EGUZKILORE

(Flor protectora contra las fuerzas negativas)

Cuaderno del Instituto Vasco de Criminología
San Sebastián, N.º 20 - 2006

EGUZKILORE
Número 20.
San Sebastián
Diciembre 2006
179 - 195

LA INVESTIGACIÓN POLICIAL EN EL ÁMBITO DE LA INFORMÁTICA

F. Javier INDA

Director del Gabinete de la Viceconsejería de Seguridad
Departamento de Interior. Gobierno Vasco

Resumen: La investigación policial en el ámbito de la informática tiene lugar cuando se produce la implicación, ya sea en calidad de medio o de "víctima", de un equipo o proceso informático en un delito. El ámbito material de este tipo de hechos delictivos requiere la existencia de un acceso físico o lógico a un sistema informático y la investigación subsiguiente se proyecta sobre evidencias directas o indirectas. Son, por tanto, requisitos para el desarrollo efectivo de una investigación policial en el ámbito de la informática, la existencia de una incidencia demostrada presuntamente delictiva, la determinación de una escena del delito y la protección de las evidencias existentes.

Laburpena: Talde edo prozesu informatiko baten inplikazioa ematen denean, nahiz baliabide nahiz "biktima" bezala, informatika eremuko polizia ikerkuntza jazotzen da. Delitu egitate hauen eremuak sarbide fisiko edo logikoa behar izaten du eta ondorengo ikerkuntza zuzeneko edo zeharkako nabaritasunean proiektatzen da. Informatikaren eremuan, polizia ikerkuntza eraginkorra betetzeko baldintzak honako hauek dira: ustez delitu den inzidentziaren existentzia, delituaren lekuko zehaztapena eta dauden nabaritasunen babesa.

Résumé: L'enquête policière dans le domaine de l'informatique a lieu au moment de l'implication, en qualité de moyen ou de "victime", d'un équipement ou d'un processus informatique dans une infraction. Le domaine matériel de cette sorte de délits requiert l'existence d'un accès physique ou logique à un système informatique, et la recherche ultérieure est projetée sur des preuves directes ou indirectes. Par conséquent, l'existence d'une incidence démontrée présumée délictueuse, la détermination d'une scène de l'infraction et la protection des preuves existantes sont les conditions pour le développement effectif d'une enquête policière dans le domaine de l'informatique.

Summary: Police investigation in computing takes place when a computer –or a computer process– is implied in a crime, as a mean or as a victim. This kind of crime requires the existence of a physical or logical access to a computer system, and the subsequent investigation will focus on direct or indirect evidence. Therefore, requirements for an effective police investigation in computer crimes are: the existence of an allegedly criminal proved event, establishing a crime scene, and protecting existing evidence.

Palabras clave: Delito informático, Investigación, Inspección, Evidencias, Estudio, Motivación.

Hitzik garrantzizkoenak: Delitu informatikoa, ikerkuntza, ikuskapena, nabaritasunak, azterketa, motibazioa.

Mots clef: Infraction informatique, Enquête, Inspection, Preuves, Étude, Motivation.

Key words: Computer crime, investigation, inspection, evidence, study, motivation.

INTRODUCCIÓN

Antes de abordar el núcleo de mi exposición es necesario realizar dos advertencias previas; la primera de ellas es relativa a la brevedad y concisión con la que forzosamente hemos de aproximarnos a lo que hoy se conoce como delincuencia informática o *ciberdelincuencia* y que daría, por sí misma, materia que excede nuestras posibilidades desde todo punto de vista; y la segunda es que, ante quienes señalan que hablar de este tema puede fomentar el perfeccionamiento de los métodos utilizados por los delincuentes informáticos, hay que decir que ello tendrá lugar en cualquier caso y que, como en el resto de ámbitos, un buen y actualizado conocimiento de la materia, unas herramientas adecuadas y una metodología de investigación eficaz nos permitirán poner a disposición judicial a los autores, los instrumentos, las evidencias y los efectos de este tipo de delitos. Y ello con independencia de los evidentes efectos preventivos que conlleva el hecho de un mejor conocimiento del "*modus operandi*" de estos delincuentes.

1. DELITOS VINCULADOS A LA INFORMÁTICA

1.1. Delitos No Informáticos

Existen una multiplicidad de conductas delictivas vinculadas a la Informática, la mayor parte de ellas subsumibles en tipos que ya recoge el Código Penal.

1.1.1. Asistidos por la Informática

– Tráfico de drogas: por ejemplo, ayudando a gestionar redes complejas de narcotráfico. Mediante la investigación pueden determinarse jerarquías, tipos de drogas, precios, etc…

– Terrorismo: por ejemplo, posibilitando el almacenamiento de información cifrada.

1.1.2. Facilitados por la Informática

– Amenazas, injurias, calumnias, etc. amparados en el anonimato de un correo electrónico o mediante teléfono móvil prepago ("*blackmail*").

– Infracciones a la Propiedad Intelectual y derechos de autor (lo que estrictamente se conoce como "piratería") en materia audiovisual o textos escritos.

– Fraudes cometidos mediante manipulación de ordenadores; en general este tipo de fraude tiene que ver con la finalidad de la empresa y se produce por empleados con acceso suficiente ("*insiders*").

