CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Aumento de ciberataques

Fecha: 08/08/2022

Problemática: Aumento en la frecuencia de ciberataques de tipo Ransomware en la región guatemalteca

Correlativo: AA-0010

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Se alerta a las instituciones de gobierno en general sobre el aumento en la frecuencia de ciberataques de tipo Ransomware que continúa expandiéndose durante la última semana por una amplia variedad de los mismos sobre el territorio nacional. Las distintas fuentes de información abiertas consultadas, evidencian que los cibercriminales no dan tregua y se encuentran realizando ciberataques dirigidos a los diferentes sectores e industrias del país.

SITUACIÓN

De acuerdo a la investigación perpetrada, generalmente la infección de Ransomware se lleva a cabo por medio de correos electrónicos de Phishing, adjuntando archivos como imágenes, pdf o enlaces donde sus víctimas hacen clic, descargan y ejecutan el archivo adjunto donde posteriormente los ciberdelincuentes pueden tomar el control del dispositivo, acceder a la información e incluso cifrar la misma. El principal objetivo de este ciberataque por lo general ha sido la extorsión para exigir el pago del rescate.

De acuerdo a las estadísticas reportadas por los distintos fabricantes de soluciones de ciberseguridad, a continuación, se muestra el listado de las versiones de Ransomware empleadas en ciberataques en la región guatemalteca.

1.	Trojan-ransom.win32.Crypmod.gen	30%
2.	Trojan-Ransom.Win32.Crypren.afmu	13.33%
3.	Trojan-Ransom.Win32.Stop.gen	13.33%
4.	Trojan-Ransom.Win32.Crypmodng.gen	10%
5.	Trojan-Ransom.Win32.Phobos.vho	6.67%
6.	Trojan-Ransom.Win32.Blocker.gen	6.67%
7.	Trojan-Ransom.MSIL.Blocker.gen	3.33%
8.	Trojan-Ransom.Win32.Blocker.pef	3.33%
9.	Trojan-Ransom.Win32.Gen.kmi	3.33%
10.	Trojan-Ransom.Win32.Zerber.vho	3.33%

Nivel de priorización

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

Matriz de Evaluación

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

RECOMENDACIONES

1. Considere 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.
2. Implementar servicios de Antivirus/Antimalware.
3. Implementar herramientas de Prevención de intrusiones en la red (IDS)
4. Restringir contenido basado en la web
5. Utilice mecanismos de autenticación de correo electrónico y contra la suplantación de identidad
6. Capacitar a sus usuarios para identificar técnicas de ingeniería social y correos electrónicos de phishing.

DICCIONARIO DE DATOS

1. Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal
2. Phishing: Estafa o fraude informático mediante correo electrónico, mensaje de texto u otro medio tecnológico donde se suplanta la identidad.
3. Ransomware: Es un tipo de malware que impide y/o secuestra el acceso a archivos del sistema infectado, en ocasiones cifrándolos, y coacciona al usuario para pagar un rescate a cambio de su liberación.
4. Enlace: Secuencia de caracteres que funciona como dirección, con lo cual se emplea para pasar de un contenido a otro.
5. Dispositivo: Mecanismo que realiza una función específica
6. 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.

REFERENCIAS

1. https://cybermap.kaspersky.com/es
2. https://www.fireeye.com/cyber-map/threat-map.html
3. https://threatmap.fortiguard.com/
4. https://attack.mitre.org/techniques/T1486/
5. https://attack.mitre.org/techniques/T1566/

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.