The destruction of APT3

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

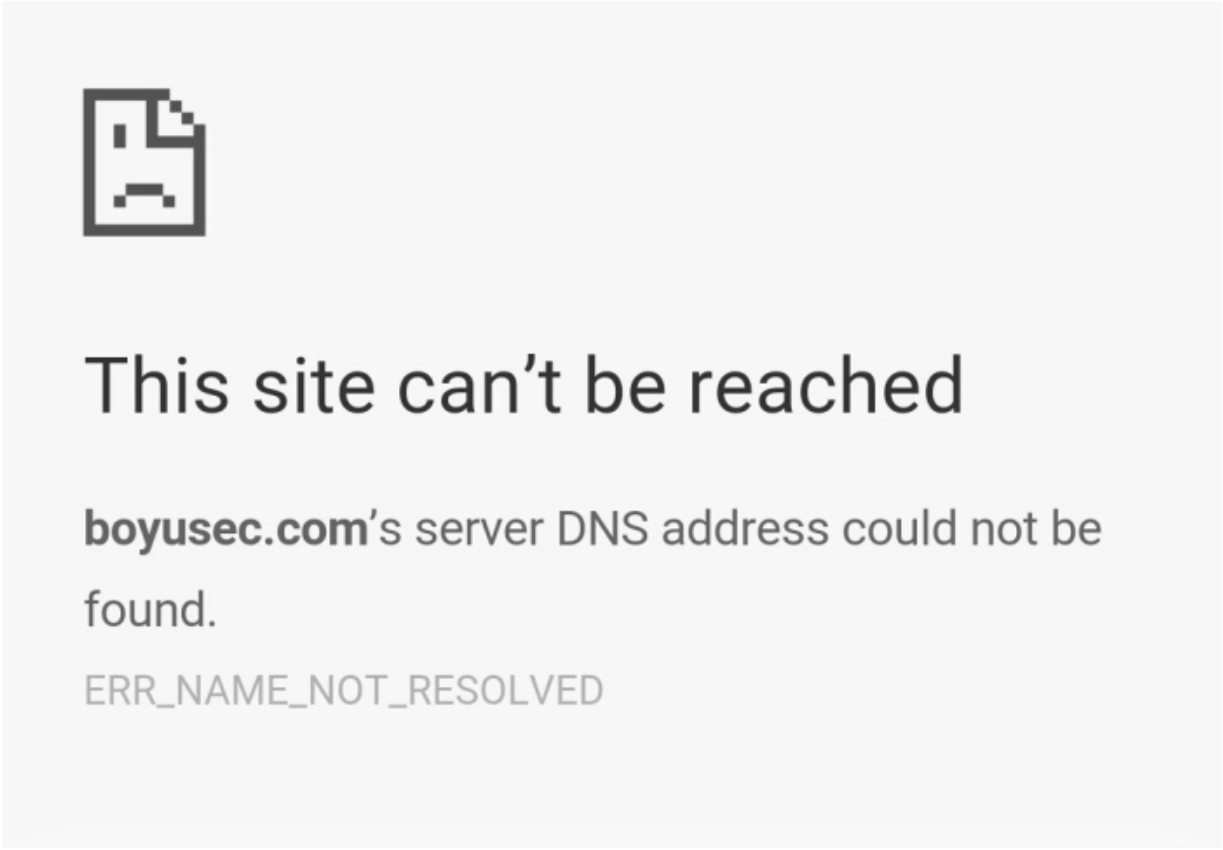
intrusiontruth May 22, 2018

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.



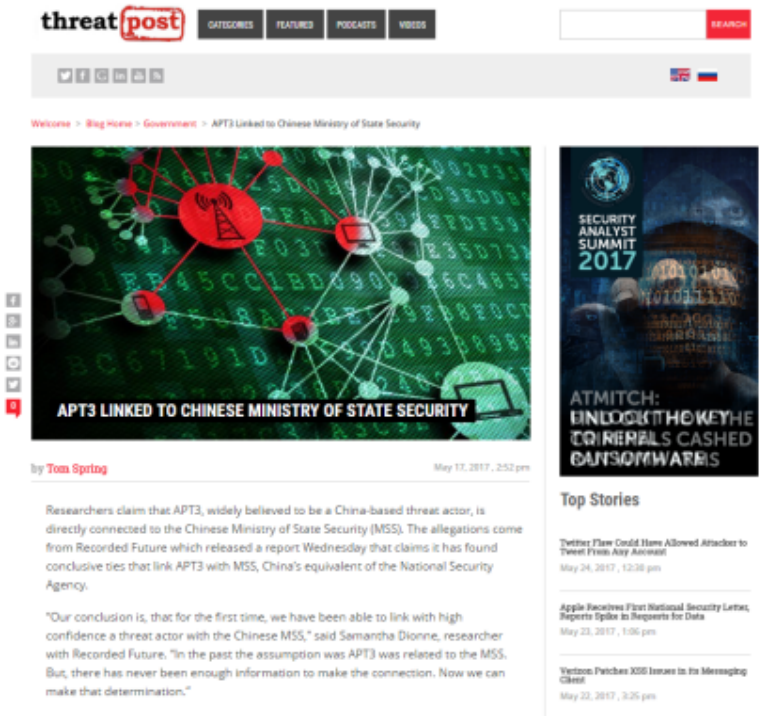
The morning after, on boyusec.com

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/0lIzSIzxjd
>
> — 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.



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

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

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

UNITED STATES OF AMERICA	)	
	)	Criminal No. 17-247
v.	)	
	)	
	)	18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(A),
WU YINGZHUO	)	1030(b)
a/k/a "mxmtmw"	)	18 U.S.C. § 1832(a)(1), 1832(a)(2),
a/k/a "Christ Wu"	)	1832(a)(5)
a/k/a "wyz"	)	18 U.S.C. § 1343
DONG HAO	)	18 U.S.C. § 1028A
a/k/a "Bu Yi"	)	
a/k/a "Dong Shi Ye"	)	
a/k/a "Tianyu,"	)	**UNDER SEAL**
XIA LEI	)	
a/k/a "Sui Feng Yan Mie"	)	

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-tasked 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 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.