Autoridades de Estados Unidos, Alemania, Países Bajos, Suiza, Francia, junto con el Centro Europeo de Ciberdelincuencia (EC3) de Europol, anunciaron la eliminación coordinada de Safe-Inet, un popular servicio de ser privada virtual (VPN) que se utilizó para actividades delictivas.

Los tres dominios en cuestión, insorg[.]org, safe-inet[.]com y safe-inet[.]net, fueron cerrados y su infraestructura incautada como parte de una investigación conjunta llamada «Operation Nova«. Europol calificó a Safe-Inet como el «*favorito*» de los ciberdelincuentes.

Una razón crucial para la incautación de los dominios fue su papel central para facilitar el ransomware, llevar a cabo ataques de skimming web, spear-phishing y toma de control de cuentas.

El servicio, que viene con soporte para los idiomas ruso e inglés y ha estado activo durante más de diez años, ofrecía *«servicios de alojamiento a prueba de balas»* a los visitantes del sitio web, a menudo por un precio elevado para el mundo criminal.

A partir del 1 de diciembre, el costo de una suscripción Pro oscilaba entre 1.3 dólares al día y 190 dólares al año para el acceso completo a toda su lista de servidores.

El alojamiento a prueba de balas (BPH), también conocido como servicios resistentes al abuso, se diferencia del alojamiento web regular en que permite al proveedor de contenido ser más indulgente con el tipo de datos que se pueden alojar en los servidores, lo que facilita eludir la aplicación de la ley.

Según un análisis de la compañía de ciberseguridad Trend Micro en octubre, un host a prueba de balas emplea varias formas de sostener los delitos que operan bajo su protección y puede asignar recursos estratégicamente a nivel mundial, teniendo en cuenta las legalidades regionales y las características geográficas. Se sabe que minimizan la cantidad de archivos de registro útiles y acceden al sistema solo desde fuentes anónimas como las redes Tor.

> *«Las actividades de un hoster a prueba de balas pueden incluir ignorar o inventar excusas en respuesta a las quejas de abuso presentadas por las víctimas de sus clientes, trasladar sus cuentas de cliente y/o datos de una dirección IP, servidor o país a otro para ayudarlos a evadir la detección, y no mantener registros»*, dijo el Departamento de Justicia (DoJ) en un comunicado.

De este modo, los servicios de BPH apoyan intencionalmente las actividades delictivas de sus clientes y se convierte en co-conspiradores en los esquemas criminales, agregó el DoJ.

Europol también dijo que identificó alrededor de 250 empresas en todo el mundo que estaban siendo espiadas por los delincuentes para lanzar posibles ataques de ransomware utilizando la infraestructura Safe-Inet.

> *«Los delincuentes pueden huir pero no pueden esconderse de las fuerzas del orden, y seguiremos trabajando incansablemente junto con nuestros socios para ser más astutos»*, dijo el director de EC3, Edvardas Sileris.