– Sabotaje informático: cuando se establece una operación de programas de cómputo, como los relativos al suministro eléctrico o al corte de líneas telefónicas, etc…

1.1.3. Exclusivos con herramienta informática

– Daños a la propiedad, patrimonio, propiedad intelectual ("sabotaje").

– Manipulación de programas, ficheros, datos de salida.

1.1.4. Vía Internet como alternativa de elección (habitualmente utilizando servidores ajenos al país donde tienen lugar los hechos)

– Pornografía infantil: por la eficacia de distribución.

– Blanqueo de dinero: por la velocidad de la operación bancaria.

– Delitos económicos: fraudes, robos y estafas bancarias o en bolsa, estafas vía correo electrónico, etc… facilitados por factores como la codicia más la inseguridad sumadas a la velocidad de operación y al supuesto anonimato del autor. Por ejemplo, la utilización fraudulenta de tarjetas de crédito para el comercio electrónico o el desvío de fondos que, a través de programas especiales, alteran datos contables y alimentan sus propias cuentas bancarias.

– Racismo y Xenofobia.

– Difamación.

– Difusión de obras protegidas por el derecho a la propiedad intelectual: música, vídeo, textos. Actualmente hay en el mercado programas que permiten compartir ficheros de este tipo entre grupos de internautas.

1.2. "*Crimeware*"

Se trata de un conjunto de amenazas (realidades, diría yo) por medio de Internet consistentes en aprovechar eventuales debilidades de los usuarios para desarrollar conductas que buscan un beneficio directo o indirecto. Entre ellas podemos señalar como más conocidas:

– ***Hacking*:** Ataque a sistemas de información. Modalidad especializada en el acceso a los sistemas informáticos, identificación de sistemas de certificaciones para conectarse a una máquina no autorizada y conseguir acceso de administrador/superusuario.

– ***Lammers* ("pringao"):** *hacker* de poco conocimiento que entra a sistemas por el placer de causar daños. Suele dejar rastros y ser identificado con rapidez. También conocidos como "*Script Kiddies*" o "*Click Kiddies*".

– ***Cracking*:** Vulneración de claves o sistemas de protección de software.

– ***Phishing*:** Fraude bancario realizado usurpando páginas web corporativas de bancos, o explotando sus vulnerabilidades, y que tiene como fin hacerse con datos bancarios.

– ***Pharming*:** Fraude "on-line" que consiste en suplantar el sistema de resolución de nombres de dominio –DNS– para conducir al usuario a una página web falsa. Aunque es una amenaza creciente y peligrosa, la solución pasa por la prevención y una solución antivirus eficaz.

– ***Spamming*:** acción de inundar los servidores de Internet y los buzones de correo electrónico con un mismo mensaje no solicitado, provocando sobrecarga y, a veces, incluyendo virus (*Warspamming*: utiliza la red inalámbrica).

– ***Warez*:** Intercambio de archivos con "*copyright*" violando sus licencias. Normalmente se hace usando "Darknet" o redes similares y no se refiere a la falsificación comercial con beneficios.

– **Ciberchantaje:** Empresas e Instituciones son víctimas ocasionales de personas que amenazan con activar a distancia "bombas lógicas".

– **Ataques por saturación:** En general se trata de ataques contra lugares de los que se afirma que contravienen los grandes principios de la red; consisten en un bombardeo de "falsas cuestiones" que generan bloqueo de la red y que provienen de ordenadores "inocentes" con cuyo control se ha hecho el "pirata".

– **Ciberescuchas:** Intercepción de correos electrónicos en la red telefónica o los prestatarios de accesos, captando la radiación electromagnética emitida por los sistemas informáticos.

– **"Pirateo" de "*web*":** Bastante utilizado en el activismo político, consiste en la modificación a distancia del contenido de páginas web.

– ***Carders*:** Especializados en robos "informáticos" de tarjetas.

– ***Mailbombing*:** Acción de bloquear la mensajería electrónica de una persona enviándole un número considerable de mensajes electrónicos.

– ***Phreaking*:** "Pirateo" de una línea telefónica. Los piratas se conectan vía módem a los ordenadores, utilizando un generador de tonos que permite utilizar gratuitamente la red telefónica, como si se tratase de los propios técnicos de mantenimiento.

– **Ataques "*DoS - Denial of Service*" (Denegación de Servicio).**

El *hacker* tiene como objetivo dejar inservibles las máquinas para sus legítimos usuarios. Se trata de ataques que pretenden saturar los servidores de red de las compañías, dejando inaccesibles los enclaves *web*.

Los tipos más frecuentes son:

– Ataque "*Smurf*": el *hacker* satura la red con mensajes de respuesta "ping" *Internet Control Message Protocol* (ICMP). Envía solicitudes "ping" ICMP dirigidas a una dirección "*broadcast*" con la dirección fuente orientada hacia la máquina que se desea atacar. Todos los "*host*" de la red seleccionada responden con respuestas "ping" dirigidas a las máquinas objetivo, amplificando cientos de veces su mensaje original y ocultando la propia dirección real.

