Se descubrió una nueva versión del troyano de acceso remoto COMpfun (RAT), que utiliza códigos de estado HTTP para controlar sistemas comprometidos en una campaña reciente contra entidades diplomáticas en Europa.

El malware de ciberespionaje, rastreado hasta Turla APT con *«nivel de confianza medio a bajo»* basado en el historial de víctimas comprometidas, se propagó por medio de un cuentagotas inicial que se enmascara como una solicitud de visa, descubrió el Equipo Global de Investigación y Análisis de Kaspersky.

Turla ATP, un grupo de amenaza con base en Rusia, tiene una gran historia de ataques cibernéticos de espionaje que abarcan distintos sectores, incluyengo gobiernos, embajadas, militares, educación, investigación y compañías farmacéuticas.

Documentado por primera vez por G-Data en 2014, COMpfun recibió una actualización significativa el año pasado bajo el nombre *«Reductor»*, después de que Kaspersky descubriera que el malware se utilizaba para espiar la actividad del navegador de una víctima al organizar ataques de hombre en el medio (MitM) en el tráfico web encriptado por medio de un ajuste en el generador de números aleatorios del navegador (PRNG).

Además de funcionar como un RAT con todas las funciones capaz de capturar pulsaciones de teclado, capturas de pantalla y filtrar datos confidenciales, la nueva variante de monitores COMpfun para cualquier dispositivo USB extraíble conectado a los sistemas infectados para propagarse aún más, recibe comandos de un servidor controlado por el atacante en forma de códigos de estado HTTP.

> *«Observamos un interesante protocolo de comunicación C2 que utiliza códigos de estado HTTP/HTTPS raros (verificar IETF RFC 7231, 6585, 4918). Varios códigos de estado HTTP (422-429) de la clase Error de cliente le permiten al troyano saber qué requieren hacer los operadores. Después de que el servidor de control envía el estado 'Pago requerido' (402), se ejecutan todos estos comandos recibidos*

> *anteriormente»,* dijeron los investigadores.

Los códigos de estado HTTP son respuestas estandarizadas emitidas por un servidor en respuesta a la solicitud de un cliente hecha al servidor. Al emitir comandos remotos en forma de códigos de estado, la idea es ofuscar cualquier detección de actividad maliciosa mientras se escanea el tráfico de Internet.

> *«Los autores mantienen la clave pública RSA y la ETag HTTP única en los datos de configuración cifrados. Creado por razones de almacenamiento en caché de contenido web, este marcador también podría usarse para filtrar solicitudes no deseadas al C2, por ejemplo, las que provienen de escáneres de red en lugar de objetivos».*
>
> *«Para filtrar los datos del objetivo al C2 por medio de HTTP/HTTPS, el malware utiliza el cifrado RSA. Para ocultar los datos localmente, el troyano implementa la compresión LZNT1 y el cifrado XOR de un byte».*

Aunque el modo de funcionamiento exacto detrás de cómo se entrega la solicitud de visa maliciosa a un objetivo sigue sin estar claro, el cuentagotas inicial, después de la descarga, ejecuta la siguiente etapa de malware, que se comunica con el servidor de comando y control (C2) utilizando un estado HTTP basado en el módulo.

> *«Los operadores de malware mantuvieron su enfoque en las entidades diplomáticas y la elección de una aplicación relacionada con la visa, almacenada en un directorio compartido dentro de la red local, ya que el vector de infección inicial funcionó a su favor»*, mencionaron los investigadores de Kaspersky.

> *«La combinación de un enfoque personalizado para sus objetivos y la capacidad de generar y ejecutar sus ideas ciertamente hace que los desarrolladores detrás de COMpfun sean un equipo ofensivo fuerte».*