FBI CYBER DIVISION

Private Industry Notification

19 May 2014

PIN #: 140519 – 002

(U) The United States Indicts Five Chinese Cyber Actors for Cyber Espionage

(U) Summary:

(U) On 19 May 2014, the Western District of Pennsylvania unsealed an indictment of five members of the People's Liberation Army of the People's Republic of China on multiple criminal charges for their cyber criminal activities targeting six US companies while those companies were engaged in negotiations or joint ventures with or were pursuing legal action against state-owned enterprises in China.

(U) United States of America V. Wang Dong, Sun Kailang, Wen Xinyu, Huang Zhenyu and Gu Chunhui

(U) Today, the Western District of Pennsylvania unsealed an indictment of five members of the People's Liberation Army of the People's Republic of China on 31 counts—including conspiring to commit computer fraud (18 U.S.C. §§ 371, 1030), accessing a computer without authorization for the purpose of commercial advantage and private financial gain (18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)), damaging computers through the transmission of code and commands (18 U.S.C. § 1030(a)(5)), aggravated identity theft (18 U.S.C. § 1028A), economic espionage (18 U.S.C. § 1831(a)(1)), and theft of trade secrets (18 U.S.C. § 1832(a)(1)). Each of the defendants provided his individual expertise to a conspiracy to penetrate the computer networks of six US companies while those companies were engaged in negotiations or joint ventures with or were pursuing legal action against state-owned enterprises in China.

(U) The defendants used a variety of techniques including malicious e-mails tailored to appear to be from individuals familiar to the targets—such as the board of directors of the targeted company—and with target relevant subject lines such as "U.S. Steel Industry Outlook". After having lured an unwitting recipient into executing malicious software, they installed backdoors to penetrate the targeted companies' network security and proceeded to acquire additional accesses and permissions, in some cases stealing thousands of passwords belonging to users of the corporate network. They then used their illegal access to exfiltrate proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs.

(U) The victims showed great commitment to supporting the FBI and DOJ in the interests of pursuing justice. Each of these companies was targeted by the government of China as part of a systematic effort to unfairly overcome the advantages that have been achieved by US manufacturers through investments in innovation and the experience of competing fairly in global markets. Protecting such companies from illegal exploitation by other governments is critical for the economic security of the United States in the global economy of the future.

- Westinghouse Electric Company was engaged in negotiations with a Chinese state-owned enterprise regarding cooperation on the construction of four nuclear power plants in China using Westinghouse's proprietary AP1000 reactor design. A defendant stole trade secrets regarding technical specifications and sensitive e-mails from senior decision-making personnel.

- The U.S. subsidiary of German company SolarWorld AG was an active litigant in trade cases against Chinese solar manufacturers. While that litigation was ongoing, a defendant stole thousands of e-mails that included detailed information about the company's financial position, production capabilities, cost structure, and business strategy.

- The United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW) was engaged in public action opposing Chinese trade practices affecting the industrial raw materials and auto parts industries. The day after the World Trade Organization published a report supporting the USW, a defendant stole sensitive e-mails about USW's strategy from the prior week from six senior USW employees.

- United States Steel Corporation was active in trade litigation against Chinese steel manufacturers, including a Chinese state-owned enterprise, alleging unfair trade practices. The litigation eventually resulted in the imposition of trade sanctions duties worth millions of dollars on the importation of specific Chinese products. A defendant gained illegal access to the U.S. Steel networks and stole network credentials that could enable a variety of further attacks.

- Allegheny Technologies Incorporated (ATI) participated in a trade dispute against a Chinese state-owned enterprise which was ultimately resolved in ATI's favor. During that dispute, a defendant stole the network credentials for more than 7,500 ATI employees; these credentials could have enabled a variety of further attacks.

- Alcoa Incorporated was engaged in a partnership with a Chinese state-owned enterprise when a defendant sent several e-mail messages with malicious attachments to several

senior Alcoa employees. Unidentified individuals subsequently stole e-mail messages from Alcoa senior managers that included internal discussions of the partnership.

(U) The defendants Wen Xinyu, Sun Kailiang, Gu Chunhui, Huang Zhenyu, and Wang Dong were officers of the Peoples Republic of China, Third Department of the General Staff Department of the Peoples Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398 at some point during the investigation. The activities executed by each defendant in the conspiracy varied according to their specialties. Sun, who held the rank of captain during the early stages of the investigation, was observed both sending malicious e-mails and controlling victim computers. Wen and Wang actually controlled victim computers. Huang was a computer programmer who also, along with Gu, managed the domain accounts used by the others. Gu also tested malicious e-mail messages. Specific intrusions would involve the expertise of different co-conspirators.

(U) This indictment represents the culmination of several years' effort and could not have been accomplished without the tenacity and courage of the victims to speak out and cooperate with law enforcement. The task force continues to identify additional prosecutorial opportunities in this space and looks forward to sharing similar successes in the future. The DOJ and FBI intend to continue using all legal tools at their disposal to counter cyber espionage from all sources.

(U) To report relevant criminal activity or for network security issues contact your local FBI field office. Media or general inquiries should be directed to the FBI Office of Public Affairs, 202-278-3519.

(U) Information contained in this product is UNCLASSIFIED. Additional information may be found in FBI FLASH A-000030-TT and the Department of Justice's Press Release.

(U) For comments or questions related to the content or dissemination of this document, please reference CYD-CC-1621