Oil Industry Open to Cyberattacks

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

A colleague recently asked me how vulnerable oil-industry installations are to cyberattack; unfortunately, the consensus seems to be “Very.”

In February 2011, a report surfaced that “Computer hackers working through Internet servers in China broke into and stole proprietary information from the networks of six U.S. and European energy companies, including Exxon Mobil Corp., Royal Dutch Shell Plc and BP Plc….”[1] Other targets included “Marathon Oil Corp., ConocoPhillips and Baker Hughes Inc., …. [a] Houston-based provider of advanced drilling technology.” Publicly traded oil-industry companies hacked by industrial spies or saboteurs might be sued by shareholders if they fail to disclose such attacks: “Investors might also argue they had a right under U.S. securities laws to be informed of the thefts, which a judge might construe as a ‘material’ fact that should have been disclosed….”

In an August 2011 report, Matt Liebowitz of the *SecurityNewsDaily* reported on a Black Hat Security Conference demonstration of hacking the programmable logic controllers (PLCs) used in many industrial systems including power plants and oil refineries.[2] Dillon Beresford, an expert penetration tester, found canonical (standard) passwords on a Siemens Simatic S7 PLC. He was able to shut down the controllers and also to “report false data to make the operator ‘think that everything's functioning normal, when in fact it's not.’”

The Duqu Trojan software detected in October 2011 by the anti-malware firm Symantec is “scarily similar to the infamous Stuxnet worm, which could disrupt computers controlling power plants, oil refineries and other critical infrastructure networks.”[3] Stuxnet is the worm that disabled the supervisory control and data acquisition (SCADA) systems in Iran’s nuclear-fuel processing facility.[4] “Symantec said whoever is behind Duqu rigged the Trojan to install another information-stealing program on targeted computers that could record users' keystrokes and system information and transmit them, and other harvested data, to a command-and-control (C&C) server.”

In December 2011, a speaker from Shell Oil at “the World Petroleum Conference in Doha … [said] … that the company had suffered an increased number of attacks …. motivated by both commercial and criminal intent.” The manager warned, “"If anybody gets into the area where you can control opening and closing of valves, or release valves, you can imagine what happens. It will cost lives and it will cost production, it will cost money, cause fires and cause loss of containment, environmental damage – huge, huge damage.”[5] The *FinancialMirror*, reporting on the same presentation, wrote that “Hackers are bombarding the world's computer controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil

[1] (Riley 2011)
[2] (Liebowitz, How Easily Can a Power Plant Be Hacked? Very. 2011)
[3] (Liebowitz, Stuxnet Clone Found Possibly Preparing Power Plant Attacks 2011)
[4] (Zetter 2011)
[5] (BBC 2011)

supply disruption. Oil company executives warned that attacks were becoming more frequent and more carefully planned."[6] They added (quoting an interview):

> "Cyber crime is a huge issue. It's not restricted to one company or another it's really broad and it is ongoing," said Dennis Painchaud, director of International Government Relations at Canada's Nexen Inc. "It is a very significant risk to our business. It's something that we have to stay on top of every day. It is a risk that is only going to grow and is probably one of the preeminent risks that we face today and will continue to face for some time."

Other speakers interviewed in the *FinancialMirror* story explained that cyberattacks could be used for financial gain: reducing the flow of oil could raise prices – and threats and incidents involving oil-industry installations could allow criminals and state-sponsored cyberattackers to profit using the futures market.

Readers interested in learning more about SCADA vulnerability testing will find a valuable resource by Joel Langill online at SCADAhacker.com, which includes dozens of professional papers by the penetration expert.[7]

Works Cited

BBC. "Oil cyber-attacks could cost lives, Shell warns." *BBC News Technology.* 12 12, 2011. http://www.bbc.co.uk/news/technology-16137573 (accessed 01 15, 2012).

FinancialMirror. "Cyber attacks could wreck world oil supply." *FinancialMirror | News | Business & Economy.* 12 11, 2011. http://www.financialmirror.com/news-details.php?nid=25208# (accessed 01 15, 2012).

Langill, Joel. "About SCADAhacker." *SCADAhacker.* 01 13, 2012. http://scadahacker.com/about.html (accessed 01 15, 2012).

Liebowitz, Matt. "How Easily Can a Power Plant Be Hacked? Very." *securitynewsdaily.* 08 03, 2011. http://www.securitynewsdaily.com/how-easily-can-a-power-plant-be-hacked-very-1023/ (accessed 01 15, 2012).

—. "Stuxnet Clone Found Possibly Preparing Power Plant Attacks." *securitynewsdaily.* 10 18, 2011. http://www.securitynewsdaily.com/stuxnet-clone-found-preparing-power-plant-attacks-1250/ (accessed 01 15, 2012).

Riley, Michael. "Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers." *Bloomberg.* 02 24, 2011. http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html (accessed 01 15, 2012).

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired.* 07 11, 2011. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 (accessed 01 15, 2012).

* * *

[6] (FinancialMirror 2011)

[7] (Langill 2012)

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/ >