Updates to History of Computer Crime

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

I've been updating chapters in the upcoming edition of a textbook and hope readers will find some of the research interesting. This week I'm posting materials I added to the chapter on the history of computer crime.

Late 2000s: Russian Business Network (RBN)

The Russian Business Network (RBN) may have originated as a legitimate Web hosting company in 2006:

> According to internet security company Verisign, which in June published an extensive investigation into the Russian outfit (tinyurl.com/ywvgpg), RBN was registered as an internet site in 2006.
>
> Initially, much of its activity was legitimate. But apparently the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. Verisign says simply that it is now "entirely illegal". Since then its activities have been monitored by a number of organisations, including the London-based anti-spam group Spamhaus. "RBN is among the world's worst spammer, child-pornography, malware, phishing and cybercrime hosting networks," says a spokesman. "It provides 'bulletproof' hosting, but is probably involved in the crime too." [1]

A researcher for the Internet Storm Center, "David Bizeul, spent the past three months researching the Russian Business Network (RBN). The RBN is a virtual safe house for Russian criminals responsible for malicious code attacks, phishing attacks, child pornography and other illicit operations…." Bizeul's study is a 70-page report with extensive documentation about the criminal activities of the RBN.[2] The group has supported malware diffusion, spam, phishing, denial of service, distribution of cyberattack tools, pornography and child pornography.

A 2011 report by David Goldman included the following useful insights:

> "It's not like the Mafia, it is a Mafia running these operations," said Karim Hijazi, CEO of botnet monitoring company Unveillance. "The Russian Mafia are the most prolific cybercriminals in the world."
>
> Organized cybercrime is a truly international affair, but the most advanced attacks tend to stem from Russia. The Russian mob is incredibly talented for a reason: After the Iron Curtain lifted in the 1990s, a number of ex-KGB cyberspies realized they could use their expert skills and training to make money off of the

hacked information they had previously been retrieving for government espionage purposes.

Former spies grouped together to form the Russian Business Network, a criminal enterprise that is capable of some truly scary attacks. It's just one of many organized cybercriminal organizations, but it's one of the oldest and the largest.

"The Russians have everyone nailed cold in terms of technical ability," said Greg Hoglund, CEO of cybersecurity company HBGary. "The Russian crime guys have a ridiculous toolkit. They're targeting end users in many cases, so they have to be sophisticated."[3]

Anonymous

In 2003, political activists with a penchant for computer skills formed a loose association calling itself *Anonymous* for collaboration in a range of cyberattacks on targets its members disliked. The philosophy of the group explicitly rejects any centralized controls; anyone can claim to be a member of Anonymous.

In 2008, self-identified members of the movement labeling their efforts *Chanology*[4] attacked the Church of Scientology (readers interested in following the reference provided above should be aware that the site is loaded with pornographic advertisements for pornography sites). Members also harassed organizations attempting to strengthen intellectual property laws and enforcement or anti-piracy restrictions. Other targets of the non-organization include the Epilepsy Foundation, hip-hop Websites, Sarah Palin's political campaign, the government of Iran, the government of Australia, and the Tea Party chapter in Oregon.

One of the most publicized campaigns was in support of Julian Assange, leader of the WikiLeaks Foundation, whose group made public more than a million documents classified by the US and other governments as restricted or secret and revealing embarrassing details of several wars and internal communications among diplomats.

In January 2013, members announced that they would release large amounts of US government restricted information. They let the world know about their plans by posting their messages on a hacked US government Website.[5]

Unlimited Operations

In May 2013, eight criminal hackers, New York City area members of a much larger worldwide ring of cybercriminals calling themselves Unlimited Operations were charged with theft of over $45M from automated teller machines (ATMs) around the planet. The gang "used sophisticated intrusion techniques to hack into the systems of global financial institutions, steal prepaid debit card data, and eliminate withdrawal limits. The stolen card data was then disseminated worldwide and used in making fraudulent ATM withdrawals on a massive scale across the globe…."

In the first phase, the criminals broke into National Bank of Ras Al-Khaimah PSC (RAKBANK) in the United Arab Emirates. Using these compromised data, the criminal network completed over 4,500 ATM transactions in 20 and stole over $5M.

The second phase began "…on the afternoon of February 19 and lasted into the early morning of February 20, 2013. This operation again breached the network of a credit card processor that serviced MasterCard prepaid debit cards, this time issued by the Bank of Muscat, located in Oman." Total losses from 36,000 transactions in 24 countries netted $40 million in cash from ATMs.[6]

Industrial Espionage

Why spend money developing competitive products when you can steal the work once it's ready to apply? Many firms in countries with little or no rule of law have taken advantage of poor security, outsourcing, and liberal immigration policies to steal intellectual property and compete at a discount with the originators of the ideas.