– Ataque TCP SYN: envía solicitudes falsas de conexión TCP (*Transmission Control Protocol*) a la máquina objetivo, sin estar completas las conexiones, desde una dirección "*spoofed*" (técnica en la que el atacante falsifica su dirección ocultando la identidad de su máquina). Tales solicitudes incompletas bloquean la "*request table*" del objetivo e impiden a éste aceptar cualquier otro tipo de solicitud de conexión.

– Ataque UDP: envía cantidad de mensajes UDP (*User Datagram Protocol*) al objetivo, saturando la amplitud de banda de la red de trabajo disponible.

– Ataque TCP: igual al anterior pero utilizando mensajes TCP, lo que crea la complicación de que la mayor parte del tráfico real en la red es de este tipo.

– Ataque *Distributed DoS*: replica el "*host*" atacante cientos de veces y lo distribuye por Internet. Controlados de forma remota y centralizada, la localización y cierre de una máquina permite que el resto siga activado.

Para todos ellos suelen utilizarse programas como *Trinoo, TFN, Stacheldraht, TFNak* y otros.

Para ello hacen uso de medios y herramientas como:

- ***Backdoor*:** puerta trasera o dispositivo insertado por el diseñador de un programa que permite eludir los controles de acceso al mismo (durante el 2006 ha supuesto un 13% de las incidencias, con tendencia a la baja).
- **Bomba lógica:** programa instalado en un ordenador y que permanece a la espera de una señal externa (utilización de un programa concreto o llegada de una fecha u hora) para activarse y causar daños importantes.
- **Caballo de Troya:** programa escondido en otro y que, al actuar éste, se activa simultáneamente, ejecutándose una serie de instrucciones para favorecer el acceso no autorizado o la destrucción (durante el 2006 ha supuesto un 50% de las incidencias, con tendencia a la baja).
- ***Sniffer*:** programa espía que intercepta las informaciones que circulan en las redes internas y las transmite al pirata.
- **Gusano (*Worm*):** programa autorreproducible que propaga copias de sí mismo a través de la red. Amenaza la integridad del sistema cuando se expande por él perturbando y sobrecargando la red (4,5% de las incidencias durante el 2006).
- **Virus:** programa que tiene como objetivo la alteración, el daño o la destrucción del sistema informático. Hay más de 15.000 virus censados y aparecen unos 200 nuevos cada día.
- ***Dialers*:** marcadores telefónicos automáticos a servicios de tarifación superior a la normal (4,0% de la incidencias producidas en 2006 y con tendencia al alza).
- ***Spyware*:** aplicaciones destinadas a obtener información del usuario sin que éste se dé cuenta.
- ***Adware*:** similar al anterior, y junto con *Spyware*, supone un 1,4% de las incidencias producidas en 2006, con tendencia al alza.
- ***Bots*:** diminutivo de "robots", suponen un 15% de las incidencias detectadas en 2006, con tendencia al alza.
- ***Rootkit*:** programas para ocultar puertas traseras en los ficheros ejecutables y servicios del sistema.
- ***Spoofing*:** herramientas para ocultar y suplantar direcciones IP.
- ***Keyloggers*:** programas que controlan el uso de un equipo y que incluso pueden ser conectados a una *webcam*.
- ***Screen recorders*:** capturadores de pantallas presentadas al usuario.

1.3. Especial referencia al fraude en Internet

Internet cuenta con un decálogo de prácticas ilegales publicado en una lista por la Comisión Federal de Comercio (FCT) de Estados Unidos en la que figuran los 10 fraudes más comunes realizados al amparo de la Red (es resultado de una iniciativa impulsada por los organismos de protección de los consumidores de varios países, entre ellos Alemania, Gran Bretaña o Canadá). En la lista se recogen hechos, además de los ya citados

anteriormente, como las estafas en subastas, fraudes con tarjetas de crédito, falsas oportunidades de negocio o engaños en vacaciones y viajes, que son algunas de las fórmulas que se recogen en la lista elaborada a partir de las reclamaciones de los usuarios.

1. Subastas: Algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos. Una vez que el consumidor ha enviado el dinero puede ocurrir que reciban algo con menor valor de lo que creían, o peor todavía, que no reciban nada.

2. Acceso a servicios de Internet: El consumidor recibe una oferta de servicios gratuitos. La aceptación lleva implícita el compromiso de contrato a largo plazo con altas penalizaciones en caso de cancelación.

3. Tarjetas de Crédito: En algunos sitios de Internet, especialmente para adultos, se pide el número de la tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años. El verdadero objetivo es cobrar cargos no solicitados.

4. Llamadas Internacionales: En algunas páginas, por lo general de material para adultos, se ofrece acceso gratuito a cambio de descargar un programa que en realidad desvía el módem a un número internacional o a un 906. La factura se incrementa notablemente en beneficio del propietario de la página (por extensión podrían añadirse los fraudes vía SMS).

5. Servicios Gratuitos: Se ofrece una página personalizada y gratuita durante un período de 30 días. Los consumidores descubren que se les ha cargado facturas a pesar de no haber pedido una prórroga en el servicio.

6. Ventas Piramidales: Consiste en ofrecer a los usuarios falsas promesas de ganar dinero de manera fácil sólo por vender determinados productos a nuevos compradores que éstos deben buscar.

