UNA GRAN AMENAZA EN INTERNET

El crimen organizado recurre a una vulnerabilidad de control de acceso a sistemas de cómputo y a una tecnología moderna de comunicación en Internet para cometer fraudes y extorsiones. La legislación y normatividad internacionales no son adecuadas para combatir a estos criminales.

1. INTRODUCCION.

Para la vida contemporánea personal, institucional y comercial Internet es indispensable. Esta es una red de redes de computadoras de cobertura mundial que permite intercambiar información, comprar, vender, intercambiar música y videos, colaborar. En fin es la herramienta que define a nuestro siglo. Interconecta a cientos de millones de computadoras y a miles de millones de personas. No se puede vivir sin usarla. Pero es una herramienta que tiene serios defectos.

Hay más de mil millones de usuarios de Internet en el mundo; quizás el número llegue una sexta parte de la población del planeta. En Canadá el 5% de los usuarios han sufrido intrusiones o ataques en sus computadoras. Si este porcentaje puede aplicarse a nivel global tenemos que considerar que más de 50 millones de usuarios han sido afectados. Por otra parte el 5% de la población global esta formada por criminales profesionales. Esto indica que puede haber unos 50 millones de usuarios de Internet que son criminales profesionales. En los EE.UU. se arresta y condena al 5% de los criminales cibernéticos; el riesgo que corren es mínimo y la recompensa potencial es alta pues, por ejemplo, en Canadá y los EE.UU. el comercio electrónico al menudeo en 2006 fue de 150 mil millones de dólares. El comercio electrónico entre empresas sumo 2 millones de millones de dólares (2,000,000,000 US$)[21]

Un grave problema de seguridad de la información que se ofrece a través de Internet es el uso de un mecanismo de autenticación

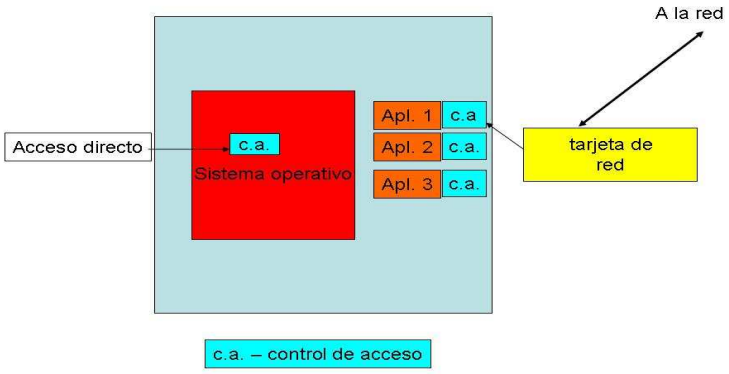
débil en una gran cantidad de computadoras y aplicaciones. El acceso a la información se otorga en base a un secreto compartido entre el acervo de información y el usuario. La debilidad radica en el usuario que puede divulgar este secreto.

Cada servidor de información tiene un mecanismo directo de interacción con sus usuarios quienes usan el sistema operativo. Los sistemas operativos incluyen mecanismos de control de acceso para impedir que accedan a sus servicios personas no autorizadas. El sistema de control de acceso mas usado es el que emplea la técnica de santo y seña (contraseña). El usuario tiene que identificarse con un nombre de usuario. En el caso de que el sistema operativo reconozca ese nombre de usuario le solicita un autenticador que es la contraseña.

Cuando se usa un método de acceso directo a un sistema de información, o sea una terminal conectada al sistema, cualquiera que conozca el nombre de usuario y la contraseña será considerado por el sistema operativo como el usuario legitimo al que pertenece esa información confidencial. Si el que usa esta información no es el usuario legítimo sucede una suplantación, o sea un robo de identidad. Cuando se suplanta al usuario de un sistema de información se elude el control de acceso y se pone en riesgo la información. Y si se daña la seguridad de la información se responsabiliza al usuario, que queda identificado por su nombre y su contraseña, aunque no haya llevado a cabo la acción dañina personalmente.

Cuando los usuarios interaccionan a través de una conexión de red con un servidor de información, una vez que un paquete llega a su destino lo recibe el sistema a través de la tarjeta de red. El servidor tiene que procesar los comandos o solicitudes que está enviando el cliente de origen. Para llevar esto a cabo debe empezar a ejecutarse o estar en ejecución el programa que preste el servicio, por ejemplo programas de correo electrónico, servidores de páginas de Web o el programa que ofrece acceso a un sistema bancario. Cada uno de estos servidores tiene sus propios mecanismos de control de acceso para autorizar o denegar

el servicio. Estos mecanismos son una barrera al uso malicioso de un servidor. Típicamente se emplea en cada servicio el paradigma de santo y seña.



