# AVISO

***Policía Real de Gibraltar***

## Gibraltar contribuye al desmantelamiento de una red de crimen organizado envuelta en delitos informáticos a gran escala

Gibraltar, 12 de diciembre de 2016

El Departamento de Delitos Económicos de la Policía Real de Gibraltar (Royal Gibraltar Police's Economic Crime Unit) ha recibido una carta de felicitación de la Oficina del Fiscal en Verden y de la Policía de Lüneburg (Baja Sajonia) en Alemania, en agradecimiento por la excelente cooperación prestada durante la larga investigación internacional sobre delitos informáticos, que se ha prolongado a lo largo de cuatro años.

Las autoridades alemanas, en estrecha colaboración con la Oficina del Fiscal de los Estados Unidos para el Distrito Oeste de Pensilvania, el FBI, la Europol, la Eurojust y otros colaboradores, han investigado y desmantelado el 30 de noviembre de 2016 una red criminal internacional utilizada como plataforma de entrega para lanzar y controlar ataques masivos de *malware* a escala mundial y para realizar trasvases de dinero de manera ilegal, que ha ocasionado más de seis millones de euros en daños a sistemas de banca online en Alemania, y de cientos de millones de euros a nivel mundial.

El caso llevó a los investigadores a realizar pesquisas en 30 países distintos, uno de ellos Gibraltar. Se elevó una petición de "Asistencia Jurídica Mutua" a las autoridades gibraltareñas, materializada por detectives del Departamento de Delitos Económicos, con pruebas que se recabaron y enviaron al equipo que lleva el proceso en Alemania. Se arrestó a cinco individuos considerados como delincuentes informáticos de primer nivel, se registraron 37 instalaciones y se confiscaron 39 servidores. Las víctimas de las infecciones por *malware* se identificaron en más de 180 países. El grupo criminal envió más de un millón de correos electrónicos con archivos adjuntos o links dañinos con una frecuencia semanal a las víctimas, que no eran conscientes de ello.

La investigación comenzó en 2012, después de que un tipo de *ransomware*[1] encriptado infectase un considerable número de equipos informáticos, lo que bloqueó el acceso de sus usuarios. También se infectaron con *malware* millones de ordenadores privados y de empresas, lo que permitió a los criminales hacerse con contraseñas de bancos y de cuentas de correo electrónico. Con esta información, pudieron realizar transferencias bancarias desde las cuentas de los afectados a las suyas, por medio de un doble *fast flux*[2]. Además, 221 servidores en total fueron inutilizados por medio de notificaciones de abuso enviadas a los proveedores

[1] *Ransomware*: tipo de malware que afecta a los ordenadores de los usuarios, impidiendo que estos accedan a los datos. Los delincuentes pueden pedir dinero al usuario a cambio de obtener contraseñas que le permitan acceder a los datos previamente incautados.
[2] *Fast flux*: técnica de evasión utilizada por los operadores *botnet* para mover un dominio específico desde un conjunto de ordenadores conectados a internet a otro.

de *hosting*. Esta intervención supone el uso más grande de *sinkholing*[3] de la historia para combatir infraestructuras *botnet*[4]; la Europol la considera una operación sin precedentes, con más de 800.000 dominios incautados, sometidos a la técnica de *sinkholing* o bloqueados.
En su carta de agradecimiento, las autoridades alemanas destacaron la importancia de la operación conjunta. "Si trabajamos juntos, podemos marcar la diferencia en la lucha contra los delitos informáticos. Este éxito no hubiese sido posible sin su compromiso y su trabajo paciente e incansable".

Países colaboradores: Armenia, Australia, Austria, Azerbaiyán, Bélgica, Belice, Bulgaria, Canadá, Colombia, Finlandia, Francia, Alemania, Gibraltar, Hungría, India, Italia, Lituania, Luxemburgo, Moldavia, Montenegro, Países Bajos, Noruega, Polonia, Rumanía, Singapur, Suecia, Taiwán, Ucrania, Reino Unido y los Estados Unidos.

