En un esfuerzo conjunto de distintas agencias de aplicación de la ley en 6 países diferentes, los funcionarios lograron desmantelar una importante red mundial de ciberdelincuencia organizada detrás del malware bancario GozNym.

GozNym es responsable de robar cerca de $100 millones de dólares a más de 41 mil víctimas en todo el mundo, principalmente en Estados Unidos y Europa, durante varios años.

El malware se creó combinando dos poderosos troyanos conocidos: Gozi ISFB, un troyano bancario que apareció por primera vez en 2012 y Nymaim, un descargador de troyanos que también funciona como ransomware.

En una conferencia de prensa celebrada este jueves, Europol informó que la operación se llevó a cabo con éxito gracias a la cooperación entre Bulgaria, Alemania, Georgia, Moldavia, Ucrania y Estados Unidos.

Estados Unidos acusó a diez miembros de la red criminal de GozNym, 5 de los cuales fueron arrestados durante varios registros coordinados que se realizaron en Bulgaria, Georgia, Moldavia y Ucrania.

Sin embargo, los cinco acusados restantes residen en Rusia y están huyendo, incluido uno que desarrolló el malware GozNym y lo arrendó a otros ciberdelincuentes al publicarlo en foros clandestinos, en idioma ruso.

Hackers buscados por el FBI por su implicación con el malware GozNym

Según la acusación presentada hoy en el Tribunal de Estados Unidos, los detenidos fueron acusados por conspiración para cometer fraude informático, conspiración para cometer fraude bancario y conspiración para cometer lavado de dinero.

Un miembro del grupo que cifró el malware GozNym para evitar la detección mediante herramientas antivirus, también fue arrestado y está siendo procesado en la República de Moldova.

Los miembros del grupo infectaron las computadoras de las víctimas con el malware de GozNym y capturaron sus credenciales de inicio de sesión en la banca en línea, mediante las que lograron robar dinero de forma fraudulenta y luego lavar los fondos utilizando las cuentas bancarias de Estados Unidos y extranjeras controladas por los demandados.

> *«Los acusados publicitaron sus servicios y habilidades técnicas especializadas en foros clandestinos en línea que hablan ruso. La red de GozNym se formó cuando estas personas fueron reclutadas en los foros por el líder de GozNym que controlaba más de 41 mil computadoras víctimas infectadas con malware de GozNym».*
>
> *«El líder de la red criminal de GozNym, junto con su asistente técnico, están siendo procesados en Georgia por la Fiscalía de Georgia y el Ministerio del Interior de Georigia»,* dijo la Europol.

Las víctimas de esta red criminal eran principalmente empresas estadounidenses y sus instituciones financieras, incluidas varias víctimas ubicadas en el Distrito Oeste de Pennsylvania.

La red de malware GozNym fue alojada y operada a través del servicio a prueba de balas *«Avalanche»*, cuyo administrador fue arrestado en Ucrania durante una búsqueda en noviembre de 2016.