CIBERGUERRA: CUANDO PASAMOS DEL ARMAMENTO A LAS COMPUTADORAS

Teniente Primero Arturo VELARDE Murillo

Resumen

La gran expansión de Internet, la considerable gran distribución de smartphones alrededor del globo, no son sólo mejoras y privilegios de los que disfrutan los civiles. Muchas de las mejoras en el avance tecnológico han sido y vienen siendo aprovechadas por los militares, comunicaciones a sólo un botón de distancia, drones armados y piloteados a miles de kilómetros, toda clase de apoyo que podamos imaginar para nuestros soldados sobre todo terreno, acompañado de un gran y largo etcétera.

Todo señala a que la guerra ya no está sólo destinada a enviar soldados y drones. Ataques a comunicaciones civiles y militares, privarnos de las redes eléctricas, causar pánico en la población, todo esto indica que los ciberataques son igual de útiles que los ataques convencionales, y eso que esto aún empieza…

INTRODUCCION Y DEFINICIONES:

¿Qué es un ciberataque? ¿Cómo se hace la ciberguerra?

Un ciberataque es la acción en la que se atacan las redes de una nación, entidad gubernamental, empresa, etc., para crear daños o caos. Ese ataque puede ser realizado por otro estado, grupo terroristas, compañías, activistas, organizaciones criminales o grupos extremistas. Está de más decir que, casi siempre, algunas "entidades" han sido acusadas de financiar estos grupos para atacar a sus enemigos.

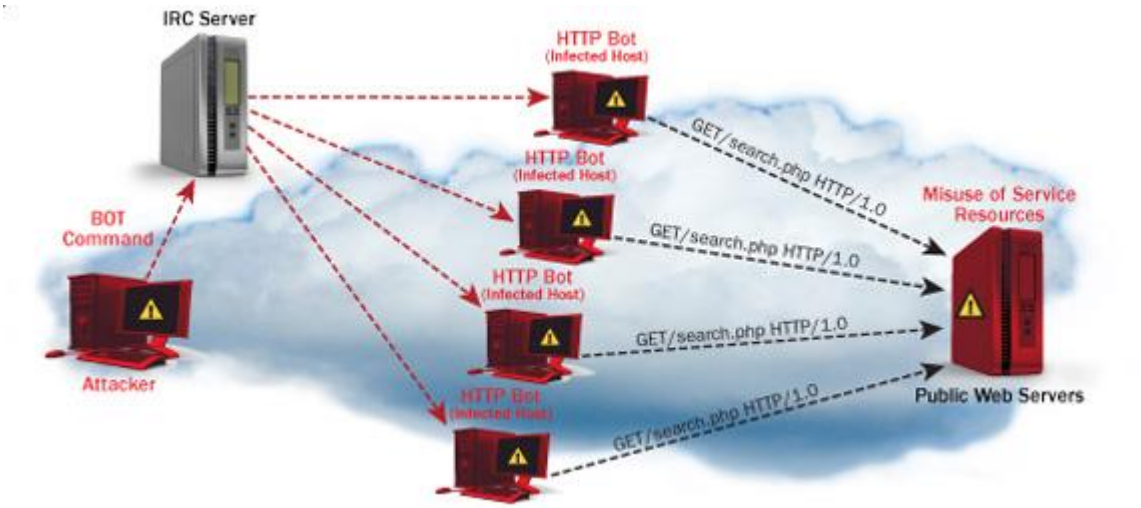
Actualmente, gran cantidad de ejércitos están integrando la ciberguerra como parte fundamental de sus operaciones, prueba de ello son los ataques a otras naciones en caso de guerra, así como también, los ataques a sus propios sistemas con la finalidad de prevenir los ataques que puedan sufrir. Y por supuesto, también son capaces de operar desde las sombras.

PAIS	FINANCIACIÓN (millones de dólares por año)	Plantilla (personas)
EE.UU.	7,000	9,000
China	1,500	20,000
Reino Unido	450	2,000
Corea del Sur	400	700
Rusia	300	1,000
Alemania	250	1,000
Francia	220	800
Corea del Norte	200	4,000
Israel	150	1,000

Los Estados que más gastan en sus fuerzas cibernéticas. (Graf. 1)

Podemos dividir los ataques en dos partes. La primera es el espionaje convencional: hackear redes para conseguir información. A pesar que el espionaje convencional y cibernético no se consideran como actos de guerra, sí causan tensiones serias entre los países involucrados. Tal vez el caso más famoso es el hallazgo de que la NSA espía a una gran cantidad de mandatarios europeos y países.

