★ Blog

Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3

Posted: **17th May 2017** By: **INSIKT GROUP**

Insikt Group

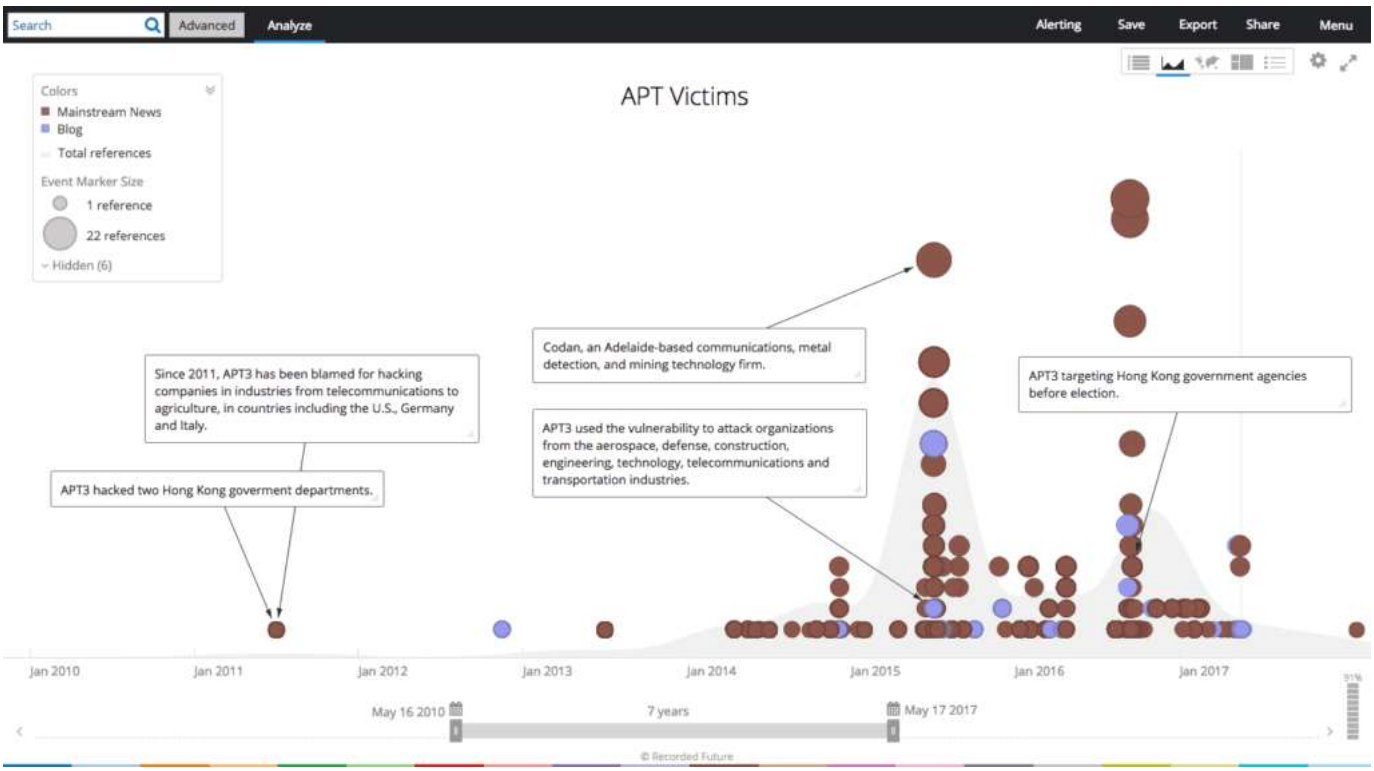
This is the first time researchers have been able to attribute a threat actor group with a high degree of confidence to the Ministry of State Security.

