Los investigadores de seguridad cibernética están llamando la atención sobre un marco de automatización de navegador de uso gratuito que los atacantes está utilizando cada vez más como parte de sus campañas de ataque.

> *«El marco contiene numerosas características que evaluamos, pueden utilizarse para permitir actividades maliciosas»*, dijeron los investigadores de Team Cymru.

> *«La barra de entrada táctica para el marco se mantiene baja a propósito, lo que ha servido para crear una comunidad activa de desarrolladores y contribuyentes de contenido, con actores en la economía clandestina que anuncian su tiempo para la creación de herramientas a medida».*

La compañía de seguridad cibernética de Estados Unidos, dijo que observó direcciones IP de comando y control (C2) asociadas con el malware como Bumblebee, BlackGuard y RedLine Stealer, estableciendo conexiones con el subdominio de descargas de Bablosoft (*«downloads.bablosoft[.]com»*), el fabricante de Browser Automation Studio (BAS).

Bablosoft fue documentado previamente por la compañía de entrega de aplicaciones y seguridad en la nube F5 en febrero de 2021, lo que apunta a la capacidad del marco para automatizar tareas en el navegador Chrome de Google, de forma similar a las herramientas de desarrollo legítimas como Puppeteer y Selenium.

La telemetría de amenazas para la dirección IP del subdominio, 46.101.13[.]144, muestra que la gran mayoría de la actividad se origina en ubicaciones en Rusia y Ucrania, con inteligencia de fuente abierta que indica que el propietario de Bablosoft supuestamente tiene su sede en la ciudad capital de Ucrania, Kyiv.

Se sospecha que los operadores de las campañas de malware se conectaron al subdominio de Bablosoft con el fin de descargar herramientas adicionales para usarlas como parte de las actividades posteriores a la explotación.

También se identificaron varios hosts asociados con malware de cryptojacking como XMRig y Tofsee, que se comunican con un segundo subdominio llamado *«fingerprints.bablosoft[.]com»* para usar un servicio que ayuda al malware de minería a ocultar su comportamiento.

> *«según la cantidad de actores que ya utilizan las herramientas que se ofrecen en el sitio web de Bablosoft, solo podemos esperar que BAS se convierta en un elemento más común del conjunto de herramientas del actor de amenazas»,* dijeron los investigadores.