RECOMENDACIONES PREVENTIVAS FRENTE A RANSOMWARE LOCKBIT 3.0

TLP: BLANCO

El Equipo de Respuesta ante Incidentes de Seguridad Informática de la Coordinación Nacional de Ciberseguridad, CSIRT de Gobierno, ha recibido información proveniente de diversas instituciones nacionales que han sido afectadas por un ataque de ransomware de la clase LockBit 3.0, entre ellas, el Instituto Desarrollo Agropecuario (INDAP) y otras entidades privadas, con posible exfiltración de datos. Los activos afectados usan sistemas operativos Windows y sistemas de virtualización VMware.

LockBit 3.0 es parte de los programas maliciosos de tipo ransomware-as-a-service (RaaS), lo que facilita su uso por toda clase de organizaciones criminales, los cuales utilizan este ransomware para tomar control de los activos digitales de las instituciones afectadas, a las que logran acceso gracias a técnicas como el phishing, la explotación de vulnerabilidades y el aprovechamiento de escritorios remotos expuestos a internet.

Además, estas organizaciones criminales combinan el uso de herramientas gratuitas y de código abierto para comprometer sus sistemas objetivo, realizar el reconocimiento de redes, el acceso remoto, la "tunelización", la recolección de información de Active Directory, la sincronización con servicios en la nube, la compresión de archivos, el volcado de credenciales y la exfiltración de archivos.

En consecuencia, el CSIRT llama a todas las instituciones a seguir esta serie de recomendaciones preventivas:

- Establecer un límite de intentos fallidos de inicio de sesión que al ser superados se bloquea la cuenta.
- Verificar, en los filtros de correo, si existieron emails sospechosos que podrían contener alguna amenaza y que no fueron bloqueados, para mejorar los parámetros de filtrado y verificar dicho correo en la estación de trabajo.
- Eliminar privilegios a nivel de firewall, minimizando los accesos a los sistemas y recursos.
- Mantener una segmentación de red interna para prevenir la propagación de un malware que logre entrar a una parte de sus sistemas.
- Mantener un registro actualizado de sus sistemas para garantizar un monitoreo efectivo.
- Realizar copias de seguridad regularmente, las que deben ser almacenadas en diferentes lugares y medios, incluyendo una copia fuera de línea o de la institución.
- Eliminar servicios que no se estén utilizando como cuentas de VPN o RDP, entre otros.
- Concientizar sobre las amenazas de phishing a los trabajadores de su institución.
- Mantener sistemas operativos de servidores y estaciones de trabajo actualizados.
- Mantener el software de los equipos actualizado y eliminar programas que ya no se utilizan.
- Mantener actualizados el firmware y los equipos de comunicación.
- Revisar los logs de los programas antivirus por lo menos 15 días hacia atrás, para identificar las amenazas que han sido bloqueadas.
- Forzar un escaneo completo, desactivando la opción de solo analizar archivos nuevos.

- Revisar en Active Directory si existen cuentas nuevas o que elevaron privilegios.
- Desactivar cuentas de Active Directory con permisos elevados mientras no se estén utilizando.
- Implementar sistemas multifactor de autentificación en las cuentas usadas por los funcionarios de la institución.
- Revisar la actividad de los eventos de Microsoft Windows (Active Directory) con los siguientes ID:
    - Tareas programadas
        - 106: El usuario registró una nueva tarea programada
        - 4702: Se actualizó una tarea programada
        - 4699: Se eliminó una tarea programada o Servicios
        - 4697: Se instaló un servicio en el sistema
        - 7034: El servicio finalizó inesperadamente
        - 7045: Se creó un nuevo servicio en la máquina local de Windows
    - Administración de cuentas
        - 4720: Se creó una cuenta de usuario
        - 4724: Se intentó restablecer la contraseña de una cuenta
        - 4782: Acceso a hash de contraseña
        - 4624: Se inició sesión correctamente en una cuenta
        - 4625: Una cuenta no pudo iniciar sesión
        - 4672: Privilegios especiales asignados al nuevo inicio de sesión
        - 4634: Cierre de sesión exitoso
        - 4776: Inicio de sesión fallido o exitoso a través de dominio
    - Manipulación del registro de eventos
        - 1100: Cierre del servicio de registro de eventos
        - 104: Archivo de registro borrado
        - 1102: Registro de auditoría de seguridad borrado
    - Red
        - 5140: Se accedió a un objeto compartido de red
        - 4778: Se volvió a conectar una sesión RDP
        - 4104: Ejecución de PowerShell

El CSIRT de Gobierno continuará monitoreando estos eventos a la espera de mayores antecedentes, los que serán compartidos a la comunidad. En caso de un incidente, por favor reportarlo a https://csirt.gob.cl

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.20 11:04:08 -04'00'