Telefónica

INSIDE ELECTIONS_

Amenazas al proceso electoral iraní

09.06.2017

CYBER SECURED BY ElevenPaths

elevenpaths.com

Amenazas al proceso electoral iraní

Visión del analista

Irán ha sido señalado como autor de la creación de diferentes herramientas que les permitirían obtener información sensible o hacerse con el control de sistemas tanto de particulares, entre los que se incluirían defensores de los derechos humanos, como de potencias extranjeras. Entre ellas se encuentran **MacDownloader**, **Infy** y las campañas **RocketKitten I y II**, todas con sesiones activas recientemente coincidiendo con el periodo de campaña electoral. Por otro lado, con el objetivo de prevenir el impacto que tuvieron las noticias falsas en las elecciones presidenciales de Estados Unidos a través de Facebook, Irán ha limitado ciertas funcionalidades de redes sociales como Telegram e Instagram.

Principales claves del país

Nombre oficial	República Islámica de Irán
Capital	Teherán
Idioma oficial	Farsi o persa
Religión	El **islam** es la religión oficial. La mayoría musulmana iraní es **chiíta**.
Forma de Estado	**República Islámica**. El sistema se basa en un **Ejecutivo** encabezado por el Presidente de la República (Hassan Rouhani) y un **Legislativo** que aprueban las leyes. Sin embargo, por encima se encuentra la figura del **Líder Máximo** (Alí Jamenei) capacitado para delinear las líneas maestras de la política.
Principales clientes	China, India, Turquía
Principales proveedores	China, EAU, Corea del Sur y Turquía
Principales exportaciones	Productos de **gas y petróleo** (73%) y productos de goma y plásticos (5,3%), principalmente.

Ruptura con Estados Unidos tras el **asalto a la Embajada de Estados Unidos** en Irán **[1979]**

La entrada de Ahmadineyad y la **cuestión nuclear iraní** provocaron un mayor desgaste de las relaciones con el mundo occidental **[2005-2013]**

Primer mandato de Rouhaní como presidente de la República. Los puntos clave de su política exterior fueron **[2013-2017]**:

Levantamiento de las sanciones económica a cambio de la paralización del *programa nuclear*. Este hecho supuso el deshielo de la relación con la UE

Proceso de paz en *Oriente Medio*: relajación del tono contra Israel

Relación con *países árabes vecinos* marcada por el conflicto sirio

Tensión con *Afganistán* por la inmigración de afganos en sus fronteras

Pertenecen a la OPEP y Foro de países exportadores de GAS

Nueva relación de fuerza con *Rusia*. Tras el levantamiento de las sanciones, Rusia se ha convertido en el primer patrocinador de petróleo iraní

Segundo mandato de Rouhaní como presidente de la República **[19 de mayo 2017]**

Tipos de amenazas identificadas

Amenazas procedentes de agentes externos

Es necesario remontarse a 2010 para identificar posibles ataques que han podido perpetrar potencias extranjeras contra la República Islámica de Irán con capacidad para afectar a la política interior y exterior del país. En ese año se descubrió Stuxnet, un gusano que afectaba a sistemas SCADA y, un año después, se detectó Duqu, muy parecido a Stuxnet, con la diferencia de que su cometido era obtener información sobre sistemas de control industrial. Ambos afectaban a infraestructuras críticas, especialmente, al desarrollo del programa nuclear iraní.

Asimismo, también en 2012, se identificó Flame, *malware* destinado a operaciones de ciberespionaje en Oriente Medio, en el que se encontraba a Irán entre sus objetivos, capaz de propagarse a otros sistemas través de la red local (LAN) y mediante memorias USB.

Amenazas procedentes de agentes internos

El uso de internet por parte de la población iraní es de un 68,3% [1] y al menos el 47% de la población se encuentra en la franja de edad de los 25 a los 34 años [2]. Acorde con estas estadísticas, los candidatos a la presidencia de Irán han utilizado las redes sociales como fuente principal para la difusión de noticias asociadas a sus campañas.