Pero además tenemos la segunda parte, el Sabotaje: ataques directos a las infraestructuras para que no puedan funcionar. Aquí podemos encontrar los ataques de denegación de servicio (DoS), los ataques distribuidos de denegación de servicio (DDoS), los mismos que consisten en atacar a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Usualmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima, o sobrecarga de los recursos computacionales del sistema atacado. Asimismo, tenemos el ataque del tipo Reflector, el cual funciona bajo el principio del DoS pero implica doblar el volumen de los datos con que se intenta desbordar al servidor, antes de bombardear este con falsas alertas.



Arquitectura de un Ataque de Negación de Servicio. (Graf. 2)

ANTECEDENTES:

El hacking, como actividad en sí, se originó de aquellas virtudes humanas llamadas persistencia y curiosidad, cuyos inicios son anteriores al de las ciencias de la computación. Es más, la palabra "Hack" se cree referida al golpe en seco que los operarios de las máquinas en el MIT, propinaban a los equipos que usaban para realizar operaciones matemáticas, y que cuando se bloqueaban requerían el famoso golpe seco.

Algunas acciones conocidas en donde los hackers aparecen en escena, las que se han desarrollado como grupo organizado o de manera independiente: (que hayan sido atrapados, o cuyo ataque ya se haya conocido).

1) Stuxnet y el proyecto nuclear iraní: Es uno de los más conocido por todos. Creado como un gusano dirigido a sistemas industriales, se corre el rumor de que es el fruto de un pacto entre americanos e israelíes, creado para sabotear el programa nuclear de Irán. Luego de analizar el código, los expertos afirman que fue hecho por un profesional, ya que tiene cuidado de sólo atacar en condiciones muy concretas, reprogramaba controladores lógicos programables y era muy complejo a la hora de esconderse. Se estima que es el responsable de acabar con la quinta parte de las centrifugadoras nucleares del país. El gusano se ocultó en las memorias USB de los ingenieros.

2) Google, China y la Operación Aurora: Es un caso peculiar, si tiene la oportunidad de ir a China, intente hacer una búsqueda en google o revisar su Gmail, desde ya le comentamos que no podrá. Todo esto se remonta al año 2010, fecha en la que Google desveló la Operación Aurora. Una serie de ciberataques realizados por un grupo cercano al Ejército Popular de Liberación a compañías estadounidenses (en donde además de Google, encontramos a Adobe, Yahoo, Symantec y Northrop Grumman) con la finalidad de encontrar datos privados de activistas chinos. La respuesta de Google fue dejar de cumplir las leyes de censuras chinas, por lo que dejó de funcionar de manera oficial en citado país.

3) El gran Hack de EE.UU. – 160 millones de usuarios: No tiene nombre oficial porque no afectó a una sola compañía, sino a una larga lista de ellas que incluía el índice bursátil NASDAQ, 7-Eleven, JC. Penney, JetBlue, Dow Jones o Global Payment entre otras. El ataque se prolongó durante siete años desde 2005, y robó los datos de tarjetas bancarias de 160 millones de clientes. Cinco personas de origen ruso fueron acusadas y condenadas por el caso.

4) En Agosto de 1999, Jonathan James atacó equipos de cómputo de la Agencia de reducción de Amenazas de la Defensa interceptando miles de mensajes confidenciales, contraseñas y el software que controlaba toda la vida en la agencia espacial internacional. Posteriormente atacó los sistemas de la NASA, la que se vio obligada a apagar sus redes por 3 semanas.

5) GhostNet: Una red de espionaje descubierta en el año 2009, la misma que afectó a 103 países, incluyendo muchos de sus gobiernos y compañías privadas. Todo inició después que el Dalai Lama pidió que se examine sus equipos por sospechas que tenía malware.
   Su origen o centro de operaciones es, aparentemente, China, aunque no queda claro que el gobierno sea responsable. Se infiltraron en al menos 1.295 ordenadores en embajadas y ministerios. Se cree que el enfoque era espiar al Dalai Lama, a gobiernos de países en el sur y sureste de Asia. Parte de las sospechas que relacionan al gobierno chino son acciones tomadas por ellos a partir de información obtenida por medio de GhostNet.
   El malware no era simplemente un agente pasivo recolectando información, también permite controlar los equipos pudiendo navegar en el sistema operativo, obtener documentos, modificarlos, o activar la webcam y el micrófono para escuchar conversaciones.

