



SEGLOSER®
Global security services

INFORMÁTICA FORENSE: HERRAMIENTA FUNDAMENTAL EN CONTRAINTELIGENCIA

ÍNDICE

1.- INTRODUCCIÓN.....	2
2.- SOFTWARE: EL NUEVO AGENTE DOBLE.....	3
3.- HARDWARE: COBERTURA PERFECTA.....	5
4.- APORTES DE LA INFORMÁTICA FORENSE A LA CI.....	6
5.- CONCLUSIÓN: 4 MEDIOS, 4 EJÉRCITOS.....	9

1.- Introducción

No sabemos cómo será la inteligencia en el futuro, pero sí podemos imaginarnos considerando el presente, que la ciencia forense aplicada a la informática, será decisiva a la hora de concebir estrategias digitales de contrainteligencia.

La informática avanza a una velocidad tal, que es absolutamente imposible que una sola persona pueda dominar con soltura todas y cada una de las disciplinas en que se divide. Es más, dentro de la disciplina de seguridad informática, el rango de especialidades es tan amplio, que para realizar un test de penetración en sistemas informáticos de cierta entidad, es necesario un equipo de personas expertas en ramas diferentes, y a veces, en niveles o lenguajes concretos (para el caso de los expertos en programación) dentro de una misma rama. Salvo raras excepciones, dado el vertiginoso avance de los sistemas, ya no es posible que un solo hacker sea capaz de entrar, en un periodo de tiempo razonable, donde se proponga.

La informática forense, que podemos decir que está en fase inicial de desarrollo, no debe ser sólo vista como una herramienta de investigación complementaria en casos policiales, sino que hay que considerarla como la base de la contrainteligencia en ese “nuevo” medio que **aún no está del todo asimilado como tal**: el ciberespacio¹.

Los ataques en internet son continuos y la intención, dentro del campo de la recopilación de información, generalmente es pasar inadvertido. Según el nivel del objetivo en cuestión es la complejidad de los ataques.

Para los casos de Seguridad Nacional (entendiendo como tales aquellos que afectan a las infraestructuras consideradas críticas y a las empresas en las que se apoya la economía nacional), donde los ataques son verdaderas obras maestras de la ingeniería informática, no basta con tener expertos en seguridad dedicados al blindaje de redes. Si el éxito de un ataque informático de alto nivel, depende de la minuciosidad y la paciencia del atacante, es fácil intuir que no será trivial detectarlos y es ahí precisamente donde entra en juego la informática forense.

¹ Recomendamos la lectura del artículo [“LA CARRERA ARMAMENTÍSTICA EN EL CIBERESPACIO”](http://www.segloser.com/articulos/seguridad_informacion/cibermisiles.pdf)
(http://www.segloser.com/articulos/seguridad_informacion/cibermisiles.pdf)

2.- Software: El “Nuevo” Agente Doble

Los intereses económicos por desarrollar herramientas de software funcionales, avanzadas, rápidas, atractivas y eficaces, han provocado que se anteponga la velocidad de producción a la seguridad en el proceso de elaboración de software. La consecuencia inmediata es, sin duda, la puesta en circulación de infinidad de productos vulnerables que facilitan la toma de control remoto de sistemas informáticos. Pero no sólo el software es preocupante, como luego veremos a la hora de describir las posibles amenazas “built-in” en el hardware.

Antes, era preciso desenmascarar a empleados propios desarrollando labores de recopilación y filtración de información al bando contrario (insiders). Ahora tenemos un nuevo actor que desempeña ese mismo papel: el software (que, repetimos, no siempre viene solo). **Este nuevo actor, es el agente doble del mundo digital en el futuro (entiéndase presente)**. Está en nuestras redes, oye lo que decimos, ve lo que hacemos, lee nuestros informes, aprovecha nuestras ideas, percibe nuestras inquietudes, comprende nuestras prioridades y además, es capaz de transmitir toda esta información a aquellos para los que realmente trabaja. Y mientras no es descubierto, campa a sus anchas por nuestros sistemas. Pero, ¿cómo es posible que esto suceda con la cantidad de personal que hay dedicado a asegurar nuestras redes informáticas contra intentos de intrusión?