Key Takeaways

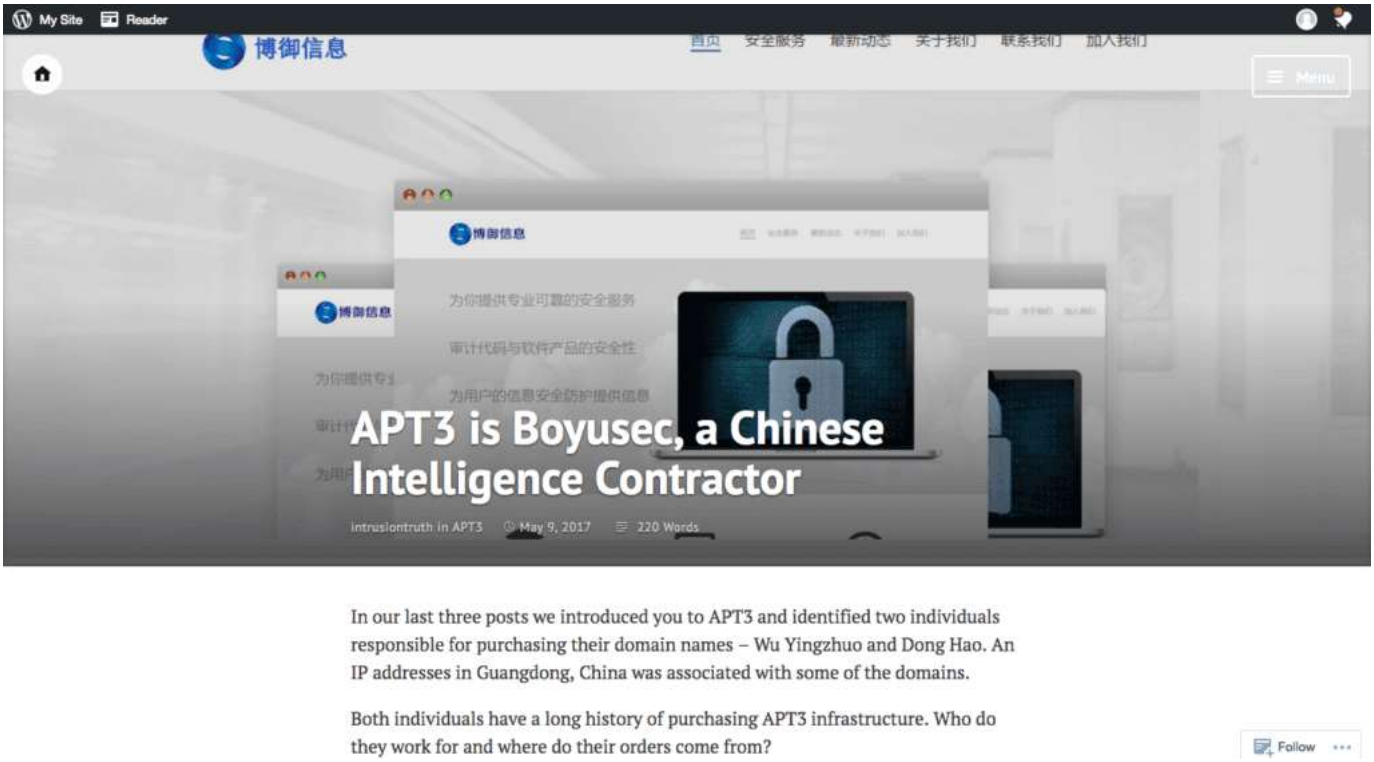
- APT3 is the first threat actor group that has been attributed with a high degree of confidence directly to the Chinese Ministry of State Security (MSS).
- On May 9, a mysterious group called "intrusiontruth" attributed APT3 to a company, Guangzhou Boyu Information Technology Company, based in Guangzhou, China.
- Recorded Future's open source research and analysis has corroborated the company, also known as Boyusec, is working on behalf of the Chinese Ministry of State Security.
- Customers should re-examine any intrusion activity known or suspected to be APT3 and all activity from associated malware families as well as re-evaluate security controls and policies.

Introduction

On May 9, a mysterious group calling itself "intrusiontruth" identified a contractor for the Chinese Ministry of State Security (MSS) as the group behind the APT3 cyber intrusions.

