¿QUÉ SON LAS AMENAZAS PERSISTENTES AVANZADAS (APTs)?

Desde hace unos años el mundo de la seguridad ha acuñado un término para definir un tipo de riesgos de ciberseguridad de mayor gravedad a los habituales ya que, a priori, poseen características que hacen que sus efectos sean mucho más dañinos: las "amenazas persistentes avanzadas" o, por sus siglas en inglés, APTs *(Advanced Persistent Threats)*.

Sus rasgos definitorios son: ser capaces de perdurar en el tiempo (infectando una máquina), poder aprovecharse de vulnerabilidades desconocidas oficialmente (lo que las hace pasar desapercibidas) y, sobre todo, tratarse de amenazas dirigidas contra un objetivo muy específico (habitualmente los recursos de una compañía). El principal fin de este tipo de ataques es el espionaje, principalmente empresarial, gubernamental y militar, obteniendo y manipulando información contenida en sus sistemas, más que atacando a objetivos físicos. En definitiva, se trata de comprometer la seguridad de una red de ordenadores para conseguir información sensible.

I Características de APTs

Las amenazas persistentes avanzadas suelen manifestarse como un programa especialmente diseñado para mantenerse oculto en el sistema atacado, puede que aprovechando vulnerabilidades desconocidas hasta ese momento o usando técnicas de ingeniería social muy concretas sobre el personal de la empresa-víctima. Esto quiere decir que se aleja del malware o amenazas comunes que, por lo general, son impersonales y generalistas.

El tipo de atacante que usa una APT es mucho más paciente que el atacante medio sin objetivo concreto. Suelen tener una mayor motivación económica para que el ataque sea exitoso y, por tanto, los recursos y tiempo empleados son superiores a los de cualquier otro atacante.

Pueden constituir un tipo de servicio demandado por competidores empresariales, cazarrecompensas, gobiernos, servicios de inteligencia, etc.

Una característica habitualmente desarrollada en este tipo de amenazas es su capacidad de fragmentación o descomposición en módulos. Una vez infectado el sistema, este puede descargar módulos encargados de diferentes tareas, tales como leer comunicaciones de red, escuchar el micrófono e incluso controlar la webcam.

II Desmitificando las APTs

Hoy en día, es frecuente una errónea utilización del término APTs para denominar ataques a organizaciones, gobiernos o empresas. Se han dado casos de malas interpretaciones, confundiendo verdaderos ataques dirigidos con errores y malas prácticas en la securización de un entorno empresarial. En este sentido, si no se establece de manera adecuada el nivel de riesgos en seguridad de la organización, un descuido, una mala gestión o una falta de previsión puede terminar en el compromiso de un sistema. Por ello, no siempre se debe poner este problema como excusa y achacar a invisibles ataques APTs el hecho, por ejemplo, de que un empleado haya abierto un correo infectado y la red de la empresa haya quedado comprometida.

Del mismo modo, no se debe caer en el error de pensar que siempre que una compañía importante sufre una intrusión ha sido víctima de una APT. Tampoco hay que dar por hecho que cuando organizaciones de menor calibre son quienes los sufren, es por una falta de seguridad.

Si tomamos como válido el concepto de APTs tendremos que identificar, pues:

- **Amenaza:** ¿Es realmente una *amenaza*? Se deberían considerar como tales aquellos que persiguen un objetivo concreto e importante (espionaje industrial, cuentas bancarias, bloqueo de infraestructuras civiles o militares, etc). Se trata, por tanto, de objetivos de cierta envergadura.

- **Persistente:** ¿Se trata realmente un ataque *persistente*? Es necesario matizar esto. El que un ataque se prolongue en el tiempo no debería ser factor tan determinante. Existen sitios web que sufren intentos de denegación de servicio durante días o semanas y también ataques que se han llevado con precisión milimétrica, bien porque se conocía de antemano la infraestructura de la empresa (un caso de estudio previo) o porque se tenía localizada una vulnerabilidad que permitía una rápida explotación sin tener que llevar a cabo posteriores intentos para acceder a la información u objetivo del ataque. En cualquiera de los dos casos, se requiere un trabajo previo. Por tanto, la persistencia no radica en la duración del ataque sino en el tiempo empleado para su ejecución.

- **Avanzada:** ¿Consiste realmente en un ataque *avanzado*? Debe aportar alguna novedad en el campo de la seguridad y ser específico para el objetivo atacado.

