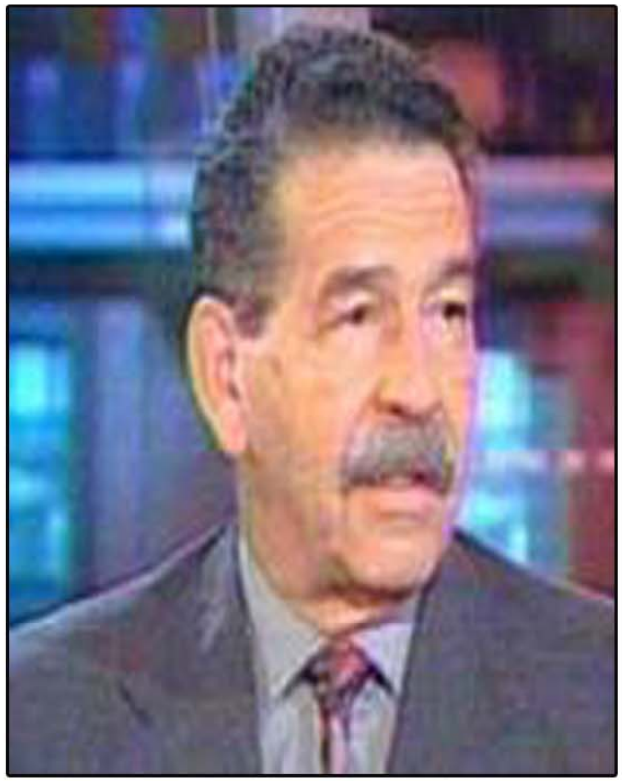
Conferencia Internacional
Delincuencia Organizada
y Derechos Humanos
Encuentro de expertos

