CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas Cibernéticas

Fecha: 13/05/2023

Problemática: Crecimiento exponencial de Malware en Guatemala

Correlativo: AC-0036

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 de un crecimiento exponencial de amenazas cibernéticas de Malware en la región, prevaleciendo la amenaza "SMB.Attack.Bruteforce" con un porcentaje del 9.28%.

SITUACIÓN

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	7.87 %
3.	JS/Adware.Adport	6.14 %
4.	RDP.Attack.Bruteforce	5.3 %
5.	JS/Packed.Agent.L	5.19 %
6.	JS/Adware.Sculinst	4.29 %
7.	HTTP/Exploit.CVE-2021-41773	3.92 %
8.	JS/Packed.Agent.K	3.77 %
9.	HTML/ScrInject	3.68 %
10.	EK-Mozi	2.96 %

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.

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.

REFERENCIAS

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