ESET descubre Casbaneiro, un nuevo troyano bancario que roba criptomonedas

La compañía de seguridad informática, ESET, identificó una campaña maliciosa que está afectando especialmente a varios países de Latinoamérica y un troyano que hace uso de diversas técnicas para ocultar la dirección de su servidor de C&C.

Buenos Aires, 3 de octubre de 2019 – El laboratorio de Investigación de ESET, compañía líder en detección proactiva de amenazas, anunció el descubrimiento de un nuevo troyano bancario que está afectando especialmente a diversos países de Latinoamérica, principalmente a México y Brasil. El mismo fue denominado Casbaneiro por el laboratorio de ESET, malware comparte funcionalidades con la familia Amavaldo, ya que ambos utilizan el mismo algoritmo criptográfico y se distribuyen con herramientas similares que buscan aprovecharse del correo electrónico.

Figura 1. Países afectados por Casbaneiro con Brasil y México entre los más destacados.

La familia Casbaneiro se aprovecha de la ingeniería social para engañar a las víctimas mediante ventanas y formularios emergentes fraudulentos. El vector inicial de ataque es el correo electrónico, el mismo método que utilizaba Amavaldo. Con estos ataques, los ciberdelincuentes invitan a la víctima a realizar ciertas acciones de forma urgente, como instalar una actualización de software o verificar una tarjeta o datos bancarios.

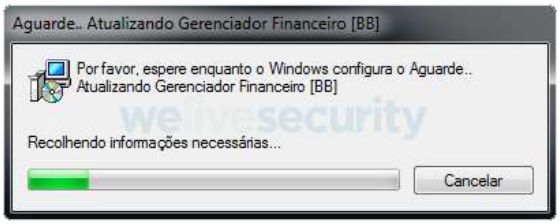

Figura 2. Falso Instalador de actualizaciones

Una vez que se ha instalado en el dispositivo de la víctima, Casbaneiro utiliza comandos de backdoor (troyano que permite el acceso al sistema infectado y su control remoto permitiendo al atacante enviar, eliminar o modificar archivos, ejecutar programas, instalar herramientas maliciosas y extraer información de la víctima para enviársela a sí mismo, con el propósito de espiar y robar datos) para realizar capturas de pantalla, restringir el acceso a webs oficiales de entidades bancarias y registrar las pulsaciones en el teclado. Además, se utiliza para robar criptomonedas analizando los contenidos del portapapeles para chequear si hay datos sobre la cartera de criptomonedas de la víctima. En caso de encontrar estos datos, el malware reemplaza la información por los datos de la cartera del ciberdelincuente.

Casbaneiro recopila la siguiente información de sus víctimas:

- Lista de productos antivirus instalados
- Versión del Sistema Operativo (SO)
- Nombre de usuario
- Nombre de la computadora
- Si alguno de los siguientes software está instalado:
    - Diebold Warsaw GAS Tecnologia (una aplicación para proteger el acceso a la banca en línea)
    - Trusteer
    - Varias aplicaciones bancarias latinoamericanas

La familia de malware Casbaneiro se caracteriza por el uso de múltiples algoritmos criptográficos utilizados para ocultar cadenas de código en archivos ejecutables y para descifrar la carga maliciosa y datos de configuración. Uno de los aspectos distintivos de Casbaneiro es su esfuerzo por esconder el dominio del servidor C&C (Centro de Comando & Control - Servidor administrado por un botmaster que permite controlar y administrar los equipos zombis infectados por un bot) y el puerto utilizado para conectarse.

ESET identificó que Casbaneiro comenzó a abusar de YouTube para almacenar sus dominios de servidor C&C, registrando dos cuentas diferentes utilizadas para este fin por parte de los operadores de la amenaza: una centrada en recetas de cocina y la otra en fútbol. Cada video en estos canales contiene una descripción donde al final hay un enlace a una URL falsa de Facebook o Instagram. El dominio del servidor C&C se almacena en este enlace.

Figura 3. Descripción de uno de los videos que el atacante publicó. En la parte inferior, el dominio cifrado del C&C está embebido en un falso enlace de Facebook (rojo).

"*Casbaneiro es un nuevo troyano bancario latinoamericano que comparte las características comunes de este tipo de malware, como el uso de ventanas emergentes falsas y la funcionalidad de backdoor. Se disfraza como una aplicación legítima en la mayoría de las campañas y se dirige principalmente a Brasil y México. Hay fuertes indicadores que nos llevan a creer que Casbaneiro está estrechamente relacionado con Amavaldo ya que utilizan el mismo algoritmo criptográfico poco común y se los ha visto distribuir una herramienta de correo electrónico muy similar.",* menciona Camilo Gutierrez, Jefe del Laboratorio de Investigación de ESET Latinoamerica. "*Este tipo de ataques se está volviendo cada vez más común apuntando a información sensible lo que permite provacar grandes daños a sus victimas, la concientización sy protección adecuadas son herramientas claves para estar protegidos*".

ESET acerca #quenotepase, con información útil para evitar que situaciones cotidianas afecten la privacidad en línea.

De manera de conocer más sobre seguridad informática ingrese al portal de noticias de ESET: https://www.welivesecurity.com/la-es/2019/10/03/casbaneiro-troyano-bancario-afecta-brasil-mexico/

Visítanos en: @ESETLA /company/eset-latinoamerica

ENJOY SAFER TECHNOLOGY™

Acerca de ESET

Desde 1987, ESET® desarrolla soluciones de seguridad que ayudan a más de 100 millones de usuarios a disfrutar la tecnología de forma segura. Su portfolio de soluciones ofrece a las empresas y consumidores de todo el mundo un equilibrio perfecto entre rendimiento y protección proactiva. La empresa cuenta con una red global de ventas que abarca 180 países y tiene oficinas en Bratislava, San Diego, Singapur, Buenos Aires, México DF y San Pablo. Para obtener más información, visite www.eset-la.com o síganos en LinkedIn, Facebook y Twitter.

Datos de Contacto de Comunicación y Prensa

Para más información se puede poner en contacto a través de prensa@eset-la.com o al +54 11 2150-3700. Además, puede visitar "Somos ESET" nuestro Blog de Comunicación de ESET con las últimas novedades, disponible en: https://www.somoseset.com/