CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas Cibernéticas

Fecha: 04/01/2023

Problemática: Crecimiento exponencial de amenazas cibernéticas de tipo Ransomware en Guatemala

Correlativo: AC-0005

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Se alerta a las instituciones Públicas y Privadas, que durante la semana del 3 al 7 de octubre se visualizó un crecimiento en la frecuencia de ciberataques, prevaleciendo la variante "SMB.Attack.Bruteforce" con un porcentaje del 9.47% sobre las demás. Por lo general este tipo de ataques están dirigidos a sistemas Windows Server, con el objetivo primordial de obtener credenciales de acceso no autorizado.

SITUACIÓN

Los ataques de fuerza bruta ("SMB.Attack.Bruteforce") son un medio para determinar una combinación de nombre de usuario y contraseña o token hash para obtener acceso no autorizado a una cuenta, archivo u otra información protegida.

Un ataque de fuerza bruta es un método de ataque basado en prueba y error que funciona adivinando credenciales, rutas de archivos o direcciones URL, ya sea a través de la lógica o ejecutando todas las combinaciones de teclado posibles. Por lo tanto, la explotación de esta vulnerabilidad tendría gran impacto en los sistemas.

A continuación, se muestra el listado de las 10 amenazas cibernéticas más relevantes en la región guatemalteca.

1.	SMB.Attack.Bruteforce	9.47 %
2.	JS/Adware.TerraClicks	7.28 %
3.	JS/Packed.Agent.L	6.64 %
4.	JS/Adware.Sculinst	5.06 %
5.	JS/Packed.Agent.K	4.82 %
6.	JS/Adware.Adport	4.61 %
7.	RDP.Attack.Bruteforce	4.34 %
8.	HTTP/Exploit.CVE-2021-41773	4.08 %
9.	JS/Adware.Popcash	4.04 %
10.	1HTML/ScrInject	3.5 %

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

A continuación, se brindan las siguientes recomendaciones para mitigar la amenaza;

- Políticas de uso de la cuenta: Establezca políticas de bloqueo de cuentas después de una cierta cantidad de intentos fallidos de inicio de sesión para evitar que se adivinen las contraseñas. Una política demasiado estricta puede crear una condición de denegación de servicio y hacer que los entornos queden inutilizables, con todas las cuentas utilizadas en la fuerza bruta bloqueadas.
- Autenticación multifactor: Utilice la autenticación multifactor. Siempre que sea posible, habilite también la autenticación multifactor en los servicios externos.
- Políticas de contraseña: Consulte las pautas de NIST al crear políticas de contraseñas (https://pages.nist.gov/800-63-3/sp800-63b.html) .
- Gestión de cuentas de usuario: Restablezca proactivamente las cuentas que se sabe que forman parte de las credenciales violadas, ya sea inmediatamente o después de detectar intentos de fuerza bruta.

DICCIONARIO DE DATOS

Ataque de fuerza bruta: Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.
Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
Amenaza cibernética: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad.

REFERENCIAS

1. https://www.virusradar.com/en/statistics/10
2. https://attack.mitre.org/techniques/T1110/
3. https://attack.mitre.org/mitigations/M1036/
4. https://attack.mitre.org/mitigations/M1032/
5. https://attack.mitre.org/mitigations/M1027/
6. https://attack.mitre.org/mitigations/M1018/