JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, May 19, 2014

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.

“This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking,” U.S. Attorney General Eric Holder said. “The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global market place should be based solely on a company’s ability to innovate and compete, not on a sponsor government’s ability to spy and steal business secrets. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market.”

“For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries,” said FBI Director James B. Comey. “The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources.”

“State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country’s flag,” said John Carlin, Assistant Attorney General for National Security. “Cyber theft is real theft and we will hold state sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws.”

"This 21st century burglary has to stop," said David Hickton, U.S. Attorney for the Western District of Pennsylvania. "This prosecution vindicates hard working men and women in Western Pennsylvania and around the world who play by the rules and deserve a fair shot and a level playing field."

Summary of the Indictment

Defendants : Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA). The indictment alleges that Wang, Sun, and Wen, among others known and unknown to the grand jury, hacked or attempted to hack into U.S. entities named in the indictment, while Huang and Gu supported their conspiracy by, among other things, managing infrastructure (e.g., domain accounts) used for hacking.

Victims : Westinghouse Electric Co. (Westinghouse), U.S. subsidiaries of SolarWorld AG (SolarWorld), United States Steel Corp. (U.S. Steel), Allegheny Technologies Inc. (ATI), the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW) and Alcoa Inc.

Time period : 2006-2014.

Crimes : Thirty-one counts as follows (all defendants are charged in all counts).

Count(s)	Charge	Statute	Maximum Penalty
1	Conspiring to commit computer fraud and abuse	18 U.S.C. § 1030(b).	10 years.
2-9	Accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain.	18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2.	5 years (each count).
10-23	Transmitting a program, information, code, or command with the intent to cause damage to protected computers.	18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2.	10 years (each count).
24-29	Aggravated identity theft.	18 U.S.C. §§ 1028A(a)(1), (b), (c)(4), and 2	2 years (mandatory consecutive).

30	Economic espionage.	18 U.S.C. §§ 1831(a)(2), (a)(4), and 2.	15 years.
31	Trade secret theft.	18 U.S.C. §§ 1832(a)(2), (a)(4), and 2.	10 years.

Summary of Defendants' Conduct Alleged in the Indictment

Defendant	Victim	Criminal Conduct
Sun	Westinghouse	In 2010, while Westinghouse was building four AP1000 power plants in China and negotiating other terms of the construction with a Chinese SOE (SOE-1), including technology transfers, Sun stole confidential and proprietary technical and design specifications for pipes, pipe supports, and pipe routing within the AP1000 plant buildings. Additionally, in 2010 and 2011, while Westinghouse was exploring other business ventures with SOE-1, Sun stole sensitive, non-public, and deliberative e-mails belonging to senior decision-makers responsible for Westinghouse's business relationship with SOE-1.
Wen	SolarWorld	In 2012, at about the same time the Commerce Department found that Chinese solar product manufacturers had "dumped" products into U.S. markets at prices below fair value, Wen and at least one other, unidentified co-conspirator stole thousands of files including information about SolarWorld's cash flow, manufacturing metrics, production line information, costs, and privileged attorney-client communications relating to ongoing trade litigation, among other things. Such information would have enabled a Chinese competitor to target SolarWorld's business operations aggressively from a variety of angles.
Wang and Sun	U.S. Steel	In 2010, U.S. Steel was participating in trade cases with Chinese steel companies, including one particular state-owned enterprise (SOE-2). Shortly before the scheduled release of a preliminary determination in one such litigation, Sun sent spearphishing e-mails to U.S. Steel employees, some of whom were in a division associated with the litigation. Some of these e-mails resulted in the installation of malware on U.S. Steel computers. Three days later, Wang stole hostnames and descriptions of U.S. Steel computers (including those that controlled physical access to company facilities and mobile device access to company networks). Wang thereafter took steps to identify and exploit vulnerable servers on that list.

Wen	ATI	In 2012, ATI was engaged in a joint venture with SOE-2, competed with SOE-2, and was involved in a trade dispute with SOE-2. In April of that year, Wen gained access to ATI's network and stole network credentials for virtually every ATI employee.
Wen	USW	In 2012, USW was involved in public disputes over Chinese trade practices in at least two industries. At or about the time USW issued public statements regarding those trade disputes and related legislative proposals, Wen stole e-mails from senior USW employees containing sensitive, non-public, and deliberative information about USW strategies, including strategies related to pending trade disputes. USW's computers continued to beacon to the conspiracy's infrastructure until at least early 2013.
Sun	Alcoa	About three weeks after Alcoa announced a partnership with a Chinese state-owned enterprise (SOE-3) in February 2008, Sun sent a spearphishing e-mail to Alcoa. Thereafter, in or about June 2008, unidentified individuals stole thousands of e-mail messages and attachments from Alcoa's computers, including internal discussions concerning that transaction.
Huang		Huang facilitated hacking activities by registering and managing domain accounts that his co-conspirators used to hack into U.S. entities. Additionally, between 2006 and at least 2009, Unit 61398 assigned Huang to perform programming work for SOE-2, including the creation of a "secret" database designed to hold corporate "intelligence" about the iron and steel industries, including information about American companies.
Gu		Gu managed domain accounts used to facilitate hacking activities against American entities and also tested spearphishing e-mails in furtherance of the conspiracy.

An indictment is merely an accusation and a defendant is presumed innocent unless proven guilty in a court of law.

The FBI conducted the investigation that led to the charges in the indictment. This case is being prosecuted by the U.S. Department of Justice's National Security Division Counterespionage Section and the U.S. Attorney's Office for the Western District of Pennsylvania.

Related Materials:

Indictment