# Amenazas Persistentes Avanzadas

* * * * *

*Antonio Villalón*
*Director de Seguridad – S2 Grupo*

NAU llibres

Nau Llibres

Periodista Badía 10. 46010 València
Tel.: 96 360 33 36
Fax: 96 332 55 82
E-mail: nau@naullibres.com
web: www.naullibres.com

Diseño y maquetación:
Pablo Navarro, Nerina Navarrete y Artes Digitales Nau Llibres

Diseño de cubierta e ilustración:
S2 Grupo

ISBNs Nau Llibres

ISBN_papel: 978-84-16926-09-1
Depósito Legal: V-2614-2016

ISBN_ePub: 978-84-16926-10-7
ISBN_mobi: 978-84-16926-11-4
ISBN_PDF: 978-84-16926-12-1

Impresión: Safekat

Para Raquel, Teresa y Lucía

# Índice

# Antes de comenzar…

Este documento ha sido realizado principalmente en trenes y hoteles de toda España, sobre todo en el trayecto en AVE Valencia-Madrid-Valencia del que disfruto con asiduidad. En él, escrito desde la perspectiva de seguridad defensiva en términos generales (aunque hay casos en los que se aplica el rol del atacante, algo que puede deducirse fácilmente por el contexto), se tratan de exponer desde los principales actores que juegan en el terreno del robo de información hasta las aproximaciones de defensa frente a los mismos, pasando por las tácticas, técnicas y procedimientos que en uno y otro lado aplicaremos. Todo ello enmarcado, o al menos tratado de enmarcar, en eso que llamamos ciberinteligencia, esa palabra tan de moda.

Como en cualquier trabajo que toca estos temas, espinosos en ocasiones, es necesario incluir el correspondiente *disclaimer*: todo, absolutamente todo lo que aparece en este trabajo refleja una aproximación personal mía y de nadie más, sobre todo para lo malo. Toda la información reflejada en el documento ha sido obtenida de fuentes públicas, y en algunos casos no expresa más que la propia opinión del autor, ya que por supuesto no existen pruebas que la sustenten. Dicho de otra forma, yo puedo opinar que un país o grupo determinado es especialmente activo o resulta una amenaza para nosotros, pero no tengo pruebas de ello y por tanto no es más que mi opinión. Adicionalmente, durante la reali-

zación del trabajo he tratado de huir en todo momento –no sé si lo habré conseguido– de términos como "los buenos" o "los malos"; en esta guerra no hay ni buenos ni malos, sino que cada uno ejerce sus tareas en el rol que tiene asignado en cada momento: hoy estás aquí, mañana estás allí… Los que tratan de robarnos información no tienen por qué ser ni peores ni mejores que nosotros.

Quiero dar las gracias a todos los que habéis leído este documento antes de ser publicado y me habéis facilitado críticas, que siempre han sido constructivas; sobre todo, una vez más, a **Ismael Ripoll** (UPV, Universidad Politécnica de Valencia), por sus acertados comentarios al borrador de este trabajo. Además de sus comentarios, también agradezco especialmente a **Félix** (CIFAS, Centro de Inteligencia de las Fuerzas Armadas) esas conversaciones relativas a seguridad, defensa e inteligencia hasta altas horas de la madrugada, en las que acabamos hablando de lo humano y lo divino.

Pero, sin duda, si a alguien tengo que darle especialmente las gracias es a **Raquel, Teresa y Lucía**. Por aguantarme a mi (y sobre todo a mis viajes) y por apoyarme en todo momento; como no podía ser de otra forma, a ellas tres van dedicadas estas páginas.

AVE Madrid-Valencia, marzo de 2016

# Prólogo

This page intentionally left blank

# 1 Introducción

## 1.1. Inteligencia

La OTAN ([24]) define el término **inteligencia** como el **producto** resultante del procesamiento de información relativa a naciones extranjeras, fuerzas o elementos hostiles o potencialmente hostiles o áreas de operaciones reales o potenciales, y también aplica el término a la **actividad** cuyo resultado es justamente este producto, esta inteligencia. Suavizando este concepto militar, podríamos hablar de inteligencia como el producto resultante de un análisis de información cuyo objeto es facilitar la toma de decisiones: alguien (una autoridad, un estado, una organización...) tiene unas necesidades de información concretas, necesidades que son satisfechas mediante la obtención y el análisis de datos para tratar de dar respuesta, con mayor o menor precisión, a esas necesidades.

Para producir inteligencia es necesario abordar una serie de etapas predefinidas y de tareas en cada una de ellas. En el *CIA Factbook on Intelligence,* se define el llamado **ciclo de inteligencia**, que especifica el proceso de generar inteligencia a partir de datos "en crudo", inteligencia que pueda ser utilizada convenientemente

para la toma de decisiones. Este ciclo consta de cinco etapas (existen modificaciones al mismo, que no lo modifican sustancialmente y que no son significativas para el presente documento):

- **Planificación**. Es la etapa inicial del ciclo, que permite identificar necesidades específicas y requerimientos de información. Será realimentada nuevamente por la diseminación de información final del ciclo.
- **Recopilación**. Es la obtención de la información necesaria para producir inteligencia a partir de múltiples fuentes –desde agentes secretos a simples periódicos–, tal y como se indica a continuación.
- **Procesamiento**. Es la conversión de la información recopilada en formatos utilizables para el análisis, desde sus aspectos técnicos (XML, texto plano...) hasta aspectos como el descifrado, la traducción o la reducción de datos.
- **Análisis y producción**. Los datos que se han procesado previamente deben ser integrados, evaluados y analizados, bien de forma automática, bien de forma manual (por especialistas en diferentes ámbitos), para integrarse en un todo coherente, contextuado y que pueda ser trasladado a quien deba tomar decisiones: la inteligencia.
- **Diseminación**. Es el último paso del ciclo, que como hemos dicho realimenta al primero. Consiste en proporcionar la inteligencia generada con anterioridad a los actores, de forma que estos tomen decisiones –que muchas veces serán nuevos requisitos de información.

