POLICY —

Security firm was front for advanced Chinese hacking operation, Feds say

The accused hacked 3 multinational corporations in pursuit of intellectual property.

DAN GOODIN - 11/27/2017, 1:19 PM

Renato Ganoza

43

Three men who worked for an Internet security firm in China have been indicted on federal charges for hacking into at least

three multinational corporations. The malware they used has been tied to the Chinese government.

Wu Yingzhuo, Dong Hao, and Xia Lei face federal charges that they conspired to steal hundreds of gigabytes of data belonging to Siemens AG, Moody's Analytics, and the GPS technology company Trimble. The indictment, which was filed in September and unsealed on Monday, said the trio used spear phishing e-mails with malicious attachments or links to infect targeted end users. The defendants used customized tools collectively known as the UPS Backdoor Malware to gain and maintain unauthorized access to the targeted companies' networks.

Wu and Dong are founding members and equity shareholders of Guangzhou Bo Yu Information Technology Company. Xia is an employee of the company.

The alleged hackers used their access to carry out a series of brazen data thefts. Some time no later than 2011, a co-conspirator placed a forwarding rule on a Moody's e-mail server that caused all messages sent to an influential company economist to be forwarded to a dummy

account created by the attackers. The economist regularly appeared in news stories aired on national TV and published in large-circulation newspapers.

In 2014, the men helped break into Siemens' network, where they helped steal employee user names and passwords and 407GB of data relating to the company's energy, technology, and transportation businesses. In 2015 and 2016, the men accessed Trimble's network and stole commercial business documents and data related to global navigation satellite systems technology Trimble spent millions of dollars developing.

The indictment doesn't overtly say the defendants worked on behalf of the Chinese government. The reference to the UPS Backdoor Malware, however, links the operation to APT 3, a so-called "advanced persistent threat group" that has used highly customized e-mail to infect targets with advanced malware since at least 2010. In May, an anonymous group calling itself Intrusion Truth published a report claiming that Guangzhou Bo Yu Information Technology, or Boyusec, was really a front for APT 3. A few days later, security firm

Recorded Future reported that APT 3—which is also known as Gothic Panda, Buckeye, UPS Team, and TG-0110—worked directly for China's Ministry of State Security. The methods described in the indictment closely match those described in reports Symantec, FireEye, and other security firms have issued on APT 3.

FURTHER READING

Obama will greet Chinese president with handshake, not cyber sanctions

The indictment comes two years after then-President Barack Obama reached an agreement with his Chinese counterpart Xi Jinping over state-sponsored espionage hacking that had targeted US intellectual property for years. Analysts have said China's compliance with the terms of the 2015 agreement have been uneven. As evidence, they cite several incidents in which Chinese cyber threat actors have allegedly targeted US defense contractors in pursuit of military technology.

"The incidents described in the court documents indicate a breach of the 2015 Obama-Xi agreement not to engage in 'cyber-enabled theft of

intellectual property,'" Elsa B. Kania, an adjunct fellow at the Center for a New American Security, told Ars. "This indictment could reflect an intensification of US pressure for China to come back into compliance with the agreement, after initial warnings seem to have gone unheeded."

Promoted Comments

iceph03nix / Ars Centurion **JUMP TO POST**

> adamrussell wrote:
> Maybe I glazed over at some point, but I did not see any mention of arrests. Are we hoping for China to hand them over?

I have a feeling the intent is to limit their options in the international community. I don't think we expect China to hand them over, but if they go to any US friendly countries under their own passports, they're likely to be flagged as wanted for espionage. It likely also opens the way for sanctions against their

company and their personal finances that have ties to the US.

356 posts | registered 8/19/2010

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 43 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS