I have been writing about industrial espionage in this series and now turn to a current case of great value in exploring issues of who is attacking the USA, how to manage an investigation without getting fired, and whether Web site operators can and should block packets from specific domains.

* * *

The immense growth and development of the Chinese economy, especially over the last decade, has been accompanied by a rising tide of industrial espionage and criminal hacking originating from the People’s Republic of China (PRC). The CIA Factbook section on China’s economy reports that since the shift away from a Soviet-style central-command economy, starting in 1978, the Chinese Gross Domestic Economy has quadrupled. “Measured on a purchasing power parity … basis, China in 2004 stood as the second-largest economy in the world after the US….” The real growth in Gross Domestic Product (GDP) is estimated at 9.1% in 2004, which accords with figures ranging from 8-12% in recent years (the US rate of increase of GDP was 4.4% in 2004).

In summary, China is already a world power and will soon be a superpower challenging the United States and Europe at all levels of geopolitical competition.

TIME Magazine recently (Aug 29, 2005) published an interesting report by Nathan Thornburgh about an investigation code-named TITAN RAIN that began in late 2003. As an information systems security officer (ISSO) for Sandia National Laboratories of the US Department of Energy, Shawn 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.”

So was Carpenter treated as a hero by Sandia managers?

Well, no. He was fired for inappropriate and unauthorized use of Department of Energy computer resources and information. I’m sorry for Carpenter, but I have already written many times in this venue and elsewhere that it is a really bad idea to use corporate resources without written permission from appropriate authorities, especially if there is any risk of being perceived as a law-breaker. Even if Carpenter had acquired written support from his US Army and FBI handlers, that still might not have protected him against termination of employment. I cannot
criticize Sandia managers on this count, and I understand that applying policy firmly is an important element of effective security management.

Nonetheless, I wonder if anyone reading about the case is in a position to help Carpenter? I would think he’d be an excellent candidate for a new job as ISSO or perhaps as a digital crimes investigator for a law enforcement agency. Let’s all wish him the best of luck and hope for a new job that uses his talents and dedication to US national security.

Incidentally, according to the TIME article, the government of the PRC denies any involvement in the hacker activity – but it also flatly refuses to cooperate with US law enforcement authorities investigating the case.

In my next column, I will look at a question raised as a result of this case about how to respond to attacks from a known source.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.