	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 087	Fecha: 13-04-2023
		Página 23 de 33

Componente que reporta	**CENTRO DE OPERACIONES CIBERESPACIALES**		
Nombre de la alerta	Nuevo malware Balada Injector infecta más de un millón de sitios web WordPress		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código malicioso		

Descripción

1. El día 10 de abril del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que, más de un millón de sitios Web de WordPress han sido infectados a través de una campaña en curso encargada de implementar un malware llamado Balada Injector.

El malware Balada Injector permite la generación de usuarios administradores falsos de WordPress, recopila datos almacenados en los hosts subyacentes y deja puertas traseras para un acceso persistente. Además, realiza búsquedas amplias en directorios de alto nivel asociados con el sistema de archivos del sitio web comprometido para ubicar directorios grabables que pertenecen a otros sitios.

Del mismo modo, el malware aprovecha todas las vulnerabilidades de complementos y temas conocidas y descubiertas recientemente para violar los sitios de WordPress. Asimismo, dicha campaña se identifica fácilmente por su preferencia por la ofuscación de String.fromCharCode , el uso de nombres de dominio recién registrados que alojan scripts maliciosos en subdominios aleatorios y por los redireccionamientos a varios sitios fraudulentos.

2. Recomendaciones:

- Se recomienda a los encargados del área de informática realizar la instalación del software WordPress, de la página oficial; asimismo se debe mantener actualizado y licenciado.
- Se recomienda a los encargados del área de informática no utilizar crakeadores o archivos que licencien de manera ilegal este software, porque puede crear puertas traseras y vulnerabilidades en el sistema.
- Se recomienda realizar una supervisión de los software y aplicaciones que se tienen en los equipos informáticos.

Fuentes de información	▪ hxxps://thehackernews.com/2023/04/over-1-million-wordpress-sites-infected.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 087**	**Fecha: 13-04-2023** **Página 26 de 33**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de ransomware “Trigona” dirigido a servidores SQL		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de subfamilia	C09
Clasificación temática familia	Código malicioso		

Descripción

1. **Resumen:**

   Investigadores de la empresa Symantec, han detectado una campaña de malware de tipo **ransomware** llamado “**Trigona**” y dirigido a servidores MS SQL. Esta nueva variante de ransomware descubierta en el 2022 exhibe cierta cantidad de similitudes con la variante de ransomware “CryLock”. Un ataque exitoso podría permitir a un actor de amenazas cifrar los archivos de su víctima a cambio de un pago por el descifrado.

2. **Detalles:**

   - Los investigadores indicaron que el ransomware Trigona se ha utilizado recientemente en ataques dirigidos a servidores SQL vulnerables o mal configurados.
   - Los atacantes implementaron el malware CLR Shell durante las primeras etapas del ataque y se utilizó, entre otras cosas, para explotar vulnerabilidades que permiten la **elevación de privilegios** y recopilar información del sistema. El ransomware Trigona agregará la extensión "._locked" a los archivos cifrados y dejará una nota de rescate en forma de un archivo .hta llamado "how_to_decrypt.hta" en cada carpeta donde se hayan cifrado los archivos.

3. **Indicadores de Compromiso (IoC):**
   Symantec ha identificado esta amenaza **crítica**, por lo siguiente:

   Basado en el comportamiento:

   - SONAR.Cryptlck!g171;
   - SONAR.TCP!gen6.

   Basado en archivos:

   - Ransom.Cryptolocker;
   - rescate.trigona;
   - Rescate.Trigona!g1;
   - Caballo de Troya;
   - Trojan.Gen.2;
   - Trojan.Gen.MBT;
   - WS.Malware.1.

   Basado en aprendizaje automático:

   - Heur.AdvML.B / Heur.AdvML.C.

4. Solución:

Symantec recomienda aplicar las siguientes medidas para ser víctima de este tipo de ataques:

- Evitar hacer clic en URL o vínculos que encuentres en correos no deseados o en sitios web que no conozcas;
- Evitar revelar datos personales o confidenciales a suplantadores de identidad (ataques de ingeniería social);
- No abrir archivos adjuntos imprevistos o no confiables y no usar memorias USB u otros dispositivos de almacenamiento que no conozcas o de dudosa procedencia;
- No descargar aplicaciones o archivos multimedia de sitios no confiables;
- Capacitar al personal sobre temas relativas a las nuevas amenazas y vulnerabilidades existentes en el ciberespacio;
- Contar con una solución de seguridad y con características especial anti-ransomware;
- Hacer copias de seguridad de datos críticos fuera de línea;
- Mantener las computadoras, dispositivos y aplicaciones parcheados y actualizados permanentemente;
- Realizar un bloqueo preventivo de los Indicadores de Compromiso.

Fuentes de información	▪ hxxps://www.broadcom.com/support/security-center/protection-bulletin