Una vez se ha decidido qué información se requiere, es decir, se han establecido las necesidades de información, y se planifica su obtención (requisitos, fuentes, posibilidades o técnicas de adquisición...), entra en juego la **adquisición** de dicha información. Para esta tarea existen diferentes disciplinas de *intelligence gathering* o adquisición de inteligencia (realmente, de información); las más habituales son las siguientes:

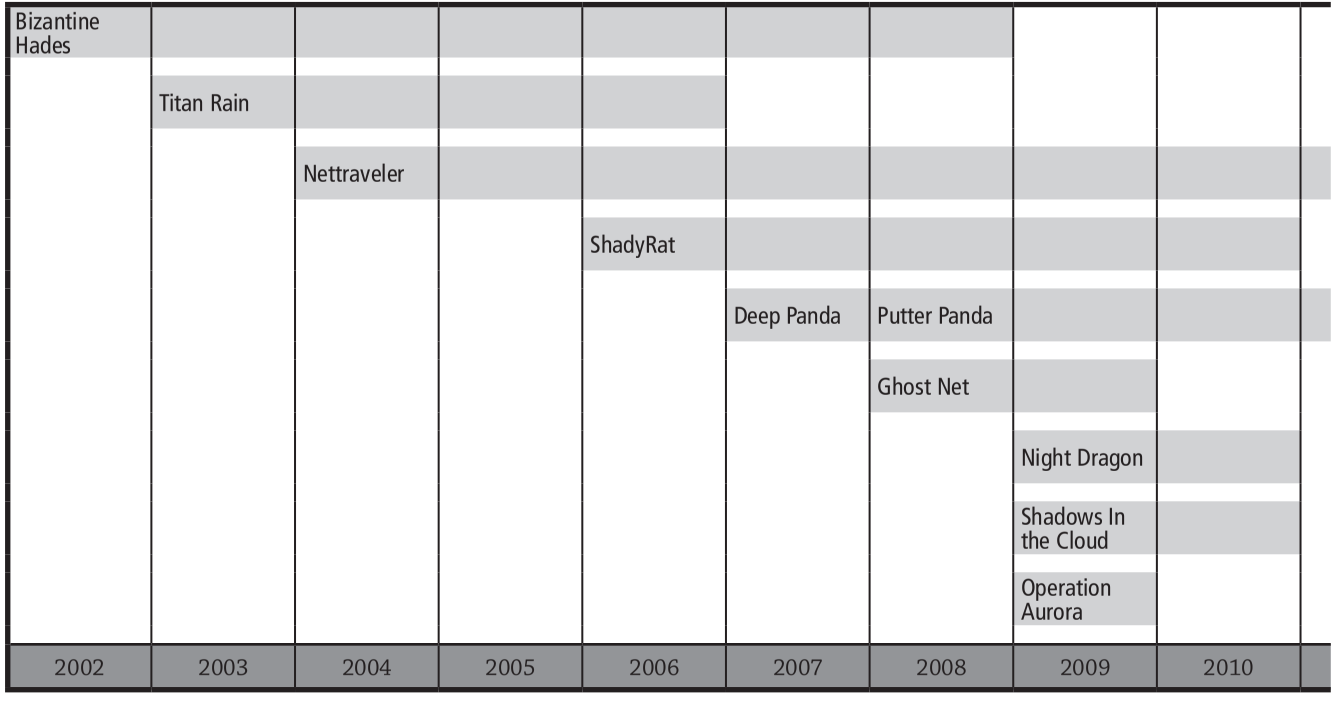
- HUMINT (*Human Intelligence*), sin duda, la disciplina de adquisición más antigua, generada mediante agentes de campo, oficiales, interrogatorios, confidentes..., técnicas en definitiva que requieren cierta interacción entre personas.

# 2 Actores principales

¿Quién está detrás de una APT? Las amenazas, hoy en día, provienen principalmente de dos fuentes: los estados y los grupos organizados, estos últimos quizás directamente ligados a los primeros o, al menos, con algún tipo de apoyo estatal. Los estados trabajan de forma habitual en el ámbito del espionaje estatal (ojo, esto incluye muchos tipos de intereses, no solo geopolíticos o de defensa), entre países amigos o no amigos, mientras que los grupos trabajan en el ámbito del espionaje industrial: nuestra competencia les paga para que nos roben información sensible –un nuevo diseño, un plano, una idea, un plan estratégico...–, información que por supuesto vale mucho dinero. ¿Cuánto cuesta el diseño de, por ejemplo, un caza de combate o, siendo más mundano, una nueva tableta? Nuestra competencia pagará hasta un euro menos por ese mismo diseño: es más barato copiar que idear y diseñar.

Presentamos en este apartado algunas reflexiones sobre la atribución de amenazas persistentes avanzadas y, con dichas reflexiones en mente, algunos de los actores presuntamente representativos en el ámbito de las APT, así como el *malware* asociado a estas que mayor impacto y repercusión ha tenido, aunque como siempre en seguridad, es de suponer que las amenazas más avanzadas y más dañinas no han visto aún la luz pública.

*Timeline de APTs atribuídas a China*



*Timeline de APTs atribuídas a China*

| 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|
| | | | | SnowMan |
| | RSA & Lockheed | | Ephemeral Hydra | Operation SMN |
| | Nitro | | | Poisioned Handover |
| | LuckyCat Redux | | | Roadming Tiger |
| Nettraveler | | | | |
| | Pitty Tiger | | | |
| Deep Panda / Putter Panda | | | | |
| | Ice Fog | | | |
| | | Hidden Lynx | | |
| | | Quantum Entanglement | | |
| | | | Deputy Dog | |

| Centro | Identificador | Unidad | Funciones |
|---|---|---|---|
| Center for Information Security | FSB CIS | 64829 | SORM. Vigilancia y contrainteligencia |
| Center for Electronic Surveillance of Communications | FSB TSRRSS | 71330 | Capacidad de ataque |
| Centre for the Security of Information and Special Communications | TsBISS | N/A | Defensa frente a intrusiones extranjeras |
| Communications Security Center | FSB CBS | 43753 | Acreditación de productos y sistemas |
| Center for Licensing, Certification and Protection of State Secrets | FSB TSLSZ | N/A | Habilitaciones de seguridad |
| Institute of Cryptography, Telecommunications and Computer Science | IKSI | N/A | Formación |

Otro de los herederos de la FAPSI es el **FSO** (identificado en [44] como la unidad militar 32152), con responsabilidad en la protección de personalidades y bienes gubernamentales, que ha asumido entre otras capacidades las asociadas a SIGINT estratégica, la garantía de explotación de los sistemas estatales –en especial en lo referente a su protección frente a servicios extranjeros– y la seguridad de la información clasificada nacional [44]. Dentro del FSO se enmarca desde 2004 (anteriormente pertenecía al FSB) el *Spetssviaz*, Servicio de Información y Comunicaciones Especiales (SSSI), considerado en la actualidad, tras el desmantelamiento de la FAPSI, el equivalente ruso a la NSA estadounidense, aunque en realidad la comunidad de inteligencia de ambos países es diferente y por tanto las atribuciones de la NSA están realmente repartidas entre agencias rusas. Este servicio incluye al menos una Dirección para la gestión de comunicaciones gubernamentales, otra para la gestión de comunicaciones gubernamentales militares, una Dirección Principal para recursos de información y otra Dirección Principal para sistemas de información ([45]).

