SSBG IT Solutions
Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

Chinese 'Security' Company Was a Den of Hackers, Feds Say

Boyusec is accused of siphoning secrets from targets including Siemens and is connected the notorious group called APT3, which has been linked to Beijing's spy services.

An obscure Chinese computer security firm acted as a front for a sophisticated hacking operation dedicated to siphoning secrets from targets around the world, according to federal prosecutors who've charged two officers and an employee of the firm for hacks against Siemens AG, Moody's Analytics and the GPS technology company Trimble.

The Chinese firm, called "Boyusec," stole "hundreds of gigabytes of data, including confidential business and commercial information, work product, and sensitive victim employee information, such as usernames and password," according to an eight-count indictment unsealed Monday in federal court in Pittsburgh.

Three Chinese citizens are charged in the indictment: Wu Yingzhuo and Dong Hao were officers of the security company, formerly known as the Guangzhou Bo Yu Information Technology Co. Xia Lei, also charged, was an employee of the firm, which was based in the city of Guangzhou northwest of Hong Kong.

Though the indictment doesn't allege the defendants were acting on behalf of the Chinese government, it connects Boyusec to a notorious hacking group variously called APT3, Gothic Panda, Pirpi and UPS, which security researchers have previously linked to China's Ministry of State Security. Considered one of the most sophisticated intrusion groups, APT3 has been active since at least 2010, and is known for using targeted phishing attacks and browser exploits against victims in the United States, Hong Kong, and elsewhere. Some attacks have wielded rare "zero-day" exploits that were unknown to the computer security world until they were seen being used by the hackers.

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

Prosecutors charge that in one of the Boyusec attacks in 2011, the hackers penetrated a mail server at Moody's Analytics and inserted a rule that covertly forwarded email for a Moody's analyst to an outside email address set up by the hackers. Xia is accused of accessing and retrieving the stolen emails as late as 2014, giving Boyusec access to Moody's "proprietary and confidential economic analyses" for years.

In May and June 2014 the gang allegedly breached Siemens AG and stole encrypted passwords. Then from June to August 2015 they allegedly siphoned 407 gigabytes of material from Siemens' technology, energy, and transportation businesses.

The indictment confirms public reports from earlier this year. Boyusec was first identified as the mysterious APT3 hacking group last May in a series of blog posts by anonymous security researchers calling themselves Intrusion Truth, who laid out a tangled chain of online evidence supporting their conclusions. The Massachusetts security company Recorded Future added more evidence that also connected Boyusec to the Chinese government.

China is notorious for its cyber espionage operations, which go beyond traditional intelligence gathering against government targets and into the realm of corporate trade secret theft and economic espionage. In 2014, the same Pittsburgh FBI office behind the new charges indicted five Chinese military officers for hacks against U.S. companies. High level diplomatic negotiations between China and the U.S. resulted in China backing off its economic espionage for a time. The new indictment, though, suggests that at least some of the intrusions have merely been outsourced to contractors. Boyusec's alleged hacks continued until at least May of this year.

Read the Chinese version at:
http://www.sohu.com/a/207089978_354899

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

Extract QR Zone to follow us
Read More to Our LinkedIn

http://qbview.url.cn/getResourceInfo?appid=62&url=https%3A%2F%2Fwww.thedailybeast.com%2Fchinese-security-company-was-a-den-of-hackers-feds-say%3Fnsukey%3Dyq63VtlT3EWYHAwIIsfT%252B%252FkOS%252FAvI4dPAyAIYtVv%252BS4tSGbrB6ZMgPmgmf65q2MvLELYcGEBrpfzKwoyZ8X5fvLI3H2Bct8YzrcTYl%252BmAyaTyRerPPnmn7gbHdZ8jnykguHIoll2wkJ%252FsUbGblwxQSbK07RnXmQdN6axOFkAvA%252Fu9kXtOdan7vVP3YYbw7srrr6Q2yTy9q2f8L1eLb9cFg%253D%253D&openid=ooa-VuAn4z7nV9kylZnSy_g4_jvs&version=10000&doview=1