Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

TROYANO BANCARIO MISPADU AUMENTA EN LATINO AMERICA.

22/Marzo/2023

CONTENIDO

INTRODUCCIÓN....3
TROYANO BANCARIO MISPADU AUMENTA EN LATINO AMERICA. 4
RESUMEN 4
ESTRATEGIAS DE INFECCIÓN. 4
PROCESO DE INFECCIÓN. 5
RECOMENDACIONES....6
INDICADORES DE COMPROMISO 7
CONTACTOS DE SOPORTE 7

INTRODUCCIÓN

Mispadu es un troyano bancario vinculado a múltiples campañas de correo tipo spam, en el último tiempo se han detectado al menos 20 campañas que han sido dirigidas contra los siguientes países: Chile, Perú, Bolivia, México, Portugal. Su objetivo principal es el robo de credenciales, además de descargar otros tipos de amenazas.

TROYANO BANCARIO MISPADU AUMENTA EN LATINO AMERICA.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_03_22_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	22/03/2023
Es día cero (0 day):	No

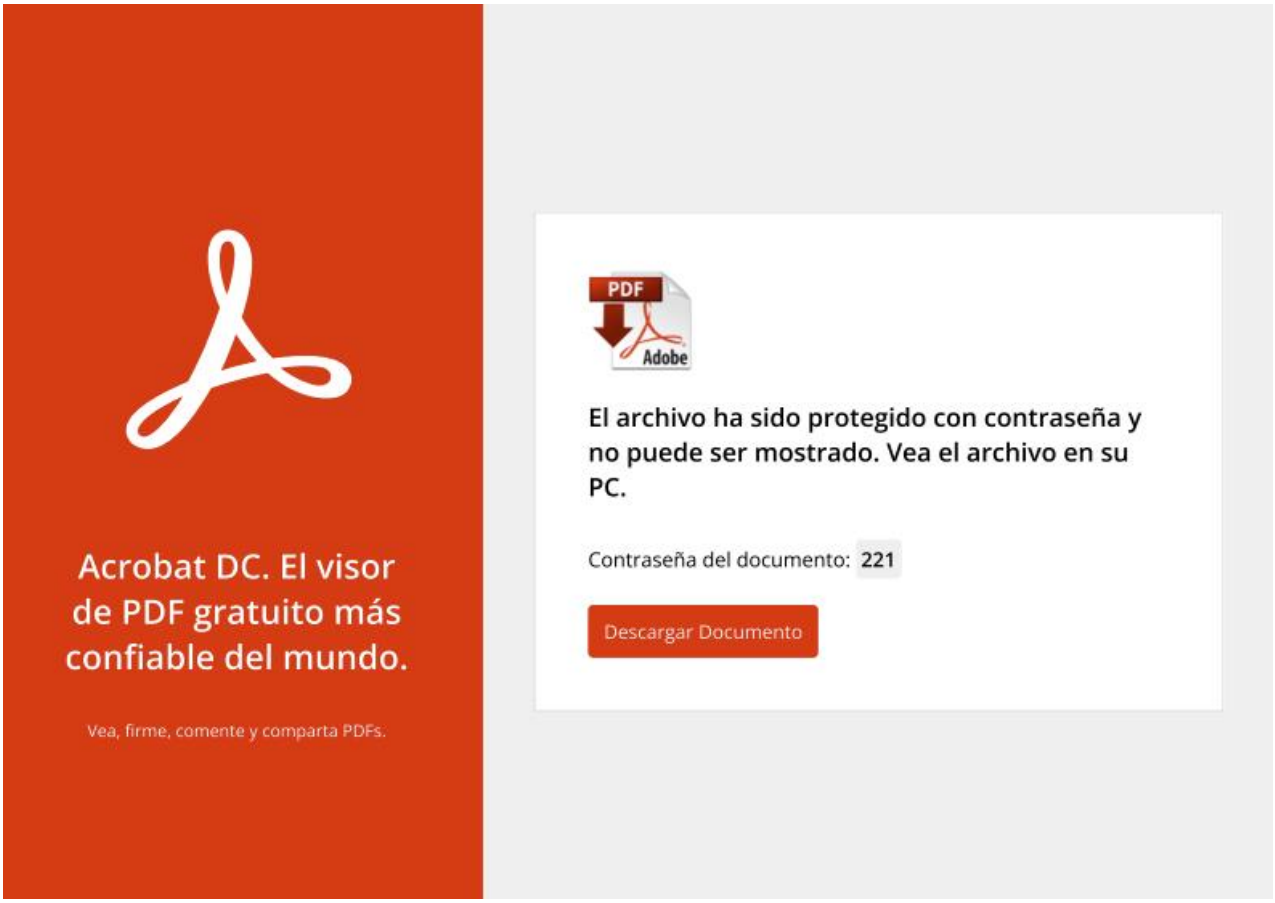
RESUMEN

Este troyano no es nuevo, ya que fue documentado por primera vez en noviembre del 2019, entre sus objetivos principales están los robos credenciales y monetarios, siendo capaz también de dejar un backdoor para tomar capturas de pantalla y detectar pulsaciones del teclado.

ESTRATEGIAS DE INFECCIÓN.

Una de sus principales formas de ataque consiste en comprometer sitios web legítimos que poseen versiones de WordPress vulnerables, el explotar estas vulnerabilidades los convierten en servidores de comando y control (C&C), para desde ahí propagar malware y dirigir sus ataques a países específicos.