7. Viajes y Vacaciones: Determinadas páginas de Internet ofrecen destinos maravillosos de vacaciones a precios de ganga, que a menudo encubren una realidad completamente diferente o inexistente.

8. Oportunidades de Negocio: Convertirse en jefe de uno mismo y ganar mucho dinero es el sueño de cualquiera. En la Red abundan las ofertas para ganar fortunas invirtiendo en una aparente oportunidad de negocio que acaba convirtiéndose en una estafa.

9. Inversiones: Las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y comportan grandes riesgos para los usuarios. Como norma general, no es recomendable fiarse de las páginas que garantizan inversiones con seguridad del 100%.

10. Productos y Servicios Milagro: Algunas páginas de Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias. Hay quienes ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

A ellas pueden añadirse:

11. Notificación de Ofertas y de Premios: Por medio de correos electrónicos o anuncios se informa de una posible oferta de empleo o de un premio.

12. Productos Promocionales: Por medio de correos electrónicos o anuncios se captan "asociados" a los que se promete el envío de una serie de productos al mes, a domicilio y totalmente gratis.

13. Publicitación de servicios sobre números de teléfono de tarificación especial (803, 806 y 807) en foros de Internet en los que no se informa del coste real de la llamada.

14. Manipulación de aparatos electrónicos sin autorización: Incluyen algunos fraudes en tarjetas telefónicas, tarjetas de televisión de pago, manipulación de máquinas tragaperras, teléfonos móviles, etc… mediante indicaciones logradas en Internet.

En general, sea cual sea el "*modus operandi*" elegido, el mejor modo de neutralizar este tipo de fraudes es difundir ampliamente la existencia de tales prácticas entre la población a los efectos de que su conocimiento evite las mismas.

2. DESARROLLO DE LA INVESTIGACIÓN

2.1. Preparación del equipo

Es conveniente disponer de un equipo mínimo de trabajo que incluya:

- CD-Rom con herramientas de sistema para diversos sistemas operativos.
- Discos duros externos: generalmente discos USB, aunque puede ser necesario disponer de discos SCSI, discos vía serie/paralelo o incluso un equipo portátil completo. Muchos sistemas operativos (Windows NT por ejemplo) no soportan el estándar USB, otros no tendrán interface SCSI...
- Disquetes.
- Cuaderno de notas.
- Cámara de fotografía o videograbación: permitirán fotografiar o filmar evidencias, posibilitando añadir documentación gráfica a nuestro informe final.

2.2. Operaciones Básicas de Investigación

- Análisis de Contenido: Estudio para determinar qué tipos de ficheros existen en un ordenador.
- Comparación de Archivos: Estudio que compara archivos informáticos con archivos y documentos conocidos.
- Análisis de Transacciones: Estudio que puede determinar datos relativos al momento y secuencia de creación de un archivo.
- Extracción: Acto de extraer archivos de datos de un ordenador o sistema de almacenamiento.
- Identificación de Ficheros Borrados: Ficheros de ordenador o sistema de almacenamiento que se pueden intentar recuperar.
- Conversión de formato: Los archivos pueden convertirse desde un formato a otro.

- Búsqueda de Palabras Clave: Técnica de localización de archivos a través de palabras o frases.
- Recuperación de Palabra de Paso: Pueden recuperarse y utilizarse para decodificar archivos codificados.
- Identificación del Código Fuente: Puede ser analizado y comparado.

2.3. Secuencia de Investigación

La secuencia habitual de la Investigación Policial en el ámbito de la Informática incluye:

1. Recepción del aviso del incidente.
2. Verificación del incidente.
3. Establecimiento del perímetro físico y protección de la escena del delito y de las evidencias. Ver a).
4. Delimitación del perímetro lógico. Ver b).
5. Obtención de evidencias: criterios de obtención, prioridades y cadena de custodia. Ver c).
6. Análisis de las evidencias. Ver d).
7. Desarrollo de la investigación. Ver e).
8. Elaboración de las conclusiones.

Como se puede ver, la secuencia introduce pequeñas variaciones sobre los procedimientos habituales en razón de la especialidad de la materia; abordaremos únicamente tales variaciones.

a) En relación a la Escena del Delito

- Premisas a considerar:

– Puede no limitarse a una localización física.

– Puede incluir equipos, sistemas operativos, redes, impresoras y papel impreso, papeleras físicas y ficheros telefónicos.

- Procedimiento estándar:

– Delimitar y asegurar la escena.

– Preparar la inspección ocular.

– Aproximarse y realizar una inspección preliminar:

- Identificar el tipo de ordenador y su(s) sistema(s) operativo(s).
- Identificar el tipo de programa de red, la ubicación de los servidores, el número de ordenadores y terminales.

