Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

31/ 01 / 2024

CONTENIDO

INTRODUCCIÓN

Se aborda un caso de intrusión cibernética que comenzó con un acceso no autorizado a un host RDP expuesto, utilizando credenciales legítimas de la cuenta de Administrador predeterminada. Lo destacado de este ataque radica en la ausencia de intentos de fuerza bruta, sugiriendo la posibilidad de acceso previo recurrente o la intervención de un intermediario de acceso. Una vez dentro, los perpetradores desplegaron diversas herramientas, incluyendo scripts por lotes, ejecutables y SoftPerfect Netscan, para realizar escaneos de red, identificar comparticiones y explorar documentos. La intrusión avanzó con movimientos laterales, deshabilitación de Windows Defender y exfiltración de datos hacia Mega.io mediante Rclone. La sorpresa llegó cuando, tras una desconexión, los atacantes se reconectaron desde una dirección IP diferente, indicando un conocimiento profundo de la red.

RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

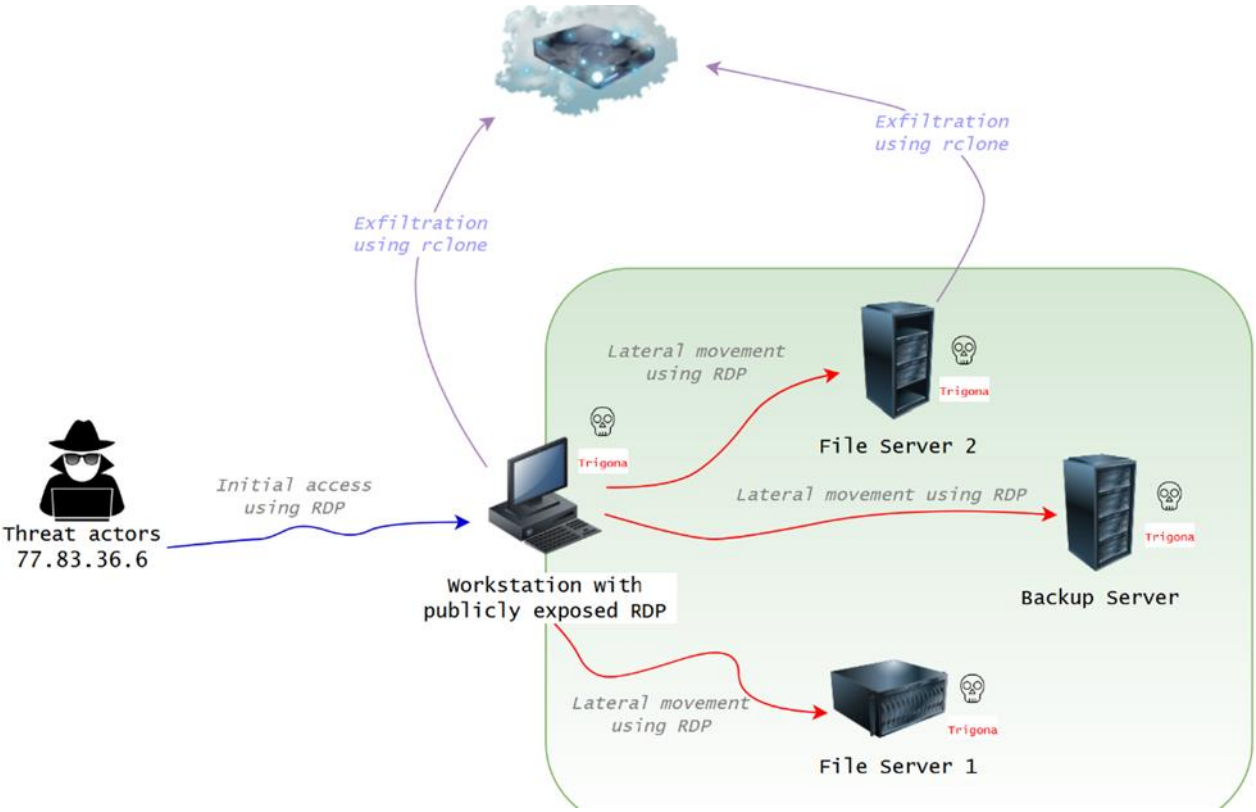
A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_01_31_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	31/01/2024
Es día cero (0 day):	No

RESUMEN

El ataque comenzó con un acceso no autorizado a un host RDP expuesto, utilizando credenciales legítimas de la cuenta de Administrador predeterminada. Lo sorprendente es que no hubo evidencia de intentos de fuerza bruta, lo que sugiere la posibilidad de la implicación de un acceso previo recurrente o la intervención de un intermediario de acceso. Una vez dentro, los atacantes desplegaron un conjunto de herramientas en el host de entrada, incluyendo scripts por lotes, ejecutables y la herramienta SoftPerfect Netscan. En un abrir y cerrar de ojos, iniciaron escaneos de red con Netscan, identificando comparticiones de red y explorando documentos a través de un navegador web.