2. ¿QUÉ HACEN LOS PESCADORES?

Los pescadores[9] engañan a la victima para que les entregue la información confidencial que permita el acceso a sus tesoros; para que entregue su nombre de usuario y su contraseña. En todos los casos el atacante debe comunicarse con la victima y engañarla. Este tipo de ataques han sido empleados por estafadores y pillos desde tiempos inmemoriales.

El éxito de los estafadores esta basado en una comprensión, las más de las veces intuitiva o basada en la experiencia, de los sesgos cognoscitivos[7] de las victimas y en su ignorancia computacional. Por ejemplo el sesgo de confirmación indica que las personas prefieren buscar y encontrar información que confirme sus ideas preconcebidas. O el sesgo de la seudo-certeza que lleva a tomar decisiones que supuestamente aumentan resultados positivos rechazándose las decisiones que supuestamente reducen los resultados negativos. O el sesgo del exceso de confianza en si mismo.

El uso de los sesgos cognoscitivos se llama pretextar[19]. Pretextar es el acto de crear y usar un escenario ficticio (el pretexto) para convencer a la victima de que debe entregar información

confidencial o de que realice una acción que lo puede dañar. Es mas que una mentira pues requiere del uso de información previa al pretexto para hacerlo mas convincente.

El método favorito de los ataques de ingeniería social es la llamada telefónica. La victima recibe una llamada que, por ejemplo, indica que hay irregularidades en su tarjeta de crédito. Por ello debe llamar al un número de teléfono que se indica, que supuestamente es de su banco o de la emisora de la tarjeta de crédito, para resolver el problema. Claro, ese teléfono es del estafador, que lo convence de que le proporcione su información confidencial. Otro ejemplo es que en la llamada se le diga que el departamento de soporte técnico de su sistema de cómputo ha detectado un problema y que debe cambiar su contraseña. Para ello se le pide que proporcione su nombre de usuario y su contraseña de inmediato. Estos ataques son dirigidos a quien recibe la llamada. Y el atacante debe de antemano estudiar si la victima vale la pena.

Otro método muy socorrido es enviar a la victima un mensaje de correo electrónico del mismo tipo, solicitando información confidencial. El atacante debe redactar el mensaje en forma tal que de la impresión de provenir de una fuente legitima. Muy frecuentemente el mensaje aparenta provenir del banco del usuario indicándole que se comunique a un teléfono o que responda al mensaje enviando información confidencial.

Los esquemas de seguridad en el ámbito computacional se han enfocado principalmente a la autenticación y a la criptografía. Pero en casi todos los casos se ha ignorado el factor humano y su impacto en los ataques a la seguridad. La avalancha de los ataques de los pescadores muestra que hay que incluir el factor humano en los modelos de seguridad.

En la actualidad muchos pescadores no utilizan llamadas telefónicas sino mensajes de correo electrónico o mensajes instantáneos de texto. Esto se debe a que se han desarrollado técnicas para enviar grandes cantidades de copias del mismo

mensaje de correo electrónico o para emplear masivamente la mensajería de textos.

El término pescador se refiere a atacantes que usan metodologías automatizadas para realizar ataques masivos, pero que más y más se enfocan a universos restringidos de victimas con mayor probabilidad de éxito. Esto reduce la visibilidad de los ataques y aumenta su probabilidad de éxito. Los atacantes reducen el riesgo de caer en trampas que los sorprendan: usan identidades falsas diseñadas para evitar ser identificados y para evitar que se les persiga en sus lugares de origen.

Si el atacante envía 10,000 pretextos y tiene éxito solamente en el 0.1 % de sus mensajes ya se habrá apoderado de 10 nombres y contraseñas. Los pescadores más experimentados llevan a cabo estudios para encontrar "nichos de mercado" en los cuales un pretexto es más efectivo que otro. Se observan gran cantidad de ataques de este tipo y el número va en aumento[17]: en junio de 2005 se reportaron 15,050 ataques, en junio de 2006 se reportaron 28,571 llegándose a un máximo histórico en enero de 2007 cuando se reportaron 29,930. Cada ataque puede involucrar a centenas de miles de personas que reciben pretextos. Una pequeña fracción de estas personas se convierte en victimas.