- Determinar si se utilizan sistemas de seguridad y cuáles: encriptación, *password*, etc…
- Determinar si las evidencias son trasladables o han de estudiarse "in situ". Si hay que trasladarlas, mejor en su embalaje y con las protecciones originales o plástico de burbujas. No utilizar *"styrofoam"* porque penetra en los aparatos. Sellar con cinta adhesiva fuerte. Trasladar en posición vertical previa colocación de etiquetas exteriores "frágil", "esta cara hacia arriba", "equipo electrónico" y "mantener alejado de imanes o campos magnéticos".
- La misma sistemática es aplicable a la electrónica de consumo como teléfonos digitales, PDA, mensáfonos, máquinas de fax, cámaras de fotografía o vídeo digital, grabadoras digitales, MP3/MP4, GPS y similares.

– Procesar el escenario del delito: narración, fotografía y vídeo.

– Valorar posibles evidencias y recogerlas (atención a la cadena de custodia).

• Normas específicas

– NO permitir acceso de usuarios habituales a los sistemas comprometidos.

– NO reiniciar ni apagar máquinas salvo estricta necesidad.

– Obtener identificación, datos y fotografías, de todos los equipos en servicio.

– Disponer de un archivo con las herramientas necesarias.

• Tomar una decisión previa en función de las circunstancias:

Circunstancia	Decisión	Ventajas	Desventajas
Investigadores no expertos	Desconectar Equipo	Evitar errores en la escena Facilita la tarea investigadora Ahorra tiempo	Sólo aplicable a PC Puede bloquearse el disco
Ordenador conectado Investigadores familiarizados	Chequear "Hardware"	Evita quejas sobre daños ulteriores	Requiere más tiempo y personal experto
Ordenador conectado Datos valiosos	Efectuar "Backup"	Evita pleitos	Mayor inversión de tiempo Riesgo de dañar la evidencia
No se traslada el ordenador Es necesario localizar inmediatamente la evidencia	Investigación "in situ"	Es el método más rápido para localizar la evidencia	Puede destruir alguna evidencia poco significativa Se incrementa el riesgo de destruir alguna evidencia crítica

b) En relación a la Delimitación del Perímetro Lógico

Dependiendo de los sistemas involucrados, y de la necesidad de servicio del cliente, así como la criticidad de los datos, podemos tener diferentes visiones del perímetro lógico según que el servicio:

A. PUEDA DETENERSE

1. Bloquear mediante un firewall todas las conexiones entrantes y salientes de/a los sistemas comprometidos (NUNCA desconectar cables de equipos ni aplicar reglas de filtrado en los equipos mismos).
2. Examinar toda la información que el sistema nos proporcione antes de iniciar una sesión (monitores, "*syslog*" remoto...).
3. Iniciar sesión en los equipos desde la consola de estos.
4. Evitar los accesos remotos (alteran las evidencias de acceso remoto, pueden existir "Caballos de Troya" que detecten el acceso remoto).
5. Obtener todas las evidencias y APAGAR LOS EQUIPOS.

B. NO PUEDA DETENERSE

1. Instalar como primera medida un analizador de tráfico ("*sniffer*", "*iris*", "*ethereal*", "*tcpdump*") que capture TODO el tráfico de/a los equipos comprometidos.
2. Iniciar sesión en los equipos desde la consola de estos.
3. Evitar los accesos remotos (alteran las evidencias de acceso remoto, pueden existir "Caballos de Troya" que detecten el acceso remoto).
4. Arrancar aplicaciones de control y captura de pulsaciones en terminales ("*keyloggers*", "*ttysniffers*"...).
5. Preparar máquinas de reemplazo para sustituir las que están dando servicio (si esto no es posible, debemos obtener de inmediato la mayor parte posible de las evidencias.

c) En relación a la Obtención de Evidencias

• Criterios:

– Generales:

1. Considerar cualquier Anomalía de Funcionamiento como un Incidente de Seguridad.
2. Intentar acceder al sistema a través de la terminal física.
3. Llevar a cabo una documentación adecuada de la anomalía (almacenamiento / fotografía).
4. Efectuar Control de la Hora y de los Relojes de los equipos involucrados ("*Timestamp*").
5. Averiguar posibles desfases horarios de los relojes de los equipos involucrados (buscar sincronización de hora, NTP, RDATE).
6. Recoger eventuales elementos anómalos de modo exacto (páginas modificadas, ficheros o usuarios añadidos) para intentar aproximarnos al método de ataque.

– Específicos:

1. Si los procesos se encuentran:

A. En ejecución
   - Obtener listado detallado de los procesos/aplicaciones en ejecución.
   - Obtener listado de módulos dinámicos corriendo dentro del *kernel* (LKM, modules).
   - Obtener listado de todos los controladores de dispositivos en uso ("Caballos de Troya").

B. En arranque
   - Examinar archivos de arranque del sistema.
   - Obtener listado detallado de las aplicaciones que se ejecuten (registro de Windows, etc…).

