Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación

Amenazas Avanzadas Persistentes
- APT -

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-4801-131106*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*06/11/2013*
N° de Páginas	*1 de 21*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar al personal de la Junta de Andalucía información sobre un tipo de amenazas que conforman una de las principales preocupaciones en ciberseguridad del momento. Hablamos de las Amenazas Persistentes Avanzadas o APTs.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía y al público en general. En éste se proporciona una visión general sobre las Amenazas Persistentes Avanzadas. Se describirán sus principales características, qué las diferencian de cualquier otro tipo de amenaza común, algunos de los métodos usados por los ciberdelincuentes para llevarlas a la práctica, y recomendaciones de seguridad para la protección de nuestro entorno.

4 INTRODUCCIÓN

"Cuesta aceptar que sea necesario crear un plan plurianual para descubrir quiénes son nuestros enemigos y cómo nos van a atacar. Es posible que, si nos limitamos a observar los datos trimestrales, no se aprecien pérdidas. Las consecuencias de un ataque podrían materializarse después de años, cuando de repente una empresa del otro extremo del mundo se convierta en el líder de nuestro sector porque ha aprovechado nuestra inversión en investigación y desarrollo".

Tim McKnight, vicepresidente y director de seguridad de la información de Northrop Grumman.

Desde hace relativamente pocos años se ha observado una notable evolución en la naturaleza de las amenazas conocidas hasta el momento. Empezó a observarse cómo pasaban de ser amenazas aisladas y dispersas, a ser de gran complejidad y sofisticación, persistentes, con objetivos muy específicos y ataques diseñados a medida. Surge así un nuevo término para referirnos a una serie de amenazas contra la seguridad extremadamente peligrosas: **Amenazas Persistentes Avanzadas** (Advanced Persistent Threats). Comúnmente se hace referencia a éstas por sus siglas en inglés: **APT** ó APTs.

En las APTs es característico su nivel de eficacia. Son amenazas muy sofisticadas, que requieren de una gran inversión de tiempo para su preparación, lo cual, junto a la persistencia con la que son llevadas a cabo, les brinda altas probabilidades de éxito y capacidad de superar todo tipo de medidas de protección.

Las expectativas de sus ejecutores suelen ser realmente elevadas. Se planifican a largo plazo. No esperan conseguir un beneficio rápido y a corto plazo (como pudieran buscar otros tipos de ataques masivos), sino que prefieren permanecer desapercibidos y constantes hasta alcanzar su objetivo, sin importar el tiempo que requiera conseguirlo. Las víctimas rara vez saben que son objetivos y desconocen el origen, alcance o autoría de dicho ataque.

En general, por su historial, se asocian a ataques contra objetivos de gran importancia, entre los que destacan el espionaje corporativo o entre gobiernos, las infraestructuras críticas, objetivos políticos y militares,

afectando a sectores tan diversos y críticos como el gubernamental, financiero, tecnológico, centros de investigación, etc.

Algunas APTs que han tenido una gran impacto en sus víctimas han sido la Operación Aurora, en la que varias multinacionales (Google, Adobe, ...) sufrieron un robo importante de información confidencial, o Stuxnet, en la que se desarrolló código malicioso contra infraestructuras críticas para el control y monitorización de procesos industriales (SCADA). Han existido muchas otras como Red October, APT1, Operación Shady RAT ó Flame.

Los principales sectores afectados, viendo las APTs pasadas, han sido gobiernos, grandes empresas y **entidades públicas**.

5 APT's vs AMENAZAS COMUNES

Definir qué es una APT puede resultar tedioso. Se trata de un concepto complejo para el que una definición muy concreta podría ser insuficiente.

Partiendo de una definición simple de **amenaza**, ésta se entiende como un hecho o circunstancia que puede provocar un daño sobre algún bien tangible o intangible. Por **persistente** podríamos entender que se tratan de amenazas que perduran en el tiempo. Y por **avanzada** podemos pensar que para su ejecución se usan técnicas complejas o con ciertos componentes de ingenio.

Es muy posible que tras la lectura de las definiciones anteriores aun no hayamos conseguido visualizar la idea tras el concepto APT.

Intentemos arrojar un poco de luz sobre esto. Iremos por partes.

- **APT (Amenaza / Threat)**

Pensemos en un ejemplo de una amenazas muy conocida: un phishing. Ciertamente, es una amenaza. ¿Debe considerarse que es una APT? No tiene por qué. Y seguramente por sí sólo, un ataque de phishing aislado no se considere una APT, pero podría ser usado en alguna fase de una APT.

Un phishing, un malware o un ataque cualquiera podrían formar parte de una APT, si están especialmente pensados para llevar a cabo un objetivo dentro de la estrategia principal de la amenaza. Debe ser, por tanto, considerado como una herramienta que podría usarse, o no, en una APT.

Se deben considerar aquellas amenazas que buscan **objetivos muy específicos**. En general suelen también asociarse a objetivos de alto valor (espionaje entre corporaciones o gobiernos, ciberterrorismo, ataques a infraestructuras críticas, ...).

- **APT (Persistente)**

Imaginemos que nuestra organización ha sufrido un ataque de DDoS (denegación de servicio distribuída) que ha durado varios días, ¿es una APT? De nuevo, no tiene por qué.

Que un ataque se prolongue en el tiempo no implica que tenga que ser considerado como APT. Es más acertado considerar, en vez del tiempo que dura el ataque o la amenaza, el tiempo que sus autores han necesitado invertir para poder llevarla a cabo. Desde su preparación y planficación, hasta su ejecución y obtención del objetivo final.

El concepto de persistencia, en las APTs, se aplica en varios sentidos:

- Insistencia de los atacantes por conseguir el objetivo. Van probando todas las posibilidades hasta ir consiguiendo sus objetivos.
- Actualización continua de los métodos de ataque e intrusión. Si algo no funciona, se cambia de estrategia.
- Y como consecuencia, la amenaza en su conjunto suele durar bastante tiempo.

Este tipo de amenazas se conciben como un proyecto y se planifican a medio o largo plazo.

- **APT (Avanzada)**

Al concebirse como un proyecto, requieren de un equipo de personas altamente cualificadas detrás. Los actores que participan en este tipo de amenazas suelen estar muy capacitados, motivados, organizados y bien financiados.

Las técnicas para llevar a cabo la intrusión serán especialmente diseñadas para el objetivo en cuestión y se valdrán de tecnologías y métodos de todo tipo:

- Es característico de las APT el uso de malwares dedicados, programados para cumplir un objetivo muy específico en el ataque.
- Uso de exploits zero-days o ataques de día cero. Aprovechan vulnerabilidades desconocidas hasta la fecha, pero presentes en el objetivo.
- Técnicas avanzadas de ingeniería social.

- **Recopilemos**

A partir de estas ideas podemos recopilar una serie de **características comunes a las APTs** y que nos permitirán dibujar un marco aproximado de lo que son.

- Objetivo específico.
- Pensadas para su ejecución a medio/largo plazo.
- Fase de recopilación previa de información profunda.
- No buscan el beneficio inmediato.

- Se enfocan como un proyecto.
- Ataques diseñados específicamente para el objetivo
  - Malware diseñado a medida.
  - Ataques especialmente diseñados para el objetivo.
  - Aprovechamiento de vulnerabilidades específicas de la organización .
  - Ingeniería social avanzada
- Equipo para llevarla a cabo muy preparado y motivado.
  - Contratación de especialistas.

6 CICLO DE VIDA

Echando la mirada hacia atrás, a partir del estudio de APTs conocidas, se han observado una serie de elementos comunes. A continuación se detallan las fases más importantes y que en la gran mayoría de APTs han estado presentes. Esto nos será de ayuda para dibujar un posible escenario de APT.

6.1 Estudio de la víctima

Una de las características más importantes en una APT es la gran cantidad información sobre el objetivo que debe recogerse antes de proceder a atacarlo. El esfuerzo invertido en esta fase será un factor clave para el éxito o fracaso.

Algunas tareas que deben cumplirse en esta fase son:

- **Definición del objetivo**: "¿Quién es y qué queremos de él?
- **Creación del equipo de trabajo**.
- **Obtención de información útil**: Cualquier información específica del objetivo que pueda resultar útil.
  - Información de la estructura y el entorno corporativo.
  - Empleados, socios y relaciones.
  - Comportamiento corporativo.
  - Eventos (cursos, conferencias, congresos, citas, reuniones, etc.).
  - Arquitectura TI.
  - Controles de seguridad físicos y lógicos.
  - (...)
- **Definición de posibles vías de entrada.**
- **Recopilación y desarrollo de herramientas para llevar a cabo el ataque.**
  - Herramientas de auditoría de seguridad.
  - Malwares a medida.
  - Exploits a medida.

- Planes de ingeniería social.
- Sitios web fraudulentos.
- (...)

- **Pruebas de detección y evasión.**

En una APT, al final de esta fase se debe disponer de lo siguiente:

- Información detallada de la organización objetivo.
- Objetivo final conocido por todo el equipo.
- Plan detallado de actuación.
- Herramientas necesarias.
- Actores que van a intervenir.
- Plan de evasión.

6.2 Acceso inicial

Los atacantes ya han realizado un estudio en profundidad de su objetivo, han definido la estrategia, han terminado de recopilar e implementar las herramientas que van a usar, y concretar los tiempos del ataque. Ahora se trata de dar una primera "pisada" sobre el terreno objetivo.

En la fase anterior se debe haber diseñado un plan que recoja todas las posibles vías de entradas a la organización objetivo y la viabilidad de cada una. Esforzándose por no ser detectados, el equipo de trabajo irá probando una tras otra, todas las posibles vías de entrada que se han recopilado en la fase inicial.

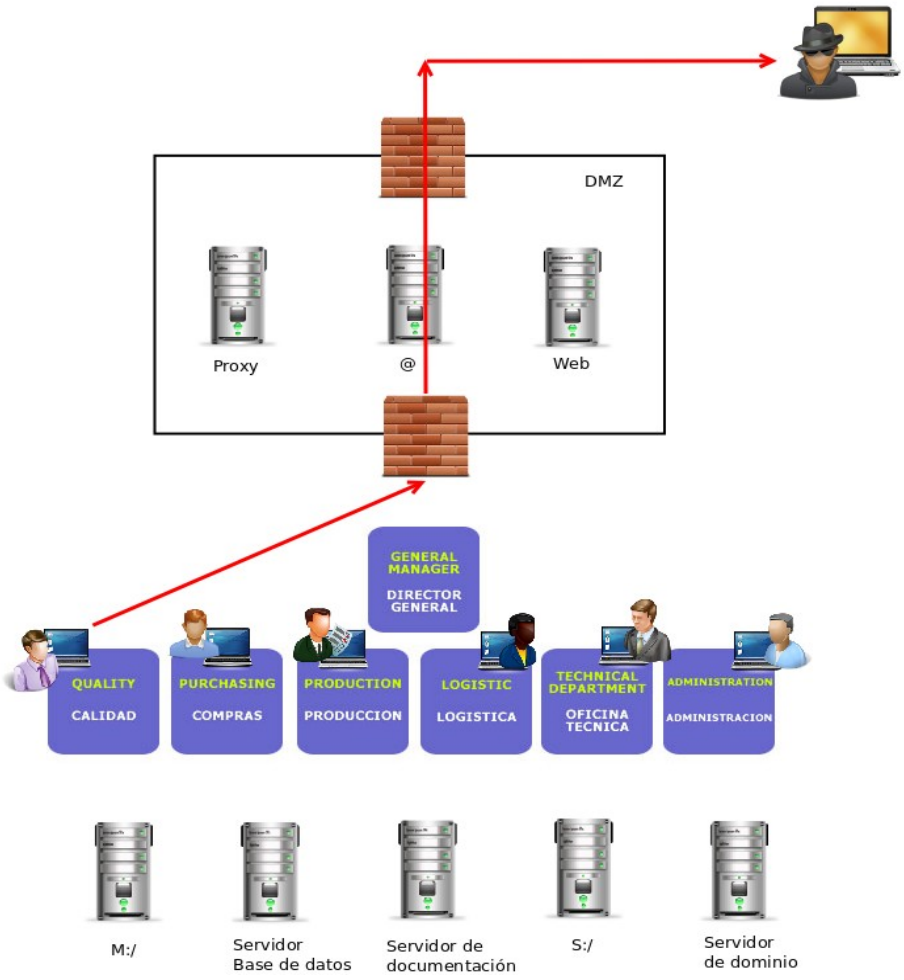
Podemos observar en esta fase una primera demostración de persistencia ya que los atacantes intentan acceder por cada una de las vías de entrada e irán determinando cuales son viables y cuales no, cuales se adecúan mejor a los objetivos definidos, cuales permiten un acceso más sigiloso, etc.

