CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Alerta por ataques a la infraestructura crítica por hackers DarkSide

Santiago, 12 de mayo de 2021

TLP: BLANCO

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Detalles de la alerta

Este resumen de ciberataques, vulnerabilidades e incidentes de seguridad cibernética tiene como propósito destacar algunos eventos de días pasados para que puedan ser interpretados y discutidos por las diferentes entidades que tengan acceso a su lectura.

Este informe reúne los antecedentes conocidos hasta el día de su publicación. La información consignada en el presente documento es catalogada como TLP BLANCO.

El 11 de mayo de 2021, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) del Departamento de Seguridad Nacional (DHS) de Estados Unidos y el Buró Federal de Investigaciones (FBI) compartieron una alerta[1] con las mejores prácticas para impedir interrupciones en el funcionamiento de las organizaciones por culpa de ataques de ransomware por parte del actor malicioso DarkSide.

DarkSide logró detener, la noche del viernes 7 de mayo, la operación del oleoducto Colonial Pipeline en el este de EE.UU., el que se mantiene sin reiniciar su funcionamiento al momento de escribir esta alerta, además de robar más de 100 GB de datos de la empresa a cargo de la infraestructura.

Colonial Pipeline transporta, desde Texas a Nueva Jersey, más de 2,5 millones de barriles de petróleo al día, un 45% del suministro de diésel, gasolina y combustible para avión utilizada en la Costa Este de Estados Unidos.

Por esto, la alerta entregada por la CISA y el FBI[2] recuerda varias prácticas que se recomienda implementar para aumentar la resiliencia de una entidad ante un ataque como el de DarkSide, las que compartimos traducidas del original y en forma resumida en el presente documento.

[1] DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks| CISA https://us-cert.cisa.gov/ncas/alerts/aa21-131a

[2] La misma información de la CISA y el FBI también está disponible en PDF: https://us-cert.cisa.gov/sites/default/files/2021-05/AA21-131A_DarkSide_Ransomware.pdf

Detalles y mitigación

En resumen: La CISA y el FBI urgen a los dueños y operadores de infraestructura crítica a adoptar un estado de alerta elevado, e implementar medidas de mitigación incluyendo una segmentación robusta entre las redes de IT y OT, testear regularmente controles manuales, y asegurar que los respaldos hayan sido implementados, testeados regularmente y aislados de las conexiones de red.

Detalles técnicos del ataque a Colpipe

Tras ganar acceso inicial a la red de la Colonial Pipeline (Colpipe), los actores de DarkSide usaron su ransomware contra la red IT de la empresa. Como respuesta al ciberataque, Colpipe indicó haber proactivamente desconectado ciertos sistemas OT para asegurar la seguridad de los mismos. Hasta el momento, no hay evidencia de que los actores maliciosos hayan podido moverse lateralmente hacia estos sistemas OT.

DarkSide es un caso de ransomeware como servicio (RaaS), lo que significa que los desarrolladores del ransomware obtienen parte de las ganancias obtenidas por los cibercriminales que las utilizan, conocidos como “asociados”.

Según reportes OSINT, actores DarkSide han sido observados obteniendo acceso inicial a través de phishing y la explotación de cuentas accesibles remotamente e infraestructura de escritorio virtual (Virtual Desktop Infraestructure, VDI). Tras ganar acceso, los actores DarkSide despliegan ransomware DarkSide para encriptar y robar datos sensibles, tras lo que exigen dinero a los dueños de la información a cambio de no difundirla.

El ransomware de DarkSide usa cifrado Salsa20 y RSA. Los actores DarkSide usan principalmente TOR (The Onion Router) para el comando y control, aunque también se los ha observado usando Cobalt Strike.

Mitigación

La CISA y el FBI recomiendan lo siguiente para reducir el riesgo de ser comprometido por un ataque de ransomware.

- Exigir autenticación multifactor a quienes acceden de forma remota a las redes OT e IT.
- Activar fuertes filtros de spam para evitar que correos de phishing alcancen a los usuarios de la organización, y filtrar los emails que contengan archivos ejecutables.
- Implementar un programa de capacitación y ataques simulados de spearphishing, para desalentar que los usuarios visiten sitios maliciosos o abran adjuntos maliciosos, y reafirmar las respuestas apropiadas de los usuarios ante emails de spearphishing.
- Filtrar el tráfico de la red para prohibir la comunicación de acceso y salida con direcciones IP conocidamente maliciosas.
- Actualizar el software, incluyendo sistemas operativos, aplicaciones y firmware en los activos de la red IT, de forma oportuna. Considerar el uso de un sistema centralizado de

administración de parches. Usar una estrategia de evaluación basada en el riesgo para determinar qué activos y zonas de la red OT deberían participar en el programa de administración de parches.