Por su parte, el **SVR** se ocupa de la inteligencia exterior rusa, proporcionando a las autoridades nacionales inteligencia que pue-

# 3 Las campañas y el malware

Sin duda la parte más visible de una APT, o al menos la más visible para los tecnólogos, es el código dañino asociado a una campaña APT o la campaña APT en sí misma. Insistimos, una APT es mucho más que un *malware*, aunque en ocasiones confundamos dicho código con la amenaza en sí y en algunas referencias se hable de la amenaza como grupo o como *malware*. No obstante, en muchos casos será contra lo único contra lo que podamos luchar los que no trabajamos en servicios de inteligencia y, por tanto, no tenemos acceso a información privilegiada, generalmente de fuentes humanas.

Un error habitual es considerar que el código dañino asociado a una amenaza persistente avanzada es necesariamente avanzado; lo avanzado es la amenaza en sí, no el *malware*. Un ataque avanzado puede realizarse con código no avanzado, ya que la amenaza será lo suficientemente inteligente para determinar si somos un objetivo fácil (blando), al que se puede atacar mediante un troyano comercial sin ser detectado y en el que no es necesario invertir cientos de miles de euros en *0-days*, o por el contrario somos un objetivo bien protegido, difícil (duro), en el que un código dañino simple o conocido no va a funcionar y se requiere de un ataque más fino. Este grado de conocimiento de su objetivo es la "A" de avanzada. Personalmente, he visto ataques de actores muy hostiles y generalmente avanzados mediante código dañino que no era más que la mutación de malware

UROBUROS tiene orígenes posiblemente rusos. Su complejidad (y por tanto su coste) y sus objetivos (grandes empresas, estados, agencias de inteligencia...) hacen sospechar, como fuente del malware, al SVR, que durante al menos cuatro años ha estado robando información de estos objetivos de forma especialmente sigilosa. En cualquier caso, sus autores son los mismos –presuntamente– que los autores de Agent.BTZ, *malware* utilizado en 2008 para atacar a los Estados Unidos. En caso que de que se detecte Agent.BTZ en el sistema, UROBUROS permanece inactivo.

UROBUROS

| | |
|---|---|
| Descubrimiento | 2014 |
| Persistencia | 4 años |
| Impacto | Robo de información sensible |
| Presunto origen | Rusia |
| Objetivo | Europa/USA |
| Comentarios | Uno de los malwares más sofisticados identificados hasta la fecha |

# 4 Arquitectura de la amenaza

Antes de lanzar un ataque contra un objetivo determinado, o al menos antes de lanzar la fase de intrusión de dicho ataque, que veremos más adelante en este mismo documento, el atacante debe desplegar unas capacidades que le permitan lograr su objetivo: generalmente el robo de información de una o más víctimas. Para ello invertirá los recursos necesarios para implantar una arquitectura que permita al *malware* (recordemos, la bomba que nos arrojan, volviendo al símil inicial) introducirse en la organización y, una vez dentro, recibir órdenes y comunicar su estado (lo que se denomina mando y control, *Command & Control* o simplemente C2) en la organización comprometida y enviar al exterior, a entornos controlados por el atacante, la información robada a las víctimas (proceso conocido como exfiltración), además obviamente de desplegarse y mantener su persistencia en el tiempo dentro de los diferentes objetivos comprometidos.

Para lograr el robo de información continuado en el tiempo, es prioritario para una APT pasar lo más desapercibida posible, ya que se ha invertido una gran cantidad de recursos, tanto económicos como humanos, en la orquestación del ataque, por lo que, con objeto de amortizar al máximo esta inversión, debe persistir en su víctima el mayor tiempo posible, robando los datos de su interés. Para que esto sea así y no ser detectado, la amenaza debe ser lo más sigilosa posible. Con estas premisas, nuestra amenaza

desplegará su infraestructura y la dejará plenamente operativa antes de comenzar la fase de intrusión en su objetivo.

La infraestructura que requiere la amenaza consta, de forma simple, de dos tipos de elementos: unos, fuera del perímetro de la víctima, y otros, en la propia tecnología de la organización comprometida, lo que denominaremos arquitectura externa y arquitectura interna de la amenaza, respectivamente. Aunque se trata de una visión simplista, esta aproximación puede resultarnos útil para conocer la infraestructura tecnológica que el atacante debe desplegar para lanzar un ataque contra su víctima; no obstante, seamos conscientes de que en el ámbito ciber se avanza muy rápido –quizás demasiado–, especialmente los atacantes, y que en ocasiones la diferenciación entre elementos externos e internos se diluye o, directamente, se modifica por completo. Veremos ejemplos de esto mismo en el presente documento.

Siguiendo nuestra aproximación simplista, los elementos externos son principalmente aquellos dirigidos por un lado a la intrusión y por otro, ya en persistencia, al mando y control y a la exfiltración, mientras que los internos serán equipos comprometidos dentro de la organización que sirven al atacante para mantener su persistencia, adquirir información y procesarla en la víctima, antes de remitirla fuera de los sistemas de esta. Veamos los principales elementos de cada parte de la infraestructura necesaria para la ejecución del ataque.

## 4.1. Arquitectura externa

Desde un punto de vista externo a la víctima comprometida, dentro de la arquitectura del ataque, la APT habrá dispuesto diferentes tipos de recursos, de servidores ajenos a la organización atacada que participan –habitualmente sin saberlo sus propietarios– en el ataque orquestado por la APT: se trata de las infraestructuras de intrusión y de persistencia, compuesta esta última por los servidores de mando y control, responsables de enviar órdenes a los equipos comprometidos en las víctimas de la amenaza y recibir respuestas de estos, y de los servidores de exfiltración, cuyo cometido es recibir

# 5 Ciclo de vida de una APT

Tras el despliegue de la infraestructura necesaria para ejecutar sus actividades convenientemente realizado, la amenaza entra en lo que denominamos el ciclo de vida de la APT, y que no es más que el proceso de ataque en sí; aunque existen varias aproximaciones al ciclo de vida, una muy clara es la denominada *kill chain* ([47]), el camino crítico que seguirá la amenaza para lograr sus objetivos y que se representa con las siguientes fases:

1. **Reconocimiento** de toda la información estratégica, táctica u operativa posible acerca del objetivo fijado: información del objetivo en redes sociales, revelación de información sobre la infraestructura tecnológica, personal, nombres de usuarios, direcciones de correo, etc.
2. Armamento o **militarización** de un objeto para empotrar el código dañino, el arma para "armar" en definitiva al objeto, en especial ficheros ofimáticos –Microsoft Office, PDF…– e incluso imágenes, y convertirlo en un arma troyanizada y empaquetada para enviarse posteriormente al objetivo. Seguramente la traducción de esta etapa por militarización o incluso directamente troyanización –aunque si somos técnicamente estrictos no sería lo mismo– no es la mejor y quizás la idea a transmitir cuando hablamos de "armar" al objeto se entiende mejor en el original inglés: *weaponization*.

ca servicios desde el exterior, para posteriormente acceder a esta zona y robar la información desde Internet, no desde la organización, sin levantar sospechas en los tráficos salientes. Esta zona es, por supuesto, la DMZ corporativa, y uno de los mecanismos más utilizados para exfiltrar es ubicar la información en un sistema públicamente disponible, sobre el que no llame mucho la atención un acceso externo: por ejemplo, un servidor web corporativo.