III Proceso de ataque

El proceso general por parte de los atacantes consta de varias partes:

1) **Estudio de la víctima.**

   Al tratarse de un ataque específico dirigido, el atacante debe conocer en profundidad su objetivo, desde la configuración de los sistemas hasta sus políticas de seguridad. Esto le permite elegir el punto más débil en la cadena para atacar.

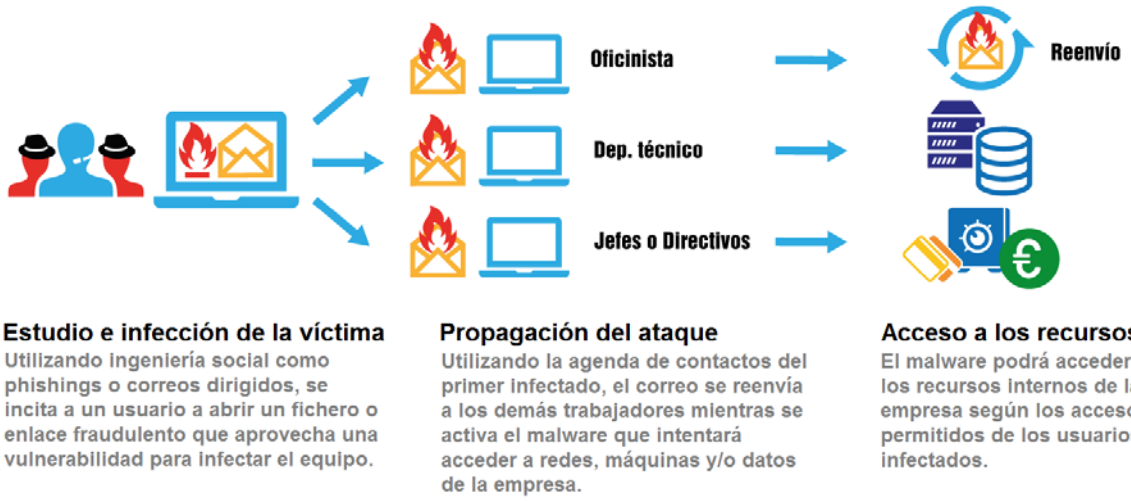
2) **Infección.**

   Consiste en instalarse o esconderse en alguna máquina de la red interna, desde donde se intenta obtener el objetivo deseado (la información). Esta máquina puede infectarse ejecutando un simple archivo, que contiene las instrucciones para futuras etapas de la infección. También incluye la lógica necesaria para descargar nuevas funcionalidades, si fuesen necesarias.

3) **Propagación.**

   Una vez infectado un equipo o sistema, la propagación consiste en extenderse a más equipos, ya sean en la red colindante (LAN) o a través de Internet. Con esto se consigue más información. Como contrapartida, el atacante asume un mayor riesgo a ser detectado.

Ilustración 1: Proceso de ataque ATP



Fuente: INTECO

IV Métodos de infección y propagación

A continuación se presentan distintos métodos que, aprovechados de una manera u otra, pueden servir para infectar sistemas o para propagar el malware.

a) Ingeniería social

Algunos ataques muy sofisticados técnicamente han comenzado con un simple engaño a uno de los usuarios de la red. La infección comienza con una ejecución. Persuadir a un usuario de que lance un ejecutable, si el sistema no cuenta con las medidas de seguridad necesarias, puede ser más sencillo que cualquier otro método.

b) *Bring Your Own Device* (BYOD)

Cuya traducción al español sería "trae tu propio dispositivo", define una nueva tendencia en las empresas a permitir a sus trabajadores a que puedan usar sus propios dispositivos personales para fines laborales, tanto dentro como fuera de la empresa. Surge con la aparición de teléfonos inteligentes y tabletas. Un ejemplo típico es traer a la oficina su portátil o la consulta del correo fuera del horario de trabajo con el móvil o la tableta.

Salvo que se tomen las medidas de gestión de seguridad adecucadas, esta política de empresa puede entrañar problemas a la seguridad corporativa, puesto que puede suponer la introducción de dispositivos no protegidos ni controlados en la red interna. Otro ejemplo clásico es el caso en que el empleado tiene acceso a una VPN[1] dentro de la empresa a través de su tableta, y esta es extraviada o sustraída. Si cae en manos de un atacante, podría obtener los credenciales de acceso, acceder a la empresa y lanzar el malware.