## Nota a redactores:

**Esta es una traducción realizada por la Oficina de Información de Gibraltar. Algunas palabras no se encuentran en el documento original y se han añadido para mejorar el sentido de la traducción. El texto válido es el original en inglés.**

Para cualquier ampliación de esta información, rogamos contacte con
Oficina de Información de Gibraltar

Miguel Vermehren, Madrid, miguel@infogibraltar.com, Tel 609 004 166
Sandra Balvín, Campo de Gibraltar, sandra@infogibraltar.com, Tel 637 617 757
Eva Reyes Borrego, Campo de Gibraltar, eva@infogibraltar.com, Tel 619 778 498

Web: www.infogibraltar.com, web en inglés: www.gibraltar.gov.gi/press-office
Twitter: @InfoGibraltar

[3] *Sinkholing*: acción por medio de la cual el tráfico de datos entre ordenadores infectados y la infraestructura criminal se redirige a los servidores controlados por las autoridades competentes o a la empresa de seguridad informática.
[4] *Botnets*: redes informáticas infectadas con malware bajo control de los delincuentes, que pueden acceder a información confidencial de las mismas.

PRESS NOTICE

12th December 2016

**Gibraltar contributes to the dismantling of an organised criminal network involved in large scale cyber crime**

A letter of thanks has been received by the Royal Gibraltar Police's Economic Crime Unit from the Public Prosecutor's Office in Verden and the Luneburg Police in Germany who have expressed appreciation for the excellent co-operation afforded during a protracted [international]cyber crime investigation spanning over four years.

The German authorities working in close co-operation with US State Attorney's Office for the Western District of Pennsylvania. the FBI, Europol, Eurojust and other partners have investigated and dismantled (on 30/11/16) an international criminal network that was used as a delivery platform to launch and manage mass global malware attacks and money mule campaigns causing in excess of EUR 6 million in damages to on line banking systems in Germany and hundred of millions of Euros worldwide.

The case led investigators to conduct enquiries in 30 different countries, Gibraltar being one of them. A request for 'Mutual Legal Assistance' was made to the Gibraltar authorities and was acted upon by detectives of the Economic Crime Unit with evidence been gathered and forwarded to the prosecuting team in Germany. 5 individuals described as top level cybercriminals have been arrested, 37 premises searched and 39 servers have been seized. Victims of the malware infections were identified in over 180 countries. The criminal group would send more than 1 million emails with damaging attachments or links every week to unsuspecting victims.

The investigation commenced in 2012 after an encryption ransomware infected a substantial number of computer systems, blocking users' access. Millions of private and business computer systems were also infected with malware, enabling the criminals to harvest bank and email passwords. With this information they were able to perform bank transfers from victim's accounts redirecting the proceeds to the criminals via a double *fast flux* . Furthermore, a total of 221 servers were put off-line through abuse notifications sent to hosting providers. This intervention marks the largest ever use of *sinkholing* to combat *botnet* infrastructures and is regarded by Europol as unprecedented in its scale with over 800,000 domains seized, sinkholed or blocked.

In the letter of thanks, the German authorities highlighted the importance of international co-operation saying '….working together, we can really make a

difference in the battle against cybercrime. None of this success would have been possible without your commitment and patient and tireless work.'

**Countries involved:** Armenia, Australia, Austria, Azerbaijan, Belgium, Belize, Bulgaria, Canada, Colombia, Finland, France, Germany, Gibraltar, Hungary, India, Italy, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Norway, Poland, Romania, Singapore, Sweden, Taiwan, Ukraine, United Kingdom and United States of America.

[1*] Sinkholing* is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses. When employed at a 100% scale, infected computers can no longer reach the criminal command and control computer systems and so criminals can no longer control the infected computers. The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and Network Owners.

[2] *Botnets* are networks of computers infected with malware, which are under the control of a cybercriminal. Botnets allow criminals to harvest sensitive information from infected computers, such as online banking credentials and credit card information. A criminal can also use a botnet to perform cyberattacks on other computer systems, such as denial-of-service attacks.

[3] *Ransomware* is a type of malware that infects the victim's PC and encrypts the victim's files, so that the victim is unable to access them. The criminal behind the ransomware then uses intimidation and misinformation to force the victim to pay a sum of money in exchange for the password that unlocks the encrypted files. Even if a password is eventually provided, it does not always work.

[4 *Fast flux* technique is an evasion technique used by botnet operators to quickly move a fully qualified domain name (a domain that points to one specific Internet resource such as www. domain .com) from one or more computers connected to the Internet to a different set of computers. Its aim is to delay or evade the detection of criminal infrastructure. In the double fast flux setup, both the domain location and the name server queried for this location are changed.