ANEXO II

HACKERS Y CRACKERS FAMOSOS

CRACKERS

DRAPER JOHN, "CAPTAIN CRUNCH"

En septiembre de 1970 John Draper, también conocido como Captain Crunch, descubre que el obsequio ofrecido en las cajas de cereal Captain Crunch duplica perfectamente la frecuencia de tono de 2600 hz. de una línea de WATS, permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT&T.

HOLLAND WAU Y WENERY STEFFEN

"Lo logramos, por fin... Sólo hay algo seguro, la infinita inseguridad de la seguridad". Fue lo que escribio Wau Holland, en su cuaderno de notas, el 2 de mayo de 1987. Los dos hackers alemanes, de 23 y 20 años respectivamente, habían ingresado sin autorización al sistema de la central de investigaciones aerospaciales más grande del mundo (NASA).

¿Por qué lo hicieron?, "Porque es fascinante, la única aventura posible está en la pantalla de un ordenador", respondieron.

Cuando Wau y Steffen advirtieron que los técnicos los habían detectado, le enviaron un telex, avisando de su intrusión.

ING-HOU CHEN

Taipei, Taiwan, Abril 30 de 1999. El autor del virus "Chernobyl", dijo a los investigadores que el creó el bug con la esperanza de humillar y vengarse de los que llamo "proveedores incompetentes de antivirus para software". Pero él admitió que no esperaba que CIH (iniciales de su autor) causara daño alrededor del mundo. Este virus devastó cientos de miles de computadoras alrededor del mundo.

Chen creó el virus en Abril, cuando todavía era estudiante de ingeniería computacional en el Instituto Tecnológico.

Este inusual virus destructivo, programado para funcionar el 26 de Abril, (13° aniversario del desastre nuclear de Chernobyl), trata de borrar el disco rígido y escribir "basura" en algunos otros componentes, evitando de este modo el futuro encendido de la computadora.

KEVIN Y RONALD

Ronald y Kevin, con los nombres de guerra Makaveli y TooShort en el ciberespacio, asaltaron los ordenadores del Pentágono en Marzo del año 1998, a la tierna edad de 17 años. Estos dos forajidos virtuales, con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las fuerzas aéreas, relacionados con centros digitales en Estados Unidos y Okinawa.

LA MACCHIA DAVID

En 1994 David La Macchia, estudiante de 20 años del prestigioso y serio MIT, reconoce que ha distribuido en Internet multitud de programas informáticos obtenidos sin licencia y por valor de un millón de dólares. Para ofrecerlos a los cibernautas montó su propia BBS.

LEVIN VLADIMIR

Un matemático ruso de 24 años, penetró vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citybank en Wall Street, Este pirata logró transferir a diferentes cuentas de EE.UU., Rusia, Finlandia, Alemania, Israel, Holanda y Suiza fondos por valor de 10 millones de dólares, según el FBI. Detenido en el Reino Unido a principios de 1995, Levin espera que los tribunales británicos se pronuncien sobre una demanda de extradición solicitada por EE.UU.

MITNICK KEVIN, "EL CÓNDOR", "EL CHACAL DE LA RED"

Como hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "solo para mirar".

La primera vez que lo detuvieron fue en 1981 por robar manuales de la Pacific Telephone. La información robada tenía un valor equivalente a los 200 mil dólares y tuvo que cumplir una condena tres meses de cárcel y a un año bajo libertad condicional.

En 1983 intentó ingresar en las computadoras de la universidad de California del Sur y poco después penetró el sistema de la agencia de créditos TRW.

En 1987 lo condenaron a treinta y seis meses de libertad condicional por robo de soft, tras hackear los sistemas del Departamento de Defensa de EE.UU. y la NASA.

Un año más tarde fue arrestado de nuevo cuando era estudiante de la Universidad del Sur de California. En esta ocasión entró ilegalmente a ARPAnet (la predecesora de Internet) y trató de acceder a la computadora del Pentágono. Lo sentenciaron a seis meses de cárcel en una prisión juvenil en California.

Durante ese tiempo le negaron el acceso a los teléfonos y a lo largo de los doce meses de rehabilitación no pudo acercarse a una computadora.

Más tarde, y ya en libertad, se apoderó de 16 códigos de seguridad de MCI y junto a un amigo, Lenny DiCicco, entraron a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet.

Ambos hackers querían obtener una copia del prototipo del nuevo sistema operativo de seguridad de Digital llamado VMS. El personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, y comenzaron a rastrear a los hackers.