Jueves 12 de junio 2008. Hotel Caracas Palace



DELITOS INFORMÁTICOS

Comisario

Elisio Antonio Guzmán Cedeño

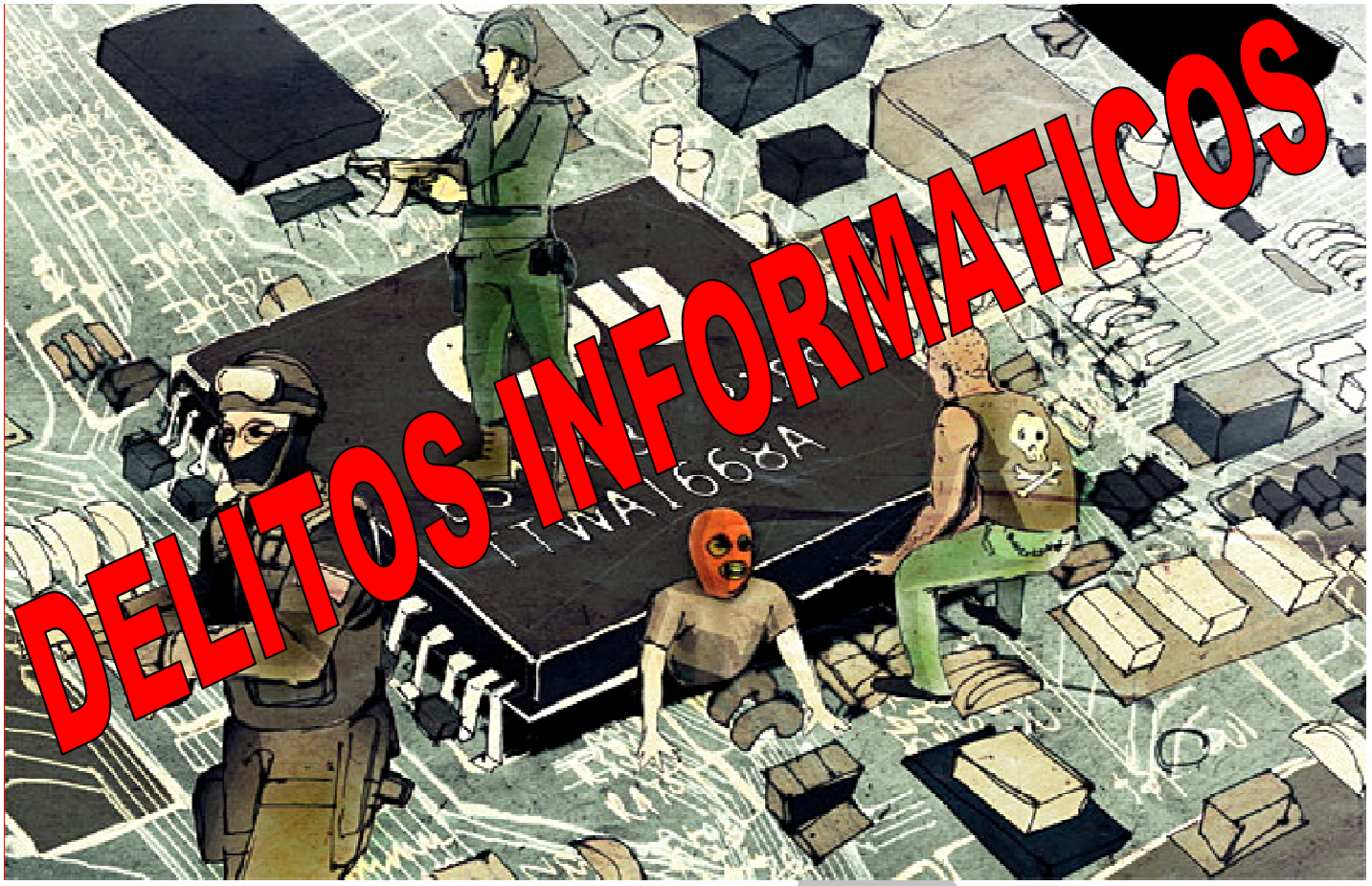
Ex director General

del Cuerpo Técnico de la Polícia Judicial

CENTRO DE ESTUDIOS DE DERECHOS HUMANOS UCV

EnCambio

Conferencia Internacional
Delincuencia Organizada
y Derechos Humanos
Encuentro de expertos
Jueves 12 de junio 2008. Hotel Caracas Palace



CENTRO DE ESTUDIOS DE DERECHOS HUMANOS UCV

EnCambio

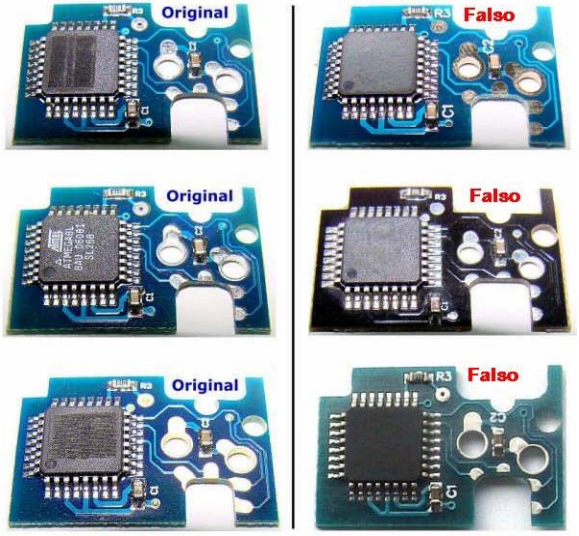
La clonación

(derivado del griego *κλων*, que significa "retoño") Puede definirse como el proceso por el que se consiguen copias idénticas de un organismo ya desarrollado, de forma asexual. Estas dos características son importantes:
- Se parte de un animal ya desarrollado, porque la clonación responde a un interés por obtener copias de un determinado animal que nos interesa, y sólo cuando es adulto conocemos sus características.

La falsificación

Es un acto consistente en la creación o modificación de ciertos documentos, efectos, bienes o productos, con el fin hacerlos parecer como verdaderos, o para alterar o simular la verdad.

Conferencia Internacional
Delincuencia Organizada
y Derechos Humanos
Encuentro de expertos
Jueves 12 de junio 2008. Hotel Caracas Palace



“Necesitamos revisar…cómo podemos asegurar que la gente no integre pequeños componentes… susceptibles de activarse de forma remota”

El pasado enero, dos hermanos de Texas, Michael Robert Edman, se presentaron ante la corte para enfrentar cargos federales por vender equipos computacionales apócrifos a organizaciones entre las que se encuentran las Fuerzas Aéreas, los Marines, la FAA, el Departamento de Energía, numerosas Universidades y contratistas de la defensa de los Estado Unidos, como Lockheed-Martin……

CENTRO DE ESTUDIOS DE DERECHOS HUMANOS UCV

EnCambio

Vemos el caso un fabricante y su teléfono celular 'Chocolate' que llegó al mercado asiático mucho más tarde que algunas falsificaciones de gran calidad.

El teléfono fue un fracaso comercial, ya que los clientes lo consideraron una mala copia de los modelos autóctonos.

Una de estas fábricas rechazó una oferta de Samsung arguyendo que ya ganaba bastante dinero vendiendo sus propios productos.

