El actor de amenazas Keksec se relacionó con una cepa de malware previamente no documentada, que se ha observado en la naturaleza disfrazada como una extensión para los navegadores web basados en Chromium, con el fin de esclavizar las máquinas comprometidas en una red de bots.

Llamado Cloud9 por la compañía de seguridad Zimperium, el complemento de navegador malicioso viene con una amplia gama de características que le permiten desviar cookies, registrar pulsaciones de teclas, inyectar código JavaScript arbitrario, extraer criptografía e incluso, reclutar al host para llevar a cabo ataques DDoS.

La extensión *«no solo roba la información disponible durante la sesión del navegador, sino que también puede instalar malware en el dispositivo de un usuario y, posteriormente, asumir el control de todo el dispositivo»,* dijo el investigador de Zimperium, Nipun Gupta.

La botnet de JavaScript no se distribuye por medio de Chrome Web Store o complementos de Microsoft Edge, sino a través de ejecutables falsos y sitios web maliciosos disfrazados de actualizaciones de Adobe Flash Player.

Una vez intalada, la extensión está diseñada para inyectar un archivo JavaScript llamado «*campaign.js*» en todas las páginas, lo que significa que el malware también podría funcionar como un código independiente en cualquier sitio web, legítimo o no, lo que podría generar ataques de pozo de agua.

El código JavaScript se responsabiliza de las operaciones de cryptojacking, abusando de los recursos informáticos de la víctima para minar criptodivisas de forma ilícita, además de inyectar un segundo script llamado «cthulhu.js».

Esta cadena de ataque, a su vez, explota vulnerabilidades en navegadores web como Mozilla Firefox (CVE-2019-11708, CVE-2019-9810), Internet Explorer (CVE-2014-6332, CVE-2016-0189) y Edge (CVE-2016-7200) para escapar del espacio aislado del navegador web e implementar malware en el sistema.

El script actúa además como un registrador de teclas y un conducto para lanzar comandos adicionales recibidos de un servidor remoto, lo que le permite robar datos del portapapeles, cookies del navegador y montar ataques DDoS de capa 7 contra cualquier dominio.

Zimperium atribuyó el malware a un atacante rastreado como Keksec (también conocido como Kek Security, Necro y FreakOut), que tiene un historial de desarrollo de una amplia gama de malware de botnet, incluyendo EnemyBot, para criptominería y operaciones DDoS.

La conexión con Keksec proviene de superposiciones en los dominios que se identificaron previamente como utilizados por el grupo de malware.

El hecho de que Cloud9 esté basado en JavaScript y se ofrezca de forma gratuita o por una pequeña tarifa en los foros de hackers, hace posible que los atacantes menos calificados obtengan fácil acceso a opciones de bajo costo para lanzar ataques dirigidos a distintos navegadores y sistemas operativos.

La divulgación se produce más de tres meses después de que Zimperium descubriera un complemento de navegador malicioso denominado ABCsoup que se hacía pasar por una herramienta de Google Translate para atacar a los usuarios rusos de los navegadores Google Chrome, Opera y Mozilla Firefox.

> *«Los usuarios deben recibir capacitación sobre los riesgos asociados con las extensiones del navegador fuera de los repositorios oficiales, y las compañías deben considerar qué controles de seguridad tienen implementados para dichos riesgos»*, dijo Gupta.