3. ARMAS MODERNAS.

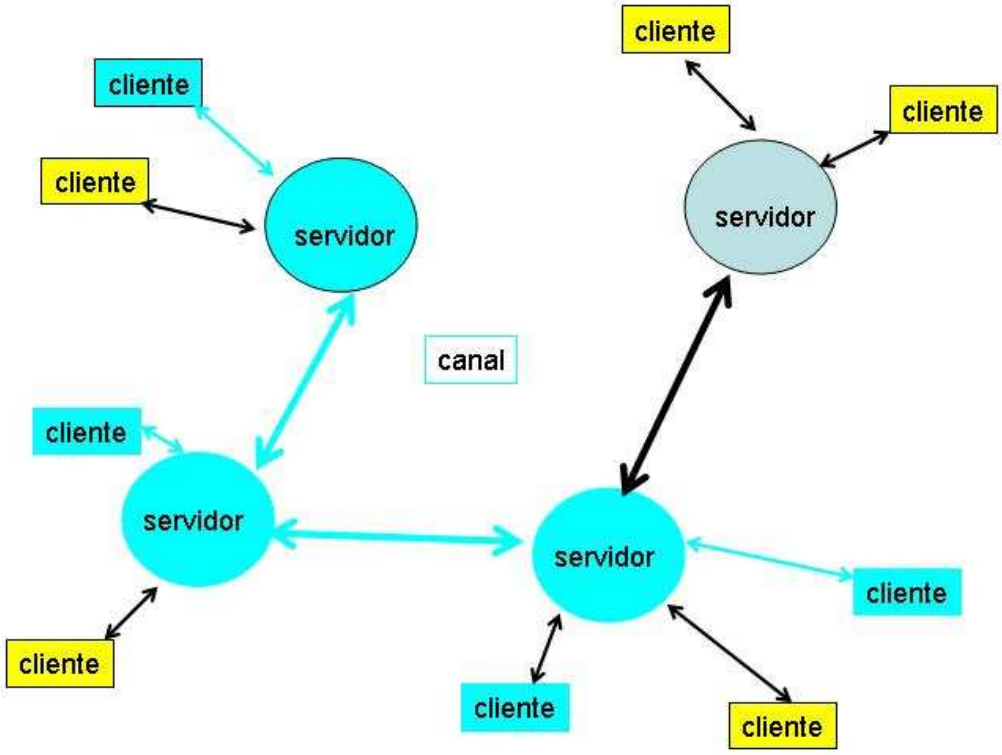
Las aplicaciones iniciales de Internet consistieron en permitir la comunicación entre dos personas (o más bien entre dos computadoras manejadas cada una por una persona). Este paradigma se llama computación uno-a-uno. Más adelante se desarrollo la comunicación que permitía a una computadora interaccionar con muchas otras computadoras. Así se creo la red mundial WWW (World Wide Web). Este paradigma recibió el nombre de uno-a-muchos. Finalmente se posibilito a muchas computadoras (y a muchas personas) intercambiar información El paradigma muchos-a-muchos es un termino que describe el

tercer paradigma de computo en Internet. Permite enlazar múltiples sitios de la WWW. Los usuarios se interconectan dinámicamente y con flexibilidad y así desaparecen las barreras artificiales entre herramientas de intercambio de información y de comunicación. La definición de “muchos” dejara de referirse a las personas y se referirá a entidades tales como organizaciones, productos, procesos, eventos conceptos y otros.

Para poder emplear este nuevo paradigma se requiere de mecanismos de mando y control. Hay una gran diversidad de tecnologías disponibles para enviar pretextos a miles de personas.

El protocolo de conversación mediante relevos en Internet, (IRC Internet Relay Chat)[12,13,14], permite tener conversaciones en tiempo real y llevar a cabo reuniones sincrónicas. Se diseño principalmente para la comunicación de grupos de conversación llamados canales. Pero también permite comunicación uno-a-uno mediante mensajes privados. Esta basado en TCP y puede además usar opcionalmente algún algoritmo de comunicación segura tal como SSL.