Antes de contestar a esa pregunta, con las respuestas que podrían encajar, vamos a recordar en qué consiste una APT o Advanced Persistent Threat. Como se deduce de su traducción al español, se trata de una Amenaza Avanzada Persistente, lo cual significa que nos enfrentamos a un ataque informático de alta sofisticación, que además está concebido para tener efecto a largo plazo. El problema es que muchos de estos ataques fueron lanzados tiempo atrás y la información que se obtuvo y se sigue obteniendo con ellos, permite al atacante elaborar los perfiles de comportamiento que le facultan para mantener y desarrollar intrusiones futuras. Es decir, que ataques pasados han obtenido tales frutos, que incluso dedicando todos los medios a nuestro alcance para asegurar nuestras redes, en algunos casos no bastaría para impedir que continuaran las intrusiones, salvo que empezáramos de cero.

Detectar pues estas APT es crucial y es ahí donde radica la importancia de la informática forense como herramienta indispensable para desenmascarar a esta nueva especie, el doble agente digital, que surge como consecuencia del desarrollo tecnológico. Un agente “entrenado” por humanos para engañar a las máquinas. Precisamente, por enfocar las soluciones principalmente en sistemas anti-intrusión, se deja como segunda prioridad la investigación de vías que podrían conducirnos al descubrimiento de procedimientos de ataque, hasta ahora impensados. **Estamos demasiado ocupados con tanto ataque “EVIDENTE”** (no olvidemos lo que nos ha enseñado la electrónica en el pasado en relación con las TSCM, con ejemplos como las paredes repletas de diodos).

Hablando en términos clásicos, tenemos básicamente dos tipos de agente doble: el infiltrado en nuestras filas y el reclutado por el bando contrario.

En el caso de la informática podemos, a grandes rasgos, hacer la misma clasificación:

- El software que adquirimos y resulta contener de serie puertas traseras o código malicioso oculto para realizar funciones de recopilación de información, se correspondería con el infiltrado
- Y el software que es fiel a nuestros propósitos, pero vulnerable de una u otra forma (bugs), es “reclutado” por los hackers para convertirse y facilitarles información (exploits).

El hecho de confiar en software no nacional (o no revisado concienzudamente por las autoridades competentes) para asuntos de Seguridad Nacional es un riesgo que jamás habríamos corrido en cuanto a recursos humanos se refiere; ¿por qué entonces se ha hecho con el software? ¿Quién de los lectores sabe exactamente qué hace y cómo lo hace el sistema operativo que acaba de recibir **gratuitamente** con los nuevos ordenadores que sustituyen a los antiguos de su departamento?

Aproximadamente, sólo un 30% de las APT son detectadas pese a tener la más alta tecnología en seguridad informática instalada. Ni siquiera los firewalls, antivirus, IDS (Intrusion Detection System) o IPS (Intrusion Prevention System), pueden detener eficazmente el avance de estos ciberataques. Sin embargo, que no haya evidencia de ataques, no es óbice para no invertir tiempo, esfuerzo y medios en su detección.

Podemos decir que hasta ahora estamos aplicando la informática forense para desenmascarar a humanos, analizando sus rastros digitales. Se analizan los archivos que contienen imágenes para revelar el uso de técnicas esteganográficas (viejas conocidas), archivos cifrados, archivos aparentemente dañados (con el encabezamiento alterado para no saber qué software permite leer la información que contiene), etc. Pero el enfoque debe ir más allá de la mera obtención de evidencias inculpatorias, dado que **nuestros mecanismos automáticos de detección, no son capaces de frenar el avance de las APT**. Es imperiosamente necesaria la presencia de equipos humanos que “manualmente” detecten, identifiquen y analicen los ciberataques de vanguardia.

La informática forense, pese a ser relativamente nueva, ya es difícil de dominar en conjunto y tal como ocurre en la medicina forense, existen diversas especialidades. Software, redes físicas, virtuales o inalámbricas, hardware, telefonía, etc., son sólo algunos campos donde se entremezclan diferentes técnicas y herramientas específicas, asociadas a los distintos elementos que podemos encontrar en el proceso de investigación de ataques informáticos.