Candidato	Twitter	Facebook	Telegram	Aparat	Instagram
Rouhani	X	X	X	-	X
Jahangiri	X	-	X	-	X
Raisi	-	-	X	X	X
Ghalibaf	-	-	X	X	X
Hashemitaba	-	-	-	-	-
Mirsalim	X	X	X	X	X

Tabla I. Principales redes usadas por los candidatos

Teniendo en cuenta que Twitter, Facebook y Youtube se encuentran baneadas, la aplicación de mensajería Telegram y la plataforma de compartición de fotografías y vídeos Instagram son las redes sociales más utilizadas tanto por los propios candidatos (ver la Tabla I) como por la propia ciudadanía [3]. Sin embargo, las autoridades del país llegaron a poner ciertos límites en esta red social como la notificación al gobierno de grupos públicos con más de 3000 usuarios. En este sentido, según el Centro de Derechos Humanos [4] de Irán, al menos doce administradores de canales de Telegram fueron arrestados a mediados de marzo.

Con el objetivo de prevenir el impacto que tuvieron las noticias falsas en las elecciones presidenciales de Estados Unidos a través de Facebook, también llegaron a bloquear las llamadas de voz en Telegram, así como la funcionalidad de la retransmisión de los videos en directo de Instagram [5]. Sin embargo, a pesar del control llevado a cabo, se registraron dos casos de noticias falsas a través de Telegram. El primero trataba sobre el asesinato de 27 personas en un centro comercial de Teherán, mientras que el segundo estaba relacionado con los supuestos avisos donde se alertaba de las actividades ilegales que estaban llevando a cabo la Policía de Internet de Irán (FATA) a través de esta red social.

No solo las redes sociales fueron objetivo de bloqueo. Algunas páginas web también han sido objetivo de la censura ejerciendo una represión continua contra los informadores, según afirma Reporteros sin Fronteras [6]. De la misma forma, también se ha ejercido cierta represión sobre los movimientos estudiantiles procedentes de las universidades. 92 organizaciones estudiantiles escribieron una carta al presidente Rouhani expresando su preocupación por las amenazas a estudiantes después de la declaración del líder supremo Alí Khamenei sobre la politización de los estudiantes. En este sentido, decenas de estudiantes fueron expulsados por razones políticas entre 2005 y

2016 por lo que no han podido reanudar sus estudios a finales de 2016 [7].

Por otro lado, recientemente, Irán ha sido señalado por diferentes investigadores de seguridad [8] como autor de la creación de diferentes herramientas que les permitirían obtener información sensible o hacerse con el control de sistemas de individuos o de potencias extranjeras. Un ejemplo es MacDownloader, una pieza de *malware* desarrollada para sistemas Mac y que ha sido utilizada para atacar a contratistas de defensa de Estados Unidos y a defensores de los derechos humanos. Camuflado en un falso instalador del *software* Flash Player o como falso antivirus, se trata de una muestra de *malware* con ciertos errores de diseño y que utiliza técnicas de persistencia obsoletas, pero que en muchos casos ha sido eficaz para obtener las credenciales de usuarios.

Otra herramienta perteneciente a su arsenal es Infy, que según investigadores de Palo Alto llevaría diez años en funcionamiento. Este tipo de *malware* se transmite habitualmente por correo electrónico, utilizando adjuntos en documentos de Word o presentaciones de PowerPoint, que contienen ficheros ejecutables comprimidos que son autoextraíbles. En su diseño se incluyeron funcionalidades de *keylogging* para la obtención de datos y herramientas para la exfiltración de los mismos, incluyendo en las últimas variantes otras utilidades de control remoto del sistema infectado. Las últimas muestras datan del 19 de marzo de 2017, apareciendo en multitud de sectores empresariales, principalmente en empresas orientadas a la venta mayorista, alta tecnología, telecomunicaciones y gobiernos. La distribución geográfica de las mismas es limitada, encontrándose entre las víctimas equipos de Irlanda, Estados Unidos, Holanda y Turquía. Los operadores de Infy han utilizado principalmente direcciones IP de los países atacados para situar los C&C como método de evasión.

