Chinese Cyber: Resources for Western Researchers

cybercto.substack.com/p/chinese-cyber-resources-for-western

Ollie

Share this post

Chinese Cyber: Resources for Western Researchers

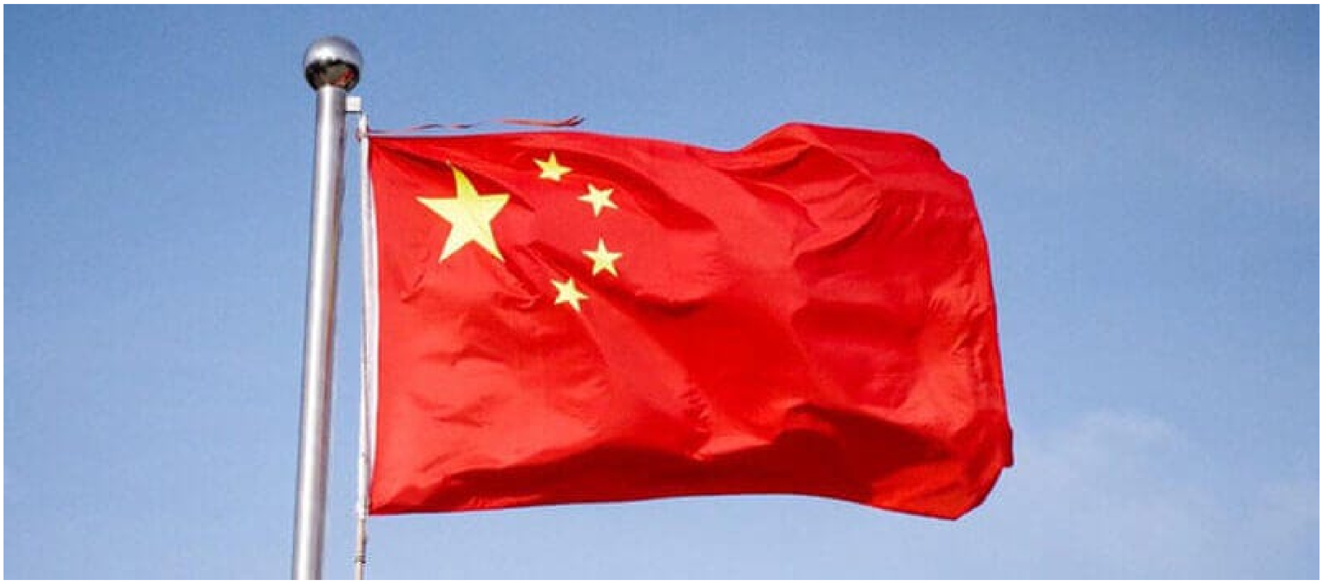
cybercto.substack.com

Discover more from Desk of a cyber CTO

Items which come across the desk of a cyber CTO which pique my interest covering business, research & development and cyber more generally.

Continue reading

Sign in



Over the years I have aggregated a set of resources which I have found useful to inform at least a superficial understanding of Chinese cyber and are used to feed /r/blueteamsec and the Blue Purple Pulse respectively. Below is the summary, if you have any others please email them over and/or add to the comments.

It goes without saying that to read most of these you will need to leverage various translation solutions be it within Browser or otherwise.

High Quality Meta Sources

A number of high quality Chinese meta sources that are highly recommended for checking daily.

360 CERT Daily

360 CERT’s daily security briefing comprised of links. Includes a lot of Western content but will also surface useful regional content as well.

Note: No content is added during the weekend of Chinese public holidays.

https://cert.360.cn/daily

Sec.today

Doesn’t just pull in solely Chinese sourced information, but does include some by virtue of being Chinese and is good for surfacing high quality technical content.

> Sec.Today cross-references multiple public data sources to build a centralized hub for all things infosec.

https://sec.today/pulses/

Cybersecurity information flow

As with the previous one above doesn’t just pull in solely Chinese sourced information, but does include some by virtue of being Chinese.

> A clean information flow push tool, biased towards every bit of the security circle, to discover high-quality content for security researchers every day.

https://i.hacking8.com/

Safety Hourglass-Scientific Research Data Exchange Platform

Provides a rich source of Chinese language cyber research both high and low level in nature.

> SecWiki has always been committed to providing the latest and most professional security information sharing platform to facilitate security personnel to obtain security events, high-quality technical articles, and technical topics.

https://www.sec-wiki.com/index.php

Code Audit

As the name implies provides a focus on code and web security specifically. Excellent source for staying appraised of the web techniques, capabilities and research focus out of China.

> "Code Audit" is a professional, cutting-edge, and original Web code security and audit discussion community. We focus on sharing original code security knowledge, vulnerability mining methods, and eliminating link transfers, data reprinting, and other behaviors.

https://govuln.com/news/

Wider Chinese Native

A number of Chinese native sources which vary in their quality and focus but all are worth reviewing semi regularly. The volume of some is hard to appreciate until you try and consume it all.

Threat Intelligence

Various open source threat intelligence reporting is available from Chinese sources which give insight into their unique perspective.

Security Star Chart Platform

A threat intelligence database from a firm in China which provides good summary reporting generally monthly in Chinese as well as other infrequent posting.

https://ti.dbappsecurity.com.cn/info

WeChat - Hash Tag Searches

WeChat is a joy to navigate as a Westerner, these hash tags will hopefully expedite some of that process.

- #APT and #apt - as their hash tags do not appear insensitive
- #APT分析 (#APT analysis) - similar to the above
- #猎影实验室 (#Hunting Shadow Lab) - a particular term used for a particular supposed Western threat actor
- #分析报告 (#analysis report) - infrequently used by one group on their South Asian threat actor tracking
- #SecWiki - a weekly summary of high quality primarily Chinese source cyber relevant links

News Sites and Super Aggregators

Numerous high volume sources and communities exist in China which provide rich sources of information and insight yet a tremendous amount of volume.

Weibo

If you thought WeChat was challenging then welcome to Weibo.

> Tencent Security Xuanwu Lab - they produce a weekly summary of URLs some Chinese some Western which is useful.

Freebuf

An absolute firehose of content with variable signal to noise ratio. Covers everything from the very high-level to the very low-level.

https://www.freebuf.com/

Safer - Safety Information Platform

A very busy cyber security news site which pulls in a lot of information with variable signal to noise ratio.

https://www.anquanke.com/index.html

Expertise, serving artificial intelligence practitioners!

Not cyber focus but does surface cyber relevant publications from academia in China and globally in the domain of machine learning and data science.

https://www.zhuanzhi.ai/

Western

Western aggregation and analysis.

ASPI Daily Cyber and Tech Digest

A daily newsletter from the Australian Strategic Policy Institute thinktank. Includes primarily high-level non-technical content.

aspiicpc.substack.com/

ETO Scout

Not just cyber but sometimes surfaces cyber relevant information.

> Welcome to Scout, ETO's discovery tool for Chinese-language news and commentary on technology issues.

https://scout.eto.tech/

Closing…

These only scratch the surface, but have been useful to help gain some understand in a vast sea of information.

2 Comments

1 more comment...