- Limitar el acceso a recursos desde la red, especialmente a través de restringir RDP. Si tras analizar riesgos RDP es considerado operacionalmente necesario, restringir las fuentes de origen y exigir autenticación multifactor.
- Programar antivirus/antimalware para que realice escaneos regulares de los activos de la red IT usando firmas actualizadas. Usar una estrategia de inventario basada en riesgo para determinar cómo se identifica a los activos de redes OT y cómo se evalúa la presencia en ellos de malware.
- Implementar la prevención de ejecución no autorizada a través de:
    - Deshabilitar los script de macros de los archivos de Microsoft Office compartidos a través de email. Considere usar software Office Viewer para abrir estos archivos en lugar de aplicaciones completas de Microsoft Office.
    - Implementar una lista permitida de aplicaciones (allowlisting), que solo permite a los sistemas ejecutar programas conocidos y aceptados por las políticas de seguridad. Implementar políticas de restricción de software (SRP) u otros controles para impedir que los programas ejecuten archivos de ubicaciones conocidas por su ransomware, como archivos temporales de populares navegadores de internet o programas de decompresión, incluyendo la carpeta AppData / LocalAppData.
- Monitorear o bloquear las conexiones entrantes de nodos de salida de Tor y otros servicios de anonimización a direcciones IP y puertos por los cuales no se esperan conecciones externas (por ejemplo, los que no son accesos VPN, de correo o web).
- Utilizar firmas para detectar o bloquear conecciones entrantes de servidores Cobalt Strike y otras herramientas de explotación para después de que la víctima ya ha sido comprometida.

La CISA y el FBI recomiendan implementar las siguientes mitigaciones para reducir el riesgo de severa degradación de negocios o funcional si se cae en un ataque de ransomware.

- Implementar y asegurar segmentación robusta entre las redes IT y OT para limitar la capacidad de adversarios de pivotear a la red OT tras comprometer la red IT. Definir una zona desmilitarizada que elimine la comunicación no regulada entre las redes IT y OT.
- Organizar los activos OT en zonas lógicas tomando en cuenta lo criticidad, consecuencia y necesidad operacional de las cuentas. Definir vías de comunicación aceptables entre las zonas y desplegar controles de seguridad para filtrar el tráfico de las redes y monitorear la comunicación entre zonas. Prohibir a los protocolos de control de sistemas industriales (ICS) el atravesar la red IT.
- Identificar las interdependencias entre redes OT e IT y desarrollar soluciones alternativas o controles manuales para asegurar que las redes ICS pueden ser aisladas si las conexiones crean riesgos a la operación segura y confiable de los procesos OT. Testear regularmente planes de contingencia como controles manuales, con tal de que funciones críticas de seguridad puedan ser mantenidas durante un ciberincidente. Asegurar que la red OT puede operar a la capacidad necesaria incluso si la red IT es comprometida.
- Testear regularmente controles manuales para que las funciones críticas puedan ser mantenidas en funcionamiento si las redes ICS u OT deben ser desconectadas.

- Implementar procedimientos regulares de respaldo de datos en las redes IT y OT. Los procedimientos de respaldo deben ser realizados con frecuencia y regularidad, y contemplar las siguientes mejores prácticas:
    - Asegurar el testeo regular de los respaldos.
    - Resguardar los respaldos por separado, aislados de las conexiones de red que podrían permitir su infección por ransomware.
    - Mantener "imágenes doradas" regularmente actualizadas de los sistemas críticos por si se necesita reconstruirlos. Esto significa mantener "plantillas" que incluyan un sistema operativo preconfigurado y aplicaciones de software asociadas que puedan ser rápidamente desplegadas para reconstruir un sistema, como un servidor o máquina virtual.
    - Conserve el hardware de respaldo para reconstruir los sistemas en caso de que no se prefiera reconstruir el sistema primario. Hardware más viejo o más nuevo que el sistema primario puede resultar en problemas de instalación o compatibilidad al reconstruir desde imágenes.
    - Conservar código fuente o ejecutables. Es más eficiente reconstruir sobre imágenes de sistema, pero algunas imágenes no se instalarán correctamente en diferente hardware. Tener acceso separado al software que se necesita ayudará en estos casos.
- Asegurar que las cuentas de usuario y proceso son limitadas a través de las políticas de uso, control de las cuentas de usuario y administración de cuentas privilegiadas. Organizar los derechos de acceso según los principios del menor privilegio y la separación de tareas.

Si su organización es impactada por un incidente de ransomware, la CISA y el FBI recomiendan las siguientes acciones:

- Aislar el sistema infectado. Remover el sistema infectado de todas las redes y deshabilitar el wifi, Bluetooth y todas las potenciales capacidades de conexiones del computador. Asegurar que todos los discos compartidos y de red están desconectados, sean wifi o alámbricos.
- Apagar otros computadores y aparatos. Apagar y remover de la red los dispositivos que compartan una red con el aparato infectado y que no hayan sido totalmente encriptados por el ransomware. Si es posible, recolectar y asegurar todos los computadores infectados y potencialmente infectados en un lugar principal, asegurándose de claramente etiquetar cualquier equipo que haya sido cifrado. Apagar y segregar los computadores infectados, y otros que puedan no haber sido encriptados completamente puede ayudar a la recuperación total o parcial de archivos por especialistas.
- Asegurar los respaldos. Asegurarse de que los datos de respaldo estén desconectados de las redes y seguros. Si es posible, escanee sus datos de respaldo con un programa antivirus para asegurarse de que esté libre de malware.

Enlaces

DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks| CISA https://us-cert.cisa.gov/ncas/alerts/aa21-131a

La misma información de la CISA y el FBI también está disponible en PDF: https://us-cert.cisa.gov/sites/default/files/2021-05/AA21-131A_DarkSide_Ransomware.pdf

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.12 17:48:46 -04'00'