Clase 24

Practica Integradora VIRUS

Grupo 5

8 de Abril 2022

Página de noticia:

https://www.welivesecurity.com/la-es/2019/10/22/navegador-tor-troyanizado-robar-bitcoins-darknet/

¿Qué tipo de amenaza es?

Se trata de un Troyano, versión troyanizada de un paquete oficial de Navegador Tor. Este Navegador Tor troyanizado es una forma atípica de malware que fue diseñado para robar monedas digitales de aquellos que visitan mercados de la darknet. Los delincuentes no modificaron los componentes binarios del Navegador Tor; en su lugar, introdujeron cambios en la configuración y la extensión "HTTPS Everywhere". Esto les ha permitido robar dinero digital, de manera inadvertida, y durante años.

¿Cómo comienza y cómo se propaga esta amenaza?

Los ciberdelincuentes promocionaron las páginas web del Navegador Tor troyanizado utilizando mensajes de spam en varios foros rusos. Dichos mensajes contenían varios tópicos, incluyendo mercados de la darknet, criptomonedas, privacidad en Internet y evasión de censura.

Entre marzo y abril de 2018, los delincuentes comenzaron a utilizar el servicio web pastebin.com para promover los dos dominios relacionados con el falso Navegador Tor. Específicamente, crearon cuatro cuentas y generaron muchos pastes optimizados para que los motores de búsqueda los clasifiquen en buenas posiciones para palabras que tocan temas como drogas, criptomonedas, omisión de censura y nombres de políticos rusos.

La lógica sobre la que se apoya esta estrategia es que una potencial víctima realizará una búsqueda en línea para palabras clave específicas y en algún momento terminará visitando uno de los pastes generados. Cada uno de estos paste tiene un encabezado que promueve el sitio web falso.

Una vez que una víctima visita su página de perfil para agregar fondos a la cuenta directamente mediante el pago con bitcoin, el Navegador Tor troyanizado intercambia automáticamente la dirección original a la dirección controlada por delincuentes.

¿Hay más de una amenaza aplicada?

Tactic	ID	Name	Description
Execution	T1204	User Execution	The trojanized Tor Browser relies on the victim to execute the initial infiltration.
Persistence	T1176	Browser Extensions	The trojanized Tor Browser contains a modified HTTPS Everywhere extension.
Collection	T1185	Man in the Browser	The trojanized Tor Browser is able to change content, modify behavior, and intercept information using man-in-the- browser techniques.
Command and Control	T1188	Multi-hop Proxy	The trojanized Tor Browser uses Tor onion service in order to download its JavaScript payload.
	T1079	Multilayer Encryption	The trojanized Tor Browser uses Tor onion service in order to download its JavaScript payload.
Impact	T1494	Runtime Data Manipulation	The trojanized Tor Browser alters bitcoin and QIWI wallets on darknet market webpages.

¿Qué solución o medida recomendarían?

Como primera medida al momento de ejecutar algún archivo o programa o recibir algún alerta en nuestro navegador, en este caso alertas sobre actualizaciones, debemos ser cuidadosos, verificar la fuente, las extensiones de estos archivos, nombres de dominios.

Por otro lado, al usar plataformas de servicio de transferencias de dinero o billeteras virtuales asegurarnos que las mismas garanticen seguridad en las transacciones y además utilizar medidas de seguridad como por ejemplo llaves de seguridad de hardware.

:)