3.- Hardware: Cobertura Perfecta



En muchas ocasiones, cuando hablamos de Seguridad Nacional, cierto grado de paranoia no es sólo habitual sino que en determinados casos está justificada. Cuando se descubrió el primer móvil con tecnología Infinity incorporada, una de las medidas de seguridad que se implementaron inmediatamente, fue la prohibición de portar teléfonos móviles durante reuniones sensibles, aunque estuvieran completamente apagados. Después vinieron el resto de dispositivos (porque no era necesario tener aspecto de teléfono para incorporar un sistema de transmisión Infinity y además ahora ya no se requiere modificar físicamente el terminal, bastando la instalación del software adecuado, que además integra **muchísimas** más funciones).

¿Paranoia? No. Simplemente aplicación profesional de protocolos de seguridad.

Al igual que ese tipo de dispositivos se distribuyen libremente, existen desde hace mucho tiempo equipos hardware o simples periféricos con capacidades extraordinarias de almacenamiento y transmisión de información. Pero no estamos aquí para hacer una relación de los equipos que pueden resultar peligrosos para la seguridad de nuestra información electrónica o informáticamente, sino para concienciar de los riesgos que se corren si no se aplican determinadas políticas.

Estamos habituados a ver como la mayoría de la población consiente un alto porcentaje de invasión en su privacidad. Quizás por no saber evitarlo, posiblemente por no considerar esos datos valiosos o por admitirlos como pago por tanto software y servicios web gratuitos (Facebook me permite “**gratis**” estar conectado con la gente que más quiero, pero, ¿de verdad no se paga con nada?).

¿Y si se aceptara también pagar el mismo “**insignificante**” precio por cierto hardware gratuito? Cuando se empezó a utilizar el Spyware con fines de espionaje comercial, nadie era consciente (al menos a nivel usuario), pero ahora que lo son, siguen sin poner barreras realmente efectivas. ¿Se acabará implantando en el hardware un software de recopilación de información del usuario? ¿Se estará haciendo ya a nivel masivo? Dejaremos sin responder estas preguntas y que el tiempo nos dé la contestación. Pero sí haremos hincapié en los numerosos casos que ya se han dado a nivel usuario, en los que se ha utilizado hardware con un software preinstalado, que permitía la vigilancia remota o el seguimiento de actividades con posterioridad (soluciones caseras algunas, pero ya en las mentes de nuestros ciudadanos...).

Sirvan como ejemplo los cientos de dispositivos físicos comunes que gozan ya de software embebido, permitiendo analizar a posteriori comportamientos, preferencias, hábitos, etc. Sin ir más lejos, los actuales ordenadores a bordo de los coches, almacenan una serie de datos que ayudan a levantar

perfiles concretos (en este caso el conductor). ¿Y si el hardware del futuro (léase de nuevo presente), empieza a incorporar, de serie, elementos de auto-diagnóstico, capaces de registrar patrones de tecleo, datos biométricos, localización y un sinfín de datos más? ¿Serían los únicos dispositivos incorporados por los fabricantes o cabe la posibilidad de sorpresas?

Las respuestas a estas cuestiones las dará la informática forense llegado el momento, en los casos en que se requiera la implementación de políticas profesionales de seguridad de la información. Pero hasta entonces no estaría de más, al menos, considerar esta opción como bastante probable, teniendo en cuenta la evolución que ha seguido el software.

4.- Aportes de la informática forense a la CI

Para desarrollar una férrea estrategia de contrainteligencia digital, se requiere detectar y evaluar cómo explotar cualquier intento ilegítimo de recopilación de información. Llevar a cabo esa detección implica considerar algunas de las siguientes sugerencias:

- a) Efectuar un minucioso análisis de software en busca, no sólo de nuevas vulnerabilidades explotables, sino de los posibles rastros dejados durante explotaciones posiblemente ya acaecidas.

