) estén protegidos por programas antivirus, antimalware y firewall con sus licencias vigentes.
- Chequear periódicamente que todo su software esté actualizado.
- Contar con respaldos para sus datos y procesos más importantes, los que deben estar separados (en el mejor de los casos, incluso físicamente) de los activos que respaldan y protegidos adecuadamente con firewalls y protocolos de seguridad.
- Reforzar la concientización de los funcionarios sobre la importancia de desconfiar de los correos electrónicos que reciben, especialmente si incluyen archivos adjuntos, y que informen a los encargados de ciberseguridad si alguien recibe un correo sospechoso.
- Verificar y fortalecer las configuraciones de sus servicios antispam, ya que los correos electrónicos son la principal vía de acceso de programas maliciosos.
- Implementar la segmentación de la red y controlar los privilegios de los usuarios para ajustarse a sus requerimientos.
- Recordar que de enfrentarse a un incidente de ciberseguridad deben informar al CSIRT de Gobierno.
- Revisar periódicamente las alertas que publica el CSIRT de Gobierno sobre las nuevas campañas de phishing y malware que detectamos: https://www.csirt.gob.cl/alertas/.
- Informarse todos los días de nuevas vulnerabilidades de importancia en programas de uso frecuente en nuestro país en https://www.csirt.gob.cl/vulnerabilidades/.

Destacamos, finalmente, que tenemos disponible gran cantidad de material de concientización gratuito en https://www.csirt.gob.cl/recomendaciones/.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.09.27 15:08:07 -03'00'