Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°274	Fecha: 16-11-2023
		Página: 4 de 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	CISA y el FBI emiten una advertencia sobre los ataques de doble extorsión del ransomware Rhysida		
Tipo de Ataque	Ransonware	Abreviatura	Ransonware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los actores de amenazas detrás del ransomware Rhysida participan en ataques oportunistas dirigidos a organizaciones que abarcan diversos sectores industriales.

Detectada por primera vez en mayo de 2023, Rhysida utiliza la táctica probada de la doble extorsión, exigiendo el pago de un rescate para descifrar los datos de las víctimas y amenazando con publicar los datos exfiltrados a menos que se pague el rescate.

"Observado como un modelo de ransomware como servicio (RaaS), los actores de Rhysida han comprometido organizaciones en los sectores de educación, manufactura, tecnología de la información y gobierno, y cualquier rescate pagado se divide entre el grupo y sus afiliados", dijeron la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA), la Oficina Federal de Investigaciones (FBI) y el Centro de Análisis e Intercambio de Información Multiestatal (MS-ISAC).

Además, los informes de fuentes abiertas 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.

2. DETALLES:

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]. También utilizan las campañas de phishing para obtener acceso inicial y persistencia dentro de una red.

También se dice que comparte superposiciones con otro grupo de ransomware conocido como Vice Society (también conocido como Storm-0832 o Vanilla Tempest), debido a patrones de orientación similares y al uso de NTDSUtil y PortStarter, que ha sido empleado exclusivamente por este último.

Las agencias describieron al grupo como parte de ataques oportunistas para violar objetivos y aprovechar técnicas de LotL (living-off-the-land), como la creación de conexiones de Protocolo de escritorio remoto (RDP) para facilitar el movimiento lateral y establecer acceso VPN. Estas técnicas incluyen el uso de herramientas de administración de red nativas (integradas en el sistema operativo) para realizar operaciones. Al hacerlo, la idea es evadir la detección mezclándose con sistemas Windows y actividades de red legítimos.

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. Los actores de Rhysida implementaron estas herramientas y scripts para ayudar al cifrado del sistema y de toda la red.

El ransomware Rhysida utiliza un ejecutable portátil (PE) de Windows de 64 bits o un formato de archivo de objeto común (COFF) compilado con MinGW a través de GNU Compiler Collection (GCC), que admite varios lenguajes de programación como C, C++ y Go. La aplicación de ransomware criptográfico primero inyecta el PE en los procesos en ejecución en el sistema comprometido.

El giro de Vice Society hacia Rhysida se ha visto reforzado a raíz de una nueva investigación publicada por Sophos a principios de la semana pasada, que decía que observó al mismo actor de amenazas usando Vice Society hasta junio de 2023, cuando pasó a implementar Rhysida.

La empresa de ciberseguridad está rastreando el clúster con el nombre TAC5279.

"En particular, según el sitio de filtración de datos del grupo de ransomware, Vice Society no ha publicado una víctima desde julio de 2023, que es aproximadamente cuando Rhysida comenzó a informar sobre víctimas en su sitio", dijeron los investigadores de Sophos Colin Cowie y Morgan Demboski .

"Las bandas de ransomware tienen personal como una empresa de TI. Y al igual que una empresa de TI, las personas a veces cambian de trabajo y traen consigo sus habilidades y conocimientos únicos. Sin embargo, a diferencia de las empresas de TI legítimas, no hay nada que impida que un ciberdelincuente se apodere de recursos propietarios (como código o herramientas) de una operación de ransomware y usarlo en otra. No hay honor entre los ladrones".

3. RECOMENDACIONES:

- Hacer uso del doble factor de autentificación.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores, para evitar que los atacantes aprovechen las vulnerabilidades y se infiltren en su red.
- Utilizar un software antivirus confiable y mantenerlo activo y actualizado.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7, ya sea internamente o en asociación con un proveedor especializado de servicios de detección y respuesta gestionadas.
- En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados.

Fuente de Información:	• hxxps://thehackernews.com/2023/11/cisa-and-fbi-issue-warning-about.html • hxxps://devel.group/blog/stopransomware-rhysida-ransomware/