Normalmente se intentarán acceder por zonas poco vigiladas o poco importantes como equipos de usuarios comunes, impresoras o redes de ofimática.

Una técnica muy común usada para lograr el acceso inicial es el phishing dirigido ó **SPEAR PHISHING** ("pesca con arpón"). Aunque lo veremos con más detalle en secciones posteriores, a grandes rasgos es un phishing diseñado específicamente para quién lo va a recibir. Se recopila información de la víctima, su actividad en Internet, si participa en algún foro, sus intereses, amigos, familiares, etc. Como podrán imaginar, el grado de éxito aumenta cuanto más familiar llegue a resultar el correo electrónico a la víctima.

El objetivo es que una vez se gane la confianza, la víctima ejecute realice algún tipo de acción (abrir un archivo, acceder a una web, etc.) y se logre comprometer el equipo.

Una vez comprometido el equipo de la víctima, una de las cosas que podría hacer es obligar a conectarse involuntariamente a un equipo remoto bajo el control de los atacantes. Es decir, se realizará una conexión desde dentro de la organización hacia un servidor externo malicioso. Esto se muestra en el siguiente gráfico.



Las herramientas usadas para conseguir este tipo de objetivos se denominan RAT (Remote Administration Tool). Permiten controlar un equipo remotamente una vez que éste ha iniciado una conexión con el equipo externo. Un ejemplo de esta herramienta es Poison Ivy.

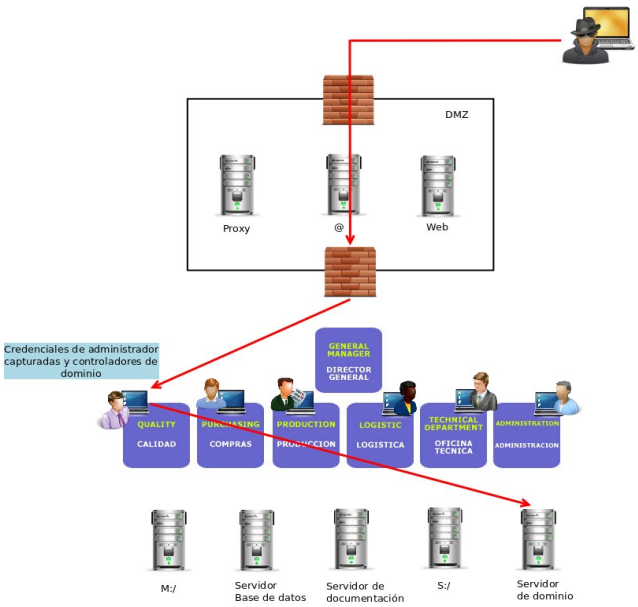
El motivo de usar este método es simple. Los sistemas de seguridad están más enfocados a proteger el interior de la organización de las amenazas externas que de las amenazas internas. Siendo la comunicación atacante-víctima iniciada en la víctima habrá más probabilidades de que no sea bloqueada.

6.3 Expansión

Ya se tiene el control de uno o varios equipos dentro de la organización objetivo. Ahora, a partir de éstos, se pretende dar el salto a los objetivos prioritarios. Esto se conoce como PIVOTAR. En ocasiones los nuevos objetivos serán directamente accesibles desde los equipos que ya se tienen comprometidos. No obstante, lo más frecuente es que antes de llegar al objetivo final haya que conseguir algunos accesos a otros equipos intermedios.

Un patrón común para llevar a cabo este proceso de expansión es el siguiente:

- En los equipos sobre los que se tiene control se escalan privilegios hasta conseguir permisos de administrador.
- En un equipo corporativo, además de acceder el usuario en cuestión, acceden los administradores para realizar tareas de mantenimiento. El atacante entonces buscará las credenciales de los administradores que puedan haberse almacenado en el equipo. Si no se encuentran se puede optar por instalar un programa que capture todas las pulsaciones de teclado y ratón (keylogger), o que grabe toda la información que se introduce en el equipo. Es muy probable que en relativamente poco tiempo el administrador tenga que acceder al equipo y entonces se consigan las credenciales buscadas.
- Una vez se tienen las credenciales de un administrador de dominio es posible acceder al controlador de dominio y obtener cuentas de todos los usuarios dados de alta, contraseñas, o por ejemplo, crear un nuevo usuario.



Otras formas de expansión podrían ser:

- Mediante el uso de ingeniería social, haciéndonos pasar por los usuarios de los equipos comprometidos.
- Distribución de dispositivos infectados (pendrives USB, DVDs, etc.).
  - Explotación de vulnerabilidades.
  - Sobornos a empleados.