Un grupo de jóvenes, de edades entre los 16 y 20 años, formaban parte de un grupo de hackers 'D.O.M. Team 2008', que ostentaba el quinto puesto en el ránking mundial de ataques informáticos según Zone-H

Compraban equipos electrónicos de elevado valor, así como bolsos, ropa y joyas de marcas exclusivas, en algunas ocasiones encargados desde Rumanía.

Conferencia Internacional
Delincuencia Organizada
y Derechos Humanos
Encuentro de expertos
Jueves 12 de junio 2008. Hotel Caracas Palace

¿Como se lleva a cabo la falsificación de tarjetas de crédito por robo de identidad?

- Recogiendo extractos e información sobre datos personales directamente de la basura.
- Robo de correspondencia de los buzones, para obtener tarjetas de crédito, estados de cuenta, ofertas personalizadas, datos del seguro social, hacienda, etc.
- Accediendo a tu informe de crédito de forma fraudulenta, por alguien que se hace pasar o es empleado de banca, empresa que te contrata etc..
- Obtener datos personales, cédula de identidad, seguro social etc.
- Espiando en los cajeros para identificar el numero PIN tecleado.
- Enviando mensajes simulando ser comunicados de tu banco solicitado datos de confirmación (phishing)

CENTRO DE ESTUDIOS DE DERECHOS HUMANOS UCV

EnCambio

Los viejos controles de vigencia y titularidad de tarjetas de crédito basados en la distribución de planillas con listados de morosos e inhabilitados fueron reemplazados por:

- ✓ **H**ologramas
- ✓ **D**ígitos encriptados verificadores tanto en el anverso como en el reverso
- ✓ **I**ncorporación de lugares inviolables para estampar la firma
- ✓ ***F**otografías
- ✓ **F**irmas incorporadas al plástico
- ✓ **A**paratos y dispositivos conectados a una base de datos que al simple paso de la tarjeta, por contacto directo refleja en una pantalla y directamente imprime
- ✓ **S**e piensa en la inserción de “Chips” con información codificada

Compradores nuevos.

Todo nuevo cliente tiene el riesgo implícito de que se desconoce absolutamente todo de el o ella. No hay historial y por lo tanto, será imposible verificar su conducta pasada. El consejo es, conocerlos. Intentar establecer relaciones de largo plazo.

Compras más grandes que las normales.

Las tarjetas robadas tienen vida activa muy corta por lo que los ladrones intentarán sacarle provecho en el menor tiempo posible. En lugar de ponerse feliz por órdenes grandes, sospeche de ellas y haga una doble verificación de los datos de su comprador.

Compras con muchos items repetidos.

Al igual que en el caso anterior, esto deberá ser tomado como un alerta mas que como una alegría.

Compradores apurados.

Cuídese de los pedidos de envío rápido por la noche. Mas allá de la compulsividad de cualquier comprador, un impostor querrá recibir cuanto antes la mercadería obtenida por medio ilegales.

WebMail.
Ordenes donde el email dado sea uno de los servicios basados en la web (webmail).

Direcciones internacionales.
Lejos de ser una medida discriminatoria, sucede que no existe verificación de domicilio (AVS: Address Verification Service) fuera de los EEUU.

Compras Repetidas.
Observe con cuidado las compras repetidas en el mismo día. Nuevamente un delincuente que tuvo éxito con su tienda la primera vez, volverá a insistir hasta que se le rechace la compra.

Observe las direcciones de entrega.

Si hay una dirección que se repite a pesar de que la compra haya sido pagada con múltiples tarjetas, no es que todos los pasajeros de un hotel estén comprando en su tienda. Seguramente está frente a un intento de fraude.

Cuídese con los domicilios repetidos

A la inversa del punto anterior, tenga especial cuidado con las transacciones múltiples que desde una sola tarjeta ordenan envíos a distintos domicilios de entrega.

Diferencias en domicilios

Si observa que la dirección de facturación es distinta a la de entrega, esté atento. Es una clara señal de alarma.

Las cuatro modalidades en la Red

Phishing:

SMS (mensaje corto); La recepción de un mensaje donde le solicitan sus datos personales.

Llamada telefónica; Pueden recibir una llamada telefónica en la que el emisor suplanta a una entidad privada o pública para que usted le facilite datos privados.

Página Web o ventana emergente; es muy clásica y bastante usada. En ella se simula suplantando visualmente la imagen de una entidad oficial , empresas, etc. pareciendo ser las oficiales. El objeto principal es que el usuario facilite sus datos privados. La más empleada es la "imitación" de páginas Web de bancos

Tampoco olvidamos sitios Web falsos con señuelos llamativos, en los cuales se ofrecen ofertas irreales y donde el usuario novel facilita todos sus datos.