El mecanismo es sencillo: en lugar de enviar la información a un servidor de exfiltración, el atacante la enviará al servidor web corporativo (por supuesto, en una ruta concreta bajo el *Document Root* de la web), lo que probablemente no generará tráfico externo y por tanto escapará a los ojos de los analistas de seguridad. Posteriormente, desde cualquier sitio de Internet, accederá a esa información a través de algo tan sencillo como un navegador, descargará los datos y enviará instrucciones al malware para que elimine la información ubicada en DMZ. Si el atacante es bueno, que lo es, y ha generado unos archivos en una ruta válida pero poco accedida por humanos –buenos ejemplos son directorios de estilos CSS o directorios de funciones PHP– y además con un nombre que no llame la atención, detectar este acceso anómalo no será, a priori, fácil para un analista, sobre todo porque no estará vigilando esta vía de acceso. A modo de ejemplo, como cuando me lo han dicho soy muy listo, me interesará detectar los objetos menos accedidos de mis servidores web: una vez eliminados falsos positivos, este control me proporcionará información útil, ya que la información exfiltrada será muy poco accedida: seguramente una única vez, por parte del atacante.

# 6 Detección del compromiso

Ya conocemos cómo la amenaza persistente avanzada orquesta su ataque contra nosotros, su objetivo, generalmente con la intención de robarnos información relevante. Conociendo estas acciones, debemos abordar ahora el principal problema al que haremos frente cuando estemos lidiando contra APT: la detección del compromiso. Esta tarea es especialmente compleja por dos motivos principales: la gran cantidad de información que debemos procesar para extraer conclusiones y el nivel de sigilo que las amenazas emplean en sus acciones. Uniendo ambos problemas, la detección es una tarea difícil (se suele decir que detectar el compromiso es buscar una aguja en un pajar), y para abordarla debemos trabajar en múltiples frentes, tanto técnicos como no técnicos, siempre con una premisa: **el atacante está dentro**. No es una hipótesis relativa a un potencial compromiso; nos ha comprometido ya, y ahora "sencillamente" debemos detectarlo. Si la amenaza persistente avanzada va de manera habitual ligada a actividades de inteligencia o, sencillamente, de espionaje, las aproximaciones para detectar y neutralizar estas actividades van ligadas al contraespionaje o a la contrainteligencia.

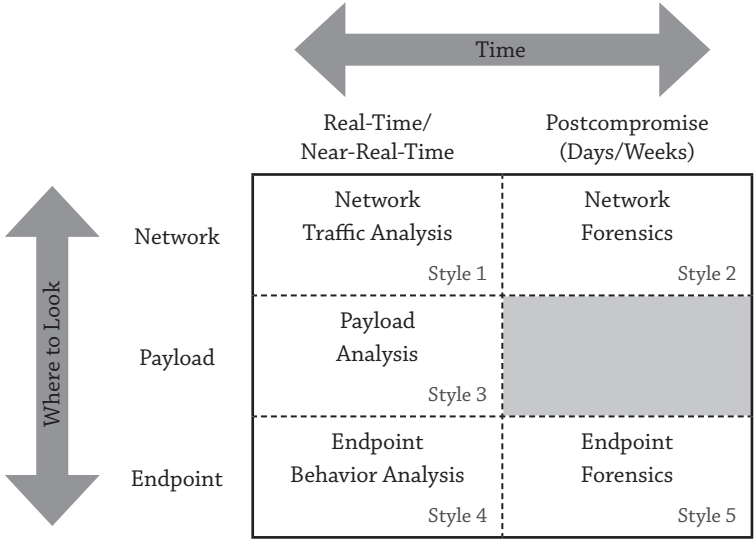
## 6.1. Contrainteligencia

Basándonos en la Ley 11/2002, reguladora del Centro Nacional de Inteligencia, podemos identificar la **contrainteligencia**, entendida como la acción de "prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población".

Evidentemente, las actividades dirigidas a combatir la presencia de amenazas persistentes avanzadas en un entorno pueden y deben englobarse en el concepto de contrainteligencia expuesto; podríamos hablar en nuestro caso de **prevenir, detectar y posibilitar la neutralización de las amenazas**. Con frecuencia hablamos de la detección, identificación y erradicación de APT desde un punto de vista técnico, y este es uno de los principales errores que podemos cometer al hacer frente a estas amenazas: debemos aplicar técnicas de contrainteligencia, que podemos considerar equivalentes a las de inteligencia pero con el objetivo contrario. Por supuesto incluyen el ámbito técnico –igual que antes hablábamos de COMINT o de SIGINT–, pero son mucho más amplias que este, pues, aparte de cubrir estos aspectos, debemos considerar algunos complementarios, como los HUMINT, mediante la infiltración y vigilancia de grupos organizados a través del análisis de fuentes de todo tipo, o los OSINT, mediante el análisis de información públicamente disponible. Además, no debemos restringirnos a la identificación y análisis de las amenazas técnicas, sino que debemos ampliar más nuestros objetivos: las actividades de inteligencia o contrainteligencia deben incluir, por ejemplo, la identificación y análisis adecuados de las capacidades del adversario (herramientas, acuerdos, capacidades, objetivos...), para lo que se hace indispensable determinar no solo cómo trabaja nuestro adversario, sino, por ejemplo, qué información busca.

## 6.2. Tecnologías de detección

Hace unos meses, un estudio de Gartner ([4]) determinaba algo que todos sabíamos: que la defensa en profundidad clásica no era suficiente –aunque por supuesto sí necesaria– para protegernos contra amenazas APT y malware avanzado. En este artículo, se identificaban cinco familias de elementos de protección, clasificados, como muestra la imagen, en función de qué datos se analizan y cuándo se realiza el análisis.




Estas cinco familias de detección son las siguientes:

1. **Análisis de tráfico de red.** Análisis de anomalías y usos indebidos en los flujos de comunicación entre sistemas, tanto externos como internos, en una organización.
2. **Análisis forense de red.** Captura y almacenamiento permanente de todos los paquetes que circulan por la red corporativa, proporcionando capacidades analíticas y estadísticas sobre los mismos como apoyo a la identificación de malware.
3. **Análisis de payload.** Análisis, vía *sandboxing*, de malware en tiempo real, preferiblemente antes de que contamine a la organización víctima.