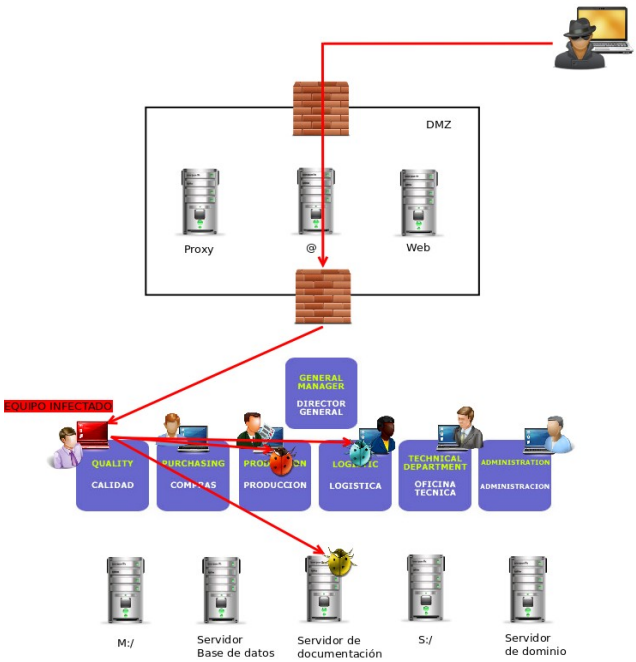
Se usará toda la creatividad y destreza posible para lograr el salto al objetivo.

6.4 Persistencia

Una vez se ha conseguido entrar, hay que intentar mantenerse dentro. Por ello, la mejor estrategia es propagar una infección extendida a través de toda la organización.

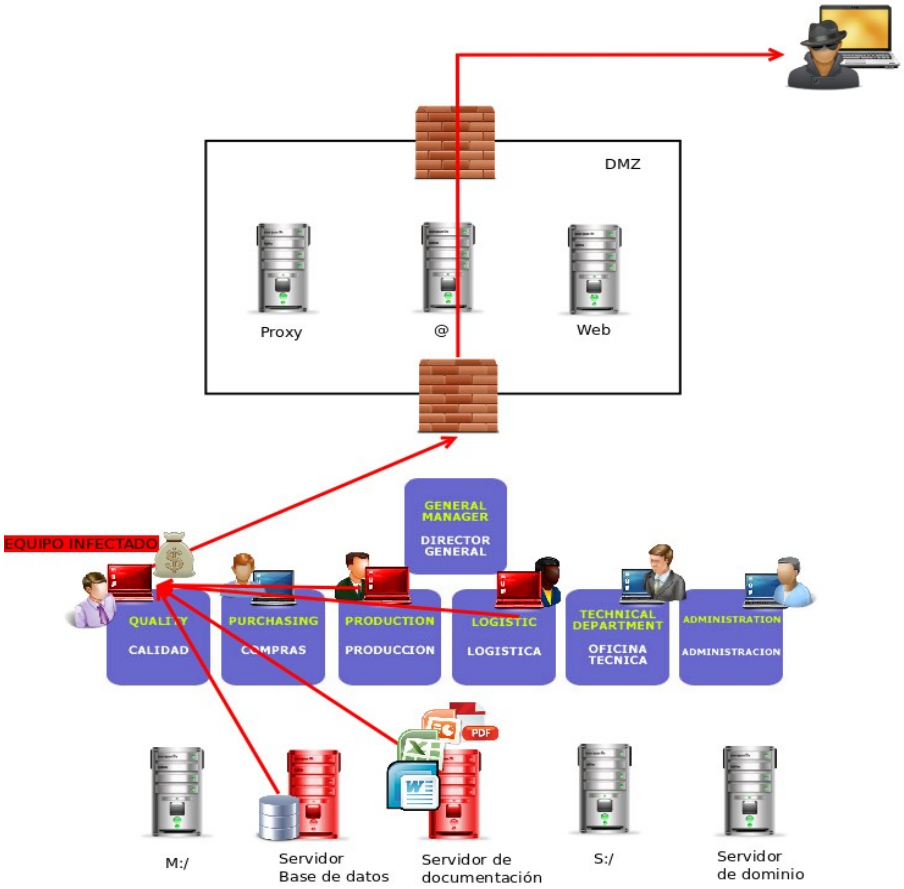
Ya hemos comentado que el atacante intentará que la intrusión no sea detectada, y propagar una infección a lo largo y ancho de la organización puede resultar muy ruidoso. Para evitar levantar sospechas puede optar por las siguientes estrategias:

- No infectar a todo el mundo con el mismo malware, sino propagar diferentes muestras.
- Activación retardada. No activar la infección en todos los equipos a la vez, sino espaciada en el tiempo.
- Infecciones en ubicaciones no comunes como en routers, impresoras, puntos de acceso WiFi, servidores o incluso en los propios firewalls.



6.5 Búsqueda y filtración

En este punto, el atacante ya tiene el control de las máquinas necesarias para llegar a aquella zona donde se encuentra el objetivo primario. Éste puede ser cualquier cosa: Documentos confidenciales, correos electrónicos, la inhabilitación de algún servicio, programas informáticos, y un largo etcétera.



En cuanto a la extracción de la información puede realizarse usando diferentes métodos y filosofías. Por un lado, los atacantes pueden optar por coger todo lo que puedan, o realizar una búsqueda selectiva. Para los métodos selectivas se pueden hacer uso de diferentes aplicaciones que buscan en los metadatos de los archivos.

6.6 Borrado de huellas

La última fase deberá consistir en desaparecer literalmente. Invertir esfuerzos en parecer que nadie a entrado ni ha ocurrido nada. Ello dependerá en gran medida de los pulcros que se haya sido durante todo el proceso de intrusión.

7 VÍAS DE COMPROMISO

En este apartado se presentan diferentes métodos que, aprovechados de una manera u otra, suelen ser usados en las APTs como herramientas para conseguir alguno de los objetivos definidos.

Las vías que puede usar una APT para acceder a la organización objetivo son múltiples. Tras la fase de estudio de la víctima, será la información relevante obtenida la que condicionará cuales son las mejores opciones para llevar a cabo la intrusión.

Entre estas posibles vías, en el caso concreto de las APT, destacan los siguientes grupos:

- Infección con malware.
- Medios físicos.
- Sitios web comprometidos.

