Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Malware Bancario Grandoreiro ataca entidades financieras en España y Mexico.

26/Agosto/2022

Contenido

Introducción

El malware bancario Grandoreiro ha vuelto a la acción realizando ataques a entidades financieras ubicadas en España y México, por medio del presente boletín compartimos con usted más información sobre el malware y su comportamiento junto con indicadores de compromiso que permitirán prevenir ataques exitosos de esta amenaza.

GRANDOREIRO

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

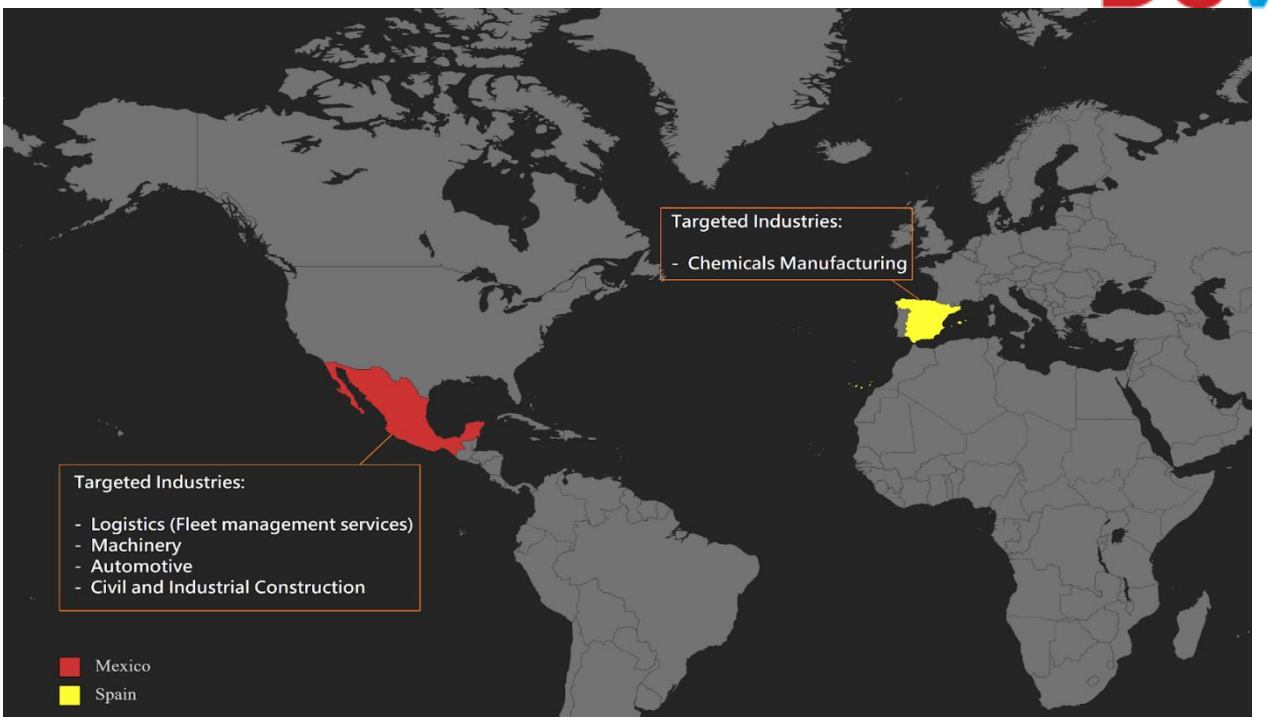
ID de alerta:	DSOC-CERT_2022_08_26_02
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/26/2022
Es día cero (0 day):	No

RESUMEN

El notorio troyano bancario 'Grandoreiro' fue detectado en ataques recientes contra empleados de un fabricante de productos químicos en España y trabajadores de fabricantes de automóviles y maquinaria en México.

El malware ha estado activo desde al menos 2017 y sigue siendo una de las amenazas más importantes de su tipo para los usuarios de habla hispana.

La campaña reciente, detectada por analistas de Zscaler , comenzó en junio de 2022 y aún continúa. Implica el despliegue de una variante de malware Grandoreiro que presenta varias funciones nuevas para evadir la detección y el anti-análisis, así como un sistema C2 renovado.