*derground* donde se maneja información más asociada al malware avanzado o al *exploiting* que a las necesidades de información de un tercero. La operación de infiltrarse en un grupo de nuestro interés sigue la misma estrategia que una APT, en este caso humana, con su reconocimiento, intrusión y persistencia correspondientes.

Las operaciones HUMINT clásicas son sin duda una actividad destacada en los servicios de todo el mundo, que siempre han tratado, con mejor o peor suerte, de infiltrar a sus agentes en países, zonas, grupos... de interés, y las técnicas, herramientas o procedimientos utilizados son, en algunos casos, incluso públicos. En el ámbito CYBINT se mantienen algunas de las claves de la infiltración clásica, por ejemplo las psicológicas, pero con diferencias muy notables entre ambas aproximaciones. La más importante es, sin duda, la relativa a la seguridad de las personas: mientras que una persona que obtiene información en un país hostil corre un riesgo físico obvio, ese riesgo se reduce a su mínima expresión si dicha adquisición se realiza de forma remota.

Como en cualquier APT, infiltrar a una persona en un grupo de interés tendrá sus correspondientes fases de reconocimiento, intrusión y persistencia, y, dentro de esta última, la adquisición y exfiltración de información. En la etapa de **reconocimiento**, deberemos analizar a nuestro objetivo para conocerlo de manera que podamos identificar dónde está la información que necesitaremos –o quién la maneja–, cuál es la estructura organizativa, cómo opera... y, por supuesto, cuál es la vía de infiltración más apropiada para nuestros intereses (rapidez, persistencia...).

Tras haber analizado nuestro objetivo, debemos **infiltrarnos** en él. Por supuesto, la técnica de intrusión dependerá tanto de nuestro propio objetivo como de los resultados obtenidos en la etapa anterior, en el análisis del mismo. Podemos hablar incluso de una intrusión física (por ejemplo, en el caso de una empresa de nuestra competencia, donde muchas veces una simple entrevista de trabajo o, directamente, la compra de información a un empleado pueden ser el mejor método), pero estas acciones quedan fuera de nuestro ámbito. La intrusión remota, telemática, es la habitual si nuestros objetivos son "virtuales" (por ejemplo, grupos *hacktivistas*, extremistas, *underground*... organizados a través de

# 7 Gestión del incidente

Ya sabemos cómo funciona una amenaza persistente avanzada y, más importante, conocemos algunas de las aproximaciones –seguro que hay más– habituales para su detección; debemos, por tanto, ser capaces de detectar el compromiso por parte de una APT, o al menos de seguir algunas directrices para intentar lograr este objetivo. Imaginemos que lo logramos, que detectamos un compromiso en nuestra organización, ¿qué haríamos en ese momento?, ¿cómo actuaríamos?, ¿a quién acudiríamos a pedir ayuda, si es que la necesitamos? Debemos, en este punto, gestionar el incidente asociado a este compromiso, con consideraciones que en otro tipo de incidentes no son de aplicación: no cometamos el error habitual de considerar a la amenaza como un código dañino, ya que una contaminación de malware se contiene, se erradica... pero unas necesidades de información NO. Dicho de otra forma, tengamos presente que el atacante volverá, antes o después, a buscar la información de su interés que pueda estar bajo nuestro control, y debemos prepararnos para ese momento futuro... o inmediato.

## 7.1. Introducción

Los códigos de buenas prácticas comúnmente aceptados para la gestión de incidentes, al menos en cuanto a las grandes fases de la gestión, tienen obviamente su reflejo en la gestión de incidentes asociados a APT; no obstante, una amenaza persistente avanzada debe ser gestionada de una manera más amplia que un incidente habitual, ya que por norma se trata de ataques dirigidos con un objetivo muy concreto y que exceden al ámbito puramente técnico. Sin duda, uno de los errores habituales a la hora de gestionar ataques APT es considerar la amenaza exclusivamente como el malware asociado a ella; tal y como se ha indicado, el malware debe considerarse la bomba que el atacante nos arroja, pero para lanzar esa bomba hace falta una infraestructura, unos conocimientos, unas capacidades... que van mucho más allá no solo del propio malware, sino de la tecnología en sí misma. Debemos contemplar un ataque APT como una capacidad de un servicio extranjero, una empresa de nuestra competencia o un grupo organizado, y además de cualquier aspecto técnico a analizar o gestionar durante un incidente asociado a estas amenazas, debemos ser capaces de responder, al menos, las siguientes cuestiones, casi idénticas a las 5W (*Who*, *When*, *What*, *Why* y *How* –el *Where* es menos importante–).

### ¿Quién?

¿Cuál es el origen de la amenaza? ¿Qué país, grupo, organización... nos está atacando? Aunque por supuesto trabajaremos siempre con hipótesis, dado que es realmente imposible identificar el origen de la amenaza, al menos debemos tratar de acotar con una probabilidad significativa dicho origen. Dicho de otra forma, si identificamos un malware con lenguaje cirílico, que utiliza conexiones RDP con el teclado en ruso y que incluso tiene, en el análisis del espécimen, nombres propios de Europa del Este, estaremos casi seguros de que su origen es Rusia. Por supuesto, podría tratarse de otro país que haya utilizado estas configuraciones para ocultar el verdadero origen de la amenaza, pero este extremo rara vez podremos saberlo.

| Etapas | Iniciativas | Análisis |
|---|---|---|
| Identificación | Análisis de los registros de conexión a C&C (proxy) | La organización debe disponer de proxy; en caso contrario será necesaria una adquisición pasiva. |
| | Identificación de características de la exfiltración | Determinación de las posibles anomalías (métodos, tipos, etc.) asociadas al malware.<br>Identificación de nuevos servidores dañinos. |
| | Identificación de equipos comprometidos | ¿Quién ha generado tráficos contra servidores dañinos? |
| | Análisis de un equipo comprometido (forense y artefactos) | Identificación de mecanismos de persistencia, comunicación lateral, etc. del malware. |
| | Despliegue de capacidades de vigilancia pasivas | ¿Qué hemos aprendido de nuestro análisis previo? |
| Respuesta | Corte y monitorización de comunicaciones con servidores externos | Elementos de seguridad perimetral. |
| | Intervención de equipos comprometidos | Adquisición de medios, apagado y sustitución. |
| Lecciones aprendidas | Análisis de los equipos | Análisis forense.<br>Análisis de artefactos. |
| | Vigilancia del entorno comprometido | Nuevas reglas de anomalía, listas negras, mutaciones, etc. |
| | General | Capacidades de identificación.<br>Despliegue de salvaguardas.<br>Evaluación de salvaguardas.<br>Valoración general. |

# 8 Otra vuelta de tuerca

## 8.1. Sabotaje

Hasta ahora, tal y como hemos indicado al principio de este documento, nos hemos focalizado en el ámbito de las amenazas persistentes avanzadas orientadas al robo de información, al ciberespionaje en cualquiera de sus facetas. No obstante, hemos hablado de APT como Stuxnet, cuyo objetivo no era robar información de sus víctimas, sino sencillamente el sabotaje de sus procesos –en este caso, el correspondiente al enriquecimiento de uranio con fines nucleares–. Este tipo de amenazas no son las más habituales –al menos que hayan salido a la luz– y, por lo avanzado de sus capacidades, su orquestación debe estar a priori reservada exclusivamente a estados.