La mayoría actúan bajo un factor determinante: la Ingeniería social.

Basándonos en los casos de APTs conocidos, el método más usado hasta la actualidad es el envío de correos de phishing dirigidos o Spear Phishing combinado con el uso de técnicas de ingeniería social. También se observa que en bastantes casos se apuesta por el aprovechamiento de vulnerabilidades desconocidas o 0-days y por el desarrollo de malwares a medida que se incluyen dentro de documentos que luego adjuntan a los correos de phishing.

Veamos las vías de compromiso usadas por algunas APTs conocidas:

APT	Método de entrada	Ingeniería social	Exploit 0-day
Oak Ridge National Laboratory (2011)	Spear phishing Attacks + IE 0-day	Si	Si
Operación ghostnet (2009)	Spear phishing Attacks (adjuntos infectados en los correos o enlaces maliciosos en los mismos)	-	-
Stuxnet (2010	USB infectados como método inicial	Si	Si (varios)
Night Dragon (2010)	Spear Phishing Attacks	Si	-
Operación Aurora (2009)	Spear Phishing Attacks + IE 0-day	Si	Si
Operación Shady RAT (2011)	Spear Phishing Attacks (documentos adjuntos Office y PDF infectados)	Si	-

7.1 Ingeniería Social

Pese a la complejidad técnica que puedan entrañar este tipo de amenazas, el engaño a las personas sigue siendo uno de los métodos más eficaces.

La ingeniería social es una de las técnicas más importantes en los ataques dirigidos, siendo útiles en diferentes fases como la recolección de información, la intrusión inicial y la expansión a través de la organización objetivo.

Como podrán imaginar, el arte del engaño puede ser usado en infinidad de escenarios. Correo electrónico, redes sociales, páginas web, llamadas telefónicas, chats o durante conversaciones en persona. Tan sólo con la información que se publica en Internet y la destreza del actor es posible modelar un plan de engaño con alta probabilidad de éxito.

En algunos casos, cabe la posibilidad de que los atacantes cuenten con un "infiltrado" en la organización objetivo y usándolo para introducir la APT, sin necesidad de vulnerar el perímetro de seguridad de la red. A ese tipo de amenazas se las considera internas y son especialmente relevantes:

- Empleados infiltrados que entran a trabajar a la organización con el objetivo de ser un topo (pueden robar credenciales de VPN, certificados digitales, instalar software malicioso en su equipo o en equipos del resto de empleados, obtener información privilegiada, etc.).
- Trabajadores descontentos que se dejen sobornar por los atacantes o que busquen hacer daño atacando a su organización.
- Contratación de servicios a terceros y que éstos sean 'maliciosos'; por ejemplo una banda criminal puede simular una empresa que vende un servicio X y ofrecer su servicio a la organización objetivo para que les contraten.

7.1.1 Ingeniería Social

Existen muchísimas estrategias para conseguir infectar a un usuario con un malware. Éstas además evolucionan a pasos agigantados, adaptándose a las nuevas tendencias de uso de las TICs por parte de los usuarios. Actualmente se usan principalmente como vías de infección las páginas webs, las redes sociales o a través de los móviles.

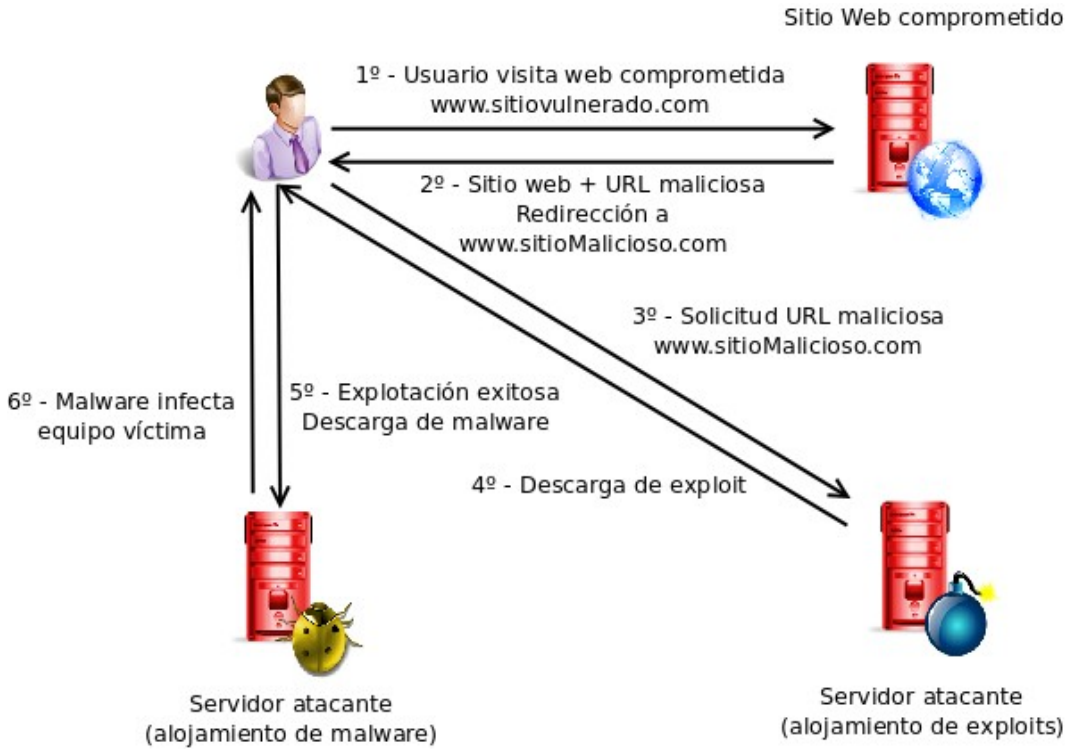
En el caso de las APT, como ya se ha comentado, el phishing dirigido es el medio más usado, aunque los sitios web comprometidos son bastante frecuentes también por el elevado uso de la web.

