CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas Cibernéticas

Fecha: 24/08/2022

Problemática: Crecimiento exponencial de Malware en Guatemala

Correlativo: AA-0014

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

De acuerdo al reporte de amenazas emitido por ESET compañía de software especializada en ciberseguridad, se alerta a las Instituciones Públicas y Privadas que durante la semana del 15 al 19 de agosto de 2022, se visualizó un crecimiento exponencial de amenazas cibernéticas de Malware en la región, prevaleciendo la amenaza "SMB.Attack.Bruteforce" con un porcentaje del 9.18%.

SITUACIÓN

La investigación realizada por el Centro Estratégico de Monitoreo-CEM, estas amenazas de tipo malware generalmente la infección se lleva a cabo debido a que un ciberdelincuente puede aprovecharse de las vulnerabilidades o fallas de software encontradas. Posteriormente a su explotación los ciberdelincuentes pueden escalar privilegios y tomar el control del dispositivo, acceder a la información e incluso cifrar la misma.

A continuación, se muestra el listado de las diez (10) principales amenazas que pueden poner en riesgo la Integridad, Disponibilidad y Confidencialidad de un sistema de información.

1.	SMB.Attack.Bruteforce	9.28 %
2.	JS/Adware.TerraClicks	7.68 %
3.	JS/Adware.Adport	6.56 %
4.	RDP.Attack.Bruteforce	6.22 %
5.	JS/Packed.Agent.K	5.52 %
6.	JS/Adware.Sculinst	5.27 %
7.	JS/Packed.Agent.L	4.34 %
8.	HTML/ScrInject	4.1 %
9.	EK-Mozi	3.35 %
10.	HTTP/Exploit.CVE-2021-41773	3.09 %

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:

5. Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
6. Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos y programas ofimáticos.
7. 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. Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal
4. Dispositivo: Mecanismo que realiza una función específica
5. 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.
6. Escalar Privilegios: Acto de explotar un error, un fallo de diseño o una supervisión de la configuración en un sistema operativo o una aplicación de software para obtener un acceso elevado a los recursos que normalmente están protegidos de una aplicación o un usuario.
7. Malware: Es un programa malicioso que tiene como característica principal su alto grado de dispersabilidad, es decir, lo rápidamente que se propaga.
8. Sistema de información: Conjunto de componentes que interactúan entre sí con un fin común

REFERENCIAS

1. https://www.virusradar.com/en/statistics/10
2. https://www.welivesecurity.com/la-es/

ÁREA PARA DEFINICIONES