Un servidor de IRC se conecta a otros servidores de IRC para crear y ampliar una red de servicio. Los usuarios se conectan a un servidor, y por lo tanto a la red IRC, mediante un cliente. Los clientes proporcionan la capacidad de conexión a usuarios de computadoras. Los clientes son programas que típicamente presentan al usuario una interfaz de texto para que puedan comunicarse interactivamente. Un canal es un grupo de uno o mas usuarios que intercambiaran mensajes entre si. Cada canal se caracteriza por un nombre y por la lista de sus usuarios. Los canales tienen algunas propiedades que pueden ser modificadas por sus miembros. Los servidores y los clientes se envían mutuamente mensajes que pueden requerir o no una respuesta. La comunicación entre servidores no requiere respuestas.



Hay muchas implementaciones de servidores y clientes. Existen miles de redes que interconectan servidores de IRC de distintos tipos, aunque no es fácil conectar a servidores de distintas implementaciones. Todos los servidores pueden recibir conexiones de los distintos tipos de clientes. Las redes de servidores IRC tienen como modelo de conexión una grafica acíclica: no hay redundancia, y si un servidor deja de funcionar la red se puede partir.

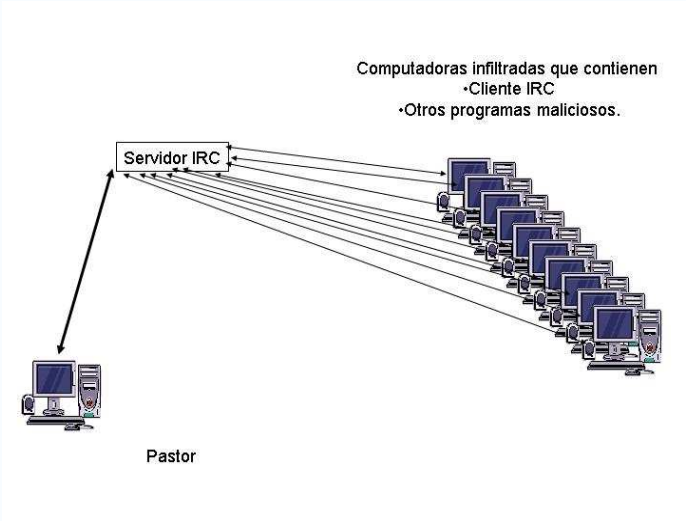
Las redes IRC han despertado el interés de malhechores que usan Internet. A quienes usan esta tecnología se les llama “pastores”.

4. ¿QUE HACEN LOS PASTORES?

Lo primero que hacen es infiltrar una computadora grande y colocar un programa servidor de IRC. Luego infiltran muchas otras computadoras pequeñas y grandes, su rebaño, y colocan un cliente IRC en cada una. Finalmente regresan al programa servidor y suscriben a todas las otras computadoras, y a la suya

propia, al canal IRC[11]. De esta manera se pueden comunicar con su rebaño y enviarles instrucciones a las computadoras infiltradas. Algunas aplicaciones de los rebaños son:

- el envío masivo de mensajes de correo electrónico no solicitado, llamado SPAM.
- apoyar el trabajo de los pescadores.



El pastor necesita la información confidencial de algún usuario de cada maquina que incorpora a su rebaño para abrir una sesión suplantándolo para colocar el cliente de IRC. A estas computadoras infiltradas y que el pastor usa sin el consentimiento del dueño se les llaman zombis.

La computadora del pastor pueden estar en cualquier nodo de Internet, el centro de comando y control también, y los zombis del rebaño pueden estar distribuidos por todo el mundo.

Los rebaños pueden ser enormes. Uno famoso[8] que emplea un programa malicioso llamado Toxbot contaba con más de un millón y medio de computadoras infiltradas. Los pastores llevan a cabo concursos mundiales, y mostrar que pueden mantener el

control de sus rebaños, lo cual es difícil porque los propietarios de las computadoras infiltradas, en cuanto se dan cuenta de que han sido atacados, eliminan el código malicioso y el cliente IRC. Los pastores no se interesan mayormente en las computadoras personales que no tienen una conexión permanente a Internet pues cuando el dueño termina la conexión se pierde el zombi. Esto crea inestabilidades en el canal. Las computadoras personales que mantienen una conexión permanente a Internet, ya sea a través de un proveedor de servicios de Internet o en una red institucional mal administrada pueden ser afectadas por los pastores. Si estas computadoras personales emplean mecanismos robustos de control de acceso quizás no se vean afectadas, pero en la mayor parte de los casos el riesgo es alto.

