POR CUAUHTÉMOC VÉLEZ MARTÍNEZ

Cápsula TI No. 33

HACKERS FAMOSOS

Aunque siempre ha existido la creencia que los gobiernos dedican millones de dólares para proteger su infraestructura informática logrando crear verdaderos bastiones, lo cierto es que durante décadas, se han visto casos de usuarios que siendo o no *hackers* experimentados, han logrado acceder a estos sistemas supuestamente impenetrables utilizando distintas técnicas que van desde la ingeniería social hasta el desarrollo de códigos altamente sofisticados y efectivos. En este artículo, revisaremos algunos casos de *hackers* que lograron fama no sólo por sus habilidades informáticas sino por las instituciones que fueron víctimas de sus ataques.

A finales de los noventa Richard Pryce, adolescente británico junto con Mathew Bevan, irrumpieron los sistemas de defensa del Pentágono robando información de la base Grifiss de la fuerza aérea así como datos sobre investigación de armas balísticas, diseño de aviones, registros de personal y correos electrónicos, entre otros. Después de dos años de investigación, fueron arrestados pero, por tratarse de menores de edad, salieron libres pagando una pequeña multa.

Otro caso fue el del británico Gary Mckinnon, también conocido como "Solo" quien logró llevar a cabo el *hacking* más largo de la historia accediendo ilegalmente a los sistemas del Pentágono y la NASA por más de un año (de febrero de 2001 a marzo de 2002) desplegando al final el mensaje *Your security is crap* (Su seguridad es una porquería). Dejó decenas de computadoras inoperables y borró cientos de archivos confidenciales. El gobierno de los Estados Unidos, ha intentado extraditarlo desde 2002 para enfrentar cargos por daños en sus sistemas militares sin embargo, aún sigue en espera de concretar este proceso.

"Astra" es el pseudónimo de un *hacker* de origen griego quien fue capaz de violentar los sistemas de la compañía francesa de aviación Dassault Group, robando información durante más de cinco años sobre el diseño de aviones militares. Una vez obtenido su botín, lo vendía a numerosos países de Europa y América ocasionando pérdidas por más de 360 millones de dólares. La identidad de este *hacker,* nunca fue revelada.

Owen Walker, también llamado "AKILL", un joven neozelandés que antes de cumplir la mayoría de edad fue capturado por la policía acusado de dirigir un grupo de *hackers* que tenían el control de más de un millón de equipos de cómputo (*netbot*) para uso de una red criminal, cuya principal actividad, era acceder a cuentas bancarias, robar tarjetas de crédito o llenar a los usuarios de *spam* (correos basura). Por ser menor de edad, su sentencia fue mínima pagando una multa y perdiendo el dinero que recibió del grupo criminal. Actualmente trabaja para TelstraClear, empresa neozelandesa de telecomunicaciones.

Sin embargo, uno de los *hackers* más famosos es Kevin Mitnick o "Cóndor", como era conocido en el medio. Actualmente convertido en consultor externo sobre seguridad informática. Durante su adolescencia, Mitnick fue capaz de realizar múltiples accesos a distintas instituciones públicas y privadas, entre ellas el Pentágono, ARPAnet (predecesor de *internet*), el sistema de defensa norteamericano, Microcorps Systems y Digital Equipment Corporation. A pesar de ser considerado por el FBI como el *hacker* más buscado y peligroso de la historia, según él, su única motivación fue tratar de burlar la seguridad de los sistemas atreviéndose a enfrentar retos cada vez más riesgosos y sofisticados. Más que un *hacker,* Mitnick se autodefine como un *phreacker* e ingeniero social. El *phreacking* es el acto de irrumpir sistemas telefónicos y para ello, Kevin era un verdadero mago, de hecho, su interés por esta actividad le permitió realizar llamadas gratuitas, clonar números de teléfono, efectuar desvíos de llamadas no autorizadas y poner a su disposición claves telefónicas a nombre de James Bond sin pagar un solo centavo; como ingeniero social, obtuvo mediante el engaño y convencimiento de personas incautas, claves de acceso, manuales técnicos y datos sensibles de grandes corporaciones. De las múltiples ocasiones en que fue capturado, su argumento ante la corte fue haber penetrado en los sistemas, aunque nunca destruyó datos, copiar información que jamás vendió y robar *software* para luego abandonarlo, afirmando que su intención jamás fue especular financieramente con sus acciones. Fue encarcelado durante cinco años además de aplicarle una restricción muy *sui géneris* para esa época: tenía estrictamente prohibido

Adrian Lamo, Kevin Mitnick, y Kevin Lee Poulsen, circa 2001. Fotografía: Matthew Griffiths

acceder a cualquier computadora o teléfono. Es por ello que Mitnick se convirtió en un personaje mítico para la comunidad *hacker*.

Así pues, el término *hacker* ha llegado a ser un símbolo ambivalente de chicos "buenos" y "malos", si bien es cierto que muchos de ellos han causado pérdidas millonarias a las empresas, también debemos reconocer su contribución para mejorar los sistemas de información haciéndolos más robustos y seguros.

Referencias

Benetto, J. (1997). "Fine for boy who hacked into Pentagon". Independent. Tomado de:
http://www.independent.co.uk/news/fine-for-boy-who-hacked-into-pentagon-1274204.html

Cîrlig, C. (2014). "Cyber defence in the EU Preparing for cyber warfare?". European Parliament. Tomado de:
http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

Hodgson, M. (2008). "Teenager guilty of million-dollar hacking campaign". The Guardian. Tomado de:
https://www.theguardian.com/technology/2008/apr/01/hitechcrime.hacking

NATO(2013). "The history of cyber attacks - a timeline". North Atlantic Treaty Organization.
Tomado de:
http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm Sheldon, J. (2013). "Cyberwar". Encyclopedia Britannica. Tomado de;
https://global.britannica.com/topic/cyberwar