6) El portal Wikileaks, en noviembre 2010, comenzó a filtrar información reservada robada a Estados Unidos. En base a esta acción varias organizaciones clausuraron las páginas de este portal así como sus canales de financiamiento (tales como EverDNS, Paypal, eBay, Amazon, Visa, Mastercard, entre otras). En respuesta a esto, el grupo de Internet Anonymous lanzó la operación de ciberataques contra estas entidades, (operación llamada PayBack). Esto originó lo que se ha llamado la primera guerra de guerrillas informática.

7) El 22 de mayo de 2012 se supo que Anonymous logró acceder al servidor del Ministerio de Justicia de EE.UU. donde estaban almacenados datos sobre todos los crímenes cometidos en territorio estadounidense.

8) El 26 de julio de 2014 un ciberataque afectó los sitios de doce instituciones públicas y la Bolsa de Venezuela. De la agresión se responsabilizaron Anonymous Venezuela y Venezuelan Hackers.

9) Ataque a Hacking Team: “Cuando los hackers son hackeados”. Cada día se producen cientos (si no miles) de ciberataques a todo tipo de compañías, gobiernos, e incluso empresas de seguridad. Pero que los propios hackers sean atacados, es menos frecuente. Hacking

Team es una controvertida firma de software italiana popular por suministrar de forma legal herramientas de espionaje e intrusión remota como spyware y malware. Entre sus clientes figuran agencias de inteligencia y gobiernos. La compañía sufrió un ataque en el 2015 de donde se han filtrado a la red 500 Gb de datos confidenciales.

10) "Cracka": El misterioso adolescente británico que hackeó al director de la CIA. El último ciberdelincuente en llamar la atención de la prensa internacional es un joven británico que a sus 16 años consiguió hackear los correos personales del Director de la CIA, el director del FBI y el Director de Inteligencia Nacional estadounidense. Además, hackeó las cuentas de teléfono de este último y reveló la identidad de 31,000 agentes del gobierno de Estados Unidos: CIA, Seguridad Nacional, FBI, etc.
    La verdadera identidad de este joven no se ha desvelado pero sabemos que se hace llamar "Cracka" y asegura ser miembro de un grupo de hackers llamado "Crackas with Attitude" que actúa en defensa del Movimiento Palestino. "Cracka" fue detenido en el 2016 en el sureste de Inglaterra.

11) WannaCry: El 12 de mayo 2017 un ataque masivo de ransomware llamado WannaCry afectó a empresas y particulares de todo el mundo, incluyendo grandes corporaciones y organismos públicos. El ataque golpeó seriamente al Servicio de Salud Británico, a la multinacional francesa Renault, al sistema bancario ruso y al grupo de mensajería estadounidense FedEx, así como al servicio de ferrocarriles alemán y a universidades en Grecia e Italia.
    Aunque era muy potente, este ransomware también presentaba (afortunadamente) defectos de diseño significativos, incluyendo un mecanismo que operativos de seguridad consiguieron usar para inutilizar el malware y detener su expansión. Funcionarios estadounidenses han relacionado la autoría del ataque con el gobierno norcoreano, pero no hay nada confirmado oficialmente.

ACTORES:

Si bien existen muchos, vamos a mencionar los más importantes:

1) Hackers: Llamados así a quienes desarrollan las herramientas y/o técnicas para penetrar sistemas o redes de cómputo. Se observa que, durante el desarrollo de actividades de Guerra informática, que también implica actividades de Seguridad informática de manera defensiva, en ambos bandos hay hackers (Black, White, Gray Hat). Podemos dividirlos en tres grupos muy definidos basado en su nivel de conocimiento, TTP (tácticas, técnicas y procedimientos) y sus auspiciadores:
    a) Script-kiddies
    b) Hackers profesionales o grupos de hackers (anonymous)
    c) Grupos de Élite (Hidden Lynx, Bureau 121, Axiom, etc)

Grupo Anonymous. (Graf. 3)

2) Especialistas de seguridad informática: Usualmente son White hackers (o hackers blancos). Expertos en computación involucrados en las actividades defensivas ante una potencial amenaza o vulnerabilidad informática. En muchas oportunidades son ex hackers que optaron por "el camino del bien".