En el Reino Unido[6] se cree que el 26% de las computadoras conectada a Internet han sido infiltradas. En los EE.UU. se piensa en un 25%. En Canadá un 8%.

La motivación principal de los atacantes en Internet se ha apartado del vandalismo y la fama y ahora se dirige a las ganancias económicas. El atacante de hoy trata de explotar a individuos y empresas para obtener ingresos o beneficios económicos. Esto causa perdidas enormes para las victimas. Un estudio realizado por las autoridades en los EE.UU. cuantifican los daños en año 2006 en 67.2 miles de millones de dólares.

5. CONSECUENCIAS.

Las herramientas que se han descrito dan al crimen organizado posibilidades nuevas. Pueden explotar la conectividad global, la integración económica y el crecimiento mundial de los servicios financieros. El criminal y el crimen no ocurren en la misma jurisdicción o el mismo país. El aspecto transnacional del crimen organizado se conjunta con desarrollos tecnológicos que hacen difícil la identificación de quienes cometen crímenes y hacen también difícil acopiar evidencia. La evidencia digital es frágil,

transitoria y las técnicas predigitales de recolectarla son poco efectivas. La creciente sofisticación de los criminales cibernéticos es un reto para la policía. La habilidad de planear y ejecutar estrategias de largo plazo para cometer crímenes es realmente peligrosa. No tiene nada que ver con los juegos de los estudiantes o con los actos aislados de empleados quejosos.

El robo de identidad definido como la obtención de información de identificación tal como:

- Nombre
- Numero de Seguro Social
- Numero de tarjeta de crédito
- Numero de serie de un teléfono celular

El defraudado normalmente no se da cuenta de lo que sucede hasta que recibe sus estados de cuenta, o cuando no paga las facturas que emiten los proveedores y estos lo acosan.

Una breve lista[16] parcial de los delitos cibernéticos que se han detectado incluye los siguientes:

1) Uso indebido de computadoras y otros recursos digitales
2) Amenazas en línea
3) Alquiler de rebaños
4) Pesca delictiva
5) Espionaje corporativo
    i) Robo de información personal de empleados y clientes
    ii) Robo de información financiera
6) Robo de propiedad intelectual
7) Lavado de dinero
8) Crímenes políticos
9) Extorsión.
10) Fraude
    i) Solicitud fraudulenta de fondos

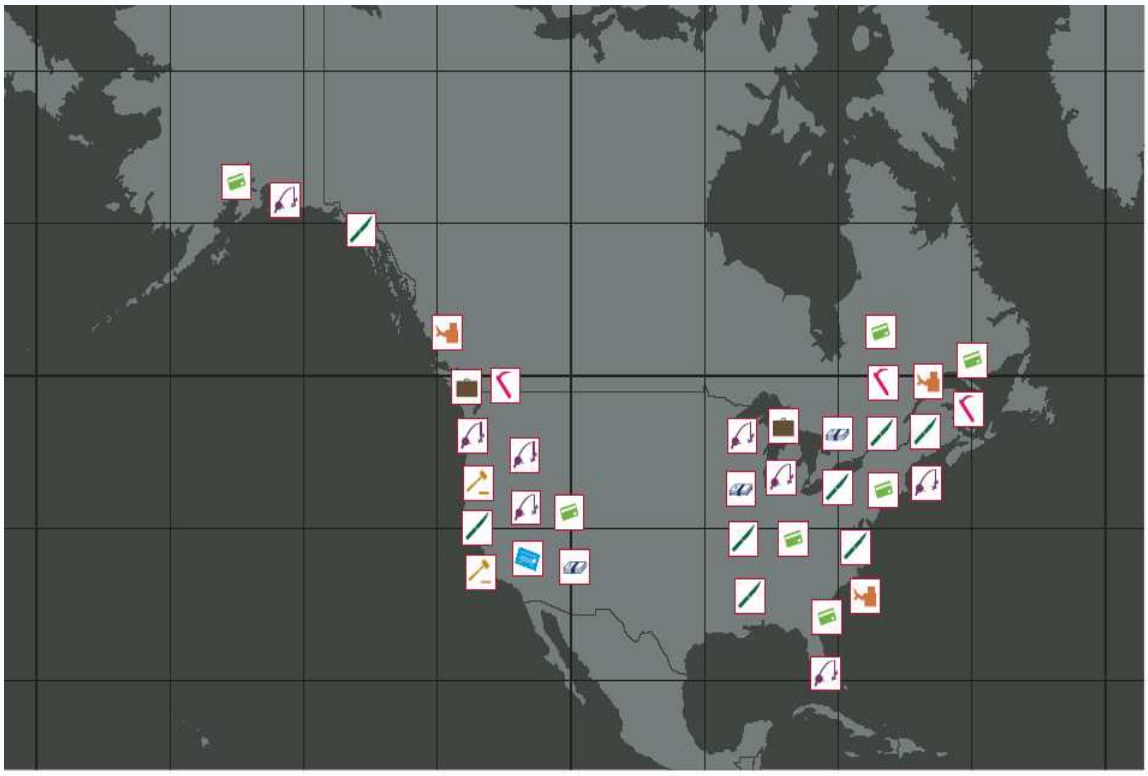
ii) Fraudes con tarjeta de crédito
iii) Fraude en subastas
iv)Operaciones fraudulentas en bolsa de valores

