Commercial cyber spying offers rich payoff

JOE McDONALD - AP Business Writer - Associated Press

For state-backed cyber spies such as a Chinese military unit implicated by a U.S. security firm in a computer crime wave, hacking foreign companies can produce high-value secrets ranging from details on oil fields to advanced manufacturing technology.

This week's report by Mandiant Inc. adds to mounting suspicion that Chinese military experts are helping state industry by stealing secrets from Western companies possibly worth hundreds of millions of dollars. The Chinese military has denied involvement in the attacks.

"This is really the new era of cybercrime," said Graham Cluley, a British security expert. "We've moved from kids in their bedroom and financially motivated crime to state-sponsored cybercrime, which is interested in stealing secrets and getting military or commercial advantage."

Instead of credit card numbers and other consumer data sought by crime gangs, security experts say cyber spies with skills and resources that suggest they work for governments aim at higher-value but better-guarded information.

A state-owned energy company in a bidding war for access to oil and gas fields abroad can save huge sums if it can find out what foreign rivals are willing to pay. Stealing formulas for chemical processing can save hundreds of millions of dollars in research costs. Suppliers can negotiate higher prices if they know their customers' internal discussions.

"There are a lot of hackers that are sponsored by the Chinese government who conduct cyber attacks," said Lim Jong-in, dean of Korea University's Graduate School of Information Security.

Mandiant said it found attacks on 141 entities, mostly in the United States but also in Canada, Britain and elsewhere. It said attackers stole information on pricing, contract negotiations, manufacturing, product testing and corporate acquisitions.

It said multiple details indicated the attackers, dubbed APT1 in its report, were from a military cyber warfare unit in Shanghai, though there was a small chance someone else might be responsible.

"We do believe that this stolen information can be used to obvious advantage" by China and Chinese state-owned enterprises, said Mandiant. Target companies were in four of the seven strategic industries identified in the Communist Party's latest five-year development plan, it said.

China's ruling party has ambitious plans to build up state-owned corporate

champions in industries from banking and telecoms to oil and steel. State companies are flush with cash from the country's boom and benefit from monopolies and other official favors but lag global rivals in skills and technology.

Last year, a group of Chinese state companies were among defendants charged in U.S. federal court in San Francisco in the theft of technology from DuPont Co. for manufacturing titanium dioxide, a chemical used in paints and other products.

In 2011, another security company, Symantec Inc., announced it detected attacks on 29 chemical companies and 19 other companies that it traced to China. It said the attackers wanted to steal secrets about chemical processing and advanced materials manufacturing.

China has long been cited by security experts as a center for a global explosion of Internet crime. They say some crimes might be carried out by attackers abroad who remotely control Chinese computers. But experts including Mandiant say there is growing evidence Chinese attackers are behind many of them.

China's military is a leader in cyber warfare research, along with its counterparts in the United States and Russia. The People's Liberation Army supports hacker hobby clubs with as many as 100,000 members to develop a pool of possible recruits, according to security consultants.

Few companies are willing to confirm they are victims of cyber spying, possibly for fear it might erode trust in their business.

"When companies admit their servers were hacked, they become the target of hackers. Because the admission shows the weakness, they cannot admit," said Kwon Seok-chul, president of Cuvepia Inc., a security firm in Seoul.

An exception was Google Inc., which announced in 2010 that it and at least 20 other companies were hit by attacks traced to China. Only two other companies disclosed they were targets in those attacks. Google cited the hacking and efforts to snoop on Chinese dissidents' email as among reasons for closing its mainland China-based search service that year.

Mandiant cited the example of an unidentified company with which it said a Chinese commodity supplier negotiated a double-digit price increase after attackers stole files and emails from the customer's chief executive over 2½ years beginning in 2008.

"It would be surprising if APT1 could continue perpetrating such a broad mandate of cyber espionage and data theft if the results of the group's efforts were not finding their way into the hands of entities able to capitalize on them," the report said.

___

AP Technology Writer Youkyung Lee in Seoul, South Korea contributed.

Source URL (retrieved on *10/20/2014 - 1:13am*):
http://www.ecnmag.com/news/2013/02/commercial-cyber-spying-offers-rich-payoff?qt-video_of_the_day=0