Podemos ver en determinadas páginas de internet, el incesante flujo de información que se publica cada día en relación con el descubrimiento de nuevas vulnerabilidades. El resultado de este trabajo es en realidad el que se obtendría de un pormenorizado análisis forense a nivel de código, que permite detectar y corregir muchas vulnerabilidades de software. Por desgracia, conocer y reparar ciertas vulnerabilidades no dificulta en gran medida la actuación de una APT una vez introducida en los sistemas. El parcheo del software no repara el daño en curso, sólo impide que no puedan acceder por esa puerta nuevas APT, pero las que están dentro siguen ahí hasta que sean descubiertas. Hasta la fecha, raro es el que analiza su ordenador en busca de evidencias de explotación tras parchear su sistema operativo. Sin embargo, si realmente queremos proteger nuestros sistemas de forma correctiva, además de intentar anticiparnos a los Black Hackers en la búsqueda de nuevas vulnerabilidades, es preciso analizar los rastros que pudieran haberse generado en la explotación de vulnerabilidades sobre las que se supone que hemos aplicado las correspondientes actualizaciones de seguridad. El factor que juega siempre en nuestra contra es el tiempo, haciendo muchas veces inviable la labor correctiva de software, restringiéndonos al análisis exclusivo de las vulnerabilidades que se informan.

¿Cuál es la solución entonces?

El desarrollo de software hoy en día es de una complejidad tal, que el número de errores que se producen en el proceso de programación es muy alto. La mayoría de las ocasiones, no se

trata de errores que repercutan directamente a la funcionalidad, incluso es posible que esos errores no se detecten nunca, pero sí permiten, como estamos viendo a diario, la inserción de código malicioso que capacita al atacante para el control de las máquinas en las que se encuentran instalados.

Una de las alternativas que podría disminuir esta posibilidad, es la integración de los criterios de seguridad durante todo el proceso de desarrollo y mantenimiento, como medida preventiva, persiguiendo la certificación (por una entidad u organismo acreditado) en materia de seguridad del software en cuestión, lo cual facilitaría el trabajo de análisis que posteriormente tuvieran que hacer los forenses de código, como acción correctiva frente a los errores que no hubieran sido descubiertos durante el desarrollo.

Aunque siendo realistas, es bastante poco probable que eso suceda a corto plazo, hasta que no se someta a mayor presión a los fabricantes, por varios motivos:

- Se provocaría una disminución notable en la velocidad de producción de software, por lo que es más probable que se sometan a pruebas de control de calidad en relación con la seguridad en las distintas etapas de creación del software (pudiendo ser sólo la etapa final), que es un proceso mucho más rápido, en el que sólo tendrían que corregirse las vulnerabilidades que se encontraran (cuyo descubrimiento depende mucho de la metodología empleada) en esas auditorías previas al lanzamiento del producto en el mercado (lo cual ya es un pequeño paso adelante en cuanto a seguridad se refiere, pero no suficiente).
- Muchos proyectos software incorporan código de terceros, que puede no cumplir los requisitos, correspondiendo pues la revisión y certificación (independientemente de quién la realice) de este software, lo que implicaría retrasos burocráticos para esclarecer responsabilidades, explotación de derechos, etc.

También con respecto al software cabe destacar la carencia (al menos comercialmente no son comunes) de herramientas destinadas a la detección automática de vulnerabilidades explotadas y diagnosticar sus consecuencias. Por ejemplo, cuando nuestro antivirus se actualiza y detecta un troyano en nuestro sistema, que antes no constaba en su base de datos de firmas peligrosas, lo elimina, pero no nos informa de los daños sufridos hasta entonces (cambios acaecidos como consecuencia del ataque, las pérdidas de datos, el robo de información, etc.).

b) Muestreo y análisis del tráfico en la red

El tráfico durante las comunicaciones informáticas es de un volumen tan gigantesco, que analizar cada paquete de lo que circula por nuestras redes supondría toda una eternidad. Pero, por otro lado, no podemos confiar exclusivamente en los sistemas detectores de intrusión (IDS) puesto que las APT están diseñadas para evitarlos sin mucho esfuerzo.

En la informática forense no se pueden analizar todos los datos obtenidos, sino sólo los relevantes. En cuestión de redes, dada la cantidad de datos, determinar la relevancia no es sencillo y habrá que proceder a analizar secciones de tráfico, seleccionadas mediante técnicas de muestreo cuidadosamente calculadas (variables para evitar predicción), en busca de posibles intrusiones no detectadas por los IDS. Mediante la aplicación de técnicas forenses de análisis de tráfico en la red, puede aumentarse la probabilidad de detección de ataques y en consecuencia diseñarse planes más acertados de desinformación, contramedidas, sistemas de almacenamiento con cifrado de posición (es decir dividiendo en “n” partes el archivo y distribuirlos en base a un algoritmo que determina las posiciones en distintos directorios dentro de uno o varios dispositivos de almacenamiento locales o remotos), etc. Implica un esfuerzo humano y técnico superior, pero no deja exclusivamente en manos de máquinas la defensa contra ataques concebidos por humanos. Al menos, mientras no exista un dispositivo que realice ese trabajo forense de forma automática, habrá que seguir pensando en cómo hacer frente a un 70 por ciento de APT’s no detectadas y cuyas consecuencias podrían estar originando miles de millones de euros en pérdidas (por intentar cuantificarlo).