7.1.2 Infección a través de sitios web

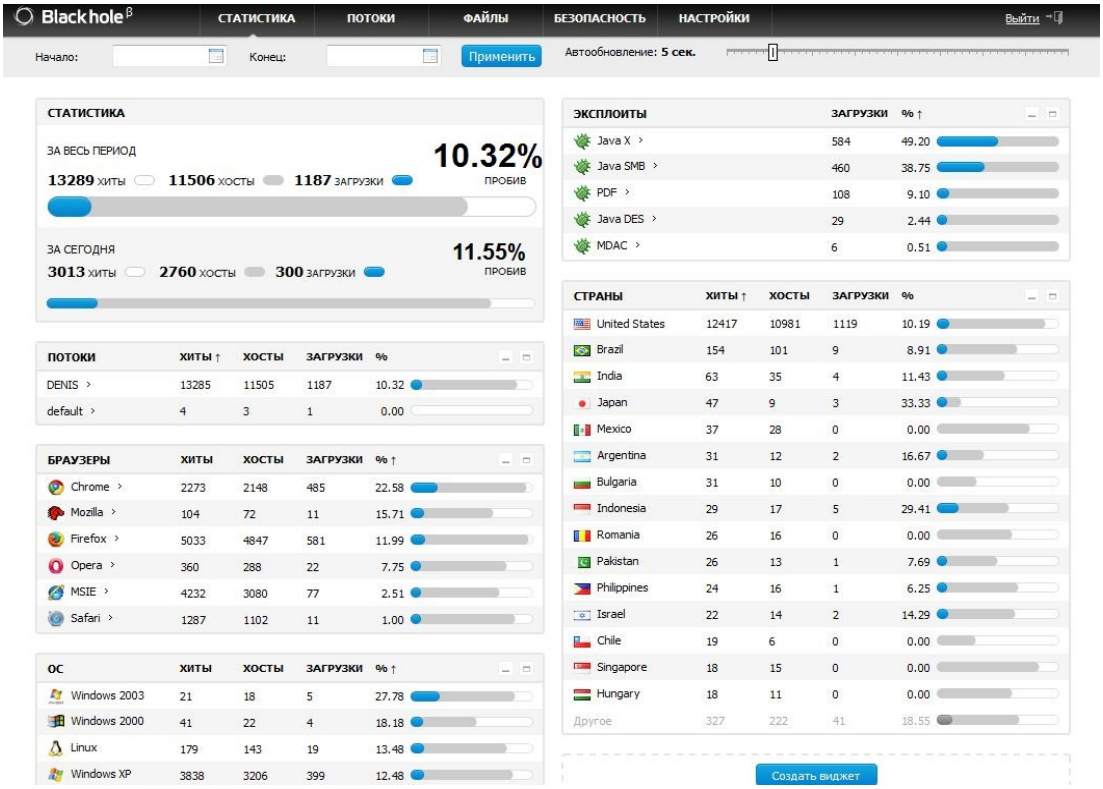
Por medio de esta vía se persigue que que el usuario se infecte con solo visitar un determinado sitio Web que haya sido previamente atacado y comprometido.

En líneas generales, el funcionamiento es el siguiente:

- Los atacantes buscan un sitio Web vulnerable e inyectan un código malicioso en la página.
- La víctima visita la página comprometida.
- El sitio Web devuelve la página consultada además del código malicioso, el cual generalmente obligará al navegador de la víctima a hacer nuevas peticiones a otros servidores Web controlados también por el atacante y desde donde se intentará explotar alguna vulnerabilidad del navegador del usuario.
- Si se consigue explotar alguna vulnerabilidad satisfactoriamente, conllevará la descarga de malware infectando al equipo del usuario.



Tras este tipo de ataques existen una serie de herramientas llamadas **Web Exploit Kits**. Actualmente existen en el mercado multitud de Web Kits Exploits que permiten automatizar todo este proceso. Estas aplicaciones no son más que repertorios de exploits en constante actualización que intentan aprovecharse de diversas vulnerabilidades en navegadores y plugins para comprometer equipos de forma masiva. Algunos kits conocidos son Blackhole, Crimepack, Phoenix, Unique, Eleonore, Liberty, Fiesta, Adpack etc.



Partiendo de este modelo, recientemente ha surgido un nuevo tipo de ataque muy usado en campañas de APT y denominado **Watering Holing**. La idea del ataque consiste en comprometer sitios Web que los usuarios de la organización objetivo suelen visitar (se supone que tras investigación previa de los hábitos de navegación de los usuarios), con la finalidad de que al visitarlos los usuarios se infecten.

7.1.3 Spear Phishing

Se trata de un caso de phishing especial. Como ya todos conocemos, un phishing no es más que un ataque en el que por medio del engaño se intenta suplantar a alguien o algo para ganarse la confianza de la víctima.

En los Spear phishing la diferencia radica en que la suplantación se hace a medida para la víctima. El emisario suplanta la identidad de alguien conocido por los objetivos.

En las campañas de APT es el método más utilizado como vía de infección. En los ataques dirigidos, estos correos suelen llevar incorporado, bien un enlace a un sitio malicioso con la finalidad de que el usuario lo visite comprometiendo su equipo, o bien un documento adjunto malicioso para infectar al

usuario. Con ayuda de diversas técnicas de ingeniería social el atacante tratará de engañar a la víctima para que visite el enlace malicioso incorporado en el correo o abra el documento anexado.

7.1.4 Archivos compartidos o redes P2P

Las redes P2P (Peer-to-peer), son redes formadas por equipos que trabajan a la vez como clientes y servidores, por las que se permite el intercambio de información entre usuarios de forma descentralizada. Bajo este escenario, en el que es muy sencillo engañar al usuario simulando que un archivo es benigno, o insertar código malicioso en programas legítimos y distribuirlos de forma masiva, las redes P2P se han convertido en un foco importante para la distribución de Malware.