Casos como Stuxnet sobrepasan el espionaje puro, en cuanto a robo de información, y llegan a lo que podríamos llamar guerra, terrorismo en algunos casos –no entraremos ahora en la polémica– o, simplemente, sabotaje, todos estos términos con o sin el prefijo *ciber*. Estas acciones nos asustan a todos los niveles, más incluso que las asociadas a operaciones de interceptación de comunicaciones, ya que cuando alguien sabotea un entorno

y que pueda ser de interés para él y permaneciendo activo o durmiente durante largos periodos de tiempo. En este caso, es una persona la que sustituye al malware en la amenaza persistente avanzada. Hemos visto como tratar de identificar una contaminación de malware en la organización pero, ¿cómo detectar la amenaza humana? Para identificar un posible *insider,* debemos tratar de realizar una monitorización de personas, siempre en los marcos legales correspondientes, determinando así el **riesgo humano** de nuestra organización.

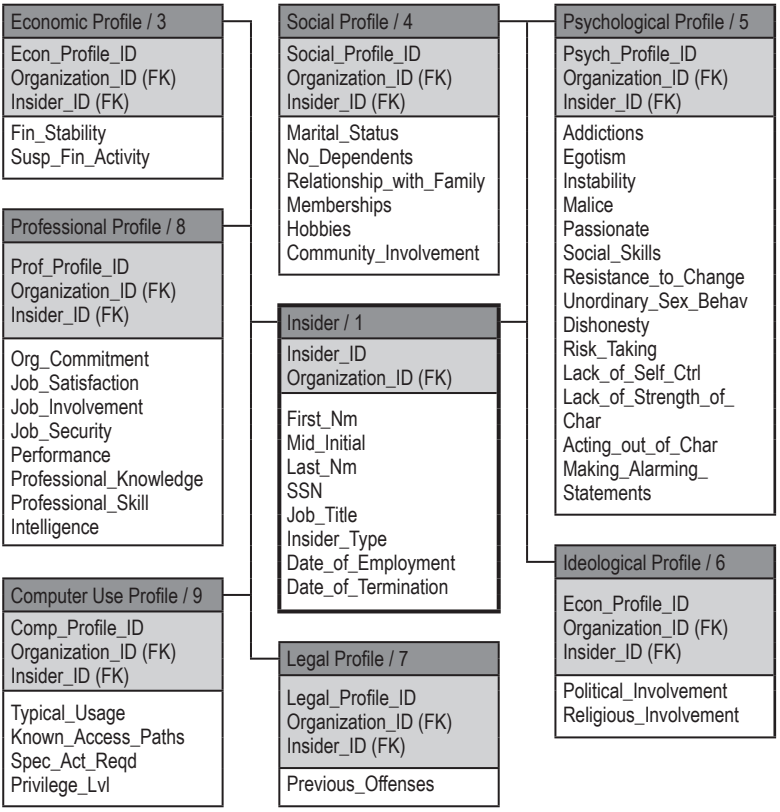
La vigilancia del riesgo humano o la monitorización de personas son habitualmente temas muy delicados desde muchos puntos de vista. Con las consideraciones que correspondan y hablando estrictamente de seguridad, debemos recordar que las personas pueden introducir riesgos muy elevados en cualquier organización, riesgos que interesa identificar y por supuesto mitigar. El paso previo al tratamiento de riesgos es, como siempre, su análisis, y para analizar estos riesgos debemos ser capaces de determinar amenazas, probabilidades e impactos que pueden causar las personas de la organización, lo que habitualmente denominamos *insiders*.

La identificación de las amenazas derivadas del factor humano son claras: todas las englobadas bajo el paraguas de amenazas corporativas (errores), las derivadas de actividades sociales (accidentes) y las derivadas de actividades antisociales (delitos). En este último apartado es donde podríamos ubicar, en el contexto de inteligencia que estamos manejando en el presente documento, a los *insiders* más preocupantes. Igualmente, la estimación de impactos asociados a estas amenazas también suelen estar más o menos clara, y estará –con toda probabilidad– en la parte más alta de la escala que queramos utilizar en nuestro análisis: el *insider* nos puede causar un daño enorme. Siendo así, teniendo más o menos claras las amenazas y los impactos derivados del riesgo humano, ¿dónde está entonces lo que más nos interesa? En la medida de la probabilidad, como casi siempre.

Para analizar probabilidades a la hora de hablar del riesgo humano, una aproximación muy interesante es la presentada en [41]. La idea resumida y simplificada es que cualquier persona

está modelizada por una serie de perfiles que la definen, perfiles afectados además por una serie de condiciones de contorno (relaciones, privilegios, motivaciones...) y de eventos externos o internos a la organización que pueden provocar cambios sustanciales en el perfil de una persona (un cambio de estado civil, un ERE, la muerte de un familiar...). Si somos capaces de vigilar esto de una u otra forma, seremos capaces de estimar probabilidades y, por tanto, de identificar posibles riesgos derivados de las personas de la organización.

Ilustración 1.
*Perfiles de modelización de personas para identificación del riesgo humano*



el tráfico en la entrada/salida a Internet para buscar anomalías –por ejemplo, en HTTP, SMTP y DNS–, tenemos que evitar a toda costa generar estas anomalías. Ya hemos hablado con anterioridad del movimiento externo sin tráfico saliente como una alternativa válida. ¿Y ahora? Si queremos evitar que alguien analice los flujos de información en busca de patrones de movimiento externo, podríamos tratar de eliminar directamente la generación de tales flujos.

¿Cómo podemos eliminar la generación de flujos en los tráficos salientes que puedan ser analizados, por ejemplo con la aproximación que hemos seguido en este documento, y por tanto ser detectados? Seguro que existen muchas aproximaciones, y una de ellas es un modelo de exfiltración que podríamos denominar *multicast,* o directamente *broadcast*, una transmisión de información desde la víctima a muchos destinos... o a todos. Pensémoslo: en lugar de utilizar servidores externos concretos –contra los que se generarían los famosos flujos de datos a analizar en busca de anomalías– lastramos ciertas comunicaciones con el exterior con la información a exfiltrar. Cuando salen los datos, en algún punto intermedio antes de llegar a su destino, se revisa cada paquete en busca de la información lastrada –robada– y, en caso de encontrarla, se extrae del tráfico y se reenvían las tramas "limpias".