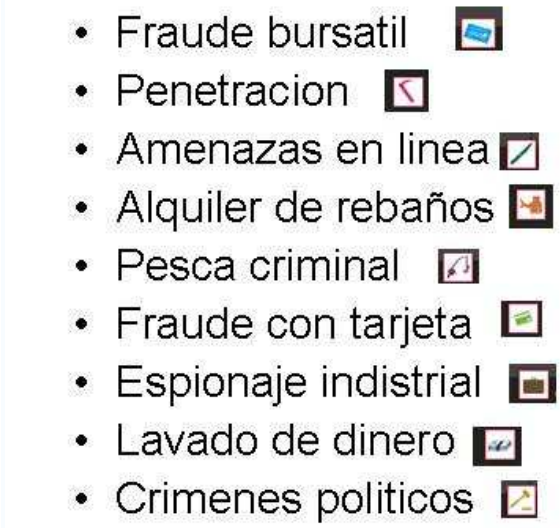
11) Denegación de servicios de misión critica
12) Destrucción de la reputación institucional.

Un ejemplo famoso[18] de un crimen organizado a nivel mundial ocurrió en España. En 2005 la policía española detuvo a 310 personas, allano 166 residencias, confisco 2000 teléfonos móviles, 327 computadoras y 165 faxes como parte de una investigación internacional, con duración de mas de dos años, sobre un alud de mensajes de correo electrónico en los que se remitente se ostentaba como poseedores de una basta fortuna que estaba "en el extranjero" y que se perdería si no era trasladada a otro país "mas seguro". El remitente solicitaba la ayuda del destinatario ara trasladar estos fondos. Su recompensa seria una parte del capital transferido. Este era el pretexto. Más de 20,000 de personas fueron defraudadas en 45 países. Los criminales obtuvieron decenas de millones de euros. El tamaño de esta operación no tenía precedente. Dado el alto numero de personas bajo arresto y el volumen de la información obtenida se duda que sea posible conocer muchos detalles de este fraude.

Algunas personas crean un rebaño de 10,000 a 30,000 computadoras y las alquilan a quien pague el alquiler. Uno de esos rebaños se puede alquilar por $20.000 U.S[10]. En Holanda la policía logro desarticular un rebaño que contaba con un millón y medio de computadoras controladas y que se dedicaba a extorsionar a empresas norteamericanas[22]. En mayo de 2007 Estonia sufrió un ataque a través de un rebaño que denegó el servicio a bancos, dependencias del gobierno y periódicos. Se sospecha que este ataque tuvo motivaciones políticas. [20]

Los tipos de delitos que se cometen usando Internet y que se han registrado se distribuyen de la siguiente manera[16]:





Como puede verse la cobertura de los criminales es global.

6. PREOCUPACIÓN LEGAL.

Los crimines cibernéticos característicamente se originan en jurisdicciones que tienen legislación débil o inexistente acerca de este tema. Un ataque de tipo viral que costo a empresas norteamericanas miles de millones de dólares fue atribuido por el FBI a un estudiante el Filipinas, donde no se le pudo acusar de un crimen. Rápidamente el gobierno filipino implanta legislación para combatir el crimen cibernético, y muchos países han intentado lo mismo. Sin embargo existen todavía vacíos legales que los criminales aprovechan. Además la naturaleza transnacional de estos delitos complica todavía mas la tarea de su combate legal.[23]

El impacto de este tipo de tecnologías ha rebasado la legislación nacional y los compromisos internacionales vigentes. Tanto la

Unión Europea[1], como las Naciones Unidas[4] y la Organización de Estados Americanos[5] han publicado diversos documentos relacionados con el crimen cibernético. Pero en realidad no se ven resultados tangibles legislativos. En un estudio detallado[2] se comenta:

"Partiendo del estudio comparativo de las medidas que se han adoptado a escala internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera de los delitos informáticos y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición."