Por otro lado, también le ha sido atribuida la campaña RocketKitten I y II en donde se utilizaba la navegación web como vía de infección. Los sectores principalmente afectados fueron empresas de alta tecnología, organizaciones gubernamentales y empresas orientadas a la venta mayorista. De la misma manera, los países afectados fueron Irlanda, Estados Unidos, Holanda, Turquía y España.

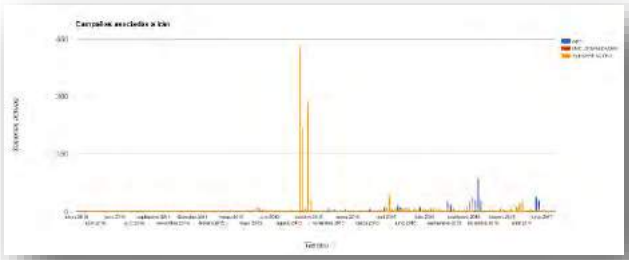

Figura 1. Número de sesiones activas de cada pieza de *malware* o campaña asociada a Irán (Fuente: Elaboración propia).

Adicionalmente existen campañas específicas como Woolen-GoldFish, también asociadas al grupo Rocket Kitten, que utilizaron ataques de *phishing* para penetrar en los sistemas de las víctimas. En este caso, la industria de la defensa, el sector de las tecnologías de la información, entidades gubernamentales y las organizaciones académicas fueron los más afectados. Una de las muestras asociadas es GHOLE, que utiliza macros para la infección. Este *malware* se comunica vía HTTP a un servidor remoto y, una vez instalado, proporciona control completo sobre la máquina víctima. El origen de esta familia de *malware* se asocia a una versión *crackeada* del *software* legítimo Core Impact, utilizado por *pentesters*.

Otras consideraciones

Hassan Rouhani fue candidato a presidente en 2013 centrando su mensaje sobre la promesa de mejorar el acceso a internet y a la información. El pasado mayo volvió a salir reelegido y la política de internet sigue siendo clave. Su éxito en este sentido ha sido mixto ya que el Consejo Supremo del Ciberespacio es el último órgano en la toma de decisiones sobre internet, en el que se incluye al poder judicial y a la Guardia Revolucionaria, pero que rinden cuentas directamente a Alí Jamenei.

[1] Internet World Stats, «Iran Internet Stats and Telecommunications Reports», 30-jun-2016. [En línea]. Disponible en: http://www.internetworldstats.com/me/ir.htm. [Accedido: 31-may-2017].

[2] Central Intelligence Agency, «The World Factbook — Central Intelligence Agency». [En línea]. Disponible en: https://www.cia.gov/library/publications/the-world-factbook/fields/2010.html. [Accedido: 31-may-2017].

[3] «¿Cómo ha logrado Telegram conquistar Irán?», *Intereconomia*, 10-mar-2017. .

[4] «Admins of 12 Reformist Telegram Channels Arrested in Iran Ahead of May 2017 Election», *Center for Human Rights in Iran*, 21-mar-2017. .

[5] «Iran's Judiciary Blocks Instagram's Live Video Service Weeks Before May 2017 Elections», *Center for Human Rights in Iran*, 28-abr-2017. .

[6] «Irán :: Informe Anual 2015 - Reporteros Sin Fronteras». [En línea]. Disponible en: http://www.informeanualrsf.es/news/iran/. [Accedido: 31-may-2017].

[7] «OHCHR United Nations Human Rights Council». [En línea]. Disponible en: http://www.ohchr.org/EN/HRBodies/HRC/Pages/HRCIndex.aspx. [Accedido: 31-may-2017].

[8] «Iran Threats: Documenting Iranian State Sponsored Hacking». [En línea]. Disponible en: https://iranthreats.github.io/. [Accedido: 04-jun-2017].

Acerca de ElevenPaths

En ElevenPaths creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Más información

www.elevenpaths.com

@ElevenPaths

blog.elevenpaths.com