| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°164 | Fecha: 12-07-2023 |
|---|---|---|
| | | Página: 8 de 27 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ** | | |
| Nombre de la alerta | Amenaza de Troyano Bancario TOITOIN en América Latina (LATAM) | | |
| Tipo de Ataque | Troyanos | Abreviatura | Troyanos |
| Medios de propagación | USB, Disco, Red, Correo, Navegación de Internet | | |
| Código de familia | C | Código de Sub familia | C02 |
| Clasificación temática familia | Código Malicioso | | |
| Descripción | | | |

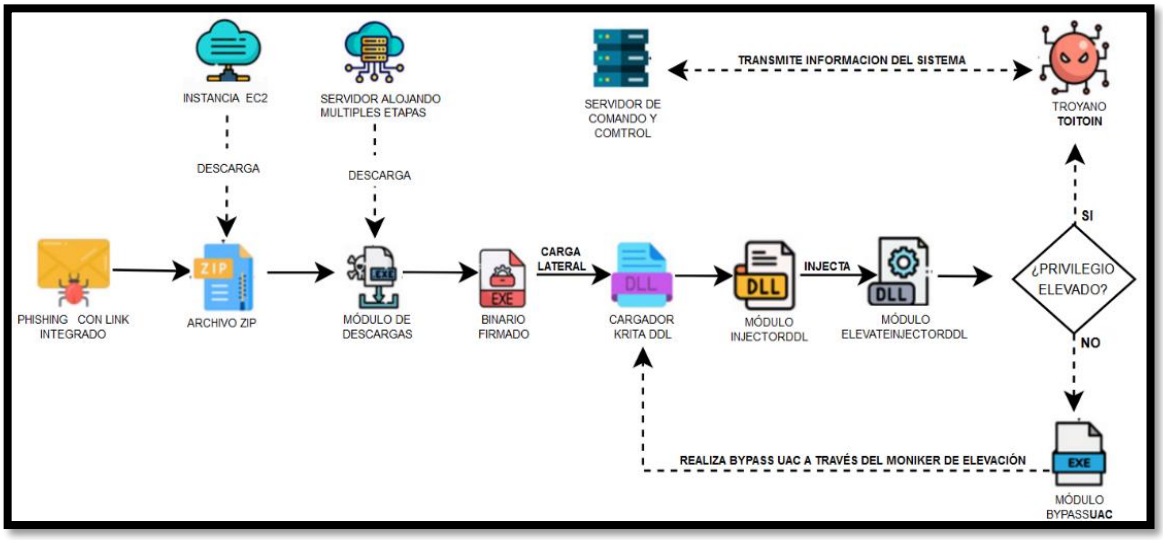
## 1. ANTECEDENTES:

El 10 de julio del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha tomado conocimiento de la presencia de un troyano bancario denominado TOITOIN, que está basado en Windows y tiene como objetivo a empresas de América Latina (LATAM).

## 2. DETALLES:

La campaña sofisticada está empleando un troyano que sigue una cadena de infección de múltiples etapas, haciendo uso de módulos especialmente diseñados en cada etapa. Estos módulos están configurados para llevar a cabo diversas actividades maliciosas, como la inyección de código malicioso en procesos remotos, eludir el control de cuentas de usuario a través de COM Elevation Moniker, y evadir la detección de Sandboxes mediante técnicas inteligentes como reinicios del sistema y verificaciones de procesos principales.

El proceso de ataque consta de seis etapas y presenta características propias de una secuencia de ataque bien diseñada. Comienza con el envío de correos electrónicos de phishing que contienen un enlace incrustado, direccionando a un archivo ZIP alojado en una instancia de Amazon EC2, lo cual permite evadir las detecciones basadas en el dominio.




Los mensajes de correo electrónico aprovechan señuelos relacionados con facturas para engañar a los destinatarios y lograr que abran los archivos adjuntos, activando así la infección. Dentro del archivo ZIP se encuentra un ejecutable de descarga diseñado para configurar la persistencia mediante un archivo LNK en la carpeta de inicio de Windows, y establece comunicación con un servidor remoto para recuperar seis cargas útiles correspondientes a la siguiente etapa, presentadas como archivos MP3.

El descargador también se encarga de generar un script por lotes que reinicia el sistema después de un tiempo de espera de 10 segundos. Esta acción se lleva a cabo con el fin de evadir la detección de entornos de prueba ("sandbox"), ya que las actividades maliciosas solo se producen después del reinicio del sistema. Entre las cargas útiles obtenidas se incluye "icepdfeditor.exe", un binario válido firmado por ZOHO Corporation Private Limited, que, al ejecutarse este archivo, descarga una DLL no autorizada ("ffmpeg.dll") con el nombre en código "Krita Loader".

Por su parte, el cargador está diseñado para decodificar un archivo JPG descargado junto con las demás cargas útiles, y lanzar otro ejecutable conocido como el módulo InjectorDLL, el cual transforma un segundo archivo JPG para formar lo que se conoce como el módulo ElevateInjectorDLL.

Posteriormente, el componente InjectorDLL procede a inyectar ElevateInjectorDLL en el proceso "explorer.exe". A continuación, se realiza una omisión del Control de cuentas de usuario (UAC). si es necesario, con el fin de elevar los privilegios del proceso, y permitir que el troyano TOITOIN se descifre e inyecte en el proceso "svchost.exe".

Esta técnica permite que el malware manipule los archivos del sistema y ejecute comandos con privilegios elevados, lo que facilita la realización de actividades maliciosas adicionales. TOITOIN cuenta con capacidades para recopilar información del sistema, así como datos de navegadores web instalados como Google Chrome, Microsoft Edge, Internet Explorer, Mozilla Firefox y Opera. Además, verifica la presencia de Topaz Online Fraud Detection (OFD), el cual es un módulo antifraude integrado en las plataformas bancarias en la región de LATAM.

Actualmente, se desconoce la naturaleza de las respuestas provenientes del servidor de comando y control (C2), ya que dicho servidor no se encuentra disponible.

A través de correos electrónicos de phishing engañosos, mecanismos de redireccionamiento intrincados y diversificación de dominios, los actores de amenazas están logrando entregar con éxito su carga maliciosa. La cadena de infección de múltiples etapas observada en esta campaña implica el uso de módulos desarrollados a medida, los cuales emplean diversas técnicas de evasión y métodos de encriptación.

## 3. RECOMENDACIONES:

- Utilizar soluciones de seguridad actualizadas, como antivirus y firewalls, que sean capaces de detectar y bloquear amenazas conocidas y desconocidas.
- Considerar la implementación de soluciones de detección y respuesta de endpoints (EDR) para una mayor visibilidad y capacidad de respuesta ante posibles incidentes de seguridad.
- Mantener al día los sistemas operativos, aplicaciones y programas, asegurándose de instalar los últimos parches de seguridad disponibles. Esto abarca sistemas operativos como Windows, navegadores web y software de seguridad.
- Reforzar la educación en materia de seguridad informática, brindando a los miembros de su organización información sobre las últimas técnicas de ataque, especialmente en lo que respecta a correos electrónicos de phishing y señuelos.

| | |
|---|---|
| Fuente de Información: | hxxps://thehackernews.com/2023/07/new-toitoin-banking-trojan-targeting.html |