Otro posible escenario se da cuando el usuario se infecta con el malware fuera de la empresa y este se propaga a través de la red interna corporativa a servidores u otros sistemas. El uso del WiFi en dispositivos portátiles puede ser un punto de propagación de amenazas, si el administrador de red de la organización no lo gestiona adecuadamente.

c) Vulnerabilidades

Todo software presenta vulnerabilidades. Si estas son suficientemente graves, pueden permitir la ejecución de código en el sistema sin que la víctima se percate. Las más graves son las más recientes y por tanto menos conocidas y con menor probabilidad de que exista parche para solucionarla. Estas suponen una brecha mayor de seguridad. De entre ellas, las vulnerabilidades conocidas como 0-day son las más peligrosas, puesto

[1] Una red privada virtual o VPN (*Virtual Private Network*) por sus siglas en inglés es una tecnología que permite la conexión de distintas redes locales o internas a través de una red mayor (Internet). Es muy utilizado en entornos empresariales donde hay distintas sedes con diferentes localizaciones físicas.

que se dan a conocer cuando ya están siendo aprovechadas por atacantes. En este caso se dan las siguientes circunstancias: 1) no existe parche conocido, y 2) alguien sabe cómo aprovechar la vulnerabilidad y además lo está haciendo para lograr tomar el control de los sistemas.

d) Phishing dirigido

El phishing es un término referido habitualmente al robo de credenciales bancarias para suplantación de identidad y robo. Normalmente, está asociado con cuentas bancarias y tarjetas de crédito, que permiten posteriormente realizar transferencias a las cuentas de los delincuentes. Habitualmente, se trata de una técnica totalmente indiscriminada: el anuncio de sitios fraudulentos se hace a través de correo electrónico, sin tener en cuenta si el destinatario es cliente de la entidad o no, por ejemplo.

En el modelo de APTs, el ataque es ligeramente diferente. Se buscan credenciales de gente involucrada en la empresa u organismo, tanto trabajadores como altos directivos, por lo que no es un ataque indiscriminado. Se personalizan los mensajes y se suplanta la identidad de administradores de red, por ejemplo. Una vez se obtienen los datos, se podría acceder a la empresa a través de, pongamos por caso, una VPN e infectar un equipo.

e) Perímetro externo

El perímetro externo de una empresa está formado por todo aquel software o sistema que está en contacto con el exterior. Para un atacante que desee entrar en la red interna es un punto más que debe conocer y analizar.

- Un **firewall** o cortafuegos es una herramienta que forma parte de la red, cuyo principal cometido es evitar el acceso no permitido desde el exterior. Una vulnerabilidad o un defecto en la configuración de un firewall podría permitir la intrusión a la red interna y la posibilidad de que un atacante deposite una APT en algún subsistema.
- Una red privada virtual (**VPN**) es considerada parte del perímetro externo de una red empresarial ya que posibilita la conexión de distintas redes internas a través de una red externa (normalmente Internet). Una configuración deficiente o una vulnerabilidad en el software usado son suficientes para perpetrar un ataque.
- Muchas empresas realizan su trabajo a través de **aplicaciones web**. Estas son herramientas que los usuarios (empleados, en el caso de una empresa) utilizan a través de navegadores. Un fallo en una aplicación de este tipo podría dejar al descubierto datos importantes, que pueden ser utilizados para perpetrar un ataque con una APT dentro de la empresa.

f) Distracciones

Una de las características de las APTs es que deben ser persistentes en el tiempo. Para que la amenaza pueda perpetuarse, los administradores del sistema no deben conocer la existencia de esta amenaza. Si la red está convenientemente configurada, cualquier movimiento en los sistemas podría quedar reflejado en los "logs" o registros automáticos de actividad internos. Para que los administradores no se percaten de esta intrusión, los atacantes pueden crear una cortina de humo atacando el sistema de otra manera.

Uno de los ejemplos típicos de estas distracciones son los ataques DDoS. Un ataque DDoS es un ataque de denegación de servicio distribuido o, lo que es lo mismo, intentar que el sistema principal deje de funcionar. Este ataque se produce realizando múltiples peticiones a un servidor (como puede ser un servidor de páginas web o de correo electrónico) desde distintos lugares. Mientras tanto, los atacantes introducen el malware. Con esto se consigue que los administradores de sistemas centren sus esfuerzos en mitigar el ataque DDoS y no presten atención a la intrusión.

Además, las posibles huellas que dejase la amenaza en los logs quedan ocultas entre otras peticiones ocasionadas por el ataque de denegación de servicio.