3) Usuarios: Son todos aquellos que usan las redes de cómputo, no importando el nivel de conocimiento en informática y seguridad que estos tengan. Suelen ser el objetivo principal de los atacantes, ya que son el eslabón más débil en la cadena de seguridad.

4) Malware (Programas de software infecciosos): Es todo aquel software usado para penetrar redes informáticas (virus, troyanos, gusanos, spyware, backdoor, keyloggers, etc.).

5) Sistemas de Seguridad: Son las herramientas de software y hardware utilizados por los especialistas en seguridad informática con la finalidad de evitar que la información y los sistemas de información sean vulnerados.

CONSIDERACIONES:

"Es probable que los ensayos de una posible guerra cibernética a gran escala se iniciaron en el 2009 con la operación Ghostnet."

Danilo Briceño E. – CISSP

Ciberguerra. (Graf. 4)

Una "Guerra clásica", presenta ciertas condiciones, como por ejemplo:

1) Es una lucha armada entre dos o más naciones o grupos beligerantes.
2) Siempre hay un motivo, generado por intereses: Guerra civil, guerra santa, guerra ideológica, guerra por riquezas o por poder, etc.
3) Existen muertos y heridos en ambos bandos.
4) Se evidencia una gran devastación material.
5) Puede haber cambio de geografía.
6) Hay grandes pérdidas económicas.
7) Existe legislación al respecto (como por ejemplo, el Derecho Internacional Humanitario).

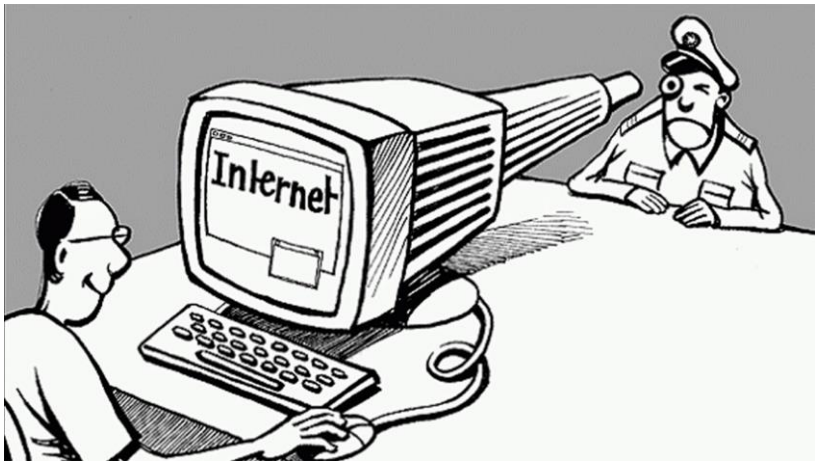
Pero en el caso de una Ciberguerra, estas condiciones no se cumplen en su mayoría:

1) Una o un pequeño grupo de personas podría estar en la capacidad de afectar a grandes ejércitos o poblaciones.
2) Se realizan actividades para robar, alterar o destruir la información y sistemas de información del o los adversarios, mientras se protege la información y sistemas propios.
3) El escenario es global, y no se reduce a áreas geográficas.
4) La conducción de la guerra necesita de expertos en informática, antes que expertos en estrategia.
5) Las características de software y hardware (tanto para el área de defensa y ataque) debe ser altamente confiables.
6) Los objetivos tácticos, operativos y estratégicos no son estrictamente objetivos militares, sino también pueden ser organizaciones e instituciones que son parte de la civilidad (bancos, empresas de comunicaciones, servicios públicos, etc.).

Lo ideal durante un ataque informático es inutilizar todos los objetivos de interés sin que el enemigo pueda reaccionar y sin que se dispare un arma de fuego. Por ello, la mayor de las fortalezas de nuestra era de la información es también la más crítica de sus debilidades: todo está conectado en red. Por lo que podemos decir que en este siglo, así como los venideros, las guerras serán muy diferentes a como las conocemos, transformando aspectos de la guerra tales como imágenes, inteligencia, información, redes informáticas, sistemas de información, sistemas de armas, sistemas de comunicaciones y capacidades de Comando y Control.