En México un análisis detallado[3] de la legislación vigente a finales de 2003 indica que:

"Lo cierto es que el desarrollo y aplicación de los avances y fenómenos informáticos llevan una inercia y una velocidad que los han hecho casi inalcanzables, cuantimás (sic) para un sistema jurídico formal, escrito, -como lo es el Sistema Latino- con un proceso legislativo pausado, enclavado en un entorno político volátil, complicado, por decirlo en una palabra que engloba todos los adjetivos que merece: mexicano."

Es de suponerse que la situación legislativa en muchos países de Latinoamérica y del resto del mundo sea similar. El crimen organizado aprovecha estas brechas legislativas, diplomáticas y políticas para delinquir y obtener enormes ganancias.

Los crimines cibernéticos característicamente se originan en jurisdicciones que tienen legislación débil o inexistente acerca de este tema. Un ataque de tipo viral que costo a empresas norteamericanas miles de millones de dólares fue atribuido por el FBI a un estudiante el Filipinas, donde no se le pudo acusar de un crimen[23]. Rápidamente el gobierno filipino implanta legislación para combatir el crimen cibernético, y muchos países han intentado lo mismo. Sin embargo existen todavía vacíos legales que los criminales aprovechan. Además la naturaleza transnacional de estos delitos complica todavía más la tarea de su combate legal.

La respuesta al creciente traslape entre el crimen organizado y el crimen cibernético requiere una estrategia de mismas amplias. Hay precedentes bien conocidos como la respuesta internacional al lavado de dinero. La Convención del Consejo de Europa[1] sobre el crimen cibernético es el primer paso importante en esta dirección al intentar fijar estándares y buenas practicas que los gobiernos deberán adoptar en su trabajo legislativo, regulatorio y policiaco.

El enfoque subyacente de la Convención es reconocer la necesidad de armonizar las legislaciones nacionales. Esto se ha logrado en materia de tratados de extradición y de asistencia legal mutua que permite a los gobiernos compartir información y evidencia. Existe el requerimiento de la llamada dualidad criminal (el acto que se investiga debe ser un crimen en ambas legislaciones. Complementariamente los gobiernos y sus policías deben tener la capacidad de aplicar las leyes. Los delitos cibernéticos frecuentemente tienen implicaciones de seguridad nacional y de procedimientos de inteligencia, lo cual complica la colaboración. Resultara útil establecer redes de confianza entre las agencias encargadas de combatir el crimen cibernético en los diversos países. [23].

7. CONCLUSIONES.

La presencia del crimen organizado en Internet obliga a los legisladores y a los abogados a estar enterados del funcionamiento de la tecnología que usan estos delincuentes. También obliga a los desarrolladores de la tecnología a estar enterados de la normatividad, legislación y recomendaciones que tienen que ver con su buen uso. La colaboración entre especialistas de disciplinas tan distantes requiere de comprensión mutua y mucha paciencia. Los usuarios de Internet están expuestos a riesgos que casi todos desconocen, y su mejor defensa es el conocimiento de la tecnología que los pone en riesgo y de la normatividad que se puede aplicar.

Referencias.

1. Convention On Cybercrime
Budapest, 23.XI.2001
European Treaty Series - No. 185
http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc
Consultado el 22 de junio de 2007.

2. Santiago Acurio Del Pino
La delincuencia Informática transnacional y la UDIMP
AR: Revista de Derecho Informático
Junio del 2006
http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/acurio.pdf
Consultado el 22 de junio de 2007

3. Verónica Batiz Alvarez y Mario Farias-Elinos
Panorama General del Marco Jurídico en Materia Informática en México
AR: Revista de Derecho Informático
Enero del 2004
http://www.alfa-redi.org/rdi-articulo.shtml?x=1246
consultado el 22 de junio de 2004.

