Tipos de amenazas

Noticia asignada:
Chinese hackers using Firefox extension to spy on Tibetan organizations

- ¿Qué tipo de amenaza es?

Phishing, malware.

- ¿Cómo comienza y cómo se propaga esta amenaza?

La cadena de infección comienza con un correo electrónico de phishing que se hace pasar por la "Asociación de Mujeres Tibetanas" utilizando una cuenta de Gmail vinculada a TA413 que se sabe que se hace pasar por la Oficina de Su Santidad el Dalai Lama en India. Los correos electrónicos contienen una URL maliciosa, supuestamente un enlace a YouTube, cuando en realidad, lleva a los usuarios a una falsa página de aterrizaje de "Actualización de Adobe Flash Player" donde se les pide que instalen una extensión de Firefox llamada "FriarFox".

Por su parte, la extensión maliciosa, llamada "componentes de actualización de Flash", se disfraza como una herramienta relacionada con Adobe Flash, pero los investigadores dijeron que se basa en gran medida en una herramienta de código abierto llamada "Notificador de Gmail (sin reinicio)" con alteraciones significativas que agregue capacidades maliciosas, incluida la incorporación de versiones modificadas de archivos tomados de otras extensiones, como Checker Plus para Gmail.
Una vez instalada la extensión, además de tener acceso a las pestañas del navegador y a los datos del usuario de todos los sitios web, viene equipada con funciones para buscar, leer y eliminar mensajes e incluso reenviar y enviar correos electrónicos desde la cuenta de Gmail comprometida.

- ¿Hay más de una amenaza aplicada ?

Se detectaron ataques en enero y febrero de 2021, un patrón que ha continuado desde marzo de 2020.