Kevin David Mitnick nació el 6 de agosto de 1963 y es considerado como uno de los hackers más famosos de la historia. Su Nick era Cóndor y también se apodó él mismo como "fantasma de los cables".

En la actualidad se dedica a la consultoría desde la óptica particular de la ingeniería social y afirma que más allá de las técnicas de hardware y software que se pueden implementar en las redes, el factor que determina la seguridad de cualquier red es la capacidad de los usuarios para poder interpretar correctamente las políticas de seguridad y hacerlas cumplir.

El 27 de mayo de 2005, en Buenos Aires, Argentina, dirigió una conferencia donde relató cómo pudo acceder fácilmente al código de un teléfono móvil en desarrollo, aún antes de ser anunciado en el mercado, mediante únicamente seis llamadas telefónicas y en pocos minutos. En 2010, se presentó en la Ciudad de México para dar una ponencia en el Campus Party.

EL HACKER MÁS FAMOSO

Mitnick comenzó en el mundo del hacking a los 16 años, cuando estaba obsesionado con las redes de computadoras
y logró romper la seguridad del sistema administrativo de su colegio, afirmando que sus acciones fueron "sólo para mirar", más no para alterar sus calificaciones.

En 1981 se le consideró por primera vez como delincuente informático, luego de que junto a dos amigos, logró entrar físicamente a las oficinas de COSMOS, de Pacific Bell. COSMOS era una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas para controlar el registro de llamadas.

Al estar dentro de las oficinas, consiguieron una lista de claves de seguridad, combinación de

puertas de acceso de varias sucursales y manuales del sistema COSMOS. Se estima que la información robada tenía un valor que rondaba los 200,000 dólares.

Fue la novia de uno de sus amigos quien los delató, y debido a que era menor de edad, una corte juvenil lo sentenció a tres meses de cárcel y un año de libertad condicional.

Al cumplir los tres meses, el oficial custodio que se encargó de su caso encontró que su teléfono fue desconectado y que en la compañía telefónica no había ningún registro de él.

Con el paso del tiempo, sus objetivos eran más grandes. En 1982, accedió de forma ilegal, vía módem, a la computadora del North American Air Defense Command, en Colorado. Antes de su intrusión, alteró el programa que se encargaba de rastrear la procedencia de las llamadas y desvió el rastro de su llamada a otro lugar.

Al paso de un año, fue arrestado nuevamente siendo estudiante de la Universidad del Sur de California. Esta vez accedió ilegalmente a ARPAnet, la predecesora de lo que ahora es Internet, y trató de acceder a la computadora del Pentágono. Por estas acciones lo sentenciaron a seis meses de cárcel en una prisión juvenil de California.

En 1987, trataba de no realizar acciones ilegales, sin embargo, fue acusado en Santa Cruz California, por invadir el sistema de la empresa Microcorp Systems. Esta vez su sentencia fue de tres años de libertad condicional, pero luego de la sentencia, su expediente desapareció de la computadora de la policía local.

Tiempo después, buscó trabajo en el Security Pacific Bank, como encargado de la seguridad de la red del banco. Sin embargo, el banco lo rechazó por sus antecedentes penales y Mitnick falsificó un balance general del banco donde se mostraban pérdidas por 400 millones de dólares y luego trató de enviarlo por la red.

Ese mismo año, comenzó el escándalo que lo convertiría en un ícono del hacking a nivel mundial. Durante meses estuvo observando de forma secreta el correo electrónico de los miembros del departamento de seguridad de MCI Communicattions y Digital Equipment

Corporation, con el fin de conocer cómo estaban protegidas las computadoras y el sistema telefónico de ambas compañías.

Cuando recabó la información suficiente, se apoderó de 16 códigos de seguridad de MCI y, con un amigo, Lenny DiCicco, lograron acceder a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet.

Los dos hackers querían conseguir una copia del prototipo del nuevo sistema operativo de seguridad de Ditial, llamado VMS. Sin embargo, el personal de seguridad se percató de forma inmediata del ataque y dieron aviso al FBI, entonces comenzaron a rastrear a los responsables.

Mitnick trató de echarle la culpa a DiCicco, mediante llamadas anónimas al jefe de éste mismo, quien trabajaba en una compañía de software como técnico de soporte. Estas acciones enfurecieron a DiCicco, por lo que confesó todo a su jefe, mismo que los denunció a Digital y al FBI.