c) Inspecciones de hardware en busca de software incorporado

Debido a que un estudio en las tendencias de recopilación de información, ya sea con finalidad comercial, militar o civil, nos revela como muy probable que pronto el hardware de forma habitual incorpore software destinado a la toma de datos (en principio inocentemente), consideramos arriesgado no proceder a la inspección de todo equipo destinado a labores relacionadas con la Seguridad Nacional altamente clasificadas.

A parte de dichas inspecciones, para los casos en que se considere necesario por la certeza de la existencia de software integrado en el hardware capaz de almacenar datos, sería recomendable considerar recurrir a fabricantes nacionales (certificados por la autoridad competente) para la adquisición de ciertos equipos que fueran a ser utilizados en tareas de máximo secreto.

Así mismo, y bajo este exagerado punto de vista, la política de sustitución de hardware en el futuro deberá ser mucho más restrictiva, destruyendo completamente, no sólo los dispositivos de almacenamiento, sino la totalidad de aquellos equipos que hubieran estado aislados dado el carácter de la información que contenían.

Muchos pensarán que en cuanto los sistemas de detección descubran un programa solicitando salir a internet por el puerto que sea (independientemente de si está incorporado en el hardware o cargado con el sistema operativo), inmediatamente será considerado una amenaza para el equipo y se le impedirá la comunicación, pero no hace falta explicar que hay muchísimas formas de concebir el protocolo de comunicación y las actualizaciones de ese software “del equipo” (por ejemplo mediante GPRS integrado).

5.- Conclusión

Lo evidente no siempre es lo más peligroso

La velocidad evolutiva de los ataques informáticos es tal, que se dedican casi todos los esfuerzos a la construcción de barreras contra los nuevos e ingeniosos ataques sufridos a diario. Esto hace olvidar la importancia de una labor investigativa, forense por supuesto, que refuerce, y en ocasiones reoriente, toda esa dedicación y empeño por evitar intrusiones.

Tan importante es frenar los ataques como descubrirlos

Sobre todo en el ámbito de inteligencia. Es por eso que estimamos acertado adelantarnos al nuevo medio, el ciberespacio, y no esperar a ver si su evolución confirma la necesidad o no de disponer de un importante sector de nuestros efectivos dedicados a la investigación forense, que formaran parte de los despliegues de vigilancia humana permanente que el ciberespacio requiere (en vista del fracaso de los dispositivos automáticos). Ha llegado el momento de **integrar y considerar a la informática forense, dentro de las TSCM (Technical Surveillance Countermeasures)**, quedando así cubiertas todas las áreas de peligro potencial para los activos de información.

La atribución, sigue siendo uno de los mayores problemas en el ciberespacio

Pero quizás, invirtiendo medios en el desarrollo de esta relativamente nueva disciplina, la informática forense **enfocada al campo de la Defensa**, puedan desarrollarse técnicas en el futuro que nos ayuden con esa incógnita (recordemos que la ciencia ha logrado desarrollar, con el paso del tiempo, diferentes técnicas de análisis para la identificación de muestras de ADN, de las que antes era imposible obtener información). Pero, para intentar lograrlo, hay



que empezar desde una buena base, introduciendo en el sistema educativo formación altamente especializada en materia de investigación informática, preparando así a nuestros futuros “cibersoldados”.

Hoy en día, una costa sin barcos, un espacio aéreo sin aviones, un territorio sin soldados o un ciberespacio sin vigilancia, conducirían irremediabilmente al más estrepitoso de los desastres dentro de una nación. **Cuatro medios, cuatro ejércitos.**

28 de Junio de 2010

Eduardo J. Orenes Nicolás
Fundador y CEO de Servicios SEGLOSER®