Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RHYSIDA RANSOMWARE

15/11/2023

CONTENIDO

INTRODUCCIÓN

La Oficina Federal de Investigaciones (FBI), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y el Centro Multiestatal de Análisis e Intercambio de Información (MS-ISAC) están lanzando esta CSA conjunta para difundir los IOC y TTP de ransomware Rhysida conocidos identificados a través de investigaciones tan recientes como septiembre de 2023. Rhysida, una variante emergente de ransomware, se ha desplegado predominantemente contra los sectores de la educación, la sanidad, la fabricación, la tecnología de la información y el gobierno desde mayo de 2023. La información de este CSA se deriva de las investigaciones de respuesta a incidentes relacionadas y el análisis de malware de las muestras descubiertas en las redes de las víctimas.

RHYSIDA RANSOMWARE

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

ID de alerta:	DSOC-CERT_2023_11_15_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	15/11/2023
Es día cero (0 day):	No

RESUMEN

La Oficina Federal de Investigaciones (FBI), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y el Centro Multiestatal de Análisis e Intercambio de Información (MS-ISAC) están lanzando esta CSA conjunta para difundir los IOC y TTP de ransomware Rhysida conocidos identificados a través de investigaciones tan recientes como septiembre de 2023. Rhysida, una variante emergente de ransomware, se ha desplegado predominantemente contra los sectores de la educación, la sanidad, la fabricación, la tecnología de la información y el gobierno desde mayo de 2023. La información de este CSA se deriva de las investigaciones de respuesta a incidentes relacionadas y el análisis de malware de las muestras descubiertas en las redes de las víctimas.

GENERAL

Se sabe que los actores de amenazas que aprovechan el ransomware Rhysida afectan a los “objetivos de oportunidad”, incluidas las víctimas de los sectores de la educación, la sanidad, la fabricación, la tecnología de la información y el gobierno. Los informes de fuentes abiertas detallan las similitudes entre la actividad de Vice Society (DEV-0832) [1] y los actores observados desplegando el ransomware Rhysida. Además, los informes de fuentes abiertas [2] han confirmado casos observados de actores de Rhysida que operan en una capacidad de ransomware como servicio (RaaS), donde las herramientas y la

infraestructura de ransomware se alquilan en un modelo de participación en las ganancias. Los rescates pagados se dividen entre el grupo y los afiliados.

ACCESO INICIAL Y PERSISTENCIA

Se ha observado que los actores de Rhysida aprovechan los servicios remotos externos para acceder inicialmente y persistir dentro de una red. Los servicios remotos, como las redes privadas virtuales (VPN), permiten a los usuarios conectarse a los recursos internos de la red empresarial desde ubicaciones externas. Se ha observado comúnmente que los actores de Rhysida se autentican en puntos de acceso VPN internos con credenciales válidas comprometidas [T1078], especialmente debido a que las organizaciones carecen de MFA habilitada de forma predeterminada. Además, se ha observado que los actores explotan Zerologon (CVE-2020-1472), una vulnerabilidad crítica de elevación de privilegios en el protocolo remoto Netlogon de Microsoft [T1190]. Nota: Microsoft lanzó un parche para CVE-2020-1472 el 11 de agosto de 2020. [3]

LIVING OF THE LAND

El análisis identificó a los actores de Rhysida que utilizan técnicas de vida fuera de la tierra, como la creación de conexiones de Protocolo de escritorio remoto (RDP) para el movimiento lateral [T1021.001]. Las técnicas de living of the land incluyen el uso de herramientas de administración de red nativas (integradas en el sistema operativo) para realizar operaciones. Esto permite a los actores evadir la detección mezclándose con los sistemas Windows normales y las actividades de red.

