	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°033	Fecha: 07-02-2024
		Página: 6 de 16

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Conoce los Peligros Ocultos de las Actualizaciones Fraudulentas en Chrome		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

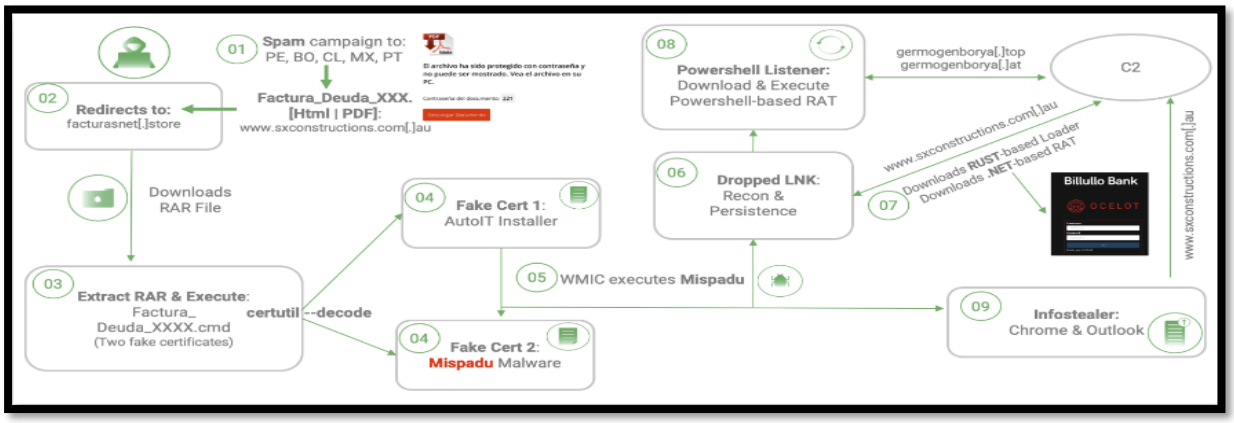
Descripción

1. **ANTECEDENTES**:

   El 06 de febrero del 2024, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha detectado una seria amenaza cibernética conocido como troyano Bancario que ha evolucionado, utiliza archivos de acceso directo a Internet maliciosos contenidos en archivos Zip falsos, para Recopilar y extraer información confidencial.

2. **DETALLES:**

   Los ciberdelincuentes utilizaron diversas tácticas, como la creación de páginas web falsas y el envío de archivos PDF protegidos con contraseña, para atraer a las víctimas y llevar a cabo la infección inicial. A pesar de que las herramientas de seguridad de los clientes lograron bloquear la carga útil inicial, los atacantes intentaron evadir la detección utilizando certificados falsos.



   Los investigadores pudieron acceder a 8 de los 20 servidores de comando y control utilizados por los atacantes, la mayoría de los cuales eran sitios web comprometidos. En estos servidores, se encontraron un total de 90.518 credenciales robadas de 17.595 sitios web únicos en diferentes sectores de la industria.

   Mispadu, es un malware que selecciona víctimas según su ubicación geográfica y configuraciones del sistema que se comunica con un servidor de comando y control (C2) para la exfiltración de datos robando credenciales bancarias y otra información financiera sensible, demostrando sofisticación y adaptabilidad, sta táctica demuestra la sofisticación de Mispadu al adaptarse a las circunstancias específicas de cada víctima y aumentar su capacidad para eludir las defensas de seguridad.

3. **RECOMENDACIONES:**

   - Capacitar al personal para que no pueda abrir archivos de Microsoft Office que contengan MACROS hasta obtener confirmación del remitente y verificar que el envío sea bajo estrictas políticas de seguridad.
   - Evitar extensiones como “exe”, “vbs” y “scr”, es necesario vigilar este tipo de archivos, ya que podrían ser peligrosos.
   - Desconfíar de los correos alarmantes, si un mensaje le indica o incentiva a tomar decisiones apresuradas o en un tiempo limitado, probablemente se trata de phishing.

Fuente de Información:	• hxxps://portal.cci-entel.cl/Threat_Intelligence/Boletines/1844/