Entonces Mitnick fue arrestado en 1998 por invadir el sistema de Digital Equipment. La empresa acusó al hacker y su amigo ante un juez federal por causarles daños por 4 millones de dólares por el robo de su sistema operativos.
Mitnick fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Además de la sentencia, el fiscal obtuvo una orden de la Corte para prohibir a Mitnick el uso de teléfono en la prisión, alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono.
Sin embargo, Mitnick logró que el juez le autorizara a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela, y esto sólo bajo supervisión de un oficial.

Este caso causó revuelo en Estados Unidos, no sólo por el hecho delictivo por parte de Kevin, sino por la táctica que utilizó la defensa, cuando el abogado del hacker convenció al juez de que su cliente sufría adicción a las computadoras, equivalente a la adicción de un drogadicto,

un alcohólico o un apostador. Gracias a esta maniobra del abogado, Mitnick fue sentenciado a sólo un año de prisión, y al salir de la misma, debía seguir un programa de seis meses para tratar su “adicción a las computadoras”.

Durante su tratamiento se le prohibió el uso de computadoras o módems, con lo que llegó a perder 45 kilos.
En 1991, era el hacker que salió en primera plana del New York Times, y uno de los reporteros de dicho diario escribió un libro narrando las aventuras de Kevin.

Pero al parecer a Mitnick no le gustó el libro, ya que después de salir a la venta, la cuenta del periodista John Markoff fue invadida, y cambió su nivel de acceso, de modo que cualquier persona podría entrar a su Correo electrónico.
Un año después, Mitnick comenzó a trabajar en una agencia de detectives, pero al poco tiempo se descubrió un manejo ilegal en el uso de las bases de datos y por lo tanto, se le abrió una investigación por parte del FBI, agencia que al poco tiempo determinó que se habían violado los términos de su libertad condicional.

Por lo tanto, allanaron su casa, pero Mitnick había desaparecido sin dejar ningún rastro, convirtiéndose ahora en prófugo de la justicia.

Ese mismo año, el Departamento de Vehículos de California ofreció una recompensa de un millón de dólares a quien lograra arrestar a Mitnick, debido a que trató de obtener una licencia de conducir de forma fraudulenta, utilizando un código de acceso y enviando sus datos por fax.

Aunque las autoridades pasaron mucho tiempo sin lograr encontrar rastros de Mitnick, dieron con la computadora de Tsutomu Shimomura, la cual fue invadida por Kevin en la Navidad de 1994.

Shimomura era un físico computacional y experto en sistemas de seguridad del San Diego Supercomputer Center. Además, era un hacker de los “buenos”, que al encontrar alguna falla de seguridad en algún sistema lo reportaba a las autoridades.

Shimomura se dio cuenta de que alguien había accedido a su ordenador en su ausencia, utilizando un método de intrusión muy sofisticado y que él no había visto nunca. El intruso le había robado el acceso a su correo electrónico, software para el control de teléfonos móviles y varias herramientas de seguridad. Por lo anterior, Shimomura se propuso atrapar al hacker que violó su privacidad.

A finales de enero de 1995, el software de Shimomura se encontró en una cuenta en The Well, un proveedor de Internet en California. Mitnick creó una cuenta fantasma en ese proveedor y desde allí utilizaba las herramientas de Shimomura para lanzar ataques a una docena de corporaciones de ordenadores, entre ellas estaban Motorola, Apple y Qualcomm.

Shimomura se reunió con el gerente de The Well y con un técnico de Sprint, descubrieron que Mitnick había creado un número móvil fantasma para poder acceder al sistema. Luego de dos semanas de rastreo, encontraron que las llamadas provenían de Raleigh, California.

Cuando Shimomura llegó a Raleigh, recibió una llamada del experto en seguridad de InterNex, otro proveedor de Internet en California. Se percataron de que Mitnick invadió nuevamente el sistema de InterNex, creando una cuenta de nombre Nancy borrando una con el nombre Bob, además de cambiar varias claves de seguridad, Incluyendo la del experto y la del gerente del sistema que posee los privilegios más altos.