Imaginemos que somos un país con capacidades de interceptación de las comunicaciones nacionales, incluyendo las entrantes de otros países (por supuesto, algo muy difícil, si no imposible, de imaginar). Si fuera así, podríamos diseñar un malware que, una vez en su objetivo, identificara los paquetes de red que vengan dirigidos hacia nuestro país –tráficos legítimos, por supuesto– y en cada uno de ellos añadiera discretamente cierta información robada. Al llegar a la infraestructura nacional, y recordando esas hipotéticas capacidades de interceptación, se podrían seleccionar los paquetes que llegasen lastrados y, por ejemplo, en grandes *routers* troncales convenientemente implantados, extraer ese lastre y entregarlos limpios a su destino.

Capacidades como la descrita aquí están al alcance de muy pocos. En primer lugar, es necesario el control de electrónica de red que podríamos denominar troncal, en mayor o menor medida,

# 9 Conclusiones

Las amenazas persistentes avanzadas son procesos dañinos orquestados por gobiernos, estados, grupos organizados, empresas..., en definitiva, de actores atacantes con muchos recursos (económicos, humanos, materiales...), mucho conocimiento y, lo más peligroso, mucho interés en sus víctimas –para ser exactos, en la información que estas manejan–. La capacidad dañina comprende, por supuesto, el malware utilizado para el robo de información, pero también aspectos puramente de inteligencia o que, al menos exceden con mucho el ámbito técnico. Recordemos el símil del bombardero y la bomba que indicábamos al principio, y hagamos referencia al término **CYBINT** que también introducíamos y que suele basarse, principalmente, en SIGINT/COMINT, HUMINT, TECHINT y OSINT. La actividad de la amenaza se engloba en un ámbito de inteligencia, en especial de adquisición de información, y de esta forma debemos entenderla, detectarla y neutralizarla.

Ser víctima de una amenaza persistente avanzada es sencillo: basta con manejar información que pueda interesar a un tercero con recursos por su interés político, militar... o simplemente comercial. ¿Quién puede serlo? Cualquier organización, pública o privada, que maneje información política, financiera, tecnológica avanzada, militar, diplomática, geográfica, de seguridad, energética... En definitiva, muchas de las empresas u organismos en los

que trabajamos pueden ser víctima de una amenaza persistente avanzada, por uno u otro motivo, con lo que insistimos: es muy fácil ser el objetivo de una amenaza. Y, muy probablemente, esa amenaza tendrá detrás a un estado o a un grupo que quizás está apoyado por un estado; son los actores principales del panorama, ya que disponen de capacidades y de interés.

Por supuesto, defenderse del ataque de la amenaza no es tan sencillo como convertirse en su víctima o, al menos, en su objetivo. Pensemos en las capacidades de nuestros atacantes y a esas capacidades unámosle un aspecto muy significativo: la persistencia. El objetivo de la amenaza es persistir en el robo de información cuanto más tiempo mejor, lo que implica garantizar que la organización, en el tiempo, permanece contaminada sin ser detectada, por lo que el malware desplegado será lo más sigiloso posible: un atacante que entre en nuestra red, borre todos los servidores e inutilice los elementos de comunicaciones nos podrá hacer mucho daño, pero desde luego no es una APT. Este malware sigiloso, avanzado o no, se moverá lateralmente por la red comprometida para adquirir y procesar la información de interés, y se comunicará con el exterior para enviar la información robada –exfiltración– o para recibir órdenes de los servidores de mando y control, C2. Todo ello de manera discreta, sin llamar la atención de un equipo de defensa o análisis, para garantizarse el mayor nivel de persistencia en la víctima.

Con este objetivo de persistencia, detectar una APT que haya comprometido nuestro entorno es complejo. Muchas veces las formas realmente eficaces pasan por aproximaciones HUMINT, mucho más que las capacidades técnicas de vigilancia, pero lo que queda claro es que detectar, identificar y gestionar adecuadamente amenazas avanzadas debe ser una actividad planificada y ejecutada en múltiples frentes, desde los técnicos (SIGINT o TECHINT) hasta los no técnicos, como HUMINT. Debemos aplicar una filosofía de contrainteligencia y trabajar en esos múltiples frentes para detectar el compromiso y, a partir de dicha detección, gestionar adecuadamente el incidente sufrido en cada caso.

A la hora de hablar de la gestión del incidente, debemos evitar en especial el error más común cuando hablamos de APT: consi-

# 10 Anexo: Anomalías HTTP

## 10.1. Resumen

El tráfico HTTP –o equivalentemente HTTPS–, el tráfico web, es uno de los mecanismos de exfiltración más utilizado por las amenazas dirigidas que tratan de robar datos, además de constituir el esquema de C&C por excelencia. Estos tráficos de salida estarán casi siempre permitidos en la organización, sus registros –si los hay– serán muy voluminosos y, por tanto, un atacante lo tiene fácil para ejecutar y camuflar comunicaciones con servidores C&C o de exfiltración. Si a partir de los registros de navegación generados somos capaces de inferir anomalías, podremos llegar a detectar estos tráficos maliciosos y, por tanto, identificar amenazas activas en nuestro entorno y responder ante ellas adecuadamente.

## 10.2. Introducción: Detección de anomalías

En 1980 James P. Anderson publicaba el informe técnico *Computer security threat monitoring and surveillance* ([35]), considerado

| Campo | Tipo de variable | Comentarios |
|---|---|---|
| TIME | Cuantitativa | Serie temporal |
| DURATION | Cuantitativa | |
| CLIENT | Cualitativa | |
| RESULT | Cualitativa | |
| BYTES | Cuantitativa | |
| METHOD | Cualitativa | |
| URL | Cualitativa | Cadenas de texto condicionadas |
| RFC931 | Cualitativa | |
| HIERARCHY | Cualitativa | |
| TYPE | Cualitativa | |

Para las variables **cuantitativas**, aquellas que pueden ser expresadas con números, podemos obtener la **distribución** de los datos que encontramos en uno o más ficheros de log del proxy (salvo en el caso de la marca de tiempo, que veremos más adelante); esto nos permitirá determinar los valores atípicos (*outliers*) para la duración de las conexiones y para la cantidad de bytes transferidos en cada una de ellas, identificando así conexiones sospechosamente lentas (o rápidas) o transferencias sospechosamente ligeras (o voluminosas). El siguiente script obtiene la distribución de un campo cuantitativo sobre un fichero de log[4]:

```
#!/bin/sh
# This script gets field distribution, in format: field,hits
# $1: Field to analyze
# $2: Log file
for i in `awk -v f=$1 '{print $f}' $2 | sort -n | uniq`; do
        export i
        k=`awk -v f=$1 '$f==ENVIRON["i"] {print $0}' $2 | wc -l`
        echo $i,$k | sed s/" "//g
done
```

4 Los scripts presentados en este documento deben ser considerados únicamente **pruebas de concepto**; no están optimizados ni, probablemente, ajustados a las mejores prácticas de programación, por no considerarse estos aspectos relevantes en el presente trabajo.