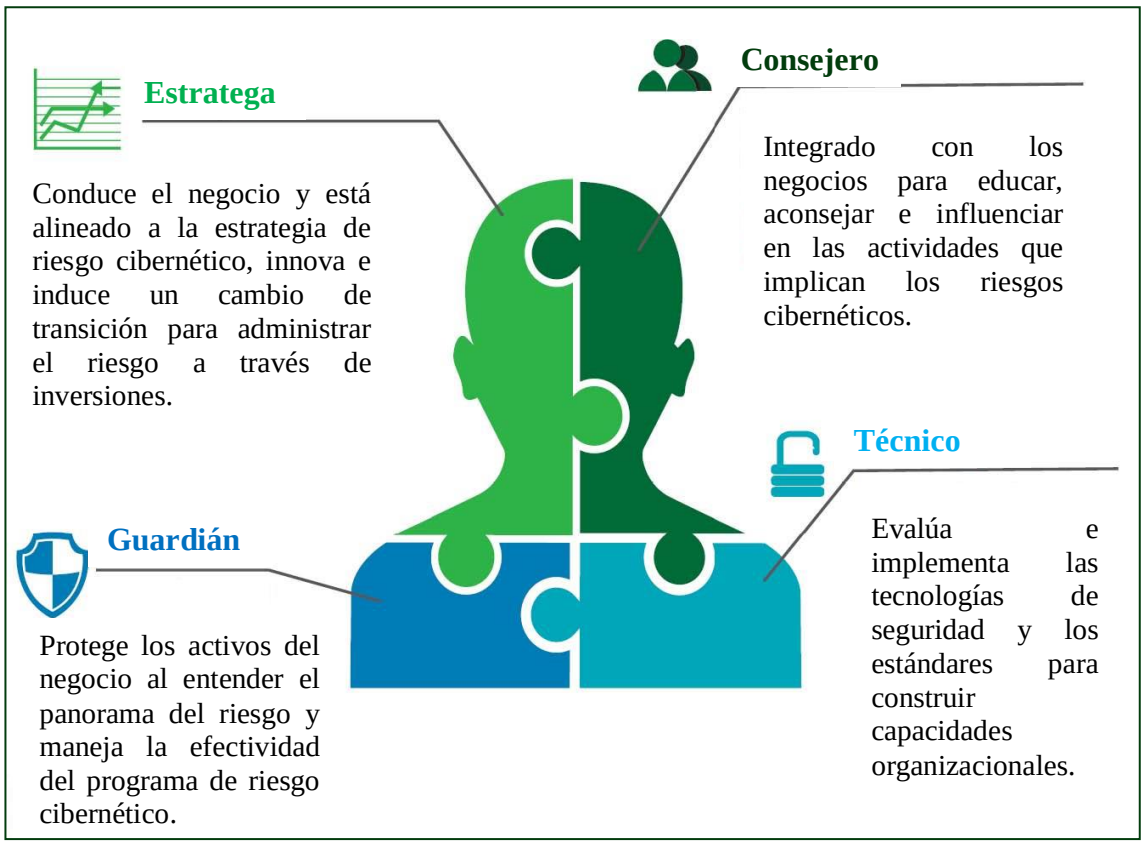
Se debe tener en cuenta, además, que no sólo los Estados o ciertas Instituciones amparadas en la legalidad pueden desarrollar esta capacidad. También organizaciones ilegales, tales como grupos terroristas, pueden tener acceso a estos conocimientos y tecnologías, lo que se puede constituir en una peligrosa arma de resultados devastadores. Basta que un ciberataque contra una central nuclear, una red militar o un sistema con información confidencial tenga éxito, para desencadenar escenarios tanto o más apocalípticos que los que se producen a través de conflictos clásicos. Ante todo esto, surge la siguiente pregunta:

¿Necesitamos una “convención digital de Ginebra”?
El presidente y director legal de Microsoft, Brad Smith, lo tiene claro: Necesitamos una ‘Convención de Ginebra’ que podamos aplicar al terreno digital. Puesto que cada vez las tensiones que generan estos ataques son mayores, los ataques pasan por infraestructuras de propiedad privada, y en muchas ocasiones son simples civiles los afectados. Para solucionarlo, Smith propone crear un ‘código de normas’ sobre la ciberguerra. Él cree que la industria debería comprometerse a defender a los usuarios. Además, afirma que debemos crear un cuerpo especializado en respuesta a ciberataques.
En cualquier caso, tiene mucha razón al decir que estos ataques están generando mucha tensión. Y esto no ha hecho más que empezar. Cada vez los ciberataques forman una parte más y más grande de un ataque. Y, ante un atacante poderoso y un defensa débil, es fácil prever una catástrofe.