En una APT los atacantes podrían usar la información obtenida de las víctimas en la fase de recolección de información inteligente para distribuir el material infectado en la red P2P y esperar que, con un poco de suerte, la víctima se lo descargue y se infecte. Por ejemplo, imagine que el objetivo es una empresa dedicada a la investigación farmacéutica, y el atacante descubre algo muy específico sobre lo que están investigando. Los empleados posiblemente busquen documentación, o cualquier tipo de material relacionado con el tema bajo investigación. Bajo este escenario, el atacante puede compartir en redes P2P un archivo PDF malicioso cuyo nombre esté muy relacionado con el tema de investigación concreto. Con suerte, es posible que alguien del equipo de investigación se tope con el archivo, lo descargue y lo abra, con lo que infectaría el equipo.

7.1.5 Software pirata

Según un estudio publicado por INTECO en 2012, en general, un usuario ante la necesidad de obtener un programa informático (sistemas operativos, actualizaciones, programas de desarrollo, diseño, de gestión empresarial, ofimática, sonido, vídeo, etc.), acude a Internet en un 66.4% (a lugares de descarga directa, redes P2P, Webs oficiales, páginas de subasta, etc.), aunque solo un 26.3% lo hace en el sitio oficial del producto. Desde el punto de vista corporativo, España se sitúa en el top 10 de países en los que el responsable de adquisición de software de la empresa recurre habitualmente a la descarga no autorizada. Con lo cual se deduce, que incluso en el ámbito corporativo la descarga de software no autorizado es una práctica extendida.

Dentro de los ataques dirigidos, se podrían plantear diferentes escenarios en los que el software pirata y derivados pudieran jugar un papel importante. Por ejemplo, tras la fase de recolección de información inteligente, el atacante consigue obtener datos acerca de los programas que utilizan los empleados, o intereses que pudieran tener algunos de ellos sobre probar un software en concreto, por ejemplo un empleado con gran afición a la fotografía estaría interesado quizá en programas de retoque de imágenes o similares. El atacante podría crear correos dirigidos, o mensajes a través de redes sociales o foros especializados de fotografía en los que el usuario víctima suela participar y ofrecerle que pruebe de manera gratuita algún determinado programa específico (diseñado específicamente por el atacante para

que sea malicioso). Si el atacante tiene suerte y el usuario se lo descarga mientras está en su puesto de trabajo, la probabilidad de que el usuario se infecte es muy alta.

Las copias no autorizadas o ilegales de software pueden poner en peligro la seguridad de los usuarios que las utilizan ya que la mayoría suelen estar infectadas con malware o fomentan malas prácticas en cuanto a seguridad del usuario. Los usuarios que descargan estas copias pirata normalmente deben instalar unos programas "extra" (cracks, keygens, serials, patchs,...) para eludir los sistemas anticopia que implementan las compañías desarrolladoras, programas de los cuales no se suele conocer ni su procedencia ni su integridad. Generalmente, muchos de ellos incluso solicitan al usuario que deshabilite su propio antivirus para poder instalarlo correctamente asegurando que no se corre ningún peligro ya que está libre de virus, la consecuencia de esta mala práctica es que el usuario se queda totalmente desprotegido.

7.1.6 Medios físicos

Otro de los métodos que también se ha utilizado en el caso de los ataques dirigidos es la introducción de malware en la organización a través de dispositivos físicos dentro de la organización. Basta con la conexión a la red de USBs, CDs, DVDs, tarjetas de memoria, o por ejemplo equipamiento IT infectados para introducir el malware en la organización objetivo.

En el caso de los ataques dirigidos con Stuxnet, la infección inicial del mismo se realizó a través de un USB infectado. En un hipotético escenario, el atacante podría, a través de técnicas de ingeniería social y otro tipo de artimañas burlar la seguridad física de las instalaciones de la organización objetivo y acceder con un USB infectado a un equipo conectado a la red corporativa. Otro escenario de ataque posible podría ser, que el atacante suplante la identidad de un cliente, colaborador, o se haga pasar por alguien interesado en el organismo objetivo en cuestión y regale, dentro de una supuesta campaña de marketing, ciertos dispositivos USBs, tarjetas de memoria, CDs o DVDs, smartphones, tablets, portátiles, o cualquier tipo de dispositivo infectado a los empleados, incluso software. Es posible que el atacante haga llegar a las víctimas software pirata malicioso empaquetado de forma que imite el empaquetado del fabricante original y que los usuarios objetivos no se den cuenta del engaño.

También, en el caso de los dispositivos móviles, recientemente han aparecido en los medios, diversos casos sobre la incorporación de backdoors en los dispositivos que vienen de fábrica, así por ejemplo el fabricante chino de smartphones ZTE Corp, confirmó la existencia de una puerta trasera que, permite tomar remotamente el control total de uno de sus smartphones comercializado en Estados Unidos poniéndose en el punto de mira de las autoridades americanas por su presunta vinculación con el gobierno chino.

Es importante por último comentar que, la entrada de malware a una organización a través de medios físicos puede incrementarse de manera considerable a raíz de nuevas tendencias en alza que se están arraigando en las organizaciones que consisten en bien fomentar o permitir el uso de dispositivos

personales (portátiles, tablets, smartphones, etc.) en el entorno de trabajo, es decir que los empleados se traigan sus dispositivos al trabajo y trabajen con ellos, es la denominada tendencia BYOD (Bring Your Own Device), o bien que además de sus propios dispositivos también aporten su propio software ,BYOT, (Bring Your Own Technology), y además existe una variante emergente, BYOC (Bring Your Own Cloud), en estos casos los empleados aportan su propia 'nube'. Estas tendencias, si no son bien gestionadas pueden suponer una importante brecha de seguridad en las organizaciones facilitando la tarea del atacante puesto que la información privada de la organización entra dentro de una red cada vez más difusa y difícil de proteger.