4. Delitos relacionados con las redes informáticas
Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente
Viena, 10 a 17 de abril de 2000
http://www.uncjin.org/Documents/congr10/10s.pdf
consultado el 22 de junio de 2007

5. Consejo Permanente De La OEA
Organización De Los Estados Americanos
13 Mayo 2004
Comisión De Seguridad Hemisférica
Estrategia Interamericana Integral Para Combatir Las Amenazas A La Seguridad Cibernética:
http://scm.oas.org/doc_public/SPANISH/HIST_04/CP12893S04.doc
consultado el 22 de junio de 2002.

6. John Leyden
Britain tops zombie PC charts
Monday 21st March 2005
The Register
http://www.theregister.co.uk/2005/03/21/botnet_charts/
consultado el 22 de junio de 2002

7. Social engineering (security)
25 June 2007
Wikipedia contributors
Wikipedia the free encyclopedia
http://en.wikipedia.org/wiki/Pretexting
consultado el 22 de junio de 2002

8. Bruce Schneier
Crypto-Gram Newsletter
January 15, 2006
http://www.schneier.com/crypto-gram-0601.html#4
consultado el 22 de junio de 2002

9. Gunter Ollmann
The Phising Guide: Understanding & Preventing Phishing Attacks
1-7-2005 Next Generation Security Software Ltd.
http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf
consultado el 22 de junio de 2002

10. David Geer
Malicious Bots Threaten Network Security
Computer, IEEE Computer Society
January 2005
http://ieeexplore.ieee.org/iel5/2/30112/01381249.pdf?arnumber=1381249
consultado el 22 de junio de 2002

11. Basudev Saha
Bots and Botnets
15-7-2005
CISSP ,Department of Information Technology,Ministry of Communications & Information,Technology,India
http://www.cert-in.org.in/training/15thjuly05/botnet.pdf
consultado el 22 de junio de 2002

12. C.Kalt
Internet Relay Chat: Server Protocol
1-4-2000 Network Working Group
ftp://ftp.rfc-editor.org/in-notes/rfc2813.txt
consultado el 22 de junio de 2002

13. C.Kalt
Internet Relay Chat: Client Protocol
1-4-2000 Network Working Group
ftp://ftp.rfc-editor.org/in-notes/rfc2812.txt

consultado el 22 de junio de 2002

14. C.Kalt
Internet Relay Chat: Architecture
2006 Network Working Group
ftp://ftp.rfc-editor.org/in-notes/rfc2810.txt
consultado el 22 de junio de 2002

15. Ramneek Puri
Bots &; Botnet: An Overview
August 08, 2003
SysAdmin, Audit, Network, Security) Institute
http://www.sans.org/reading_room/whitepapers/malicious/1299.php
consultado el 22 de junio de 2002

16. McAfee Virtual Criminology Report**,**
July 2005.
http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf
consultado el 22 de junio de 2002

17. Phishing Attack Trends Reports
The Anti-Phishing Working Group (APWG)
Abril 2007.
http://www.antiphishing.org/phishReportsArchive.html
Consultado el 22 de junio de 2007.

18. Clarín.com
El Mayor Operativo Contra Una Banda Internacional
20/07/2005
http://www.clarin.com/diario/2005/07/20/um/m-1017724.htm
Consultado el 22 de junio de 2007.

19. Diccionario De La Lengua Española - Vigésima Segunda Edición

(Pretextar), (Pretexto)
http://buscon.rae.es/draeI/
consultado el 22 de junio de 2002

20. Mason Inman
File sharing sites are being subverted for Web attacks
NewScientist.com news service
30 mayo 2007
http://technology.newscientist.com/article.ns?id=dn11949&feedId=online-news_rss20
consultado el 22 de junio de 2002

21. McAfee Virtual Criminology Report
McAfee North America Criminology Report
Organized crime and the Internet 2007
Realtime Publishers
http://www.realtime-websecurity.com/mwswp7.asp
consultado el 22 de junio de 2002

22. Gregg Keizer
Dutch Botnet Bigger Than Expected
TechWeb News
Oct. 21, 2005
http://www.informationweek.com/story/showArticle.jhtml?articleID=172303265
consultado el 22 de junio de 2002

23. Phil Williams
Organized Crime and Cybercrime: Synergies, Trends, and Responses,
International Information Programs
An Electronic Journal of the U.S. Department of State –
August 2001 Volume 6, Number 2
http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

consultado el 22 de junio de 2002