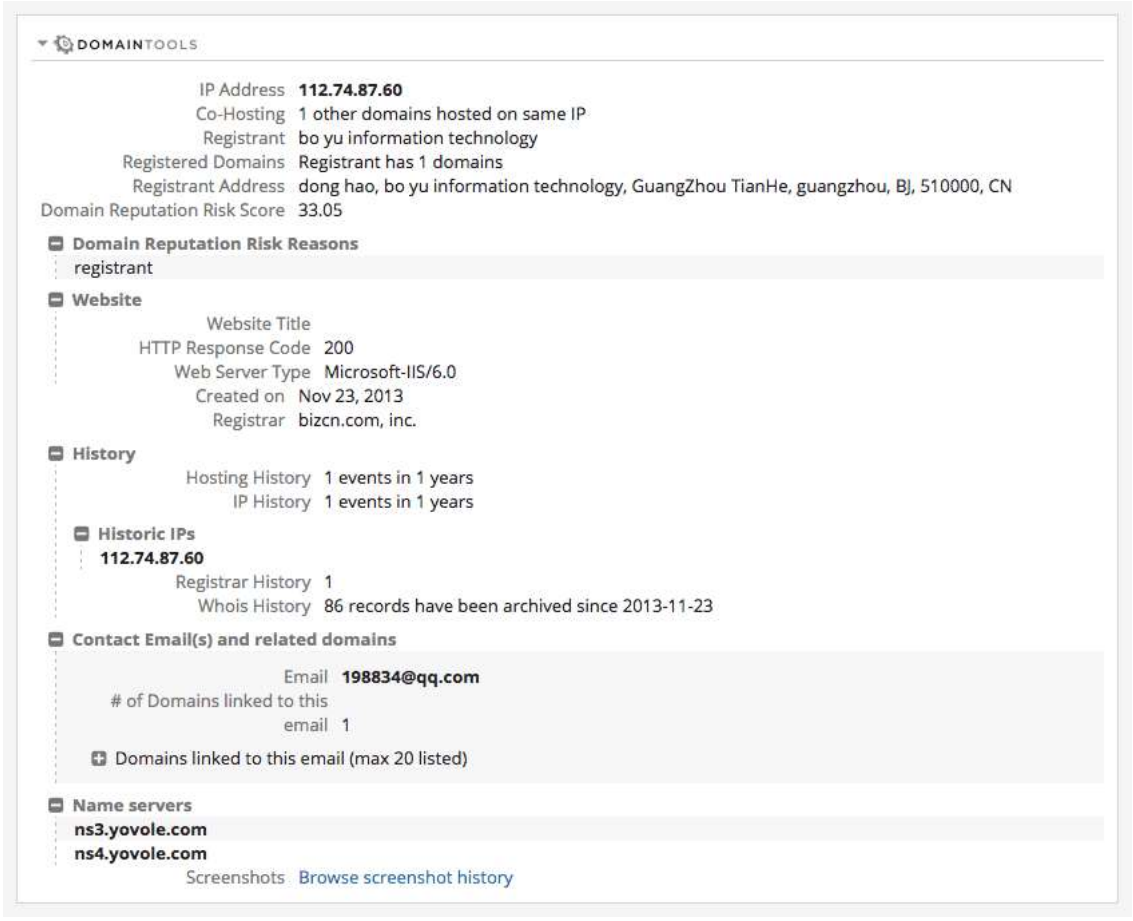


Recorded Future timeline of APT3 victims.