2. Verificar tareas programadas: examinar *crontabs* y *schedulers* de todos los usuarios.
3. Si es posible, obtener un *backup* de la memoria de la máquina.
4. Identificar y obtener listado de librerías precargadas y librerías dinámicas (se puede configurar la carga).
5. Obtener listado de conexiones abiertas (puertos TCP/UDP,…).
6. En relación a los ficheros: obtener listados completos de todos los ficheros (verificar su no modificación a través de firmas MD5 o SHA1) de modo recursivo (total, de los abiertos, por tipos de archivo, por fechas de creación o modificación, de ejecutables, de ficheros SETUID, de archivos de configuración, de ficheros con clave de usuario o de sistema).
7. Obtener listado de librerías abiertas (DLL).
8. Obtener históricos: copia de los históricos del sistema operativo y de las aplicaciones (Visor de Eventos de Microsoft).
9. Extraer archivos de configuración: los vinculados a procesos del arranque o en ejecución.
10. Obtener imagen física del disco duro: pueden recuperarse ficheros borrados.
11. En relación a Sistemas Adjuntos: actuar de modo similar en el mismo segmento de la red o accesibles.

• Prioridades

El orden de prioridad en la obtención de evidencias requiere inspeccionar:

1. Microprocesadores, Registros (eax, ebp,…), *Caché*, Memoria de Periféricos (RAM de vídeo).
2. Memoria física, "*Swap*", "*Kernel*" (RAM a través de direcciones físicas, "*swap*" como partición del sistema operativo, etc…).
3. Conexiones y Estado de Red (si existen conexiones abiertas, puertos escuchando, etc…).

4. Procesos en Ejecución (incluido llamadas al sistema que hagan los procesos).
5. Discos Duros Locales (posibles directorios modificados, ficheros borrados, discos de arranque o de sistema afectados, etc…).
6. Discos externos, unidades de *backup* (RW).
7. CD-Rom, discos de solo lectura o documentos impresos.

• Cadena de Custodia

Es necesario:

1. Definir las herramientas admitidas: cuáles, para qué y en qué ámbito.
2. Identificar los Responsables de Área según su especialidad.
3. Establecer Puntos, Pasos y Responsables, en la Cadena de Custodia de Evidencias (incluyendo firma o "*log*" de cada acción).
4. Definir métodos de almacenamiento y etiquetado comprensible de evidencias (junto a su TIMESTAMP y su MD5 ó SHA1).
5. Definir los métodos de recuperación y localización de evidencias (a través de una aplicación específica o una base de datos normal).

d) En relación al Análisis de las Evidencias

• Discos

1. Observar como premisa fundamental: trabajar siempre sobre imágenes de discos.
2. Utilizar "*strings*" y "*grep*".
3. Obtener todos los MAC (Modification Access Creation Timestamp).
4. Obtener listados de ficheros.
5. Obtener listados de "*inodes*" para intentar recuperar "trazas" borradas.
6. Obtener firmas MD5 y/o SHA1 de todos los ficheros (para poder comparar con ficheros oficiales).
7. Realizar búsquedas de palabras clave dentro de los ficheros.

• Ficheros

1. Observar como premisa fundamental: trabajar siempre sobre imágenes de disco.
2. Tener presente que encontraremos medidas de seguridad (borrado seguro, reposicionamiento de ficheros, etc…).
3. Obtener imágenes del espacio no utilizado (ficheros eliminados).
4. Buscar cadenas de texto típicas en lo recuperado (por ejemplo, trozos de código fuente en "C").

e) En relación al Desarrollo de la Investigación

• Análisis de Redes

Las redes informáticas con las que nos podemos encontrar son, en general, de cinco tipos:

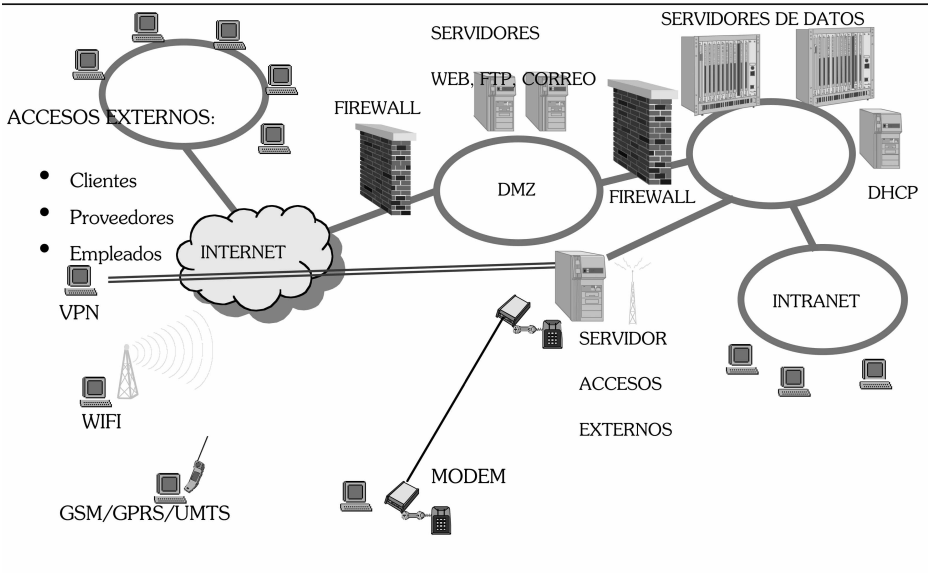
1. Redes pequeñas: los problemas se plantean frecuentemente por fallos de seguridad en la máquina PROXY (que suele ser Microsoft con Proxy Server y actúa como PDC de la red).

