| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 152 | Fecha: 28-06-2023 |
|---|---|---|
| | | Página 7 de 30 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ** | | |
| Nombre de la alerta | Mallox ransomware ataca industrias de TI con un nuevo patrón de ataque | | |
| Tipo de Ataque | Ransonware | Abreviatura | Ransonware |
| Medios de propagación | USB, Disco, Red, Correo, Navegación de Internet | | |
| Código de familia | C | Código de Sub familia | C01 |
| Clasificación temática familia | Código Malicioso | | |

Descripción

**1. ANTECEDENTES:**

El 26 de junio del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que Una nueva variante del ransomware Mallox, también conocida como ransomware "Empresa de destino", adopta un método único de agregar el nombre de la empresa de destino como una extensión de archivo para cifrar los archivos y lanzar el ataque de ransomware.

**2. DETALLES:**

El actor de amenazas Mallox distribuye ransomware a través de un programa de descarga adjunto a correos electrónicos no deseados al apuntar a servidores Microsoft SQL no seguros con acceso a Internet. El ransomware Mallox cifra los archivos en las máquinas comprometidas y, por lo general, agrega una extensión ". mallox" extensión a los archivos afectados.


Mallox se dirige a industrias como los sectores de fabricación, energía y servicios públicos, TI e ITES y servicios profesionales.

Mallox ransomware inicia el ataque a través de un archivo adjunto malicioso que puede ser un archivo ejecutable que descarga Bat Loader desde un servidor remoto o puede contenerlo directamente.

La nueva variante no necesita un programa de descarga para recuperar la carga útil del ransomware desde un servidor remoto. El cargador de murciélagos se entregará directamente a través del archivo adjunto en un correo electrónico de phishing, en cambio, la carga útil del ransomware está contenida dentro de un script por lotes, que luego se inyecta en "MSBuild.exe", sin guardarlo en el disco.

**3. RECOMENDACIONES:**

Realice prácticas regulares de respaldo y mantenga esos respaldos fuera de línea o en una red separada.

Manténgase actualizado en su computadora, dispositivo móvil y otros dispositivos conectados siempre que sea posible y pragmático.

Use un paquete de software antivirus y de seguridad de Internet de renombre en sus dispositivos conectados, incluidos PC, portátiles y dispositivos móviles.

Absténgase de abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar su autenticidad.

| | |
|---|---|
| Fuentes de información | hxxps://gbhackers-com.translate.goog/mallox-ransomware/?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wapp |