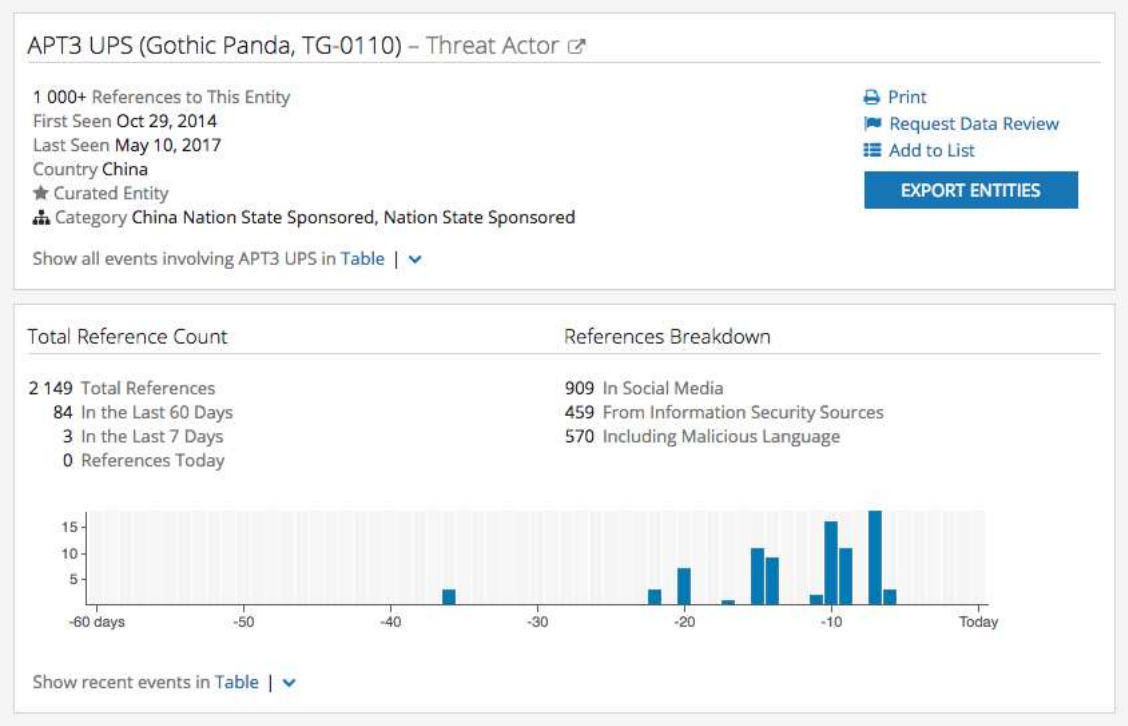
Screenshot of a blog post from "intrusiontruth in APT3."

"Intrusiontruth" documented historic connections between domains used by an APT3 tool called Pirpi and two shareholders in a Chinese information security company named Guangzhou Boyu Information Technology Company, Ltd (also known as Boyusec).



Registration information for a domain linked to the malware Pirpi. The details show the domain was registered to Dong Hao and Boyusec.

APT3 has traditionally targeted a wide-range of companies and technologies, likely to fulfill intelligence collection requirements on behalf of the MSS (see research below). Recorded Future has been closely following APT3 and has discovered additional information corroborating that the MSS is responsible for the intrusion activity conducted by the group.



Recorded Future Intelligence Card™ for APT3.

Background

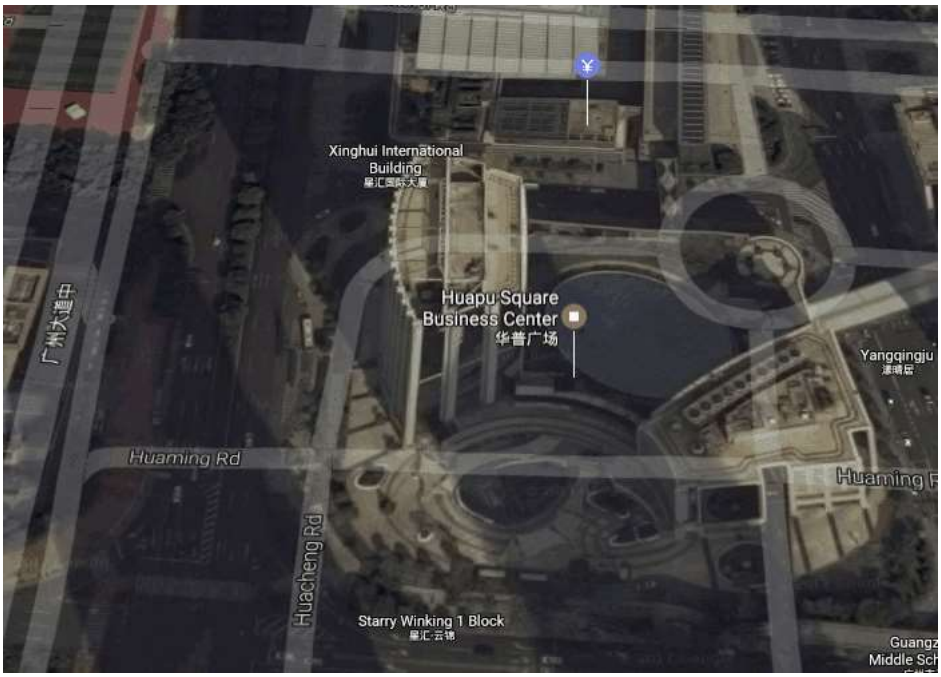
APT3 (also known as UPS, Gothic Panda, and TG-011) is a sophisticated threat group that has been active since at least 2010. APT3 utilizes a broad range of tools and techniques including spearphishing attacks, zero-day exploits, and numerous unique and publicly available remote access tools (RAT). Victims of APT3 intrusions include companies in the defense, telecommunications, transportation, and advanced technology sectors — as well as government departments and bureaus in Hong Kong, the U.S., and several other countries.