Mitnick fue arrestado en 1988 por invadir el sistema de Digital Equipment. La empresa acusó a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizó a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y sólo bajo supervisión de un oficial de la prisión.

Este caso produjo revuelo en los Estados Unidos, no sólo por el hecho delictivo sino por la táctica que utilizó la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador. Gracias a esta maniobra de la defensa Mitnick fue sentenciado a sólo un año de prisión y al salir de allí debía seguir un programa de seis meses para tratar su "adicción a las computadoras". Durante su tratamiento le fue prohibido tocar una computadora o un módem y llegó a perder más de 45 kilos.

Para 1991 ya era el hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gustó el libro ya que luego de salir a la venta, la cuenta en Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera de que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

En 1992, y luego de concluir su programa, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determinó que había violado los términos de su libertad condicional. Se ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick.

Luego de convertirse en prófugo de la justicia cambió de táctica y concluyó que la mejor manera de no ser rastreado era utilizando teléfonos celulares.

Luego de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura la cual invadió en la Navidad de 1994. Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen hacker, pero era de los "chicos buenos", ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros hackers.

Shimomura notó que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que él nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al hacker que había invadido su privacidad.

Más tarde, El 16 de febrero de 1995, Mitnick fue capturado, juzado y condenado a 25 años de prisión, lejos de computadoras y teléfonos.

Pero, el 22 de marzo de 1999, se consigue un acuerdo con jueces y fiscales. Los términos concretos se desconocen, pero se sabe que en marzo de 2000 Mitnick quedaría en libertad con la condición irrevocable de no poder acercarse a una computadora.

Kevin Mitnick, este sencillo nombre, oculta la verdadera identidad de uno de los mayores crackers de la historia. Fue una de las mayores pesadillas del Departamento de justicia de los Estados Unidos. Entró virtualmente en una base de misiles, llegó a falsificar 20.000 números de tarjetas de crédito y a causar pérdidas millonarias a varias empresas.

MORRIS ROBERT

En noviembre de 1988, Morris lanzó un programa "gusano", diseñado por él mismo, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de y más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millones de dólares.

Como consecuencia, se creo el CERT (Equipo de Respuesta de Emergencias Computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado.

MURPHY IAN, "CAPTAIN ZAP"

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o gubernamentales. "Captain Zap" mostró la necesidad de hacer mas clara la legislación. Con cargos de robo de propiedad, finalmente, Murphy fue multado por US$ 1000 y sentenciado a 2½ años de prueba.

"PAINT" Y "HAGIS"

Estos son los seudónimos de los dos hackers que el 10 de Diciembre de 1997 accedieron a uno de los buscadores mas utilizados en Internet. Los terroristas informáticos autodenominados "Paints & Hagis", accedieron al servidor del popular navegador Yahoo! y dejaron un mensaje amenazante a los casuales visitantes.

Este ataque no resultó ser más de una modificación de una página web, y un ejemplo temprano de las muchas que se modifican hoy día a día.

PETERSON JUSTIN TANNER, "AGENT STEAL"

Peterson crackeaba las agencias de crédito. Esta falta de personalidad le llevó a su caída y a la de otros. Tiempo después, se dice, obtuvo un trato con el FBI. Esto le facilitó su salida de la cárcel y "no" pudo ser demostrado un fraude mediante una trasferencia de dinero.

POULSEN KEVIN, "DARK DANTE"

En diciembre de 1992 Kevin Poulsen fue acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusó Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y fue condenando a 10 años en la cárcel (salió bajo palabra a los 5 años).

Como Cracker, siguió el mismo camino que Kevin Mitnick, pero fue más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a "ganar" un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue. Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional. Esto fue lo que lo llevó a su estancia en la cárcel, 5 años, fue liberado en 1996, supuestamente "reformado".

SMITH DAVID

Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, "Melissa". Entre los cargos presentados contra él, figuran el de "bloquear las comunicaciones publicas" y de "dañar los sistemas informáticos". Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta 10 años de cárcel.

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de U$S 10000. Melissa en su "corta vida" había conseguido contaminar a más de 100.000 computadoras de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar. Compañías informáticas siguen alertando que aún pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus, que han venido apareciendo últimamente como Happy99 o Papa.

THE MENTOR Y GRUPO H4G13

El autodenominado grupo H4G13, con Mentor a su cabeza quería demostrar hasta donde eran capaces de llegar, y lo dejaron plasmado de una manera efectiva, colocando en la pagina principal de la NASA, durante media hora, el "manifiesto" hacker más conocido hasta el momento. Ver Capítulo 5.