Mapa de víctimas de la última campaña de Grandoreiro

COMIENZA CON UN CORREO ELECTRÓNICO

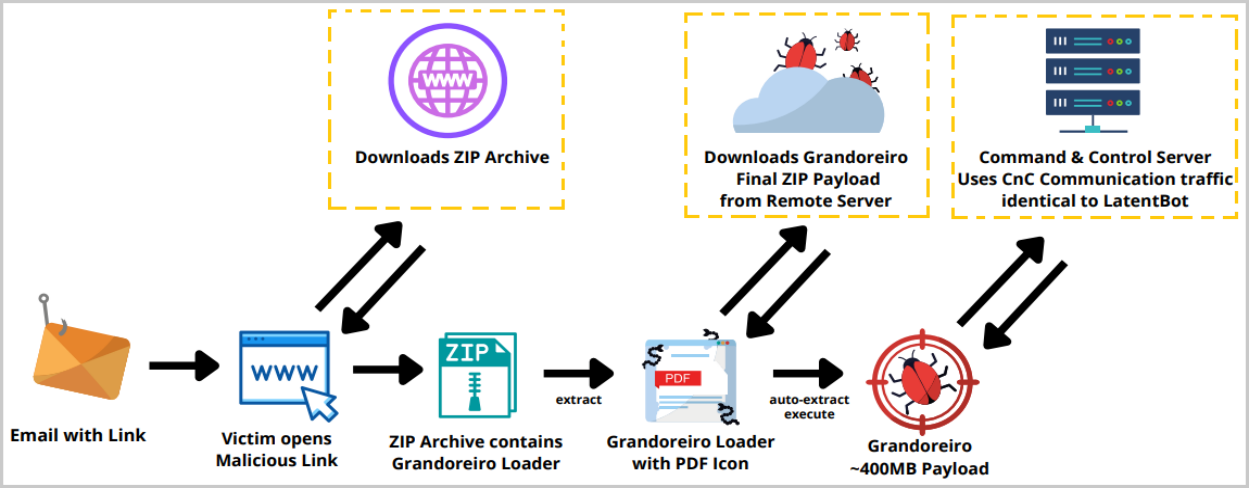
La cadena de infección comienza con un correo electrónico que pretende provenir de la Procuraduría General de Justicia de la Ciudad de México o del Ministerio Público español, según el objetivo.

El tema del mensaje gira en torno a reembolsos estatales, avisos de cambios en litigios, cancelación de préstamos hipotecarios y más.

Uno de los correos electrónicos de phishing utilizados en la última campaña

El correo electrónico contiene un enlace que redirige a las víctimas a un sitio web que descarga un archivo ZIP. Ese archivo incluye el módulo cargador Grandoreiro disfrazado de archivo PDF para engañar a la víctima para que lo inicie.

