Resumen ataque

Esta intrusión comenzó cuando un atacante obtuvo acceso a un host expuesto de RDP. Es notable que el inicio de sesión utilizó credenciales legítimas para la cuenta de Administrador predeterminada, sin evidencia de fuerza bruta. Los registros revelaron múltiples inicios de sesión remotos en el mismo host en las semanas anteriores, lo que sugiere la presencia de un adversario recurrente o la posible participación de un intermediario de acceso.

Una vez obtenido el acceso, el atacante desplegó un conjunto de herramientas en el host de entrada, que incluía una variedad de scripts por lotes, ejecutables y la herramienta SoftPerfect Netscan. Luego iniciaron escaneos de red utilizando Netscan, utilizando una configuración personalizada para automatizar acciones de descubrimiento típicas, como se detalla en la sección de descubrimiento. Mientras Netscan enumeraba la red, el atacante identificó recursos compartidos de red y comenzó a explorarlos, accediendo a varios documentos a través de un navegador web.

Aproximadamente 20 minutos después del acceso inicial, el atacante comenzó el movimiento lateral al establecer una conexión RDP con uno de los servidores de archivos. Luego copiaron su conjunto de herramientas al servidor de archivos. Después de esto, el atacante preparó Rclone en el host de entrada. Sin embargo, antes de ejecutarlo, procedieron a ejecutar una secuencia de comandos destinados a desactivar Windows Defender. Con el camino despejado, procedieron a ejecutar un script por lotes responsable de iniciar el proceso de exfiltración de Rclone a Mega.io. Además, utilizaron RDP para acceder a un segundo servidor de archivos, donde ejecutaron los scripts de Rclone nuevamente.

Aproximadamente 45 minutos después de la extracción de datos, el atacante alteró su conexión de Protocolo de Escritorio Remoto (RDP). Cerraron la sesión y luego iniciaron sesión en el host de entrada desde una dirección IP diferente. Aunque la nueva IP y el nombre de host difieren del ingreso inicial, es importante destacar que el atacante poseía un conocimiento integral de la red, interactuaba con los hosts comprometidos anteriormente y empleaba técnicas idénticas a las observadas anteriormente. Esta evidencia indica fuertemente que este acceso fue una continuación de la intrusión en curso, posiblemente ejecutada por el mismo individuo o un colaborador dentro del grupo.

Ambos servidores de recursos compartidos recibieron el mismo tratamiento de desactivación de Windows Defender que el host de entrada. También se estableció una conexión RDP con un servidor de respaldo dentro del entorno, y se ejecutaron las mismas series de comandos de desactivación. Luego, el atacante preparó un binario de ransomware en cada uno de los hosts a los que tenían acceso. Después de esto, iniciaron el binario de ransomware en cada host a través de sus sesiones de RDP.

En este caso, el ransomware Trigona, se ejecutó aproximadamente dos horas y 49 minutos después del acceso inicial. Tuvo consecuencias de gran alcance, afectando no solo al host donde se ejecutó inicialmente, sino también propagándose a todos los hosts accesibles a través del protocolo Server Message Block (SMB).

Como resultado, la víctima enfrentó un impacto de doble extorsión, que incluía tanto la exfiltración de datos sensibles como el cifrado de sistemas mediante el uso del ransomware Trigona.