2. PYME: suelen atacar el servidor web con el objetivo de alcanzar la máquina PROXY y utilizarla como reflector (tiene lugar la intrusión y lo convierte en PROXY de sus propias conexiones) para intentar aprovechar un posible acceso privilegiado que la PYME pueda tener con otra empresa más grande. A veces, el problema está en una máquina interior.

3. PYME Grande: habitualmente utilizan un cortafuegos (firewall) para separar la red interna del exterior (servidores de correo, web, etc…). Es importante revisar el cortafuegos y la gestión de las conexiones externas.

4. Pequeño ISP (proveedores de servicios): en general disponen de equipos dedicados a las conexiones de clientes en las que, a veces, está disponible un IDS. El seguimiento de los log de los "firewall", del IDS y del servidor de terminales puede ser de utilidad.

5. Grandes Sistemas Corporativos: en la práctica son una suma de los anteriores. Su investigación requiere descomponer el problema, investigarlo por apartados y encajar los resultados.



Estructura Básica de un Sistema Corporativo

3. EJEMPLOS DE LOCALIZACIÓN DE INTRUSOS

3.1. Supuesto TCP/IP

1. Identificación de Dirección IP de destino

– Asociada a un nombre de dominio público

– Registrada en una base de datos accesible o un log de otro servidor

– Obtenida a través de RIPE/ARIN/APNIC

– Conseguida por procedimientos aleatorios

2. Identificación de Dirección IP de origen ("*inetnum*")

– Direccionamiento privado: suele utilizarse para lanzar ataques desde los rangos 10.0.0.0/8 – 192.168.0.0/16 – 172.16.0.0–172.31.255.255.

– Acceder a "*whois*" via *web* (www.ripe.net/ripencc/pub-services/db/whois/whois.html) o utilizar herramienta similar.

– Obtenido el "*netname*" sabemos con quién contactar y quienes gestionan las direcciones (*admin-c* y *tech-c*).

– Podemos efectuar una localización geográfica (latitud y longitud):

http://www.networldmap.com/TryIt.htm
http://visualroute.visualware.com/
http://www.caida.org/tools/utilities/netgeo/
http://netgeo.caida.org/perl/netgeo.cgi

– "*Backtrace*": se investiga la ruta hasta la dirección IP de origen ("*tracert*" en Windows); a veces resulta complicado si es a través de varios países; puede requerir una orden judicial pero hay que tener en cuenta que el titular de la supuesta IP de origen puede ser a su vez sólo un Receptor o Amplificador.

3.2. Correo electrónico

1. Datos de Cabecera

Return-path: emisor original y reenvíos intermedios

Received: una referencia añadida por cada salto

Delivered to: receptor real

To: receptor aparente

Reply to: destinatario real de la respuesta al correo electrónico

X-Mailer: programa de correo que envió el mensaje

2. Datos de Cuerpo

Detalles del emisor

3.3. Logs y otras Bases de Datos accesibles

1. Buscar IP en listas de "*spammer*" (http://www.spancop.net) o alianzas de detectores de intrusos (http://www.incidents.org ó http://feed.dshield.org/block.txt)
2. Buscar en directorios como *four11, whitepages* y otros.

4. LA MOTIVACIÓN EN EL DELITO INFORMÁTICO

Tras habernos aproximado de un modo general al "*modus operandi*" de los delincuentes informáticos y haber repasado algunos de los aspectos más básicos de la investigación de estos delitos, desde el ámbito de la Criminología nos queda efectuar un esbozo sobre las motivaciones que impulsan a este tipo de delincuentes que, sin ánimo de exhaustividad, podemos resumir en las siguientes:

a) Económicas

Orientadas al mero beneficio personal.

b) Lúdicas

Como expresión de ocio y distracción.

c) Ideológicas

Con connotaciones políticas y, habitualmente, objetivos institucionales.

d) Psicológicas:

– **Individuales:**

• **Compensación**

Se trataría de personas que aquejan una falta de confianza en sí mismas y que intentan recuperarla utilizando medios de baja agresividad, con la idea de que la víctima puede sentirse atraída por su conducta.

• **Asertividad**

Este tipo de personas manifiestan una necesidad compensatoria que intentan satisfacer utilizando medios altamente agresivos, expresados incluso a través del control o humillación de la víctima, intentando recuperar un sentido de autoridad.

• **Desplazamiento de la angustia**

Esta alternativa sugiere expresiones de rabia de los autores hacia personas o colectivos específicos, que llegan a ser materializadas incluso con gran variedad de lesiones o muertes. No se trata de sádicos sino de hiperagresivos.

• **Sadismo**

En este caso, los autores obtienen gratificación sexual del dolor y sufrimiento de sus víctimas ocasionado a través de este tipo de conductas delictivas.

– **Grupales:**

Mediante sus conductas pretenden fortalecer la relación de pertenencia a un grupo o comunidad concreta de usuarios informáticos vinculados a este tipo de dinámicas delictivas, creando una subcultura propia.

DIRECCIONES DE INTERÉS

- Ertzaintza
  delitosinformaticos@utap.ej-gv.es
- Internacional
  www.cert.org

AGRADECIMIENTOS

El autor agradece al Centro de Elaboración de Datos para el Servicio Policial - CEDSP, órgano adscrito a la Viceconsejería de Seguridad, y a sus integrantes, la colaboración prestada para llevar a buen fin el presente trabajo.