Analysis

On Boyusec's website, the company explicitly identifies two organizations that it cooperatively partners with, Huawei Technologies and the Guangdong Information Technology Security Evaluation Center (or Guangdong ITSEC).

Screenshot of Boyusec's website where Huawei and Guangdong ITSEC are identified as collaborative partners.

In November 2016, the *Washington Free Beacon* reported that a Pentagon internal intelligence report had exposed a product that Boyusec and Huawei were jointly producing. According to the Pentagon's report, the two companies were working together to produce security products, likely containing a backdoor, that would allow Chinese intelligence "to capture data and control computer and telecommunications equipment." The article quotes government officials and analysts stating that Boyusec and the MSS are "closely connected," and that Boyusec appears to be a cover company for the MSS.



Imagery ©2017 DigitalGlobe, Map data ©2017

Boyusec is located in Room 1103 of the Huapu Square West Tower in Guangzhou, China.

Boyusec's work with its other "cooperative partner," Guangdong ITSEC, has been less well-documented. As will be laid out below, Recorded Future's research has concluded that Guangdong ITSEC is subordinate to an MSS-run organization called China Information Technology Evaluation Center (CNITSEC) and that Boyusec has been working with Guangdong ITSEC on a joint active defense lab since 2014.

Guangdong ITSEC is one in a nation-wide network of security evaluation centers certified and administered by CNITSEC. According to Chinese state-run media, Guangdong ITSEC became the sixteenth nationwide branch of CNITSEC in May 2011. Guangdong ITSEC's site also lists itself as CNITSEC's Guangdong Office on its header.

According to academic research published in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, CNITSEC is run by the MSS and houses much of the intelligence service's technical cyber expertise. CNITSEC is used by the MSS to "conduct vulnerability testing and software reliability assessments." Per a 2009 U.S. State Department cable, it is believed China may also use vulnerabilities derived from CNITSEC's activities in intelligence operations. CNITSEC's Director, Wu Shizhong, even self-identifies as MSS, including for his work as a deputy head of China's National Information Security Standards Committee as recently as January 2016.

Recorded Future research identified several job advertisements on Chinese-language job sites such as jobs.zhaopin.com, jobui.com, and kanzhun.com since 2015, Boyusec revealed a collaboratively established joint active defense lab (referred to as an ADUL) with Guangdong ITSEC in 2014. Boyusec stated that the mission of the joint lab was to develop risk-based security technology and to provide users with innovative network defense capabilities.


web渗透测试工程师
广州博御信息技术有限公司

3) 法定休假年假;
4) 年底双薪

公司简介
广州博御是信息技术有限公司是一家从事信息安全领域服务、咨询、评估与测评相关工作的综合服务商。团队技术实力雄厚，面向国内大中型企事业单位提供信息安全一体化解决方案。2014年，广州博御信息技术有限公司与广东省信息安全测评中心紧密合作，成立主动防御联合实验室（ADUL）。实验室研究发展基于风险的的安全技术。为用户提供创新的网络防御能力。

我们是安全业内的精英团队，聚集了一批优秀的人一起战斗!
我们是刚成立起来的公司，虽然人数不多，但都是业界里的佼佼者!
你不需要具有很牛逼的技术,但只要你有扎实的基础,满怀的激情,以及远大的理想，你就是我们要找的人才!

