

The destruction of APT3

intrusiontruth.wordpress.com/2018/05/22/the-destruction-of-apt3/

intrusiontruth

May 22, 2018

Twelve months have passed since this blog exposed Wu Yingzhuo, Dong Hao, their company 'Boyusec' and the Chinese Ministry of State Security (MSS) as being behind APT3. APT3 was, at the time, one of the most damaging APT attacks to hit Western companies. One year on, we take a look back at what happened after our publication.

The disappearance of APT3

We published our [explosive analysis](#) in April and May 2017. It was the first time that the Chinese Intelligence Services had been conclusively linked to an APT and followed [similar revelations](#), years previously, linking People's Liberation Army (PLA) Unit 61398 to APT1.

The Boyusec website went offline the morning after the exposure and it hasn't been back online since.



This site can't be reached

boyusec.com's server DNS address could not be found.

ERR_NAME_NOT_RESOLVED

The morning after, on boyusec.com

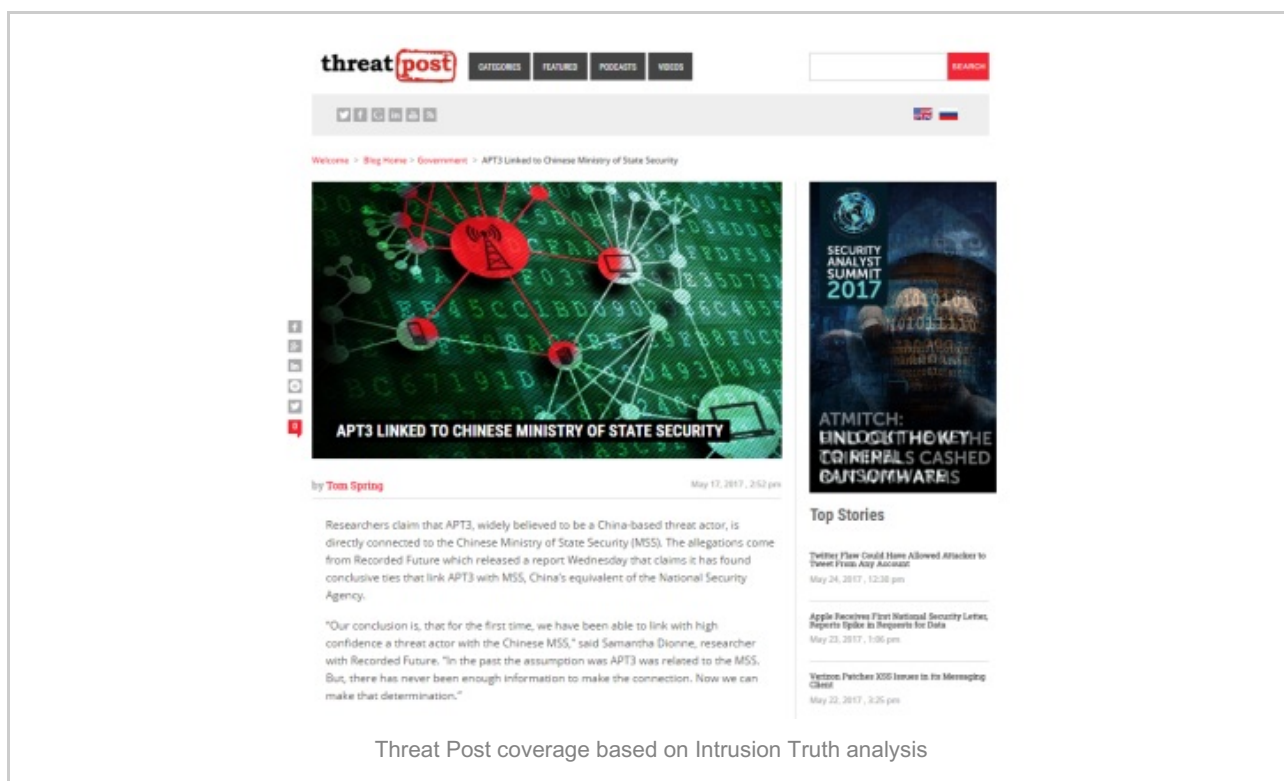
Boyusec disappeared into the shadows without making any effort to contact us or to refute any of the conclusions of our analysis. These were not the actions of innocent individuals.

Where did these guys run off to? Perhaps not proud of their work as APT3? [#buckeye](#)
[#gothicpanda](#) [#apt3](#) [#boyusec](#) [#cyber](#) pic.twitter.com/0IIzSIzxd

— Intrusion Truth (@intrusion_truth) [May 10, 2017](#)

Corroboration by the community

A fortnight after our publication, a series of articles appeared online drawing on our work and corroborating it. Our analysis formed the basis of articles by, among others, [Security Week](#), [Dark Reading](#), [Recorded Future](#), [Threat Post](#) and [Security Lab](#). The Information Security community agreed with our conclusion that Boyusec and MSS were behind the APT3 attacks. “There has been a lot of accumulated evidence that these guys are tied to the state” John Hultquist, Director of Analysis at FireEye, said to [Foreign Policy](#) magazine.