Keyloggers

Son spywares (existen también piezas de hardware)

Usualmente los keyloggers van registrando información entrada en su computadora utilizando el teclado

Las contraseñas recopiladas son almacenadas en un archivo y luego enviadas a la persona que desea hacer el hurto de la información.

Se infecta a través de los mensajes de correo electrónico con attachment. Típicamente, este tipo de correo electrónico captura el interés, activa la curiosidad o convence al usuario de abrir o hacer doble click a los archivos en attachment.

Otra fuente de infección es a través de páginas de Internet de baja o dudosa reputación.

Se recomienda instalar un programa de aplicación para detección y remoción de spywares

Zombies:

Los zombies son programas catalogados como virus y que una vez infectan y toman control de su computadora, notifican al individuo que los creó para más tarde realizar de forma masiva los daños o molestias que su creador desea realizar

Un tipo de utilización que le dan los hackers a estos programas generar una sobrecarga a los equipos que componen la red de comunicaciones de datos para provocar que los mismos queden temporalmente inoperantes (Denial of Service o DoS). (Denegación de Servicio)

La mejor forma de evitar este tipo de infección es borrar cualquier email cuya procedencia o remitente sea desconocido o que le indique a usted que abra el attachment. Además, el tener instalado un programa antivirus y mantenerlo actualizado contribuye significativamente a evitarlos

- **Mientras que el phishing es la actividad fraudulenta más visible, están proliferando los troyanos,**
- **Últimamente los kits de troyanos y phishing se están popularizando, lo que facilita la elaboración del ataque a un delincuente poco preparado.**
- **Los casos recogidos corresponden a alertas producidas en el seguimiento constante de la red de este tipo de ataques.**
- **Muchos de los casos, afortunadamente, son erradicados en un periodo de tiempo mínimo,**
- **Cada día los ataques son más sofisticados y provienen de mafias organizadas de ciberdelincuentes por lo que se deben emplear unas herramientas de detección avanzadas, acordes a la dificultad de la amenaza.**
- **Si bien antes este tipo de delincuencia se ejercía de manera puntual y aislada, ahora se ha convertido en una práctica generalizada**
- **El phishing sigue siendo uno de los grandes peligros de Internet y constituye un problema que está aumentando rápidamente.**

Según el Antiphishing Working Group, una de las formas más frecuentes consiste en el envío masivo de emails, los cuales contienen enlaces que dirigen a los consumidores a webs diseñadas para capturar los datos privados del usuario, como números de tarjetas de crédito, nombres de usuarios de cuentas, contraseñas y números de la seguridad social. Suplantando la identidad de los bancos, empresas de comercio electrónico y compañías de tarjetas de crédito, los phishers consiguen convencer a los receptores para que utilicen el enlace del correo como vía de acceso a la página web fraudulenta.

Un segundo tipo de ataque consiste en la introducción de malware (software malicioso) en los ordenadores para robar las claves directamente, a menudo usando programas espía y troyanos. Éste último es un programa que oculta dentro otro programa potencialmente peligroso para el ordenador y que por tanto al no estar visible instalamos en nuestro ordenador como cualquier otro dispositivo convencional.

Los últimos troyanos detectados permiten a terceras personas tomar el control total de un ordenador de forma remota, al igual que lo haría e propietario del mismo, por lo que es necesario mantener actualizados convenientemente los antivirus para evitar este tipo de fraude.

Pharming:

Implica técnicas para redirigir a los usuarios a sitios Web fraudulentos o a servidores proxy, a través de DNS infectadas o creadas ex profeso para el robo de claves.

Para el usuario, este ataque es totalmente transparente, ya que él introduce la dirección correcta de su entidad bancaria.

En el sector bancario, otra versión novedosa de estafa online es la práctica del vishing, (troyano+VoIP) a través de la cual los delincuentes consiguen los detalles de los datos bancarios de las víctimas a través de un correo electrónico que les pide que llamen supuestamente a su banco.

Como cada vez más se va abriendo el abanico de las tipologías de fraude online, es necesario contar con todos los recursos y conocimientos sobre seguridad para afrontar las posibles amenazas.

El fraude online afecta principalmente a entidades bancarias,

Pese a la complejidad de algunos troyanos, cada vez es menos necesario contar con conocimientos especializados para poner en marcha un ataque a gran escala.

En muchos ámbitos se ha popularizado la venta de kits de phishing y troyanos que realizan todo el trabajo. De esta manera, tan sólo es necesario disponer de un servidor Web para instalar toda la infraestructura y comprar uno de estos kits para comenzar a infectar ordenadores y disponer de todos los datos capturados en cuestión de horas.