BIBLIOGRAFÍA

BUGGISCH W.; KERLING Ch. "'Phishing', 'Pharming' und ähnliche Delikte". Kiminalistik 8-9 pp. 531-536 (2006).

CARRIER B. "File System Forensic Analysis". Pearson Education Inc N.J. (2005).

CASEY E. "Digital Evidence and Computer Crime". Academic Press London (2000).

CASEY E. "Handbook of Computer Crime Investigation". Academic Press London (2002).

CHIEN E. "Ciberviruses". Rev. Intersec, Vol. 10 Issue 11/12, pág. 378 y ss. (Nov/Dic 2000).

CLARK F.; DILIBERTO K. "Investigating Computer Crime". CRC Press Florida (1996).

COENRAETS "Cybersquatting. Un nouveau defi pour le federal Computer Crime Unit". Vigiles. Revue de droit de police num. 2 pp. 63-74 (2001).

CONSEIL DE L'EUROPE "Criminalité Organissée en Europe. La menace de la cybercriminalité". Strasbourg (2006).

CSI/FBI 1999 CSI/FBI Computer Crime and Security Survey (www.gocsi.com).

DEL MORAL TORRES A. "La Investigación de delitos informáticos". Rev. Guardia Civil pp. 30-32. Dic. (1997).

DUMORTIER J.; VAN OUDENHOVE B.; VAN EECKE P. "La Nouvelle Legislation belge relative a la criminalité infromatique". Vigiles. Revue du droit de police num. 2 pp. 44-62 (2001).

GOMEZ VIEITES "Enciclopedia de la Seguridad Informática". Ed. RA-MA Madrid (2006).

HERNÁNDEZ J.C.; SIERRA J.M.; RIBAGORDA A.; RAMOS B.; "Técnicas de detección de Sniffers". Rev. SIC. Agorasic, Noviembre, (2000).

HUERTA Ángel, "Ataques Denial - of - Service (DoS)". Rev. Seguritecnia. Marzo, pág. 160 y ss. (2000).

ICOVE D.; SEGER K.; VONSTORCH W.; "Computer Crime". O'Really & Associates Inc. CA (1995).

KINDLER W. "Kiminalität im Zusammenhang mit Iuk-Teknologien". Rev. Kriminalistik pp. 76 y ss. Núm. 2 (2004).

LATORRE J.I. "Protección de la información". Cuadernos de Seguridad pp. 77 y ss. (2001).

L'Essor – "Internet". Rev. L'Essor de la Gendarmerie Nationale, Núm. 316, Juillet, pág. 4, (2000).

LEVRANT MICELI S.; SANTANA S.A.; FISHER B.S. "Cyberagression: Safety and Security Issues for Women Worldwide". Security Journal. Perpetuity Press pp. 11-27 (2001).

MARSHALL A.M.; TOMPSETT B.C. "Span'n'chips. A discussion of internet crime". Science & Justice Vol. 42 pp. 117-122 (2002).

MÜLLER W. "Internetauktionen Gefahrenm Risiken und Vorsorge". Bayerns Polizei _ pág. 27-29 (2005).

NIELSEN D. "Criminalidad Informática y Cibernética". Congreso Int. "Nuevos retos en la investigación de delitos". Escola de Policia de Catalunya (1998).

PANG B. "Fighting Cyber-crime through global partnerships". Gazette RCMP Vol. 68 No. 3 pp. 34-35 (2006).

PANSIER F-J.; JEZ E. "La criminalité sur l'internet". Presses Univertitaires de France. Paris (2000).

PAYNTER R.L. "Tools for Cyber Sleuths". Rev. Law Enforcement Technology. July, pág. 86 y ss (2000).

R. ZARCO J.M. "La Investigación de los Delitos Informáticos, un reto profesional". Rev. Security Management núm. pp. 16-24 (?).

RAMÍREZ R. "Seguridad en Sistemas de Información". Chase The Sun. Parque Tecnológico de Alava (2005).

REBOLLO L. "Derechos Fundamentales y Protección de Datos". Ed. Dykinson S.L. Madrid (2004).

RODRÍGUEZ ALVAREZ DE SOTOMAYOR J.A. "Concepto de Delito Informático". Rev. Guardia Civil, Febrero, pág. 99 y ss. (1999).

ROSENBLATT K.S. "High Technology Crime". KSK Publications California (1995).

SOLER DE ARESPACOCHAGA JOSÉ A. "El Delito Informático ante el Nuevo Siglo". Cuadernos de Seguridad, Diciembre, pág. 23 y ss. (2000).

SPRANZA F.; SPRANZA M. "Filling the Ciber cop's toolbox". Law EnforcementTechnology pp. 174-183 Octubre (2000).

SPRANZA I. "Bringing Cyber Investigations inhouse". Law Enforcemente Technology February (2001) pp. 56-60.

U.S. Dept. of Justice "Handbook of Forensic Services". FBI Laboratory Publication (2003).

ZETTEL N. "Phishing". Bayerns Polizei _ pp. 30-31 (2005).