The image shows a screenshot of a Threat Post article. The article title is "APT3 LINKED TO CHINESE MINISTRY OF STATE SECURITY" by Tom Spring, dated May 11, 2017. The article text states: "Researchers claim that APT3, widely believed to be a China-based threat actor, is directly connected to the Chinese Ministry of State Security (MSS). The allegations come from Recorded Future which released a report Wednesday that claims it has found conclusive ties that link APT3 with MSS, China's equivalent of the National Security Agency. 'Our conclusion is, that for the first time, we have been able to link with high confidence a threat actor with the Chinese MSS,' said Samantha Dionne, researcher with Recorded Future. 'In the past the assumption was APT3 was related to the MSS. But, there has never been enough information to make the connection. Now we can make that determination.'" The screenshot also shows a "Top Stories" section with three items: "Twitter Plans Could Have Allowed Attacker to Tweet From Any Account" (May 24, 2017, 12:38 pm), "Apple Receives First National Security Letter, Requests Spike in Requests for Data" (May 23, 2017, 1:00 pm), and "Verizon's Pwn2016 XSS Issues to its Messaging Client" (May 22, 2017, 3:26 pm).

Threat Post coverage based on Intrusion Truth analysis

US Government charges Wu and Dong

But the story doesn't quite end there. Six months after our publications the US Justice Department unsealed indictments against Wu Yingzhuo, Dong Hao and Xia Lei for computer hacking, theft of trade secrets, conspiracy and identity theft. They had been prepared in September 2017.

Three US victims were identified in the indictment – Trimble, Siemens and Moody's Analytics – one for each of the 'co-conspirators'.

FILED

SEP 13 2017

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

WU YINGZHUO

a/k/a "mxmtmw"

a/k/a "Christ Wu"

a/k/a "wyz"

DONG HAO

a/k/a "Bu Yi"

a/k/a "Dong Shi Ye"

a/k/a "Tianyu,"

XIA LEI

a/k/a "Sui Feng Yan Mie"

Criminal No. 17-247

18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(A),
1030(b)

18 U.S.C. § 1832(a)(1), 1832(a)(2),
1832(a)(5)

18 U.S.C. § 1343

18 U.S.C. § 1028A

UNDER SEAL

INDICTMENT

The grand jury charges:

1. At all times relevant to the indictment:

BOYUSEC

a. The defendants were owners, employees and associates of the Guangzhou

The indictment document released by the US Government

Though the indictments didn't mention the Chinese Government, Justice Department spokesman Wyn Hornbuckle said that prosecutors only *"included the allegations that we are prepared to prove in court with admissible evidence"*.

Wu, Dong and Xia are no longer able to travel internationally without fear of arrest and trial. The maximum sentence for their crimes? 20 years.

Contractors vs employees

The Chinese Intelligence Service, MSS, had perhaps tried to be more careful than their military colleagues in the People's Liberation Army. They used commercial hackers rather than government employees, probably thinking that it lent them some additional deniability. But, given that the company involved was identified as MSS-tasks in any case, that choice may have been a mistake.

As private citizens, Wu, Dong and Xia are vulnerable to action by other countries that may choose to treat them as common criminals rather than government officials. The three have already been charged by the US government and now risk being arrested, deported, tried and imprisoned.

What happened to APT3?

This blog has been contacted by several InfoSec professionals who had been following APT3. Without exception they reported a complete cessation of APT3 activity in May 2017. Following the US indictment announcement in November 2017, the Wall Street Journal also reported that Boyusec had been disbanded.

The screenshot shows the top of the Wall Street Journal website. At the top, there is a black bar with market data: DJIA Futures 24942 (0.89% ▲), Stoxx 600 395.67 (0.25% ▲), U.S. 10 Yr -5/32 Yield 3.078% ▼, Crude Oil 71.45 (0.24% ▲), and Euro 1.1772 (0.02% ▲). Below this is the main header with 'THE WALL STREET JOURNAL' in large letters, 'Subscribe Now | Sign In', and a 'SPECIAL OFFER: JOIN NOW' button. The navigation bar includes 'Home', 'World', 'U.S.', 'Politics', 'Economy', 'Business', 'Tech', 'Markets', 'Opinion', 'Life & Arts', 'Real Estate', and 'WSJ Magazine'. A search icon is on the right. Below the navigation bar is a carousel of featured articles with thumbnails and titles: 'POLITICS: Justice Department to Review FBI Probe of Trump Campaign', 'BUSINESS: U.S. Ambassador to China on Open Markets and National Security', and 'OPINION: The FBI Informant Who Wasn't Spying'. Below the carousel is a sponsored advertisement for Barclays with the headline 'Can you beat your urge to splurge? Take control of your finances with these simple steps'. Below the ad is a social media sharing section with icons for email, print, and Facebook. The main article headline is 'Chinese Firm Behind Alleged Hacking Was Disbanded This Month' with sub-headlines 'WORLD | ASIA | CHINA' and 'Boyusec shareholders are accused of hacking into emails of a Moody's Analytics economist and stealing information from Siemens'. At the bottom of the article preview, it says 'The Wall Street Journal claims that Boyusec was disbanded in late 2017'.

In addition to the evidence above, the press release announcing the American indictments against Wu, Dong and Xia refers to May 2017 as the final date of their activity. Our conclusion? It seems that APT3 is no more.

What's next?

The 'P' in APT stands for Persistent. But this episode goes to show that Chinese APT hackers will only persist whilst their activity remains anonymous. APT3 was one of the biggest APT threats to Western companies, yet it was completely silenced by shining a light on its activities and exposing the identities of those behind the group to the world.

Analysts working with this blog are continuing their efforts to identify the individuals, companies and state institutions behind the damaging attacks that hit the West. We have accumulated evidence on several groups over the last twelve months and hope to share some of it soon.