Según investigaciones, un proveedor de software de videovigilancia con sede en Barcelona, llamado Variston IT, plantó subrepticiamente software espía en dispositivos específicos al explotar varias vulnerabilidades de día cero en Google Chrome, Mozilla Firefox y Windows, algunas de las cuales datan de diciembre de 2018.

> *«Su marco Heliconia explota las vulnerabilidades de n-day en Chrome, Firefox y Microsoft Defender, y proporciona todas las herramientas necesarias para implementar una carga útil en un dispositivo de destino»,* dijeron Clement Lecigne y Benoit Sevens, investigadores del Grupo de Análisis de Amenazas (TAG) de Google.

Variston, que tiene un sitio web básico, afirma *«ofrecer soluciones de seguridad de la información a la medida de nuestros clientes, diseñar parches de seguridad personalizados para cualquier tipo de sistema patentado y respaldar el descubrimiento de información digital por parte de las fuerzas del orden»,* entre otros servicios.

Se cree que las vulnerabilidades, que fueron corregidas por Google, Microsoft y Mozilla en 2021 y principios de 2022, se usaron como días cero para ayudar a los clientes a instalar el malware de su elección en los sistemas objetivo.

Heliconia comprende un trío de componentes, a saber, Noise, Soft y Files, cada uno de los cuales es responsable de implementar exploits contra errores en Chrome, Windows y Firefox, respectivamente.

Noise está diseñado para aprovechar una falla de seguridad en el motor de JavaScript del motor Chrome V8 que se parchó en agosto de 2021, así como un método de escape de sandbox desconocido llamado *«chrome-sbx-gen»* para habilitar la carga útil final (también conocido como *«agente»*) para ser instalado en los dispositivos de destino.

Sin embargo, el ataque se basa en el requisito previo de que la víctima acceda a una página web con una trampa explosiva para activar la explotación de la primera etapa.

El comprador puede configurar adicionalmente Heliconia Noise mediante un archivo JSON para establecer distintos parámetros, como la cantidad máxima de veces para servir los exploits, una fecha de vencimiento para los servidores, URL de redirecionamiento para visitantes no objetivo y reglas que especifican cuándo un visitante debe ser considerado un objetivo válido.

Soft es un marco web que está diseñado para entregar un documento PDF de señuelo que presenta un exploit para CVE-2021-42298, una falla de ejecución remota de código que afecta a Microsoft Defender que fue corregida por Redmond en noviembre de 2021. La cadena de infección, en este caso, implicó al usuario visitando una URL maliciosa, que después sirvió el archivo PDF armado.

El paquete de archivos – el tercer marco – contiene una cadena de explotación de Firefox para Windows y Linux, que aprovecha una vulnerabilidad use-after-free en el navegador, que se informó en marzo de 2022 (CVE-2022-26485). Sin embargo, se sospecha que probablemente se abusó del error desde al menos 2019.

Google TAG dijo que se dio cuenta del marco de ataque de Heliconia después de recibir un envío anónimo a su programa de informes de errores de Chrome. Además, dijo que no hay evidencia actual de explotación, lo que indica que el conjunto de herramientas se ha dejado de lado o ha evolucionado más.

El desarrollo llega más de cinco meses después de que la división de seguridad cibernética de Google vinculara un spyware móvil de Android previamente no atribuido, denominado Hermit, al equipo de software italiano RCS Lab.

> *«El crecimiento de la industria del spyware pone en riesgo a los usuarios y hace que Internet sea menos seguro, y aunque la tecnología de vigilancia puede ser legal según las leyes nacionales o internacionales, por lo general se usa de forma dañina para realizar el espionaje digital contra una variedad de grupos»,* dijeron los investigadores.