US hacking victims fell prey to mundane ruses

May 20 2014, by Jack Gillum

This May 19, 2014 file photo shows Attorney General Eric Holder taking questions during a news conference at the Justice Department in Washington where he announced that a U.S. grand jury has charged five Chinese hackers with economic espionage and trade secret theft. In a 31-count indictment, the Justice Department said five Chinese military officials operating under hacker aliases such as "Ugly Gorilla," "KandyGoo" and "Jack Sun" stole confidential business information, sensitive trade secrets and internal communications for competitive advantage. The U.S. identified the alleged victims as Alcoa World Alumina, Westinghouse, Allegheny Technologies, U.S. Steel, United Steelworkers Union and SolarWorld. China denied it all. (AP Photo/Charles Dharapak, File)

The hacking techniques the U.S. government says China used against American companies turned out to be disappointingly mundane, tricking employees into opening email attachments or clicking on innocent-looking website links.

The scariest part might be how successfully the ruses worked. With a mouse click or two, employees at big-name American makers of nuclear and solar technology gave away the keys to their computer networks.

In a 31-count indictment announced on Monday the Justice Department said five Chinese military officials operating under hacker aliases such as "Ugly Gorilla," "KandyGoo" and "Jack Sun" stole confidential business information, sensitive trade secrets and internal communications for competitive advantage. The U.S. identified the alleged victims as Alcoa World Alumina, Westinghouse, Allegheny Technologies, U.S. Steel, United Steelworkers Union and SolarWorld.

China denied it all on Tuesday.

"The Chinese government and Chinese military as well as relevant personnel have never engaged and never participated in so-called cybertheft of trade secrets," Foreign Ministry spokesman Hong Lei said in Beijing. "What the United States should do now is withdraw its indictment."

That's unlikely. What the Justice Department is doing is spelling out exactly how it says China pulled it off.

The U.S. says the break-ins were more slapstick than professional spy work. In some cases, the government says, the hackers used "spear-phishing"—a well-known scam to trick specific companies or employees into infecting their own computers.

The hackers are said to have created a fake email account under the misspelled name of a then-Alcoa director and fooled an employee into opening an email attachment called "agenda.zip," billed as the agenda to a 2008 shareholders' meeting. It exposed the company's network. At another time, a hacker allegedly emailed company employees with a link to what appeared to be a report about industry observations, but the link instead installed malicious software that created a back door into the company's network.

"We are so used to solving problems by clicking an email link, looking at the information and forwarding it on," said Chris Wysopal, a computer security expert and chief technology officer of the software-security firm Veracode. "And if hackers know about you and your company, they can create really realistic-looking messages."

And use of the rudimentary efforts the Justice Department described doesn't mean foreign governments and others won't use more sophisticated and harder-to-detect techniques, said Joshua Corman, the chief technology officer for Sonatype, which helps businesses make their software development secure. Determined hackers escalate their attacks when necessary, he said, but in the cases cited in the federal indictment announced Monday, they didn't have to escalate very far.

Corman noted that the U.S. has much higher investments in research and intellectual property, making America's risk of loss in such thefts disproportionately higher than China's.

Other security layers failed in the hackings blamed on China, too. More-effective antivirus or security software could have blocked the malicious attachments or prevented users from visiting risky web links. Back-end server filters could have prevented dangerous emails from reaching employees. Intrusion-detection systems on corporate networks could have more quickly raised red flags internally after a successful break-in.

"The problem is the technology hasn't advanced enough to detect malicious code," said Kevin Mitnick, the famous hacker who now works as a corporate security consultant. Tricking someone to let you into the system is far easier than identifying hidden vulnerabilities that can be exploited.

Even worse: Employees, by their nature, are socially conditioned to want to open and respond to an email that purports to be from the boss—never mind that the message may actually be a trick.

"If you start with an incorrect assumption that every email that comes in is a real email," said Hossein Eslambolchi, chief executive at security company CyberFlow Analytics, "you're putting yourself and your corporation at a major risk."

Citation: US hacking victims fell prey to mundane ruses (2014, May 20) retrieved 6 May 2024 from https://phys.org/news/2014-05-hacking-victims-fell-prey-mundane.html