Ilustración 2: Técnicas comunes usadas por APT

Fuente: INTECO

V Ejemplos de APTs

Las APTs más conocidas han resultado tener la forma de malware. Han supuesto un paso más allá en los ataques dirigidos conocidos hasta el momento, y han puesto de manifiesto la peligrosidad de los ataques de esta naturaleza. A continuación se describen algunos ejemplos de APTs especialmente significativos:

Stuxnet

Stuxnet es una APT que se detectó en julio de 2010 por la empresa antivirus *VirusBlokAda.* Este malware fue diseñado para infectar indiscriminadamente a equipos Windows y afectar a únicamente a sistemas SCADA[2]. Según estudios posteriores a su descubrimiento, iba dirigido a infraestructuras industriales controladas con el software WinCC[3] para sistemas SCADA.

Esta APT, que se considera un gusano, ya que es capaz de auto-distribuirse. Su modus operandi fue el siguiente:

1. Infección: se realizó utilizando una vulnerabilidad de auto-ejecución de archivos en dispositivos de almacenamiento USB infectados. Utilizó una técnica desconocida hasta el momento para ejecutarse.
2. Propagación: una vez infectado un equipo, se propagó a través de la red a otros sistemas con WinCC (SCADA) utilizando dos vulnerabilidades 0-day, una en la cola de impresión y otra en el servidor de compartición de archivos.
3. En el equipo infectado se utilizaron otras dos vulnerabilidades 0-day, esta vez para escalar privilegios en el sistema y convertirse en administrador.

Esta amenaza también se aprovechó de otro error muy habitual en la seguridad de los sistemas, que consiste en mantener la contraseña por defecto. En total usó cuatro vulnerabilidades desconocidas hasta el momento para ejecutar código en las máquinas infectadas. Esto lo hacía eficaz contra cualquier sistema Windows. Solo los administradores que hubiesen tomado las máximas precauciones, como evitar la ejecución de programas desconocidos, limitar privilegios u otras medidas similares, se habrían podido librar de la amenaza.

Además, esta APT era capaz de actualizarse, bien para incluir nuevas funcionalidades o buscando nuevas maneras de mantenerse oculta, a través de redes P2P.

[2] SCADA (*Supervisory Control And Data Acquisition*) son sistemas, como su propio nombre indica, para la adquisición, control y supervisión de datos de procesos industriales. Con ellos se pueden controlar desde las revoluciones de un motor hasta un sistema de temperatura de un frigorífico industrial.

[3] WinCC es un software desarrollado por Siemens para la adquisición, control y supervisión de datos, que funciona sobre el sistema operativo Windows. Además, provee de una interfaz para su utilización.

Se encontraron muestras de Stuxnet en sistemas e infraestructuras de distintos países, principalmente en Indonesia, India, Irán y China, aunque, como posteriormente informaron los medios de comunicación, su objetivo principal eran las centrales nucleares iraníes.

Otra de las características por las que tardó tanto en ser detectado por los motores antivirus fue porque los drivers de Stuxnet utilizados como *rootkit* estaban firmados digitalmente.

Algunas herramientas antimalware confían la legitimidad de ciertos archivos a su firma y no proceden a escanearlos.

En un primer momento, se firmó con un certificado robado a la empresa china Realtek. Microsoft entonces trabajó con Verisign (empresa emisora de estos certificados) y Realtek para revocarlos en todos sus sistemas. Posteriormente, los atacantes modificaron el certificado y usaron otro válido, esta vez de una empresa Taiwanesa, llamada JMicron.

Todas estas cualidades hicieron pensar que el troyano fue concebido no solo por una mafia organizada, sino que iba más allá: formaba parte de un entramado de mayor nivel en el que podían llegar a estar involucrados organismos influyentes, hablándose incluso de la implicación de los gobiernos de Estados Unidos e Israel en su creación[4].

Stuxnet consiguió pasar desapercibido muchos meses en los sistemas infectados, y se especuló sobre cuánto tiempo antes llevaba actuando en realidad.

[4] The New York Times, 'Obama Order Sped Up Wave of Cyberattacks Against Iran' http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

Ilustración 2: Repercusión de Stuxnet en los medios

Fuentes: Varias[5]

TheFlame

TheFlame es otra APT que fue descubierta en mayo de 2012, aunque hay investigadores que afirman que su origen se remonta a 2008. Usa dos vulnerabilidades de Windows que ya fueron usadas en Stuxnet, pero al contrario que este, no se transmitía indiscriminadamente.

