CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenaza Cibernética

Fecha: **25/10/2022**

Problemática: **Actores de amenazas de ransomware**

Correlativo: **AA-0059**

Institución / Sector: **Instituciones Públicas y Privadas**

CONTEXTO

La Oficina Federal de Investigaciones (FBI) emitió un comunicado para informar sobre la actividad maliciosa que se encuentra realizando el actor de amenazas "Daixin Ransomware". El grupo "Daixin Rsnwomware" es un grupo de extorsión de datos y ransomware que se ha dirigido al sector de salud con operaciones de extorsión de datos y ransomware desde al menos junio de 2022 y el grado de afectación es crítico debido a las técnicas que utilizan para vulnerar los sistemas. Los atacantes utilizan servidores VPN para obtener acceso y luego servicios de SSH y RDP para propagarse a través de las redes. Este grupo de actor de amenazas se enfoca directamente en la cadena de suministros de servicios de salud.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

SITUACIÓN

De acuerdo a la información obtenida por el Centro Estratégico de Monitoreo – CEM, el actor de amenazas "Daixin Ransomware" se dirige a servidores VPN (Virtual Private Network) poco protegidos, y para ello utilizan técnicas de phishing para lograr su objetivo. Después de acceder a la VPN (Virtual Private Network,) el grupo utiliza los protocolos remotos SSH (Secure Shell) y RDP para moverse lateralmente, luego busca cuentas privilegiadas a través del volcado de credenciales y 'pasar el hash', donde los atacantes usan hash de contraseñas robadas para moverse lateralmente entre los sistemas.

Técnicas utilizadas por el actor de amenazas según MITRE ATT&CK

Táctica	Técnica	Identificación
Reconocimiento	Suplantación de identidad	T1598.002
Acceso inicial	Aprovechar la aplicación orientada al público	T1190
	Cuentas válidas	T1078
Persistencia	Manipulación de cuenta	T1098
Acceso a Credenciales	Volcado de credenciales del sistema operativo	T1003
Movimiento lateral	Secuestro de sesión de servicio remoto: secuestro de SSH	T1563.001
	Secuestro de sesión de servicio remoto: secuestro de RDP	T1563.002
	Usar material de autenticación alternativo: pasar el hash	T1550.002
exfiltración	Exfiltración a través del servicio web	T1567
Impacto	Datos cifrados para impacto	T1486

RECOMENDACIONES

- Priorizar la aplicación de parches a los servidores VPN, el software de acceso remoto, el software de máquinas virtuales y las vulnerabilidades conocidas.
- Restrinja el protocolo de bloque de mensajes del servidor (SMB) dentro de la red para acceder solo a los servidores que sean necesarios y elimine o deshabilite las versiones obsoletas de SMB (es decir, la versión 1 de SMB). Los actores de amenazas usan SMB para propagar malware entre organizaciones.
- Revise la postura de seguridad de los proveedores externos y aquellos interconectados con su organización. Asegúrese de que todas las conexiones entre los proveedores de terceros y el software o el hardware externos se supervisen y revisen en busca de actividades sospechosas.
- Implemente políticas de listado para aplicaciones y acceso remoto que solo permitan que los sistemas ejecuten programas conocidos y permitidos.
- Abra lectores de documentos en modos de visualización protegidos para ayudar a evitar que se ejecute el contenido activo.
- Implemente un programa de capacitación para usuarios y ejercicios de phishing para crear conciencia entre los usuarios sobre los riesgos de visitar sitios web sospechosos, hacer clic en enlaces sospechosos y abrir archivos adjuntos sospechosos. Refuerce la respuesta adecuada del usuario a los correos electrónicos de phishing y spearphishing.
- Utilice contraseñas seguras y evite reutilizar contraseñas para varias cuentas. Consulte el Consejo de CISA sobre cómo elegir y proteger contraseñas y la Publicación especial 800-63B del Instituto Nacional de Estándares y Tecnología (NIST) : Directrices de identidad digital para obtener más información.
- Requerir credenciales de administrador para instalar el software.
- Audite las cuentas de usuario con privilegios administrativos o elevados y configure los controles de acceso teniendo en cuenta los privilegios mínimos.
- Instale y actualice periódicamente el software antivirus y antimalware en todos los hosts.
- Utilice únicamente redes seguras y evite el uso de redes Wi-Fi públicas. Considere instalar y usar una VPN.
- Considere agregar un banner de correo electrónico a los mensajes que provienen de fuera de sus organizaciones.
- Deshabilite los hipervínculos en los correos electrónicos recibidos.

ÁREA PARA DEFINICIONES

REFERENCIAS

1. https://www.cisa.gov/uscert/ncas/alerts/aa22-294a
2. https://attack.mitre.org/versions/v11/techniques/T1598/002/
3. https://attack.mitre.org/versions/v11/techniques/T1190/
4. https://attack.mitre.org/versions/v11/techniques/T1078/
5. https://attack.mitre.org/versions/v11/techniques/T1098/
6. https://attack.mitre.org/versions/v11/techniques/T1003/
7. https://attack.mitre.org/versions/v11/techniques/T1563/001/
8. https://attack.mitre.org/versions/v11/techniques/T1563/002/
9. https://attack.mitre.org/versions/v11/techniques/T1550/002/
10. https://attack.mitre.org/versions/v11/techniques/T1567/
11. https://attack.mitre.org/versions/v11/techniques/T1486/

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Virtual Private Network VPN: Red de ordenadores que permite una extensión segura de la red de área local LAN) sobre una red pública o no controlada como Internet.
- Secure Shell – SSH: Protocolo de acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.
- Remote Desktop – RDP: Protocolo de acceso remoto
- Cifrado: Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido.

ÁREA PARA DEFINICIONES