

APT3 is Boyusec, a Chinese Intelligence Contractor

By intrusiontruth

Published: 2017-05-09 · Archived: 2026-04-05 16:17:02 UTC

In our last three posts we introduced you to APT3 and identified two individuals responsible for purchasing their domain names – Wu Yingzhuo and Dong Hao. An IP addresses in Guangdong, China was associated with some of the domains.

Both individuals have a long history of purchasing APT3 infrastructure. Who do they work for and where do their orders come from?

Boyusec

Well, the answers to those questions are reasonably easy to find. Wu Yingzhuo (吴颖卓) and Dong Hao (董浩) are both shareholders in the same company.

[This listing](#) is for a [Chinese cyber security firm called 博御信息](#) (or Boyusec – the Guangzhou Boyu Information Technology Company, Ltd) that was licensed in December 2013 and is based in Guangdong. It lists both 吴颖卓 and 董浩 as major shareholders.

The screenshot shows a company listing for 广州博御信息技术有限公司 (Guangzhou Boyusec Information Technology Co., Ltd.). The page includes a header with navigation links, a search bar, and a main content area with a company profile, a list of shareholders, and a QR code for the mobile app.

工商基本信息

统一社会信用代码:		注册号:	440106000859775
组织机构代码:			
企业类型:	有限责任公司(自然人投资或控股)	经营状态:	存续
法定代表人:	董浩	成立日期:	2013-12-02
注册资本:	50.000000万元人民币	营业期限:	2013-12-02 —
发照日期:	2013-12-02	网 址:	
登记机关:	广州市工商行政管理局天河分局		
企业地址:	广州市天河区华明路9号1103房(本住所限办公用途)		
经营范围:	信息技术咨询服务;信息系统集成服务;五金零售;五金产品批发;电子、普通与自动控制技术研究、开发;软件服务;电子元器件批发;软件开发;网络技术的研究、开发;会议及展览服务;计算机、软件及辅助设备零售;计算机技术开发、技术服务;数据处理和存储服务;		

股东信息

股东信息	股东	认缴出资(金额/时间)	实缴出资(金额/时间)
孙进	自然人		8.000000万元
张德强	自然人		8.000000万元
吴颖卓	自然人		8.500000万元
董浩	自然人		25.500000万元

Company listing showing 吴颖卓 and 董浩 as shareholders of Boyusec

The Ministry of State Security

On the 29th of November 2016, freebeacon.com reported that Pentagon intelligence officials had [identified Boyusec as being a contractor for the Chinese Ministry of State Security](#) (MSS). The MSS is one of China's Intelligence Services and is an active player in their Cyber programme.

Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service

Joint Staff warns of cyber espionage dangers

SHARE TWEET EMAIL

BY: Bill Gertz [Follow @BillGertz](#)

November 29, 2016 5:00 am



Chinese soldiers browse online news on desktop computers / AP

TWITTER G+ IN JUBO PINTEREST

A Chinese cyber security firm is covertly working with Beijing's Ministry of State Security intelligence service in conducting cyber espionage operations, according to Pentagon intelligence officials.

The company known as Boyusec, officially the Bo Yu Guangzhou Information Technology Co., is also working with China's global telecommunications company Huawei Technologies, which has been identified by

U.S. intelligence agencies as linked to the Chinese military.

According to an internal report by the Pentagon's Joint Staff J-2 intelligence directorate, Boyusec and Huawei are working together to produce security products that will be loaded into Chinese-manufactured computer and telephone equipment. The doctored products will allow Chinese intelligence to capture data and control computer and telecommunications equipment, said Pentagon officials familiar with the report.

"It's closely connected to the [Ministry of State Security] and Huawei and they are developing a start-up program that will use malware allowing for capturing and controlling devices," said one official of Boyusec.

Today's STORIES



The conclusion?

Either a Chinese InfoSec company called Boyusec, known to be involved with Chinese Intelligence Cyber operations, has two shareholders with the same names as two apparant APT3 actors, or **Boyusec is APT3**.

Discover more from Intrusion Truth

Subscribe to get the latest posts sent to your email.

Post navigation

Source: <https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/>