CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Código Dañino

Fecha: 30/08/2022

Problemática: Crecimiento exponencial del Ransomware “VICE SOCIETY - Neshta”.

Correlativo: AA-0016

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Con base al reporte de amenazas emitido por el Centro Criptológico Nacional - CCN de España, institución especializada en ciberseguridad, se alerta a las Instituciones Públicas y Privadas en un contexto global sobre el crecimiento exponencial de amenazas de tipo Malware identificado como código dañino “VICE SOCIETY - Neshta”, mismo que es una variante del ransomware. VICE SPIDER

SITUACIÓN

La investigación realizada por el Centro Estratégico de Monitoreo-CEM, devela la actualización sobre la amenaza de tipo malware que posee la siguiente particularidad:

Neshta es un código dañino del tipo “file infector” con capacidad de autorreplicarse en otros ejecutables del sistema. El código que se inyecta se ejecuta cada vez que se abre un archivo “exe” y se copia en otros ficheros del mismo tipo. En otros casos, también pueden añadir algún código dañino que puede ser utilizado para otros fines como el robo de datos o credenciales propiciando así la afectación directa sobre la integridad de la información, así como la confidencialidad derivado a que el mismo tiene la capacidad de exfiltrar data.

Por su parte VICE SOCIETY, también conocido como VICE SPIDER, es un actor malicioso que utiliza diferentes familias de ransomware como Zeppelin, Spider, Death Kitty para versión de Linux y Hive como RaaS (Ransomware as a service) para cifrar los archivos de sus víctimas. El vector de entrada que suele utilizar son las credenciales legítimas comprometidas de servicios de VPN o RDP para así acceder a la red de las víctimas.

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	Alta	Alta	Alta

RECOMENDACIONES

Considere implementar:

1. Servicios de Antivirus/Antimalware.
2. Herramientas de Prevención de Intrusiones en la red (IDS)
3. Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
4. Herramientas de Detección y Respuesta Extendidas (XDR)

Es importante:

1. Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
2. Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos y programas ofimáticos.
3. Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.

DICCIONARIO DE DATOS

1. Endpoint Detection and Response-EDR (Detección y Respuesta de Amenazas de Puntos Finales): Tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas
2. Extended Detection and Response - XDR (Detección y Respuesta Extendidas): Tecnología de ciberseguridad que monitorea y mitiga las amenazas de ciberseguridad
3. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
4. Malware: Es un programa malicioso que tiene como característica principal su alto grado de dispersabilidad, es decir, lo rápidamente que se propaga.
5. IDS (Intrusion Detection System): Un sistema de detección de intrusos es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.
6. Virtual Private Network Red privada virtual (VPN): Tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.
7. Remote Desktop Protocol (RDP) (Protocolo de Escritorio Remoto): Protocolo desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor Windows.

REFERENCIAS

1. Publicación código dañino Neshta https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/12012-publicado-el-nuevo-informe-de-codigo-danino-id-09-22-sobre-el-ransomware-neshta.html
2. Informe Técnico del código dañino ID-09/22 sobre el ransomware Neshta https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6690-ccn-cert-id-09-22-vice-society-neshta-1/file.html

ÁREA PARA DEFINICIONES

La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.

La presente herramienta tiene aplicación práctica derivado a un proceso previo de análisis con base al contexto y la situación del evento, sin embargo, se aclara que el presente sirve como guía y marco de referencia.