Para comprometer a las víctimas e iniciar la primera fase de infección los cibercatores están enviando correos electrónicos maliciosos, aplicando técnicas de ingeniería social, instan a las víctimas a abrir archivos adjuntos que poseen facturas vencidas falsas en formato HTML o archivos PDF con clave, como se puede apreciar en la siguiente imagen:

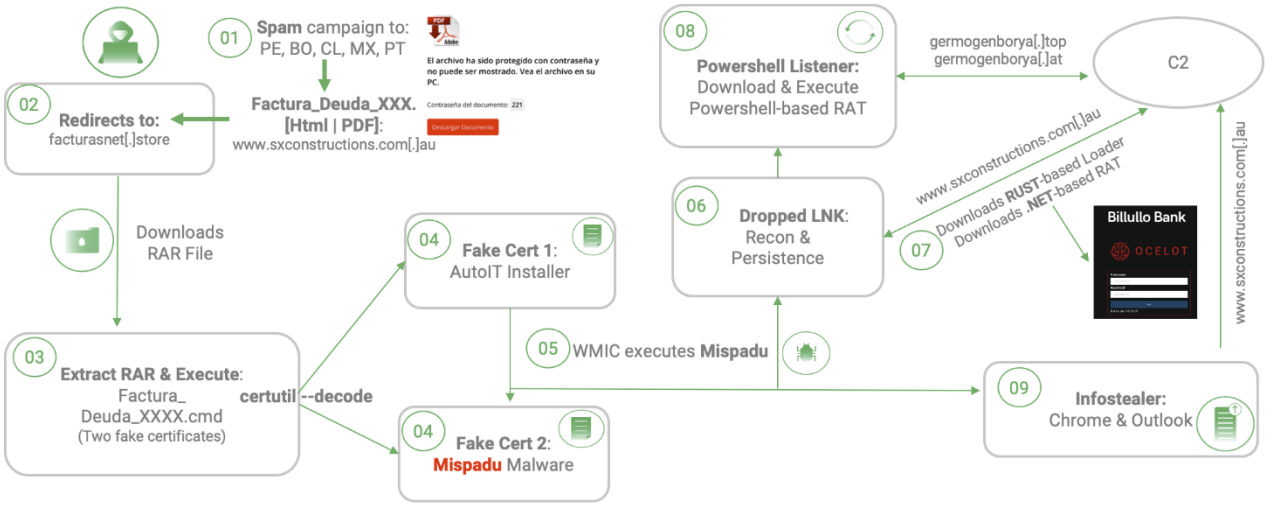


PROCESO DE INFECCIÓN.

Si un usuario desprevenido abre el archivo adjunto HTML o PDF recibido en su bandeja de correo electrónico no deseado, este documento malicioso efectuará una comprobación verificando que fue abierto en un dispositivo de escritorio para posteriormente establecer una comunicación con su servidor remoto y descargar un archivo comprimido en RAR o ZIP, iniciando con ello el proceso de infección.

Adicionalmente al descomprimir y ejecutar este archivo se cargan dos certificados de validación falsos que contienen las cargas útiles maliciosas, una es el troyano Mispadu y el otro un instalador de AutoIT que tiene como función principal decodificar y ejecutar el troyano haciendo uso de la línea de comandos certutil legítima de Windows.

A continuación, se muestra el proceso completo de infección:



RECOMENDACIONES

- Generar una regla personalizada para bloqueos de IOC's en perfiles entrantes perimetrales.
- Las campañas de phishing se caracterizan por tener faltas de ortografía o errores en el diseño. Revisa el contenido con detención, y desconfía de correos con imperfecciones.
- Desconfía 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.
- Disponer de sistemas antispam para correos electrónicos, de esta manera se reducen las posibilidades de infección a través de campañas masivas de malspam por correo electrónico.
- Proteger el protocolo RDP:
  - Deshabilita los servicios RDP, si no es necesario. La desactivación de servicios no utilizados e innecesarios ayuda a reducir su exposición a las vulnerabilidades de seguridad, y es una buena práctica de seguridad.
  - Si no es posible cerrarlos, límita las direcciones de origen que pueden acceder a los puertos.
  - Proteger el acceso a los sistemas RDP, bloqueando el sistema local en lugar del sistema remoto. Incluso si el primero no tiene valor, la sesión RDP solo estará protegida limitando el acceso al sistema cliente.
  - Desconectar sesiones RDP en lugar de bloquearlas, esto invalida la sesión actual, lo que impide una reconexión automática de la sesión RDP sin credenciales.
  - Bloquear bidireccionalmente el puerto TCP 3389 utilizando un firewall o hacerlo accesible sólo a través de una VPN privada.
  - Habilitar la autenticación de nivel de red (NLA).
- Tener políticas de respaldo periódico que se almacenen fuera de la red organizacional.
- Escanear todos los archivos adjuntos, antes de abrirlos, con un antivirus que detecte comportamientos para combatir los ransomwares.
- Mantener una buena estrategia de respaldo de información: sistemas de copias de seguridad que deben estar aisladas de la red; y políticas de seguridad. Lo anterior permitirá neutralizar el ataque, restaurar las operaciones y evitar el pago del rescate.

- Actualizar los equipos con Windows a las últimas versiones.
- Nunca seguir la instrucción de deshabilitar las funciones de seguridad, si un correo electrónico o documento lo solicita.
- Establecer políticas de seguridad en el sistema para impedir la ejecución de ficheros desde directorios comúnmente utilizados por Ransomware (App Data, Local App Data, etc.)
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrás identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 "Concienciación con educación y capacitación en seguridad de la información" o NIST PR.AT-1: "Todos los usuarios se encuentran entrenados e informados", a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas, haciendo énfasis en cómo proceder al recibir correos de orígenes desconocidos, objeto prevenir que los usuarios sean víctimas de entes maliciosos.

INDICADORES DE COMPROMISO

INDICADORES DE COMPROMISO.

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente