THE OMNIVORE BITES BACK

Okay, okay, I should have used a pun on "Echelon" for my title here, not "Carnivore." After all, it was that earlier SigInt program that the US and its Anglophone partners used to steal industrial secrets in the 1990s.

The point being that, while I am concerned by McAfee's description of the extent of the data theft carried out in the last six years using a hack it calls Shady RAT, I am also cognizant that the US has used equivalent tactics to steal intellectual property in the past and present.

> What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth — closely guarded national secrets (including from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, SCADA configurations, design schematics and much more has "fallen off the truck" of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries.
>
> What is happening to all this data — by

> now reaching petabytes as a whole — is still largely an open question. However, if even a fraction of it is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat not just to individual companies and industries but to entire countries that face the prospect of decreased economic growth in a suddenly more competitive landscape and the loss of jobs in industries that lose out to unscrupulous competitors in another part of the world, not to mention the national security impact of the loss of sensitive intelligence or defense information.

McAfee provides all the clues to make it clear China is behind these hacks—though it never says so explicitly.

> The interest in the information held at the Asian and Western national Olympic Committees, as well as the International Olympic Committee (IOC) and the World Anti-Doping Agency in the lead-up and immediate follow-up to the 2008 Olympics was particularly intriguing and potentially pointed a finger at a state actor behind the intrusions, because there is likely no commercial benefit to be earned from such hacks. The presence of political non-profits, such as the a private western organization focused on promotion of democracy around the globe or U.S. national security think tank is also quite illuminating. Hacking the United Nations or the ASEAN (Association of Southeast Asian Nations) Secretariat is also not likely a motivation of a group interested only in economic gains.

The report is perhaps most interesting because of some of the entities—along with the defense contractors and US and other government agencies—described as targets of this hack: a number of construction companies (which could include companies like KBR), real estate firms, various state and county governments, two think tanks, and the NY and Hong Kong offices of a US media company. These are where the secrets China wants to steal are kept.

The problem, of course, is that our intellectual property is one of the few advantages the US has left. Our exports are increasingly limited to things that rely on legally enforcing intellectual property to retain its value: drugs, movies and music, software, GMO ag. Which sort of makes China's ability to sit undetected in the servers of these kinds of organizations for up to 28 months a bit of a problem.

Good thing the FBI is busy going after hacktavists and whistleblowers instead.