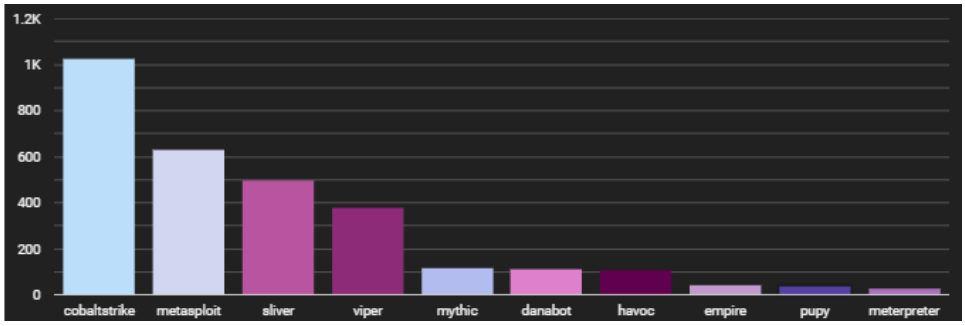
Después de unos 20 minutos de acceso, los actores iniciaron el movimiento lateral estableciendo una conexión RDP a uno de los servidores de archivos. Copiaron su arsenal al servidor de archivos y procedieron a ejecutar un conjunto de comandos para deshabilitar Windows Defender. Después de asegurar el camino, ejecutaron un script por lotes responsable de iniciar el proceso de exfiltración de datos hacia Mega.io a través de Rclone. Además, utilizaron RDP para acceder a un segundo servidor de archivos, donde ejecutaron nuevamente los scripts de Rclone.



Aproximadamente 45 minutos después de la extracción de datos, los atacantes alteraron su conexión RDP. Se desconectaron y volvieron a conectarse al host original desde una dirección IP diferente. Aunque la nueva IP y el nombre de host difieren del acceso inicial, la evidencia sugiere que estos atacantes conocían a fondo la red y utilizaban técnicas idénticas a las observadas previamente. Todo apunta a que este acceso era una continuación de la intrusión, posiblemente ejecutada por el mismo individuo o un colaborador dentro del grupo.

Ambos servidores de archivos recibieron el mismo tratamiento de desactivación de Windows Defender que el host original. Se estableció una conexión RDP con un servidor de respaldo y se ejecutaron los mismos comandos de desactivación. Luego, los atacantes prepararon un binario de ransomware en cada uno de los hosts a los que tenían acceso. Finalmente, lanzaron el ransomware Trigona en cada host a través de sus sesiones RDP.

Tras aproximadamente dos horas y 49 minutos desde el acceso inicial, el ransomware Trigona se ejecutó. Este ransomware no solo afectó al host donde se ejecutó inicialmente, sino que se propagó a todos los hosts accesibles a través del protocolo Server Message Block (SMB). El resultado: doble impacto de extorsión, con la exfiltración de datos sensibles y la cifrado de sistemas.



Durante la intrusión, los atacantes utilizaron Netscan de SoftPerfect para realizar diversas operaciones de descubrimiento. Además, se mencionan recursos adicionales para obtener más información sobre el ransomware Trigona.
El acceso inicial se realizó a través de una conexión RDP desde una dirección IP ubicada en Ucrania. Aunque el método exacto de acceso inicial no puede determinarse con certeza, la ausencia de intentos de fuerza bruta y el uso de credenciales válidas sugieren la posibilidad de que los actores hayan obtenido la contraseña del Administrador de dominio, posiblemente a través de filtración o compra.

Durante la intrusión, todos los movimientos se llevaron a cabo a través de RDP, utilizando PowerShell y sesiones Cmd para ejecutar varios scripts. Se observó la ejecución de scripts detallados en la sección de exfiltración, así como otros que se mencionan en el informe.
Los actores dejaron archivos para crear nuevos usuarios locales y agregarlos a grupos específicos. Estos archivos indican la creación de usuarios con nombres como "sys" y "Support", junto con la desactivación de notificaciones para el usuario "Support".

Los atacantes desplegaron scripts por lotes para deshabilitar herramientas de seguridad, específicamente Windows Defender. Aunque algunos scripts no se ejecutaron, se observaron comandos manuales para desactivar características de Windows Defender.

Después del acceso inicial, se realizaron comandos comunes de descubrimiento utilizando utilidades de Windows integradas y se empleó la herramienta Netscan de SoftPerfect para realizar operaciones de descubrimiento más avanzadas. Los atacantes exploraron archivos remotamente y utilizaron herramientas como MS Paint para revisar imágenes en sistemas remotos.

RECOMENDACIONES

- Asegúrese de que todos sus programas y aplicaciones estén actualizados. Los ciberdelincuentes a menudo explotan vulnerabilidades en software desactualizado.
- Utilice un firewall para bloquear todo el tráfico no autorizado hacia y desde tu ordenador.
- Utilice una Red Privada Virtual (VPN) cuando te conectes a redes públicas para asegurar tu conexión a Internet.
- Mantenga un registro de toda la actividad de la red. Esto puede ayudarle a detectar cualquier actividad sospechosa.
- Mantenga actualizados sus programas antivirus para proteger su sistema contra las últimas amenazas.
- Implemente la autenticación de dos factores siempre que sea posible para añadir una capa adicional de seguridad.
- Evite visitar sitios web no seguros o de reputación dudosa. Utilice la navegación segura en tu navegador para bloquear sitios web maliciosos.
- Realice copias de seguridad periódicas de los datos críticos y almacénelos en ubicaciones seguras e independientes. Esto facilitará la recuperación en caso de un ataque de ransomware.

NOTICIA COMPLETA

https://devel.group/blog/ransomware-trigona-desencadena-alarmas-de-ciberseguridad-en-la-region/

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240131_01_TrigonaRansomware

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente