National Gendarmerie, la agencia de aplicación de la ley francesa, anunció hoy que eliminó exitosamente uno de los mayores malware de botnet, RETADUP, y explicó la forma en que desinfectó remotamente más de 850 mil computadoras en todo el mundo con ayuda de investigadores.

A inicios de este año, los investigadores de seguridad de la firma Avast, que estaban monitoreando activamente las actividades de la botnet RETADUP, descubrieron una falla de diseño en el protocolo C&C del malware que podría haber sido explotada para eliminar el malware de la computadora de las víctimas sin ejecutar ningún código adicional.

Sin embargo, para esto el plan requería que los investigadores tuvieran control sobre el servidor C&C del malware, que estaba alojado con un proveedor ubicado en la región de Ile-de-Framnce, en el centro norte de Francia.

Debido a esto, los investigadores se comunicaron con el Centro de Lucha contra el Cibercrimen (C3N) de la Gendarmería Nacional Francesa a fines de marzo pasado, compartieron sus hallazgos y propusieron un plan secreto para poner fin al virus RETADUP y proteger a las víctimas.

Según el plan propuesto, las autoridades francesas tomaron el control del servidor RETADUP C&C en julio y lo reemplazaron con un servidor de desinfección preparado que abusó de la falla de diseño en su protocolo y ordenó que las instancias conectadas del malware RETADUP en las computadoras infectadas se autodestruyeran.

> *«En el primer segundo de su actividad, varios miles de bots se conectaron a él para obtener comandos del servidor. El servidor de desinfección respondió a ellos y los desinfectó, abusando de la falla de diseño del protocolo C&C. Al momento de publicar este artículo, la colaboración ha neutralizado más de 850 mil infecciones únicas de RETADUP»,* dijeron los investigadores.

Según Jean-Dominique Nollet, jefe del Servicio Nacional de Inteligencia Criminal de la

Gendarmería Nacional, las autoridades mantendrán el servidor de desinfección en línea por unos meses más ya que algunas computadoras infectadas aún no se han conectado con el servidor de C&C controlado por la policía, algunas han estado desconectadas desde julio, mientras que otras tienen problemas de red.

La policía francesa también contactó al FBI luego de encontrar algunas partes de la infraestructura de C&C de RETADUP en los Estados Unidos. El FBI los eliminó el 8 de julio, dejando a los autores del malware sin control sobre los bots.

> *«Ya que era responsabilidad del servidor de C&C dar trabajos de minería a los bots, ninguno de los bots recibió nuevos trabajos de minería para ejecutar después de este derribo. Esto significaba que ya no podrían agotar el poder informático de sus víctimas y que los autores de malware ya no recibían ninguna ganancia monetaria de la minería»,* dicen los investigadores.

Creado en 2015 e infectando principalmente computadoras en América Latina, RETADUP es un malware de Windows multifuncional que es capaz de extraer criptomonedas utilizando la potencia informática de las máquinas infectadas, la infraestructura DDoSing utilizando el ancho de banda de las víctimas y la recopilación de información para el espionaje.

Hay distintas variantes de RETADUP, algunas de ellas se han escrito en Autoit o utilizando AutoHotkey. El malware ha sido diseñado para lograr la persistencia en las computadoras con Windows, instalar cargas de malware adicionales en las máquinas infectadas y también realizar periódicamente otros intentos de propagación.

Además de distribuir malware de criptomonedas como carga útil, RETADUP, en algunos casos, también difunde el ransomware Stop y el ladrón de contraseñas Arkei.

> *«El servidor de C&C también contenía un controlador .NET para un AutoIt RAT llamado HoudRat. Al observar las muestras de HoudRat, está claro que HoudRat es*

> *solo una variante de RETADUP más rica en características y menos prevalente. HoudRat es capaz de ejecutar comandos arbitrarios, registrar pulsaciones de teclas, tomar capturas de pantalla, robar contraseñas, descargar archivos arbitrarios y más»,* afirmaron los investigadores.

Hasta ahora, las autoridades han neutralizado más de 850,000 infecciones únicas de RETADUP, y la mayoría de las víctimas son de habla hispana en América Latina, incluyendo a México.