Shimomura se comunicó con el FBI y ésta agencia envió un grupo de rastreo por radio. El equipo de rastreo contaba con un simulador de celda, que era utilizado para probar teléfonos móviles, pero lo modificaron para rastrear el teléfono de Mitnick, mientras estuviera encendido y aunque no se encontrara en uso.

Mientras el FBI se ocupaba del rastreo, InterNex, The Well y Netcom se encontraban sumamente preocupados por los movimientos que Mitnick hacía de forma simultánea en cada uno de sus sistemas.

Cambiaba las claves de acceso que él mismo había creado y que tenían menos de 12 horas de creadas, utilizando códigos extraños e irónicos como “no”, “panix”, “fukhood” y “fuckjkt”.

Estaba creando nuevas cuentas con mejores niveles de seguridad, como si sospechara que lo estuvieran vigilando.

El FBI, Shimomura y el equipo de Sprint se reunieron para planificar la captura.
Shimomura envió un mensaje codificado al buscapersonas del encargado en Netcom para advertirle que el arresto se iba a realizar al siguiente día, 16 de febrero. Shimomura envió varias veces el mensaje por equivocación, lo que ocasionó que el encargado creyera que Mitnick ya había sido arrestado, y se adelantó a realizar una copia de respaldo de todo el material que Mitnick había almacenado en Netcom como evidencia y borrando las versiones almacenadas por Mitnick.

Por lo tanto, había que realizar el arresto inmediatamente antes de que se diera cuenta de que su información fue borrada.

A los pocos minutos para dar la orden, el simulador de celdas detectó una nueva señal de transmisión de datos vía teléfono móvil y simultánea a la de Mitnick, muy cerca de esa zona. Shimomura supo que Mitnick estaba haciendo algo raro con las líneas móviles, por lo que trató de dar aviso al FBI.

El FBI no planeaba una entrada violenta ya que creían que Mitnick no estaba armado, sin embargo, tenían que actuar rápido, ya que estaban conscientes del daño que podría causar en pocos minutos con un ordenador. Se acercaron al apartamento de Mitnick y anunciaron su presencia, con la idea de que si en cinco segundos no abría la puerta, la derribarían, pero Mitnick abrió con toda calma y el FBI procedió con el arresto, así como decomisar todo el material pertinente, como discos, computadoras, teléfonos, manuales, entre otros.

Cuando Shimomura regresó a su hotel, quiso comprobar el contestador telefónico de su residencia en San Diego, se quedó paralizado cuando escuchó la voz de Mitnick, quien le dejó varios mensajes con acento Oriental en tono de burla.

El último mensaje lo había recibido ocho horas después del arresto y antes de que la prensa se enterara de todo el asunto.

Hasta la fecha es un misterio cómo se realizó esa llamada, al igual que el origen y objetivo de la segunda señal.
En la actualidad Kevin Mitnick aconseja a los jóvenes informáticos a no seguir su camino.

Desde el año 2000, Mitnick ha sido consultor de seguridad, orador y autor. Hace consultoría de seguridad para las compañías Fortune 500 y realiza pruebas de penetración para las empresas más grandes del mundo, además de impartir clases de ingeniería social para decenas de empresas y agencias gubernamentales.

Mitnick es el co-autor, junto a William L. Simon, de dos libros de seguridad informática y su autobiografía, estos se titulan “El arte del engaño”, “El arte de la intrusión: Las historias reales detrás de las hazañas de hackers, intrusos y estafadores”, y “Fantasma en los cables: Mis aventuras como el hacker más buscado del mundo”.

En el año 2014, durante la convención anual de hackers DEF CON, en Las Vegas, Kevin afirmó que era capaz de robar la identidad de cualquier persona en tan sólo 3 minutos. Añadió seguridad a su afirmación cuando pudo descubrir en línea el número de seguridad social de un voluntario del público.

En la película Algoritmo – The Movie Hacker, de 2014, el protagonista hace referencia a Kevin Mitnick.
En días actuales, Mitnick dirige una empresa de seguridad llamada Mitnick Security Consulting LLC, la cual ayuda a probar las fortalezas de una empresa de seguridad, debilidades y vulnerabilidades potenciales, además de ser el jefe oficial de la compañía de formación de conciencia de seguridad KnowBe4.