Cuando somos observados y no lo sabemos. (Graf. 5)

Y a todo esto, ¿Quién se encarga de evitar que entren por “la puerta trasera”?
El CISO (por sus siglas en inglés Chief Information Security Officer), es un ejecutivo de alto nivel en la organización, responsable de alinear las iniciativas de seguridad con los programas corporativos y los objetivos de negocio, garantizando que los bienes y tecnologías de la información están adecuadamente protegidos.



Perfil de un CISO. (Graf. 6)

CONCLUSIONES:

1) Un principio básico en seguridad es que no existe objetivo chico o poco importante, entonces, ¿Qué podemos hacer? Por todo lo anterior, entendemos que la ciberguerra y el ciberespionaje ya están aquí, y han estado por muchos años, se nutren de

capacidades y conocimientos, los mismo que no podemos salir a la calle y comprarla al por mayor, ya que se requiere de experiencia, tiempo, perseverancia, equivocarse y volver a empezar, paciencia y mucha voluntad. Además, claro está, de inversión, investigación y desarrollo, y una clara y definida política favorable.

2) Se deben crear y afirmar las capacidades propias para proteger y atacar objetivos que sean militares o no. Asimismo, se debe tener a las personas idóneas y con potencial, operativamente adecuadas y en los puestos correctos para el desarrollo de estas capacidades de ataque y defensa. El no hacerlo, anulará el intento aún antes que se inicie. Como en toda estrategia, las decisiones se deben tomar con la cabeza fría y sin ambiciones o pasiones personales.

3) Aquel gobierno o entidad que utilice la tecnología para espiar, alterar o controlar los principales sistemas de una nación: Transporte, Comunicaciones y Energía, serán gobiernos con poder cibernético.

4) Debemos preocuparnos por tener CISO's capacitados, comprometidos con la Institución, a fin de poder liderar eficientemente el grupo humano encargado de hacer frente a cualquier ataque a nuestra información.

5) Actualmente el activo más importante de toda organización es la información, y justamente por eso, los ataques cibernéticos son cada vez más y más recurrentes a nivel mundial. Hasta el mismo dinero se ha convertido en un conjunto de datos virtuales que se mueven constantemente en ese mundo virtual paralelo a la realidad.
   Ahora, si esto lo llevamos al ambiente militar, en donde la tecnología también ha tenido un desarrollo exponencial en los últimos 10 años, estamos hablando que cualquier tipo de dispositivo tecnológico militar (armamento, equipo de comunicaciones, bases de datos del personal, etc.) podría ser vulnerado e inoperativizado por un ataque cibernético. Las bases de datos confidenciales y críticas de las organizaciones, podrían ser alteradas o hasta desaparecidas. Ante esta situación, implementar estrategias de ciberseguridad, concientizar al personal en el ejercicio de estas estrategias y capacitarlos en este tema, es inmensamente importante.

Referencias:

Briceño E, Danilo. – CISSP, Cybersecurity Evangelist & Advisor en NeoSecure (2017). Ciberguerra.

Fuchs V., Alf. – PMP, Project Manager en NeoSecure (2017). Ciberguerra.

Ciberguerra: cuando el arma más poderosa es un ejército de hackers. (2017). Retrieved 7 October 2017, from http://omicrono.elespanol.com/2017/03/ciberguerra-ejercito-hackers/

Los 10 mayores ataques informáticos de la Historia. (2017). Retrieved 30 October 2017, from http://es.gizmodo.com/los-10-mayores-ataques-informaticos-de-la-historia-1580249145

Los hackers más famosos de la historia. (2017). Retrieved 4 October 2017, from https://www.pandasecurity.com/spain/mediacenter/malware/hackers-mas-famosos-historia/

Ataque de denegación de servicio. (2017). Retrieved 13 October 2017, from https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

Rusia, entre el 'top 5' de Estados con mayor capacidad de ciberguerra. (2017). Retrieved 11 October 2017, from https://actualidad.rt.com/actualidad/228187-rusia-top-estados-mayores-capacidades-ciberguerra

Sabotajes desde Servidores DNS. (2017). Retrieved 16 October 2017, from https://diarioti.com/nuevo-tipo-de-sabotaje-cibernetico-opera-desde-servidores-dns/10914

The Ultimate Guide to DoS Attacks. (2017). Retrieved 15 October 2017, from https://www.guru99.com/ultimate-guide-to-dos-attacks.html