# 11 Anexo: Acrónimos

**AET** (*Advanced Evasion Techniques)*. Técnicas de evasión avanzadas.

**APT** (*Advanced Persistent Threat*). Amenaza persistente avanzada.

**AVT** (*Advanced Volatile Threat*). Amenaza volátil avanzada.

**C2, C&C** (*Command & Control*). Sistemas de mando y control del malware, generalmente entornos comprometidos por los atacantes, sin relación directa con ellos.

**CNA** (*Computer Network Attack*). Ataque de redes y sistemas (subdivisión de CNO).

**CND** (*Computer Network Defense*). Defensa de redes y sistemas (subdivisión de CNO).

**CNE** (*Computer Network Exploitation*). Explotación de redes y sistemas (subdivisión de CNO).

**CNO** (*Computer Network Operations*). Operaciones de redes y sistemas.

**COMINT** (*Communications Intelligence*). Inteligencia de Comunicaciones.

**CYBINT** (*Cyber Intelligence*). Ciberinteligencia.

**DLP** (*Data Loss Prevention*). Soluciones para detectar la fuga de información, especialmente voluntaria, de una organización.

**DNS** (*Domain Name System*). Sistema de nombres de dominio, que asocia nombres y direcciones IP.

**FCFA** (*First Cut Forensic Analysis*). Análisis inicial de un sistema sospechoso para determinar si la probabilidad de compromiso es significativa o no.

**FFCCSE**. Fuerzas y Cuerpos de Seguridad del Estado.

**FQDN** (*Fully Qualified Domain Name*). Nombre de sistema unido a nombre de dominio.

**FTP** (*File Transfer Protocol*). Protocolo de transferencia de ficheros.

**GIR**. Grupo de Intervención Rápida.

**HTTP** (*Hyper Text Transfer Protocol*). Protocolo de transferencia de hipertexto, usado habitualmente para navegación web.

**HTTPS** (*Secure Hyper Text Transfer Protocol*). HTTP seguro mediante técnicas de cifrado.

**HUMINT** (*Human Intelligence*). Inteligencia de fuentes humanas.

**IDS** (*Intrusion Detection System*). Sistema de detección de intrusos.

**IOC** (*Indicator of Compromise*). Indicador de compromiso.

**IPS** (*Intrusion Prevention System*). Sistema de prevención de intrusiones.

**IRC** (*Internet Relay Chat*). Protocolo de comunicación en tiempo real, basado en texto plano.

**ISAC** (*Information Sharing and Analysis Center*). Centros de intercambio de información estadounidenses.

**LMS** (*Longest Meaningful Substring*). Subcadena más larga con significado dentro de una cadena de texto.

**MILDEC** (*Military Deception*). Decepción, engaño al contrario en el ámbito de operaciones militares.

**OSINT** (*Open Source Intelligence*). Inteligencia de fuentes abiertas.

**P2P** (*Peer to Peer*). Protocolo de intercambio de información punto a punto.

**PAN** (*Personal Area Network*). Red de área personal.

**P&V** (*Patches & Vulnerabilities*). Parches y vulnerabilidades (habitualmente referido al procedimiento operativo).

# 12 Referencias


[1] CIA Factbook on Intelligence, 2002.

[2] Ley 11/2002, reguladora del Centro Nacional de Inteligencia.

[3] Ramón Pinuaga, Miguel Ángel Hernández. *Operaciones APT famosas*. http://www.areopago21.org/2014/04/operaciones-apt-famosas.html

[4] Gartner. *Five Styles of Advanced Threat Defense*. Agosto, 2013.

[5] Wikipedia. *List of intelligence gathering disciplines*. http://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines

[6] Nikos Virvilis, Dimitris Gritzalis. *What we did wrong in APT detection?* 2013 International Conference on Availability, Reliability and Security.

[7] Office of the Director of National Intelligence. *Intelligence Community Information Sharing Strategy*. 2008.

[8] Eric Cole. *Advanced Persistent Threat. Understanding the danger and how to protect your organization*. Elsevier, 2013.

[9] CIH. *The Malware Encyclopedia*. http://malware.wikia.com/wiki/CIH

[10] GData Security Labs. *Uroburos: highly complex espionage software with Russian roots*. Febrero, 2014.

[11] Kaspersky. *Unveiling "CARETO" - the masked APT*. Febrero, 2014.

[12] Mandiant. *APT1. Exposing one of China's Cyber Espionage Units*. Febrero, 2013.

[13] ZScaler. *Alleged APT Intrusion Set: "1.php" Group*. 2011.

[14] CrySyS. *Duqu: a Stuxnet-like malware found in the wild*. Laboratory of Cryptography and System Security. Budapest University of Technology and Economics. Octubre, 2011.

[15] Kaspersky. *The NetTraveler*. Junio, 2013.

[16] Dmitri Alperovitch. *Revealed: Operation Shady RAT*. McAfee. Agosto, 2011.

[17] Cliff Stoll, *The cuckoo's egg: tracking a spy through the maze of computer espionage*. Pocket books, 1989.

[18] Cassidian CyberSecurity Blog. *APT Kill chain – Part 3: Reconnaissance*. http://blog.cassidiancybersecurity.com/tag/APT

[19] George Pajari. *USB Flash Storage Threats and Risk Mitigation in an Air-Gapped Network Environment*. CANSECWEST Vancouver 2014.

[20] Daniel Crowley. *Jack of all Formats*. Trustwave SpiderLabs, 2010.

[21] Securelist. *Full analysis of Flame's Command & Control servers*. Septiembre, 2012. http://securelist.com/blog/incidents/34216/full-analysis-of-flames-command-control-servers-27/

[22] Peter Mattis. *The analytic challenge of understanding Chinese Intelligence Services. Studies in Intelligence*. Vol 56, No. 3. Septiembre, 2012.

[23] Ptacek, Newsham. *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*. Enero, 1998.

[24] NATO. *NATO glossary of terms and definitions. AAP-6 (2008)*. NATO Standarization Agency. 2008.

[25] Karl de Leeuw, Jan Bergstra (Ed.). *The history of Information Security. A Comprehensive Handbook*. Elsevier, 2007.

[26] INSA. *Operational levels of cyber intelligence*. Intelligence and National Security Alliance. Cyber Intelligence Task Force. Septiembre, 2013.