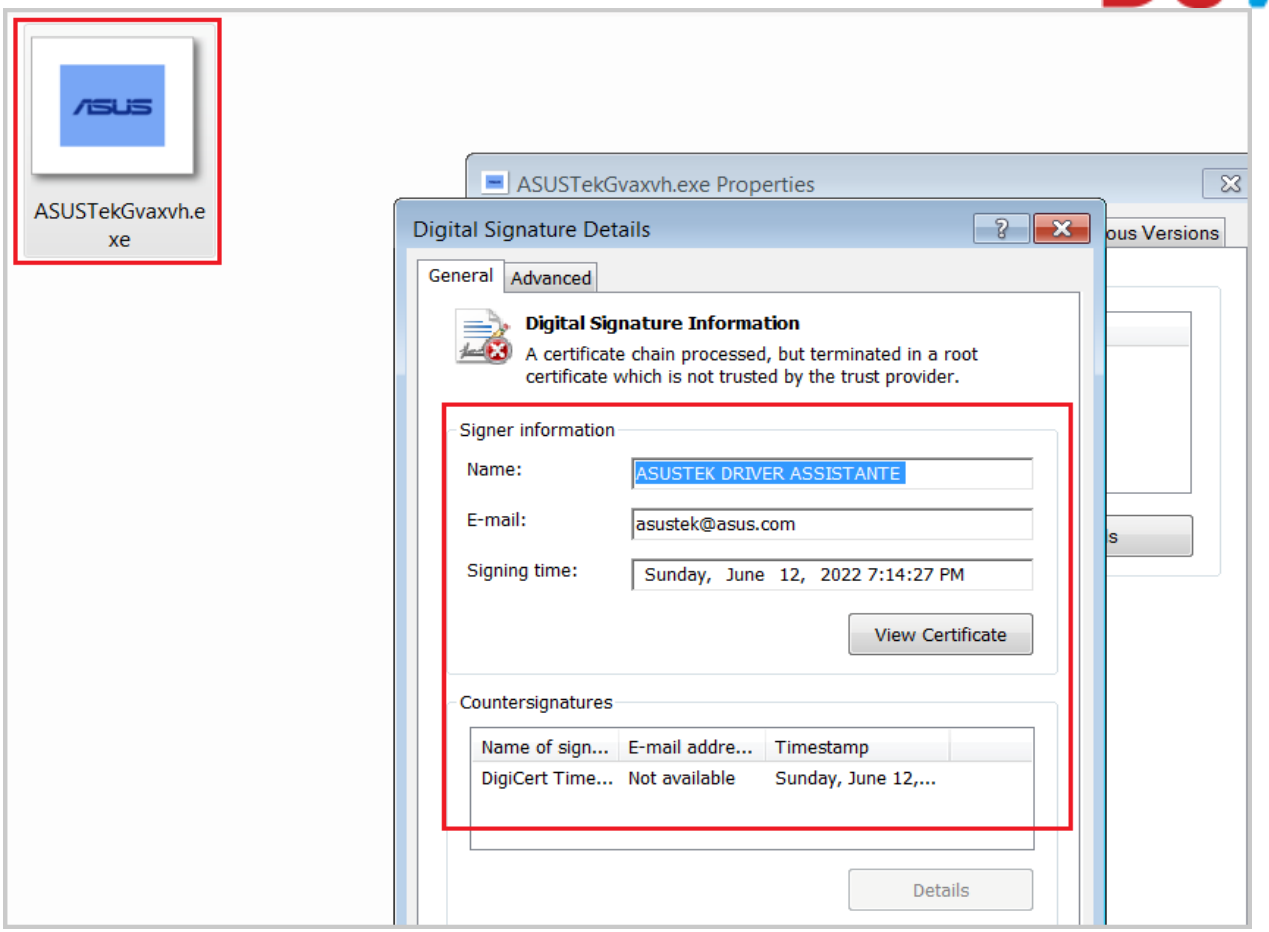
Una vez que esto sucede, se obtiene una carga útil de Delphi desde un servidor de archivos HTTP remoto ("http://15[.]188[.]63[.]127:36992/zxeTYhO.xml") en forma de un archivo comprimido de 9,2 MB. ZIP y es extraído y ejecutado por el cargador.



La última cadena de contagios de Grandoreiro *(Zscaler)*

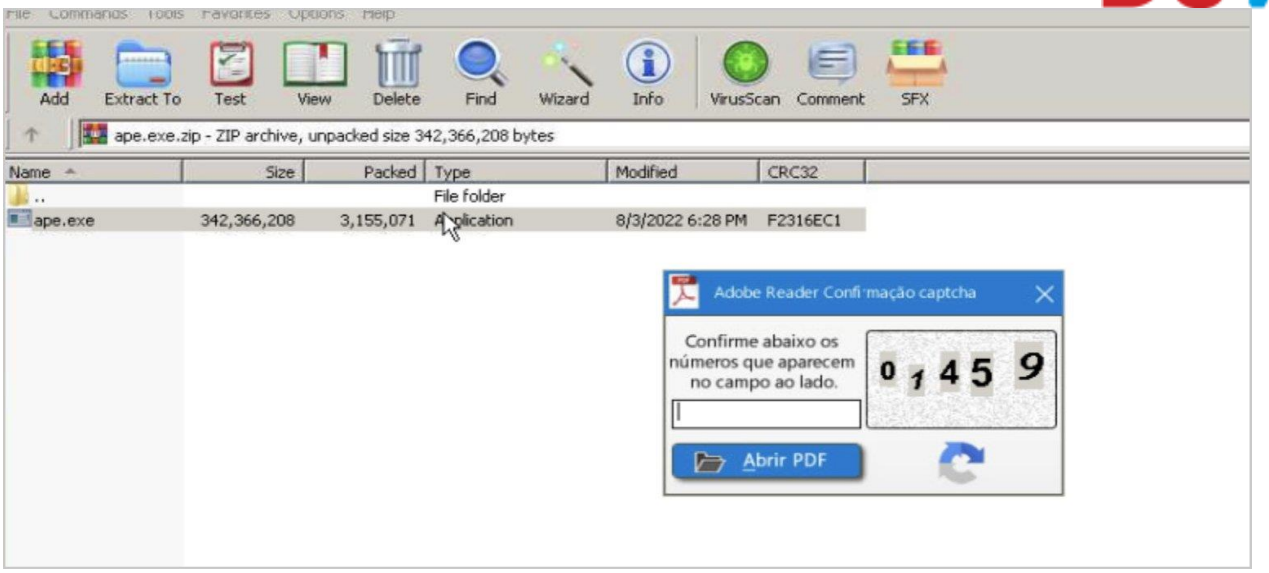
Durante esa etapa, el cargador recopila información del sistema, recupera una lista de programas AV instalados, billeteras de criptomonedas y aplicaciones de banca electrónica, y las envía al C2.