Añadir para finalizar, que el emergente uso de los códigos QR hace que se conviertan en una nueva vía de infección a tener en cuenta de cara a campañas de APT. Como bien se indica en este documento, no sería difícil pensar en un escenario en el que un atacante dispense folletos de publicidad dirigida con el código QR suplantado por uno falso para que los empleados de cierta organización objetivo visiten la determinada URL infectada y comprometan su equipo.

8 CÓMO PROTEGERSE ANTE APT

Cuando se habla de ataques de APT se habla de organización, premeditación, persistencia, sofisticación y novedad. A día de hoy, constituyen uno de los peligros mas importantes y de mayor expansión a los que se enfrentan los profesionales de la seguridad, y son prácticamente inevitables para la mayoría de las organizaciones, y es por ello que la cuestión principal que se ha de plantear en el panorama actual frente a este tipo de amenazas es cómo detectarlas.

Disponer de una estrategia para preparar a una organización contra los peligros asociados con las APT es un proceso continuo. Al igual que en los procesos de desarrollo, despliegue y mantenimiento, los errores ocurren pero se debe reconocer su existencia y estar preparados para su aparición y mitigación. Estamos hablando de la gestión del riesgo que como todos sabemos, se trata de un proceso cíclico y en constante evolución.

Por todo lo anterior, toda organización necesita disponer de personal preparado que disponga de los medios tecnológicos necesarios para gestionar cualquier riesgo asociado a las APTs. Algunos de los retos que se deberán resolver son:

- **Vigilancia constante mediante herramientas automatizadas de monitorización en tiempo real** que permitirán en cierta medida adelantarse a las acciones que pueda realizar una amenaza antes de que ocurran los incidentes.

- Puesto que la utilización de medidas tecnológicas son necesarias pero pueden ser insuficientes, en muchas ocasiones será necesario **buscar comportamientos anómalos en la infraestructura TIC**, asumiendo que los ataques están ocurriendo.

- Debe existir una **vigilancia permanente relativa a lo que entra y sale desde nuestras redes y hacia dónde se dirige ese tráfico**, ya que prácticamente la totalidad de APTs tratan de establecer distintos tipos de comunicaciones con los objetivos esenciales para bien enviar la información sustraída a un servidor o descargarse nuevos funcionalidades en forma de módulos que aporten más persistencia, más vectores de ataque, etc.

- Promover la **concienciación y educación** al personal de la organización; sobre todo a aquellos que son más susceptibles de sufrir incidentes ya que, según las estadísticas, el factor humano y el uso de la ingeniería social para engañar a los usuarios es uno de los elementos más utilizados como punto de entrada de una APT.

- **Cualquier nueva tecnología añade nuevos riesgos que deben estudiarse y mitigarse**; la defensa perimetral hace tiempo que dejó de ser efectiva por sí sola por esta razón, las organizaciones deben ser especialmente cautas a la hora de implementar tecnologías sin haber realizado un análisis de riesgos previo.

- **Utilizar los conocimientos adquiridos en la organización a través de las lecciones aprendidas de incidentes de seguridad anteriores**, esto incluye la experiencia acumulada con la utilización de herramientas trampa como Honeypots, en procesos de análisis forenses, de estudio de anomalías detectadas o de otras actuaciones que permitan adquirir conocimientos útiles en la detección de nuevas amenazas.

Todas estas medidas, apoyadas en profesionales cualificados así como en los servicios de detección, alerta temprana y respuesta ofrecidos por los CERTs, nos proporcionarán unos niveles de madurez adecuados en términos de protección frente a este tipo de amenazas.

9 CONCLUSIONES

Las APTs no son una novedad, existen desde hace años. No obstante, ponen de manifiesto un escenario de amenazas en continua evolución. Estos ataques se dirigen, principalmente, contra grandes organizaciones. Sin embargo, los usuarios domésticos tampoco están a salvo porque pueden convertirse en una pieza más de la cadena para llegar al objetivo final.

Lo primero que hay que saber es que no existen antídotos o soluciones definitivas. Lo más recomendable es seguir un buen plan de gestión de la seguridad y aprender de las experiencias pasadas.

Aunque no haya una poción mágica, según Jaime Blasco: *"Son necesarias ciertas tecnologías que nos protejan frente a las amenazas, pero, en mi opinión, la mejor solución es la combinación de procesos, tecnología, prevención y educación"*.

Costin Raiu añade: *"estudiar las víctimas de las APTs es realmente útil. Así, es posible saber que el 95% de estos ataques se dirigen contra compañías con estándares de seguridad no muy estrictos. Desconocen los riesgos o las prácticas de seguridad y no instalan parches o no usan software antivirus. En primer lugar, las compañías deberían asegurarse de que han actualizado los programas y el sistema operativo; además, deberían utilizar un navegador seguro (como Chrome o Firefox) con todos los parches descargados. Por supuesto, también es necesario educar a los usuarios. Si unimos todos estos ingredientes, entonces, estaremos mejor preparados frente a estas amenazas"*.

Neil Thacker incluye: *"no podemos olvidarnos de educar a ciertos trabajadores"*.

Como conclusión, las APTs seguirán aumentando y existiendo mientras las organizaciones posean información atractiva. No existe otro remedio que la prevención y educación dentro de las organizaciones como medidas preventivas. Siempre debemos ser conscientes de que no existe la seguridad al 100% y que es necesario estar en constante alerta.

10 REFERENCIAS

- INTECO-CERT, CSIRT-CV: "Detección de APTs". 2013
- Operation Aurora
- Information Warfare Monitor. "Tracking GhostNet: Investigating a Cyber Espionage Network". 2009
- Stuxnet
- McAfee. "Global Energy Cyberattacks: 'Night Dragon'". 2011
- Flame
- CSIRT-CV. "Identifican red de espionaje industrial que roba archivos de AutoCAD". 2012
- Hispasec. "Duqu, ¿el nuevo malware descendiente de Stuxnet?". 2011
- Kapersky Labs. "The Red October Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies". 2013
- Mandiant. "APT1: Exposing One of China's Cyber Espionage Units". 2013