Ipconfig [T1016], y se han utilizado varios comandos para enumerar los entornos de las víctimas y recopilar información sobre los dominios. En un caso de uso de credenciales comprometidas, los actores aprovecharon los comandos dentro de PowerShell para identificar a los usuarios que habían iniciado sesión y realizaron un reconocimiento en las cuentas de red dentro del entorno de la víctima. Nota: Los siguientes comandos no se ejecutaron en el orden exacto indicado. .whoaminltestnetnet

- net user [username] /domain [T1087.002]
- net group “domain computers” /domain [T1018]
- net group “domain admins” /domain [T1069.002]
- net localgroup administrators [T1069.001]
-

El análisis de la tabla maestra de archivos (MFT)[4] identificó que el sistema víctima generó el subárbol de registro, que se creó cuando el usuario comprometido inició sesión en el sistema por primera vez. Esto se consideró anómalo debido a la línea de base de la actividad normal para ese usuario y sistema en particular. Nota: El MFT y alberga información sobre un archivo, incluido su tamaño, marcas de fecha y hora, permisos y contenido de datos.ntuser.dat

HERRAMIENTAS

Se recomienda a las organizaciones que investiguen y examinen el uso de estas herramientas antes de realizar acciones correctivas.

Nombre	Descripción
cmd.exe	La utilidad nativa del símbolo del sistema de la línea de comandos.
PowerShell.exe	Una herramienta nativa de línea de comandos que se usa para iniciar una sesión de Windows PowerShell en una ventana del símbolo del sistema.
PsExec.exe	Una herramienta incluida en la suite PsTools que se utiliza para ejecutar procesos de forma remota. Los actores de Rhysida aprovecharon en gran medida esta herramienta para el movimiento lateral y la ejecución remota.
mstsc.exe	Una herramienta nativa que establece una conexión RDP con un host.
PuTTY.exe	Se ha observado que los actores de Rhysida crean conexiones PuTTy de Secure Shell (SSH) para el movimiento lateral. En un ejemplo, el análisis del historial de host de la consola de PowerShell para una cuenta de usuario comprometida reveló que los actores de Rhysida aprovecharon PuTTy para conectarse de forma remota a los sistemas a través de SSH [T1021.004].
PortStarter	Un script de puerta trasera escrito en Go que proporciona funcionalidad para modificar la configuración del firewall y abrir puertos a servidores de comando y control (C2) preconfigurados. [1]
Secretsdump	Script utilizado para extraer credenciales y otra información confidencial de un sistema. Se ha observado que los actores de Rhysida utilizan esto para el vertido de NTDS [T1003.003] en varios casos.
ntdsutil.exe	Una herramienta estándar de Windows que se utiliza para interactuar con la base de datos NTDS. Los actores de Rhysida usaron esta herramienta para extraer y volcar la base de datos del controlador de dominio que contenía hashes para todos los usuarios de Active Directory (AD). NTDS.dit **Nota**: Se recomienda encarecidamente que las organizaciones realicen restablecimientos de contraseña en todo el dominio y restablecimientos de contraseña TGT de Kerberos dobles si se encuentra algún indicio de que el archivo se vio comprometido.NTDS.dit
AnyDesk	Un software común que puede ser utilizado maliciosamente por los actores de amenazas para obtener acceso remoto y mantener la persistencia [T1219]. AnyDesk también admite la transferencia remota de archivos.
wevtutil.exe	Una herramienta estándar de la Utilidad de eventos de Windows que se usa para ver los registros de eventos. Los actores de Rhysida utilizaron esta herramienta para borrar un número significativo de registros de eventos de Windows, incluidos los registros del sistema, las aplicaciones y la seguridad [T1070.001].
PowerView	Una herramienta de PowerShell que se usa para obtener conocimiento de la situación de los dominios de Windows. La revisión de los registros de eventos de PowerShell identificó a los actores de Rhysida que usan esta herramienta para realizar comandos adicionales basados en reconocimiento y recopilar credenciales.

