ALERTA DE SEGURIDAD
IOC'S DE DISTINTAS AMENAZAS CIBERNÉTICAS

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT, comparte algunos indicadores de compromisos de fuentes abiertas, nacionales e internacionales, de dos amenazas detectadas recientemente en nuestro país.

Una de ellas es una campaña de ransomware identificada como BlackCat, un conocido ransomware de servicio (Ransonware-as-a-Service), que aprovecha las credenciales de usuarios comprometidas para tener acceso a los sistemas.

Los vectores de entrada de esta amenaza pueden ser diversos, como las vulnerabilidades en las plataformas expuestas a internet, técnicas de ingeniería social, entre otros. Su objetivo principal es obtener acceso al Active Directory donde genera políticas de grupo (GPO) para la implementación de ransomware, aprovechando scripts de PowerShell, herramientas administrativas de Windows y Microsoft Sysinternals.

Sugerimos a las organizaciones, especialmente a la Red de Conectividad del Estado, evaluar la aplicación de cuarentenas sobre estos IoC, revisar el tráfico desde y fuera de su red.

IoC ransomware

Direcciones IP C2

89.44.9.243
142.234.157.246
45.134.20.66
146.0.77.15
37.120.238.58
185.220.102.253
152.89.247.207
198.144.121.93
94.232.41.155
89.163.252.230
45.153.160.140
23.106.223.97
139.60.161.161

HASH

1b90e6f959db883fb4a036dac06242be724a7637708058e2c439e2250222d6d1
0d095acccaeeceea7f8cce241e23512ef995ccc2a7b9507bd0c583144bab4acc
1fd42d07b4be99e0e503c0ed5af2274312be1b03e01b54a6d89c0eef04257d6e
2c27d6456cbdf106e03f07785947f826f0b96b57902eeb010f270ed319f994c9
0d095acccaeeceea7f8cce241e23512ef995ccc2a7b9507bd0c583144bab4acc

Más información, en el siguiente enlace:
https://www.ic3.gov/Media/News/2022/220420.pdf

Por otra parte, durante los últimos meses se han conocido distintos casos de accesos no autorizados. Por esto, el CSIRT de Gobierno recomienda revisar sus plataformas expuestas a internet, con el fin de evitar que los atacantes comprometan su infraestructura y/o exfiltren datos confidenciales.

Los IoC´s asociados a los accesos no autorizados son los siguientes:

186.122.63.75
103.50.33.1

En caso de que las organizaciones públicas o privadas detecten alguno de estos indicadores pueden comunicarse con nosotros al correo soc@interior.gob.cl o al teléfono 1510, ambos canales disponibles en modalidad 7/24, para prevenir futuros ataques y apoyar en la respuesta de la emergencia.

El CSIRT de Gobierno hace un llamado a todas las organizaciones que se vean afectadas por un incidente a realizar las denuncias respectivas en virtud de la ley de delitos informáticos (Ley 21459) vigente en nuestro país.

En el caso de las organizaciones de la Red de Conectividad del Estado y de la administración pública, cabe recordar que todo incidente debe ser notificado al CSIRT de gobierno de acuerdo con lo dispuesto en el D.S. 273/2022.

Recomendación en caso de estar infectado:

- Rápidamente identificar y aislar los focos de actividad potencialmente maliciosos de la red.
- Analizar, identificar y verificar sesiones externas que pudieren atribuirse a un acceso no autorizado y restringirlas de manera preventiva.
- Proteger o aislar información sensible de la institución de forma inmediata.
- Proteger o aislar las copias de seguridad que para no sean afectadas por la amenaza.
- Evaluar la desconexión de estaciones de trabajo y servidores en producción.
- Generar un plan de recuperación, con el equipo IT y proveedores.
- Revisar en estaciones de trabajo, servidores, controladores de dominios de nuevas cuentas de usuarios no reconocidos.
- Revisar la elevación de privilegios de cuentas de usuarios.
- Revisar las tareas programadas de los activos infectados.
- Proteger o aislar las copias de seguridad que para no sean afectadas por la amenaza.
- Verificar la utilización de las siguientes herramientas PsEXec - MegaSync - RClone -Adfind - Rubeus – Stealbit - Softperfect Netscan.
- Verificar tráfico de salida a internet de servidores o estaciones infectadas.
- Verificar las directivas de grupo (GPO).

Recomendaciones preventivas:

- Revisar los registros de la consola de administración de antivirus, revisar amenazas detectadas, desactivación de antivirus en las estaciones.
- Monitorear actividades de en los ID log de los controladores de dominio.
- Activar en los antivirus la protección de análisis de actividad de red.
- Implementar la segmentación de la red (sucursales, servidores, estaciones críticas).
- Generar un plan de recuperación o acciones que se deben tomar ante un incidente.
- Instalar actualizaciones de sistemas operativos, software y firmware.
- Utilice la autenticación multifactor cuando sea posible.
- Activar las protecciones Anti-Cryptor de los antivirus.
- Utilizar métodos seguros de almacenamiento de claves para los equipos TI.
- Deshabilite los protocolos o puertos no utilizados en los sistemas.
- Generar un plan de mantenimiento de reglas en los equipos de seguridad Firewall.
- Generar auditorias de cuentas de usuario con privilegios y accesos elevados en la red.
- Verificar periódicamente el funcionamiento de los antivirus de todos los equipos.
- Evitar la interconexión de equipos a redes WIFI sin seguridad a red corporativas sin pasar por un análisis de seguridad.
- No utilizar script que contengan cuentas con privilegios y sus contraseñas visibles.
- Agregar mensaje a los correos que provienen fuera de su organización.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.21 14:41:11 -03'00'