Los ciberdelincuentes menos arriesgados cuentan con la opción cada vez más frecuente de comprar datos que ya han sido capturados sin tener que desplegar toda esa infraestructura de fraude en su ordenador.

Actualmente, se venden datos capturados por troyanos, que pueden ser adquiridos a través de técnicas de pago on line sin comprometer la identidad del interesado.

La mala utilización de los recurso tecnológicos, adaptándolos a las necesidades menudas del ciudadano común ha hecho que se desvirtúe el uso de algunas herramientas, recientemente hemos conocido un caso en el interior del país donde se utilizaron las tarjetas de débito como instrumentos de crédito las cuales eran entregadas al agiotista, suministrándole la clave y dejándolas en prenda hasta que la nómina se hiciese efectiva.

Lo que luego ocurrió fue que se hicieron retiros por más de lo pactado y posteriormente se pretendió que el Banco reconociera la pérdida aduciendo el desconocimiento del retiro o en todo caso no haber realizado la operación.

Creemos que nunca serán muchos los esfuerzos por generar en el público en general una responsabilidad en el uso de las claves y passwords, no sólo en el área bancaria sino también en todo lo atinente a la protección de la identidad y su seguridad en general.

En otro caso la brecha se ubicó en el personal interno de una Institución Bancaria donde un miembro desleal de una importante instancia tecnológica, copió de manera ilegal por supuesto, importante información de los clientes y los códigos que permitían desencriptar esa información, asignar y reasignar claves, ¡¡¡ en una laptop!!!, falsificando una importante cantidad de tarjetas perfectamente reconocibles para los cajeros de cualquiera de nuestras redes.

Con una máquina lectograbadora e información de los números de cuenta que había obtenido tomaban cualquier tarjeta (había una de un Cyber) y le grababa los números de cuenta. Si la tarjeta todavía no tenia PIN (clave), le grababa una y extraía el dinero que el titular pudiera tener en la cuenta. Operó durante un tiempo y hubo que montar todo un largo operativo de análisis e investigación para contrarrestarlo

Esto nos lleva a pensar en afinar herramientas para verificaciones durante los procesos de pre-empleo y las verificaciones de lealtad de las personas ubicadas en todas las áreas de las instituciones con énfasis en las que manejan procesos tecnológicos sensibles

Conferencia Internacional
Delincuencia Organizada
y Derechos Humanos
Encuentro de expertos
Jueves 12 de junio 2008. Hotel Caracas Palace

Algunas recomendaciones generales

CENTRO DE ESTUDIOS DE DERECHOS HUMANOS UCV

EnCambio

Esté consciente de que la seguridad es un aspecto crítico para el negocio. En nuestros días, el valor fundamental de una compañía son los activos intangibles.

Además, en determinados sectores, como la banca y el comercio electrónico, es necesario generar confianza en los consumidores y usuarios

Cuente los recursos destinados a proteger la seguridad de sus sistemas de información como una inversión, no como un gasto

Conozca sus debilidades. Encargue a profesionales especializados un estudio de vulnerabilidades de sus sistemas de información, tanto externos (hackers, troyanos…) como internos (mal uso de la información por parte de empleados o acceso de éstos a información confidencial)

Actualice el software, antivirus y firewalls de su empresa.

Vigile los accesos y el tráfico de información de sus sistemas informáticos

Relacionando todos esos datos entre sí, se pueden detectar intentos de acceso fraudulento o extracciones anómalas de información y comprobar si efectivamente se trata de un intento de delito

Manténgase atento a los movimientos sospechosos que puedan producirse en su entorno.

Los servicios de vigilancia digital permiten detectar el registro de dominios o sitios Web que intenten suplantar el nombre de la organización, copiar su home o utilizar fraudulentamente su marca.

Establezca una política clara de acceso a la información. Ya sea a través de un sistema de claves o de cualquier otro, defina claramente quién puede acceder a cada información y en qué condiciones

Ponga en marcha un plan de formación interna en materia de seguridad.

Todos los miembros de la organización, así como clientes, proveedores y todo aquel que tenga acceso a los sistemas de información deben recibir formación en materia de seguridad e implicarse en la tarea de mantenerla, desde el director general hasta el último trabajador.

Deje la seguridad de la organización en manos de profesionales. Sólo los expertos podrán analizar sus necesidades y ofrecerle lo que más le conviene, protegiendo sus sistemas de información y liberando al personal interno de esa tarea.

Instaure una verdadera cultura de seguridad en su organización. Implíquese, implique a todos los miembros de su equipo, trate la seguridad como un aspecto estratégico para su negocio y déjela en manos de expertos