In 2001, Junsheng Wang of Bell Imaging Technologies pled guilty to violation of 18 USC 132(a)(2) by stealing trade secrets fom Acuson Corporation. The Counterintelligence News and Developments (CIND) report noted, "In pleading guilty, Wang admitted that prior to August 24, 2000, that he took without authorization and copied for Bell Imaging a document providing the architecture for the Sequoia ultrasound machine that contained the trade secrets of Acuson Corporation. According to Wang's plea agreement, he had been able to obtain access to the Acuson trade secret materials because his wife was employed as an engineer at that company and because she had brought that document into their home. After he had copied the document, he took it with him on business trips to the People's Republic of China, turning it over to Bell Imaging during 2000."[7]

In May 2001, Federal authorities arrested two Lucent scientists and a third man described as their business partner on May 4, charging them with stealing source code for software associated with Lucent's PathStar Access Server and sharing it with Datang Telecom Technology Co., a Beijing firm majority-owned by the Chinese government. The software is considered a "crown jewel" of the company. Chinese nationals Hai Lin and Kai Xu were regarded as "distinguished members" of Lucent's staff up until their arrests. The motivation for the theft, according to court documents, was to build a networking powerhouse akin to the "Cisco of China." The men faced charges of conspiracy to commit wire fraud, punishable by a maximum five years in prison and a $250,000 fine.[8] In April 2002, the two were also charged with stealing secrets from four companies in addition to Lucent: Telenetworks, NetPlane Systems, Hughes Software Systems, and Ziatech. An additional Chinese national, Yong-Qing Cheng was also charged. They developed a joint venture with the Datang Telecom Technology Company of Beijing to sell a clone of Lucent's Path Star data and voice transmission system to Internet providers in China.[9]

In September 2002, the 3DGeo company in Mountain View, CA accused Shan Yanming, an employee of the China National Petroleum Corporation on loan to the company, of industrial espionage for trying to steal the software designed for using seismic data to map oil deposits. He was caught trying to download corporate data to his personal computer and ws arrested by FBI agents.[10]

In April 2003, the United States Attorney's Office for the Northern District of California announced that Tse Thow Sun pled guilty on April 9, 2003 to theft of trade secrets. He admitted that in early 2002, while working for a language translation company, he delivered a laptop computer and a hard drive that contained trade secrets and confidential proprietary information to a competitor and asked for $3M in payment. Mr. Sun, 32, a citizen of Singapore, was indicted by a federal Grand Jury on April 9, 2002. He was charged with theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(3); attempted theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(4); and interstate transportation of stolen goods, in violation of 18 U.S.C. § 2314. Under the plea agreement, Mr. Sun pled guilty to theft of trade secrets.[11]

In May 2003, three Swedish employees of LM Ericsson were charged with espionage for allegedly stealing intellectual property and sending it to Russian spies. "[Afshin] Bavand was arrested Nov. 5, 2002, while talking to a Russian intelligence agent in a Stockholm suburb. Police searched the Russian, who wasn't identified, and found $4,000 in cash and Ericsson documents."[12]

The series of attacks codenamed *Titan Rain* was discovered by Shawn Carpenter in late 2003. Carpenter noticed a flood of expert hacker activity focusing on data theft from a wide range of "the country's most sensitive military bases, defense contractors and aerospace companies." Carpenter discovered that "the attacks emanated from just three Chinese routers that acted as the first connection point from a local network to the Internet." Carpenter worked with US Army and FBI investigators to learn more about the attacks and the attackers. According to Thornburgh, various analysts judge that "Titan Rain is thought to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced."[13]

In July 2004, an Indian software engineer employed by a US company's software development center in India was accused of "zipping up" proprietary software source code for printing identification cards and uploading it to her personal e-mail account. Jolly Technologies shut down its Mumbai operations as a result of the breach of security.[14]

In 2005 and 2006, EMC filed lawsuits against several employees for allegedly stealing trade secrets.[15]

In December 2006, two Chinese nationals, Fei Ye and Ming Zhong, pleaded guilty in December 2006 to charges of economic espionage on behalf of the People's Republic of China. They were arrested in November 2001 with stolen trade secrets in their luggage; the information was taken from Sun Microsystems and Transmeta Corporation. The agents were planning to design a competing microprocessor using the stolen designs; profits were to have been shared with the City of Hangzhou and the Province of Zhejiang. The agents' company was funded in part by the National High Technology Research and Development Program of China.[16]

In April 2008, sleeper agent Chi Mak, a naturalized US citizen who lived peacefully in Los Angeles for 20 years, was sentenced to 24.5 years in federal prison for industrial espionage. He stole detailed plans for US Navy equipment including submarine propulsion systems and tried to send them to China via his brother and sister-in law.[17]

In 2009, Siobhan Gorman, writing in *The Wall Street Journal*, reported as follows:

Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials. The

spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war. "The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians." The espionage appeared pervasive across the U.S. and doesn't target a particular company or region, said a former Department of Homeland Security official. "There are intrusions, and they are growing," the former official said, referring to electrical systems. "There were a lot last year."[18]

The Office of the National Counterintelligence Executive (ONCIX) published its *Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011* with the title *Foreign Spies Stealing US Economic Secrets in Cyberspace.* The Executive Summary included this commentary:

"Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.

Chinese actors are the world's most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC cannot confirm who was responsible.

Russia's intelligence services are conducting a range of activities to collect economic information and technology from US targets.

Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities."[19]

A March 2012 report detailed how a successful supervisory control and data acquisition (SCADA) software company, American Superconductor Corporation (AMSC), was practically destroyed economically by its major customer, the Chinese Sinovel company, which stole its proprietary wind-turbine software and then stopped paying for any further software services.[20]

By early 2013, Symantec's 2012 Internet Security Threat Report, Vol, 18 reported that small businesses were increasingly targeted for cyber attacks and industrial espionage: "In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. In fact, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them."[21]

* * *

Copyright © 2013 M. E. Kabay. All rights reserved.

END NOTES FOR PUBLICATION

[1] (Warren 2007)
[2] (Bizuel 2007)
[3] (Goldman 2011)
[4] (Anonymous 2012)
[5] (Ferenstein 2013)

[6] (US Department of Justice 2013)
[7] (San Francisco Business Times 2001)
[8] (Backover 2001)
[9] (New York Times 2002)
[10] (Markoff 2002)
[11] (US Department of Justice 2003)
[12] (USA TODAY 2003)
[13] (Thornburgh 2005)
[14] (Ribeiro 2004)
[15] (Wallack 2006)
[16] (US Department of Justice 2006)
[17] (Warrick and Johnson 2008)
[18] (Gorman 2009)
[19] (Office of the National Counterintelligence Executive (ONCIX) 2011)
[20] (Riley and Vance 2012)
[21] (Symantec 2013)

REFERENCES FOR PUBLICATION

"Ms Smith". "DHS: Imported Tech Tainted with Backdoor Attack Tools." *NetworkWorld | Privacy and Security Fanatic*. 07 12, 2011. http://www.networkworld.com/community/blog/dhs-imported-tech-tainted-backdoor-attack-too (accessed 05 16, 2013).

Anonymous. "Portal: Anonymous/Chanology." *Encyclopedia Dramatica*. 10 29, 2012. https://encyclopediadramatica.se/Portal:Anonymous/Chanology (accessed 05 16, 2013).

Backover, Andrew. "Feds: Trio stole Lucent's trade secrets." *USA TODAY*. 05 03, 2001. http://usatoday30.usatoday.com/life/cyber/tech/2001-05-03-lucent-scientists-china.htm (accessed 05 16, 2013).

Bizuel, David. "Russian Business Network study." bizuel.org. 11 20, 2007. http://www.bizeul.org/files/RBN_study.pdf (accessed 05 16, 2013).

Ferenstein, Gregory. "Anonymous Threatens Massive WikiLeaks-Style Exposure, Announced On Hacked Gov Site." *TechCrunch*. 01 26, 2013. http://techcrunch.com/2013/01/26/anonymous-threatens-massive-wikileaks-style-exposure-announced-on-hacked-gov-site/ (accessed 05 16, 2013).

Finkle, Jim. "Researchers say Stuxnet was deployed against Iran in 2007." *Reuters*. 02 26, 2013. http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226 (accessed 05 16, 2013).

Goldman, David. "The cyber Mafia has already hacked you." *CNNMoney*. 07 07, 2011. http://money.cnn.com/2011/07/27/technology/organized_cybercrime/index.htm (accessed 05 16, 2013).

Gorman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies." *Wall Street Journal*. 04 08, 2009. http://online.wsj.com/article/SB123914805204099085.html (accessed 05 16, 2013).

Javelin Strategy & Research. "2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a

Treasure Trove for Fraudsters." Javelin. 2013. https://www.javelinstrategy.com/brochure/276 (accessed 05 16, 2013).

Langton, Lynn. "Identity Theft Reported by Households, 2005-2010." *Bureau of Justice Statistics*. 11 30, 2011. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2207 (accessed 05 16, 2013).

Markoff, John. "Silicon Valley Concern Says It Thwarted Software Theft." *New York Times*. 09 20, 2002. http://www.nytimes.com/2002/09/20/technology/20SOFT.html (accessed 05 16, 2013).

New York Times. "Trade-Secret Case Is Expanded." *New York Times*. 04 12, 2002. http://www.nytimes.com/2002/04/12/technology/12LUCE.html (accessed 05 16, 2013).

Office of the National Counterintelligence Executive (ONCIX). "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-1011." Office of the National Counterintelligence Executive. 11 03, 2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed 05 16, 2013).

Ribeiro, John. "Source code stolen from U.S. software company in India: Jolly Technologies blamed an insider for the theft." *Computerworld*. 08 05, 2004. http://www.computerworld.com/s/article/95045/Source_code_stolen_from_U.S._software_company_in_India?taxonomyId=082 (accessed 05 16, 2013).

Riley, Michael, and Ashlee Vance. "Inside the Chinese Boom in Corporate Espionage." *Bloomberg Businessweek*. 03 15, 2012. http://www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage (accessed 05 16, 2013).

San Francisco Business Times. "Guilty pleas in trade secret case." *San Francisco Business Times*. 04 27, 2001. http://www.bizjournals.com/eastbay/stories/2001/04/23/daily42.html (accessed 05 16, 2013).

Symantec. "Internet Security Threat Report 2013." Symantec. 04 15, 2013. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (accessed 05 16, 2013).

Thornburgh, Nathan. "Inside the Chinese Hack Attack." *TIME*. 08 25, 2005. http://www.time.com/time/nation/article/0,8599,1098371,00.html (accessed 05 16, 2013).

US Department of Justice. "Chicago, Illinois Man Pleads Guilty to Theft of Trade Secrets, Offered to Sell Online Interpreter's Information." US Department of Justice | Northern District of California. 04 11, 2003. http://www.justice.gov/criminal/cybercrime/press-releases/2003/sunPlea.htm (accessed 05 16, 2013).

—. "Eight Members of New York Cell of Cybercrime Organization Indicted in $45 Million Cybercrime Campaign." US Department of Justice | Eastern District of New York. 05 09, 2013. http://www.justice.gov/usao/nye/pr/2013/2013may09.html (accessed 05 16, 2013).

—. "Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit

China." US Department of Justice | Northern District of California. 12 14, 2006. http://www.justice.gov/criminal/cybercrime/press-releases/2006/yePlea.htm (accessed 05 16, 2013).

USA TODAY. "Three charged in Ericsson spy investigation in Sweden." *USA TODAY*. 05 08, 2003. http://usatoday30.usatoday.com/tech/news/2003-05-08-ericsson_x.htm (accessed 05 16, 2013).

Vijayan, Jaikumar. "Stuxnet renews power grid security concerns: First known SCADA malware program to target control systems prompts new questions about security of U.S. power grid." *NetworkWorld*. 07 26, 2010. http://www.networkworld.com/news/2010/072610-stuxnet-renews-power-grid-security.html (accessed 05 16, 2013).

Wallack, Todd. "EMC sues ex-employees to guard trade secrets." *Boston Business Journal*. 10 09, 2006. http://www.bizjournals.com/boston/stories/2006/10/09/story4.html?page=all (accessed 05 16, 2013).

Warren, Peter. "Hunt for Russia's web criminals: The Russian Business Network -- which some blame for 60% of all internet crime -- appears to have gone to ground. But, asks Peter Warren, has it really disappeared?" *Guardian*. 11 15, 2007. http://www.guardian.co.uk/technology/2007/nov/15/news.crime (accessed 05 16, 2013).

Warrick, Joby, and Carrie Johnson. "Chinese Spy 'Slept' In U.S. for 2 Decades: Espionage Network Said to Be Growing." *Washington Post*. 04 03, 2008. http://www.washingtonpost.com/wp-dyn/content/story/2008/04/02/ST2008040204050.html (accessed 05 16, 2013).

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *

Copyright © 2013 M. E. Kabay. All rights reserved.