La carga útil final, firmada con un certificado robado de ASUSTEK, asume un tamaño inflado de 400 MB a través del método de "relleno binario" para evadir el análisis de espacio aislado.



El certificado que firma el payload final

En un caso destacado por el analista de seguridad Ankit Anubhav en Twitter , Grandoreiro incluso le pide a la víctima que resuelva un CAPTCHA para ejecutarlo en el sistema, que es otro intento de evadir el análisis.



CAPTCHA servido a la víctima

Finalmente, la persistencia entre reinicios se mantiene agregando dos nuevas claves de registro, configurando Grandoreiro para que se inicie al iniciar el sistema.

Name	Type	Data
(Default)	REG_SZ	(value not set)
ASUSTek_847974537Z2340CVU5BJP5MN	REG_SZ	C:\ProgramData\GmLgMOsN\ASUSTekGvaxvh.exe
ASUSTek_Y9IO2RH4V4TZ8Y44IJ	REG_SZ	cmd.exe /c start C:\ProgramData\GmLgMOsN\ASUSTekGvaxvh.exe

Claves de registro agregadas en sistemas violados

GRANDOREIRO CARACTERISTICAS

Una de las nuevas incorporaciones en la última variante de Grandoreiro muestreada por Zscaler es el uso de DGA (algoritmo de generación de dominio) para las comunicaciones C2, lo que hace que mapear la infraestructura del malware y eliminarlo sea un desafío.

El patrón de comunicación C2 ahora es idéntico al de LatentBot, utilizando balizas "ACCIÓN+HOLA" y respuestas de valores de cookies basadas en ID.

El bloguero portugués de ciberseguridad Pedro Taveres detectó por primera vez los puntos en común entre las dos cepas de malware en 2020 , pero la asimilación de las técnicas de comunicación C2 en el código de Grandoreiro se completó recientemente.

Las capacidades de puerta trasera del malware en el host incluyen:

- Registro de teclas
- Actualización automática para versiones y módulos más nuevos
- Web-Injects y restricción de acceso a sitios web específicos
- Ejecución de comandos
- manipular ventanas
- Guiar el navegador de la víctima a una URL específica
- Generación de Dominio C2 a través de DGA (Algoritmo de Generación de Dominio)
- Imitar los movimientos del ratón y el teclado

PANORAMA

La campaña reciente indica que los operadores de Grandoreiro están interesados en realizar ataques altamente dirigidos en lugar de enviar grandes volúmenes de correos electrónicos no deseados a destinatarios aleatorios.

Además, la evolución continua del malware, que le otorga características más sólidas de antianálisis y evitación de detección, sienta las bases para operaciones más sigilosas.

Si bien el informe de Zscaler no profundiza en los objetivos específicos de la campaña actual, los operadores de Grandoreiro históricamente han demostrado motivos financieros, por lo que se supone que el caso sigue siendo el mismo.

Recomendaciones

- Agregue los IOC disponibles en sus respectivas consolas.
- Procure concientizar de forma continua a sus usuarios sobre los riesgos del phishing.
- Solicite a su SOC monitoreo permanente en sus dispositivos más importantes.

Noticia Completa

https://devel.group/el-malware-bancario-grandoreiro-apunta-a-fabricantes-en-espana-y-mexico/

Visualizar IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220829_01_Grandoreiro

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