ZINN HERBERT, "SHADOWHACK"

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de "Shadowhawk", fue el primer sentenciado bajo el cargo de Fraude

Computacional y Abuso. Zinn tenia 16 cuando violó el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US$ 174000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publico contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$ 10000.

HACKERS

ARDITA JULIO CESAR, "EL GRITÓN"

Es considerado el hacker más famoso de Argentina. Nació en Río Gallegos, el 28 de marzo del 1974. Utilizó su primera computadora mientras realizaba su secundaria. En quinto año, junto con dos compañeros ayudaron a informatizar el sistema de notas y facturación del colegio en el cual estudiaba.

Este muchacho, saltó a la fama el 28 de diciembre de 1995, día de los Santos Inocentes, cuando su domicilio fue allanado por la Justicia Argentina luego de que los Estados Unidos alertaran sobre reiteradas intrusiones a varias de sus redes informáticas de Defensa, entre ellas la del Pentágono.

Las intrusiones provenían de una computadora conectada a una línea telefónica desde un departamento de Barrio Norte, en la Capital Federal. "El Gritón" ingresaba en la red de computadoras de la empresa Telecom a través de líneas gratuitas 0800, para luego realizar intromisiones en sistemas informáticos ajenos.

En la causa argentina número 45048/95, con carátula "Ardita Julio C., sobre defraudación", el juzgado de Instrucción número 38 a cargo de la jueza Wilma López, dispuso que Ardita compareciera ante un tribunal oral pero por fraude telefónico (estimado por la empresa Telecom en $50), ya que las intrusiones informáticas no están contempladas en el Código Penal.

Sin embargo, por el mismo episodio, Ardita ya tuvo que recorrer una espinosa demanda penal en los Estados Unidos, donde las intrusiones informáticas, las violaciones de códigos secretos y la posesión de claves ajenas sí son delitos graves. El proceso terminó el 19 de mayo 1999, cuando un tribunal de la ciudad de Boston, lo condenó a 3 años de libertad condicional y a pagar una multa de U$S5000 por haber vulnerado, entre otros varios, el sistema informático de la Marina.

Hoy en día, con 27 años, Julio Cesar Ardita paga religiosamente sus facturas telefónicas; se levanta temprano por las mañanas y camina hasta la zona de Tribunales. Allí está Cybsec S.A., la exitosa empresa de seguridad informática que el ex–Gritón administra junto a su socio.

BARAM PAUL

Posiblemente el mayor hacker de la historia. Ya hackeaba Internet antes de que existiera. El fué quien introdujo el concepto de hacker.

FARMER DAN

Trabajó con Spafford en la creación de COPS (1991) y al mismo tiempo con el famoso Computer Emergency Response Team (CERT). Tiempo más tarde Farmer ganó gran notoriedad al crear el System Administrator Tool for Analyzing Networks (SATAN). Una gran herramienta para analizar vulnerabilidades en redes.

GATES BILL Y ALLEN PAUL

En sus tiempos de aprendices, estos dos hombres de Washington se dedicaban a hackear software. Empezaron en los 80 y han creado los mayores imperios de software de todo el mundo.

RITCHIE DENNIS, THOMSON KEN Y KERRIGHAN BRIAN

Programadores de los Laboratorios Bell. Son los desarrolladores de UNIX y C. Se los considera los padres de la informática masiva al desarrollar el sistema operativo y el lenguaje más poderosos de la actualidad.

SPAFFORD EUGENE

Profesor de informática. Colaboró para crear el Computer Oracle Password Security System (COPS) un sistema de seguridad semiautomático. Es un hombre muy respetado en el campo de la seguridad.

STALLMAN RICHARD

Se unió al Laboratorio de inteligencia artificial de la MIT en 1971. Fue ganador del premio McArthur por sus desarrollos de software. Fue fundador de Free Software Foundation, creando aplicaciones y programas gratis.

TORVALDS LINUS

Torvalds empezó a conocer el UNIX y a tomar clases de programación en C sobre los 90. Un año después empezó a escribir un SO parecido al UNIX. Después de otro año, lo subió a Internet pidiendo colaboración; hoy es llamado LINUX.

VEHEMA WIETSE

Vehema viene de la Universidad de Tecnología de Eindhoven, en los Países Bajos. Un gran programador, con un don para ello, además de tener un amplio historial en programas sobre seguridad. Es el coautor del SATAN con Farmer. Vehema escribió el TCP Wrapper, uno de los programas de seguridad más usado en el mundo.