El Departamento de Justicia de Estados reveló ayer la identidad de dos hackers rusos y los acusó de desarrollar y distribuir el troyano bancario Dridex, con el que ambos piratas informáticos robaron más de 100 millones de dólares en un período de 10 años.

Maksim Yakubets, líder del grupo de piratería Evil Corp, y su colega Igor Turashev, distribuyeron principalmente Dridex, también conocido como Bugat y Cridex, por medio de campañas de correo electrónico multimillonarias, y se dirigieron a numerosas organizaciones en todo el mundo.

El Departamento de Estado también anunció una recompensa de hasta 5 millones de dólares, la mayor recompensa ofrecida hasta ahora para un sospechoso por delitos cibernéticos, a quien proporcione información que pueda conducir al arresto de Yakubets, quien sigue en libertad.

> *«Bugat es un paquete de malware multifunción diseñado para automatizar el robo de información personal y financiera confidencial, como credenciales bancarias en línea, de computadoras infectadas»,* dijo el Departamento de Justicia en un comunicado de prensa.
>
> *«El malware Bugat fue diseñado específicamente para derrotar a los antivirus y otras medidas de protección empleadas por las víctimas. Las versiones posteriores del malware fueron diseñadas con la función adicional de ayudar en la instalación del ransomware».*

Además del desarrollo y distribución de Dridex, Yakubets también fue acusado por conspiración para cometer fraude bancario en relación con el infame malware bancario Zeus, que robó 70 millones de dólares a las cuentas bancarias de las víctimas.

A partir de mayo de 2009, Yakubets y sus cómplices supuestamente emplearon intrusiones informáticas generalizadas, software malicioso y fraude en un esfuerzo por robar millones de

dólares de numerosas cuentas bancarias en Estados Unidos y otros países.

Los piratas informáticos infectaron miles de computadoras comerciales con malware que capturaba contraseñas, números de cuenta y otra información necesaria para iniciar sesión en cuentas bancarias en línea, luego utilizaron los datos robados para robar dinero de las cuentas bancarias de sus víctimas.

> *«Yakubets supuestamente se involucró en una ola de delitos cibernéticos de una década de duración, que desplegó dos de las piezas de malware financiero más dañinas que se hayan usado y causó pérdidas de decenas de millones de dólares a las víctimas en todo el mundo»*, dijo Brian A. Benczkowski, Asistente del Fiscal General de la División Criminal del Departamento de Justicia.

Según el Departamento de Justicia, el FBI descubrió las identidades de ambos ciberdelincuentes rusos con la ayuda de su homólogo extrajero, la Agencia Nacional del Delito (NCA) en el Reino Unido.

La NCA comenzó su investigación sobre el grupo Dridex en 2014 y recopiló material probatorio durante varios años que respalda los cargos presentados por el FBI.

Mientras derribaba la infraestructura que soportaba Dridex en 2015, NCA también ayudó al FBI a arrestar a Andrey Ghinkul, uno de los distribuidores del malware Dridex.

> *«Las investigaciones en el Reino Unido por parte de la NCA y la Policía Metropolitana también se ha dirigido a la red de lavadores de dinero de Yakubets que han canalizado sus ganancias a Evil Corp. Ocho personas fueron condenadas a un total de más de 40 años en prisión»,* dijo la NCA.

La investigación conjunta reveló que Yakubets *«también brinda asistencia directa al gobierno*

ruso», mediante el robo de documentos confidenciales a través de ataques cibernéticos patrocinados por el estado.

Se acusa a ambos hackers de haber atacado a 21 municipios específicos, compañías privadas, bancos y organizaciones sin fines de lucro en California, Illinois, Massachusetts, Ohio, Texas, Washington, Iowa, Kentucky, Maine, Nuevo México y Carolina del Norte, incluias algunas entidades en Nebraska y una congregación religiosa.

Estados Unidos ha implementado también sanciones contra otras 17 personas y 7 empresas rusas por su conexión con el grupo de piratería Evil Corp.

> *«El tesoro está sancionando a Evil Corp como parte de una acción radical contra una de las organizaciones cribercriminales más prolíficas del mundo. Esta acción coordinada tiene la intención de interrumpir las campañas masivas de phishing organizadas por este grupo de piratas informáticos con sede en Rusia»*, dijo Steven T. Mnuchin, Secretario del Tesoro.

En la actualidad se cree que YAkubets reside en Rusia, pero si alguna vez sale del país, sería arrestado y extraditado a Estados Unidos.