ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

34/2012 13 junio de 2012

Mª José Caro Bejarano

FLAME: UNA NUEVA AMENAZA DE CIBERESPIONAJE

FLAME: UNA NUEVA AMENAZA DE CIBERESPIONAJE

Resumen:

A finales de mayo se ha descubierto un nuevo tipo de ataque cibernético conocido como Flame. Se trata de un conjunto sofisticado de herramientas de ataque. Supera en complejidad a los anteriores Stuxnet y Duqu. Esto despierta el dilema del uso de los ciberataques como arma.

Abstract:

At the end of May, a new type of cyber attack, called Flame, has been discovered. It is a sophisticated set of attack tools. It exceeds the complexity of the previous Duqu and Stuxnet. This raises the dilemma of using cyber attacks as a weapon.

Palabras clave:

Flame, Stuxnet, Duqu, ciberespionaje, ciberarmas.

Keywords:

Flame, Stuxnet, Duqu, cyber espionage, cyber arms.

FLAME: UNA NUEVA AMENAZA DESTINADA AL CIBERESPIONAJE.

Aparición de una nueva amenaza cibernética: virus Flame

A finales de mayo la empresa rusa Kaspersky[1] informó de la aparición de un nuevo conjunto de herramientas de ataque conocido como Flame. Flame es un gusano de ciberespionaje altamente sofisticado que ha afectado a ordenadores de muchos países de Oriente Próximo[2] y Europa del Este.

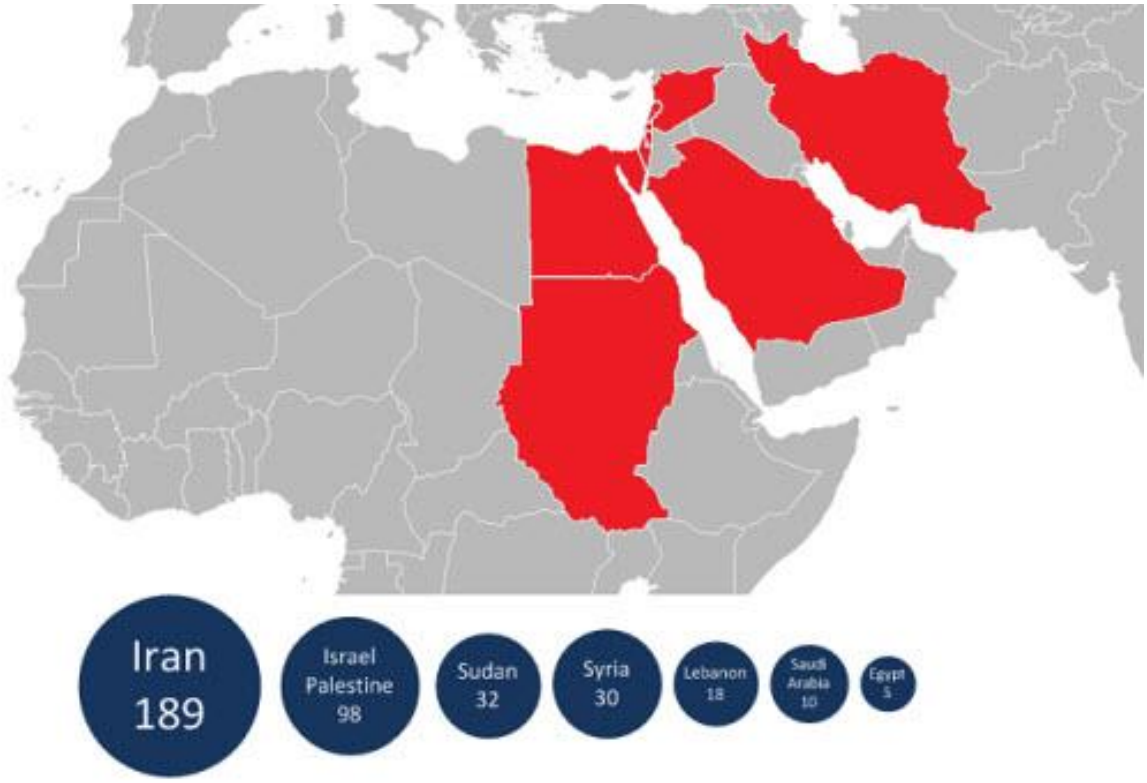

Ilustración 1. Países afectados. Fuente: securelist.

Kaspersky Lab inició su investigación en abril tras las informaciones de un supuesto sabotaje del sector petrolífero iraní. Posteriormente el organismo International Telecommunication Union (UIT en sus siglas en español, la agencia de la ONU especializada en las Tecnologías de la Información y las Comunicaciones-TIC) solicitó su ayuda para detectar un código dañino que estaba borrando información sensible en ordenadores de Oriente Próximo. Mientras se buscaba este código denominado Wiper, descubrieron otro código nuevo al que llamaron Flame.