TheFlame se basaba en tomar el control de una red interna y lo hacía de la siguiente manera:

1. Infección: el método de infección "inicial" de esta APT es a través de dispositivos de almacenamiento USB.
2. Propagación: la importancia de TheFlame reside en este punto. Era capaz de replicarse a través de la red interna o LAN a través de un ataque conocido como MitM[6] u hombre-en-el-medio, simulando ser una actualización de Windows.

[5] Stuxnet: Anatomy of a Computer Virus http://vimeo.com/25118844.

Researchers warn of new Stuxnet worm http://www.bbc.co.uk/news/technology-15367816.

Stuxnet was work of U.S. and Israeli experts, officials say http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Stuxnet: The New Face of 21st Century Cyber Warfare Infographic http://www.veracode.com/blog/2012/08/stuxnet-the-new-face-of-21st-century-warfare-infographic/

Una vez infectado un equipo, este hacía la función de "proxy". A grandes rasgos, cuando un sistema perteneciente a la misma red que el equipo infectado intentaba actualizarse, preguntaba en la red local si hay algún proxy y el equipo infectado se ofrecía a serlo. Redirigía las peticiones de Windows Update a un servidor controlado por los atacantes y desde este se servía una nueva actualización (que, por supuesto, no era oficial) y contenía a TheFlame. Para que fuera posible la ejecución de este código a través de Windows Update, también era necesario que estuviese firmado, y esta actualización lo estaba.

El certificado con el que fue firmado TheFlame no fue robado esta vez. Los creadores son auténticos expertos en criptografía y han conseguido generar un certificado falso y válido mediante técnicas de colisión de la función hash[7] MD5.

Otro de los problemas que tiene un malware es que debe soportar los reinicios del sistema, esto es, una vez el sistema se apaga y se vuelve a encender, debe volver a ejecutarse para seguir capturando datos. Esto lo solventó TheFlame instalándose como driver de audio falso y así, Windows lo inicia automáticamente en el arranque del sistema.

Esta APT es muy modular, es capaz de grabar audio, hacer capturas de pantalla, pulsaciones de teclado, escanear el tráfico de red, grabar conversaciones de Skype y hasta controlar el bluetooth del equipo. Este último módulo se utiliza para escanear dispositivos bluetooth cercanos (móviles, tabletas,...), por lo que tiene especial interés en un ámbito organizacional y no doméstico. Con el total de módulos instalados, esta APT podía alcanzar un tamaño de hasta 20 megabytes.

TheFlame también es adaptativo, es decir, cambiaba su comportamiento dependiendo el antivirus encontrado en el sistema, haciendo más difícil su detección.

Los sistemas infectados actuaban como "zombis", ya que podían ser controlados por los atacantes recibiendo instrucciones desde ciertos servidores, pudiendo los atacantes causar su autodestrucción a través de un comando "kill". También, los datos robados eran enviados a servidores repartidos por todo el mundo.

Los países Oriente Medio fueron los más afectados por este malware.

[6] MitM (Man-in-the-Middle) es un tipo de ataque en el que el atacante es capaz de situarse entre el cliente y un servidor legítimo, pudiendo leer, modificar y/o eliminar cierta información que fluya entre estos.

[7] Una función hash es una fórmula matemática que permite generar, a partir de unos datos variables, una cadena de caracteres con una longitud fija. Es un proceso irreversible, teniendo la cadena no se puede obtener el cuerpo original. Es determinista, por lo cual, si se calcula 2 veces el hash de un mismo cuerpo, el valor es igual.

Medre

Medre fue descubierto en junio de 2012 por la compañía Eset. Ha sido considerado por los medios generalistas (y algunos especializados) como una APT, aunque en realidad no cumple plenamente con su definición como tal, por lo que podemos afirmar que no lo es.

En primer lugar, está claro que sí cumple la condición de ser una amenaza para las empresas infectadas.

En segundo lugar, hay múltiples malware que son capaces de robar documentos CAD, pero Medre es muy nuevo, fue descubierto con apenas unos meses de vida, por lo cual no cumple la característica de las APT de ser persistente.

En tercer lugar, como decíamos al comienzo del artículo, una de las características de una APT es que debe ser un malware "avanzado". Si bien Medre es un malware con objetivos industriales y militares, capaz de robar documentos CAD (de AutoCad[8]), su simplicidad hace que no cumpla esta característica.

Este malware obtiene los archivos del sistema infectado, los comprime, los cifra (siempre con la clave “1”) y los envía por correo electrónico a servidores situados en China. El ataque fue especialmente dirigido a objetivos situados en Perú.