TLP: BLANCO

ALERTA DE SEGURIDAD CIBERNÉTICA
RANSOMWARE EN PODER JUDICIAL

1. Antecedentes generales.

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, constató este lunes 26 de septiembre los alcances de un incidente de ciberseguridad que afectó al Poder Judicial.

El incidente en cuestión se trata de un ransomware, específicamente LockBit Black, el que se comenzó a manifestar este domingo 25 de septiembre, mientras se propagaba por los dispositivos y sistemas de la organización afectada.

La organización informó que tomó medidas que permitieron contener el ataque y está en la etapa de aplicar las mitigaciones correspondientes, a partir de los respaldos que mantiene.

El CSIRT de Gobierno pudo analizar algunas muestras y está en condiciones de compartir indicadores de compromiso para que las entidades de la administración pública del Estado, organizaciones en convenio de colaboración y otros organizamos interesados puedan utilizar a la brevedad posible.

2. Ataque: Ransomware LockBit Black.

LockBit Black (también conocido como LockBit 3.0) es un ransomware diseñado para bloquear el acceso de los usuarios a sus sistemas informáticos y demandar rescate para restablecerlo.

La infección de este ransomware tiene como consecuencia la interrupción de las operaciones y la extorsión de la organización víctima a partir de los datos potencialmente comprometidos.

El atacante entrega dos mensajes de secuestro. En uno de ellos señala que los datos serán publicados en diferentes sitios TOR en caso de no pagar el rescate exigido. Como prueba del robo de información, el actor malicioso ofrece una muestra gratis, la que puede ser obtenida de un enlace en otro sitio TOR.

En un segundo mensaje, un tanto contradictorio con el anterior, el atacante indica que los datos no han sido robados, pero en caso de no entablar una negociación utilizando un correo y un ID que se especifican en el mensaje, podrían dar acceso a otros actores maliciosos a las redes de la entidad víctima. El mensaje indica que el rescate puede ser pagado en criptomonedas (Monero o Bitcoin).

Junto con buscar contenidos valiosos, este ransomware se caracteriza por propagar la infección y cifra los sistemas informáticos accesibles en una red.

El análisis de la muestra a la que tuvo acceso el CSIRT de Gobierno permitió observar que el ransomware utilizó movimientos laterales como técnica para desplazarse a través de la red afectada.

Lockbit también utilizó un *dropper* (programa malicioso diseñado para entregar otros malware a la computadora víctima) el que utilizó para descargar bibliotecas dinámicas y otros archivos como **netscan.exe,** el cual utilizó para escanear equipos (uno de cada 100 dispositivos), para luego auto replicarse utilizando los nodos accesibles de la red infectada. Expresado de otra manera, LockBit Black se copiaba a sí mismo cada vez que alcanzaba un número de 100 escaneos para luego realizar nuevamente esta operación en busca de infectar a otros 100 dispositivos.

Otro comportamiento atribuido al ransomware es una instrucción de ejecución para imprimir al menos 500 veces la nota de rescate cuando existe una impresora al alcance del atacante.

El ransomware LockBit Black también se caracteriza por contener un indicador de auto destrucción lo que hace casi imposible su análisis forense.

LockBit Black fue avistado en el mundo por primera vez en junio de 2022.

3. Indicadores de Compromiso

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

- LB3.dll
  SHA256: 2783DBAD6D2B6F24F4F772470E1E94DE83254B0526E8A620E9E5A115E30E0888

- run1.bat
  SHA256: 33D1D0467BB85E6D6678DE80E651C340AA30CF96AB4DA86C8DCE327798CBB0BE

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 para que 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 00:02:38 -03'00'