[1] Eugene Kaspersky es el director y cofundador de la compañía rusa que lleva su nombre.
[2] Básicamente unos 189 ordenadores en Irán, 30 en Siria, 98 de la Autoridad Nacional Palestina e Israel, 32 de Sudán o 5 de Egipto.

Flame comparte muchas características con otros códigos dañinos como Stuxnet y Duqu. Sin embargo, Flame es uno de los códigos más complejos detectados hasta ahora. Es grande y sofisticado. Hace replantearse las nociones de ciberguerra, ciberterrorismo y ciberespionaje.

Según el análisis realizado por los investigadores de seguridad, Flame se ha clasificado como un conjunto de herramientas de ataque, que contiene tres componentes principales:

- Acceso backdoor (por puerta trasera) para acceder a los sistemas infectados
- Funcionalidad de troyano para realizar el robo de información
- Puede infectar otros sistemas en red local o en dispositivos removibles mediante comandos remotos.

Tiene un tamaño considerable, en concreto es un malware de unos 20 MB de tamaño. Al infectar un ordenador primero carga unos 6 MB de código; entonces comienza a desplegar hasta 20 módulos distintos que realizan funciones más concretas de espionaje y ataque, según las circunstancias.

Una vez infectada una máquina, Flame inicia un conjunto de operaciones complejas: recopilar archivos de datos, cambiar la configuración de forma remota en los equipos, encender los micrófonos de los equipos para grabar conversaciones cercanas, así como interceptar el teclado, tomar capturas de pantalla y registrar los chats de mensajería instantánea y las comunicaciones telefónicas por VoIP.

También puede activar las comunicaciones inalámbricas basadas en Bluetooth y comprometer dispositivos inalámbricos cercanos. Todo esto está disponible al operador de Flame mediante un servidor de comando y control. Es decir, no destruye como hacía el virus Stuxnet sino que espía de manera invisible, por ello, es más peligroso y difícil de detectar.

Numerosos investigadores de malware, entre ellos Kaspersky Lab, aseguran que el código de Flame, también conocido como "sKyWIper", tiene numerosas semejanzas con Stuxnet y el gusano Duqu, ya que utiliza vulnerabilidades similares. Como método de propagación de ejecución automática emplea la técnica shell32.dll, se propaga de una manera muy similar a Stuxnet, mediante la misma brecha de seguridad del sistema Windows de Microsoft. Su tamaño es considerablemente mayor (unos 20MB) contiene hasta 20 veces más código que Stuxnet y tiene cerca de 100 veces más cantidad de código que un virus típico diseñado para robar información financiera.

En declaraciones de Eugene Kaspersky: "Cuando vimos a Flame por primera ve, tuvimos mucho miedo, ya que enseguida nos dimos cuenta que era un proyecto muy bueno,

complejo y serio. Calculo que para crearlo se necesitó no menos de 100 millones de dólares, para pagar a ingenieros, expertos, analistas, técnicos, maquinas de café, etc."[3]