工作地点：广州天河区华普广场西塔华明路9号

Job posting where Boyusec highlights the joint lab with Guangdong ITSEC. The translated text is, "In 2014, Guangzhou Boyu Information Technology Company and Guangdong ITSEC cooperated closely to establish a joint active defense lab (ADUL)."

Conclusion

The lifecycle of APT3 is emblematic of how the MSS conducts operations in both the human and cyber domains. According to scholars of Chinese intelligence, the MSS is composed of national, provincial, and local elements. Many of these elements, especially at the provincial and local levels, include organizations with valid public missions to act as a cover for MSS intelligence operations. Some of these organizations include think tanks such as CICIR, while others include provincial-level governments and local offices.

In the case of APT3 and Boyusec, this MSS operational concept serves as a model for understanding the cyber activity and lifecycle:

- While Boyusec has a website, an online presence, and a stated "information security services" mission, it cites only two partners, Huawei and Guangdong ITSEC.
- Intrusiontruth and the *Washington Free Beacon* have linked Boyusec to supporting and engaging in cyber activity on behalf of the Chinese intelligence services.
- Recorded Future's open source research has revealed that Boyusec's other partner is a field office for a branch of the MSS. Boyusec and Guangdong ITSEC have been documented working collaboratively together since at least 2014.
- Academic research spanning decades documents an MSS operational model that utilizes organizations, seemingly without an intelligence mission, at all levels of the state to serve as cover for MSS intelligence operations.
- According to its website, Boyusec has only two collaborative partners, one of which (Huawei) it is working with to support Chinese intelligence services, the other, Guangdong ITSEC, which is actually a field site for a branch of the MSS.

Graphic displaying the relationship between the MSS and APT3.

Impact

The implications are clear and expansive. Recorded Future's research leads us to attribute APT3 to the Chinese Ministry of State Security and Boyusec with a high degree of confidence. Boyusec has a documented history of producing malicious technology and working with the Chinese intelligence services.

APT3 is the first threat actor group that has been attributed with a high degree of confidence directly to the MSS. Companies in sectors that have been victimized by APT3 now must adjust their strategies to defend against the resources and technology of the Chinese government. In this real-life David versus Goliath situation, customers need both smart security controls and policy, as well as actionable and strategic threat intelligence.

APT3 is not just another cyber threat group engaging in malicious cyber activity; research indicates that Boyusec is an asset of the MSS and their activities support China's political, economic, diplomatic, and military goals.

The MSS derives intelligence collection requirements from state and party leadership, many of which are defined broadly every five years in official government directives called Five Year Plans. Many APT3 victims have fallen into sectors

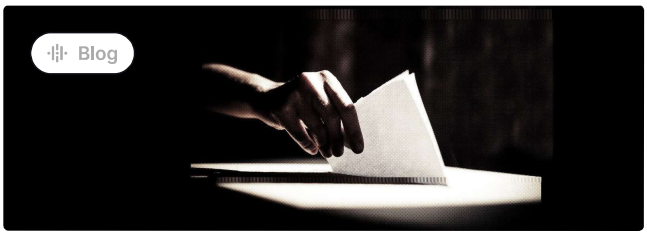
highlighted by the most recent Five Year Plan, including green/alternative energy, defense-related science and technology, biomedical, and aerospace.

Related Blog

Monitoring the Dark Web with Threat Intelligence

Explore effective dark web monitoring to safeguard your data. Learn how to detect and respond to cyber threats from the

View Blog



Navigating Election Risks: A Guide for Executives

Are you prepared to respond to election season risks posed to

View Blog

Contact us **today**