CARACTERÍSTICAS DE RHYSIDA RANSOMWARE

En una investigación, los actores de Rhysida crearon dos carpetas en la unidad C:\ etiquetadas y , que servían como directorio de ensayo (ubicación central) para alojar ejecutables maliciosos. La carpeta contenía nombres de archivo de acuerdo con los nombres de host en la red de la víctima, probablemente importados a través de una herramienta de escaneo. La carpeta contenía varios archivos enumerados en la Tabla a continuación. Los actores de Rhysida implementaron estas herramientas y scripts para ayudar al cifrado del sistema y de toda la red. in out in out

Archivo	Hash (SHA256)	Descripción
conhost.exe	6633fa85bb234a75927b23417313e51a4c155e12f71da3959e168851a600b010	Un binario de ransomware.
psexec.exe	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b	Un archivo utilizado para ejecutar un proceso en un host remoto o local.
S_0.bat	1c4978cd5d750a2985da9b58db137fc74d28422f1e087fd77642faa7efe7b597	Un script por lotes que probablemente se utiliza para colocarlo en los sistemas de las víctimas con fines de preparación de ransomware [T1059.003]. 1.ps1
1.ps1	4e34b9442f825a16d7f6557193426ae7a18899ed46d3b896f6e4357367276183	Identifica una lista de extensión bloqueada de archivos que se van a cifrar y no se van a cifrar.
S_1.bat	97766464d0f2f91b82b557ac656ab82e15cae7896b1d8c98632ca53c15cf06c4	Un script por lotes que copia (el binario de cifrado) en una lista importada de nombres de host dentro del directorio de cada sistema.conhost.exeC:\Windows\Temp
S_2.bat	918784e25bd24192ce4e999538be96898558660659e3c624a5f27857784cd7e1	Se ejecuta en sistemas víctimas comprometidos, que cifran y anexan la extensión de en todo el entorno.conhost.exe.Rhysida

ENCRIPTACIÓN

Después de mapear la red, el ransomware encripta los datos utilizando una clave de encriptación RSA de 4096 bits con un algoritmo ChaCha20 [T1486]. El algoritmo cuenta con una clave de 256 bits, un contador de 32 bits y un nonce de 96 bits junto con una matriz de cuatro por cuatro de palabras de 32 bits en texto sin formato. Los comandos de modificación del Registro [T1112] no se ofuscan, se muestran como cadenas de texto sin formato y se ejecutan a través de .cmd.exe

El encriptador de Rhysida ejecuta un archivo para cifrar y modificar todos los archivos cifrados para mostrar una extensión. [5] Después del cifrado, un comando de PowerShell elimina el binario [T1070.004(el vínculo es externo)] de la red mediante una ventana de comandos oculta [T1564.003]. El encriptador Rhysida permite argumentos (seleccionar un directorio) y (eliminación de archivos), definidos por los autores del código como parseOptions. [6] Una vez que las líneas de cadenas binarias completan sus tareas, se eliminan a sí mismas a través del panel de control para evadir la detección. .rhysida-d-sr

EXTORSIÓN

Según los informes, los actores de Rhysida participan en una "doble extorsión" [T1657]: exigen el pago de un rescate para descifrar los datos de las víctimas y amenazan con publicar los datos confidenciales exfiltrados a menos que se pague el rescate. [5] Los actores de Rhysida dirigen a las víctimas para que envíen pagos de rescate en Bitcoin a direcciones de billeteras de criptomonedas proporcionadas por los actores de amenazas. Como se muestra en la Figura 1, el ransomware Rhysida deja caer una nota de rescate llamada "CriticalBreachDetected" como un archivo PDF: la nota proporciona a cada empresa un código único e instrucciones para ponerse en contacto con el grupo a través de un portal basado en Tor.

Identificado en el análisis y también incluido en los informes de código abierto, el contenido de la nota de rescate se incrusta como texto sin formato en el binario del rescate, lo que ofrece a los defensores de la red la oportunidad de implementar la detección basada en cadenas para alertar sobre la evidencia de la nota de rescate. Los actores de amenazas de Rhysida pueden dirigirse a sistemas que no utilizan sistemas operativos de línea de comandos. El formato de las notas de rescate en PDF podría indicar que los actores de Rhysida solo se dirigen a sistemas que son compatibles con el manejo de documentos PDF. [8]

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20231115_01_RhysidaRansomware

NOTICIA COMPLETA

https://devel.group/blog/stopransomware-rhysida-ransomware/

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