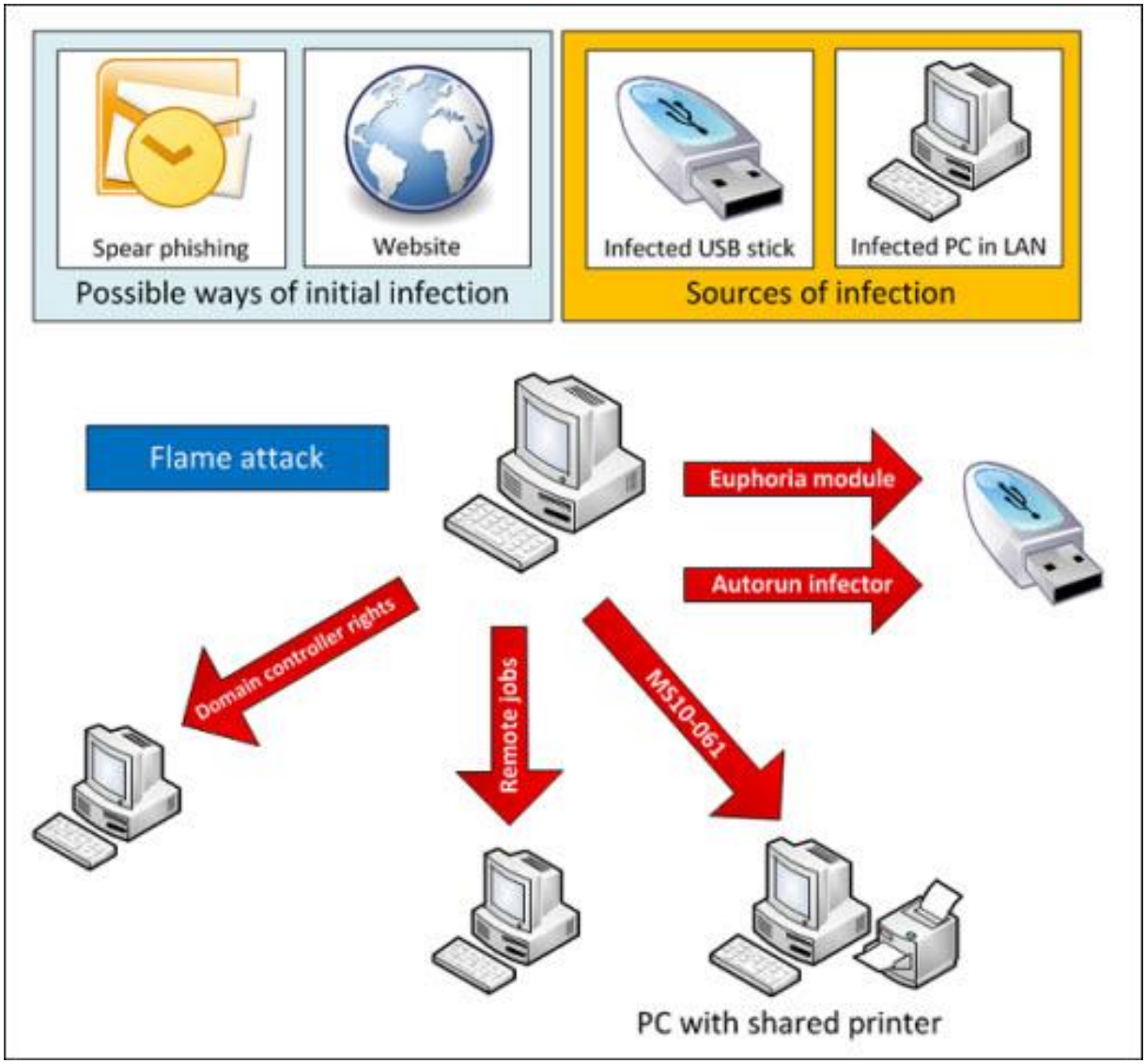

Ilustración 2. Funcionamiento de Flame. Fuente: securelist

Hasta ahora se han detectado más de 5.000 equipos infectados. Naciones Unidas usará la red ITU-IMPACT, formada por 142 países y varias empresas, para alertar a los gobiernos y a la comunidad sobre esta amenaza cibernética.

Otros ataques anteriores

El caso de Stuxnet no fue el primero en que se usaron armas cibernéticas. Otros precedentes son Kosovo en 1999, Taiwán en 2003 (atacada por China), Estonia en 2007 (que pidió ayuda

[3] www.elmundo.es/elmundo/2012/06/07/navegante/1339045745.html.

a la OTAN), Georgia en 2008, etc. En 2010 se detectó Stuxnet que fue diseñado para atacar el programa nuclear iraní aprovechando un fallo de seguridad del sistema SCADA que lo controlaba. Fue el primer virus informático conocido capaz de sabotear, por sí mismo, procesos industriales, en concreto, instalaciones atómicas iraníes, sobre todo, aquellas capaces de fabricar misiles con cabezas nucleares. En 2011 se detectó Duqu, éste usaba las mismas técnicas que Stuxnet para infectar sistemas e infraestructuras, al menos, en Europa, para recabar información de forma silenciosa.

¿Posibilidad de una ciberguerra? ¿Se ha abierto la caja de Pandora de los ataques cibernéticos?

En un libro[4] que acaba de aparecer en EEUU., la Casa Blanca reconoce la implicación del presidente norteamericano Back Obama en los ataques cibernéticos contra el programa nuclear de Irán[5]. Este programa conocido Olympic Games, había sido iniciado con la administración Bush. Obama decidió acelerar estos ataques, incluso después de que accidentalmente un elemento del programa se hiciera público en el verano de 2010, el gusano Stuxnet.

El gobierno de EEUU sólo reconoció recientemente estar desarrollando ciberarmas, pero nunca ha admitido su uso, aunque se contempló su uso durante la pasada campaña de Libia como un posible ataque a los sistemas de defensa aéreo que finalmente se descartó.

Según fuentes del New York Times, los ataques norteamericanos podrían no limitarse a Irán, sino extenderse a Corea del Norte, Siria, Al Qaeda. Sin embargo, todo esto conlleva un notable riesgo, para un país desarrollado como EEUU y vulnerable a un ataque a sus infraestructuras. La pregunta es ¿se debería experimentar o lanzar un ciberataque si no se está preparado para defenderse ante un ataque físico y cibernético sofisticado? En el ciberespacio la amenaza real procede de actores estatales y también de actores no estatales como el terrorismo y el crimen organizado, ante los que no funciona la disuasión.

María José Caro Bejarano
Analista Principal IEEE

[4] *"Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,"* David E. Sanger.
[5] "Obama Order Sped Up Wave of Cyber attacks Against Iran". The New York Times, published June 1, 2012.