SentinelLABS

CHINA'S CYBER REVENGE | WHY THE PRC FAILS TO BACK ITS CLAIMS OF WESTERN ESPIONAGE

Author: Dakota Cary

January 2024

SentinelLABS Research Team

TABLE OF CONTENTS

EXECUTIVE SUMMARY

- China launched an offensive media strategy to push narratives around US hacking operations following a joint statement by the US, UK, and EU in July 2021 about China's irresponsible behavior in cyberspace.

- Some PRC cybersecurity companies now coordinate report publication with government agencies and state media to amplify their impact.

- Allegations of US hacking operations by China lack crucial technical analysis to validate their claims. Until 2023, these reports recycled old, leaked US intelligence documents. After mid-2023, the PRC dropped pretense of technical validation and only released allegations in state media.

- The cyber-focused media campaign preceded the 2023 efforts of the MSS to disclose accounts of western spying in the PRC.

SentinelLabs Team

IT'S NOT WHAT YOU SAID, IT'S HOW YOU SAID IT.

Since 1963, the Chinese Communist Party has concerned itself with "public opinion warfare". Under its Three Warfares doctrine, which also includes psychological warfare and legal warfare, the Party aims to influence the world's view of China. But it seems the CCP dropped the ball on global public opinion on its behavior in cyberspace. For nearly two decades, evidence of Chinese industrial espionage captured headlines. Despite this, the facts suggest that China's leaders were unaware of how tarnished their image was until mid-2021. In the winter of that year, a PRC hacking team was taking advantage of four vulnerabilities in Microsoft Exchange Servers. When intelligence that the company was planning to patch reached the team, they shared the vulnerability with others and automated their attack for scale. After years of successful PRC hacking operations, it was this scaling that moved governments to action. That is when the U.S., U.K., and the EU jointly issued a statement condemning China's behavior in cyberspace. Only then did China wake up to its reputation.

China prefers to engage with countries in a one-on-one, bilateral, way. This approach to diplomatic engagement favors China. As a self-described large country, it is easier to negotiate with small countries if they do not band together. This is why China refers to its encroachments into Philippine waters as a bilateral issue between the two countries. Preferring to frame it this way to cut out the Permanent Court of Arbitration and the U.S. So when the EU, UK and US all agreed to sign a statement condemning China's actions in cyberspace, Beijing sat upright.

After the summer of 2021, China's cybersecurity industry took steps to conceal or defend its hacking. In 2023, the Tianfu Cup cybersecurity competition stopped naming the iPhone as one its targets. Instead the organizers chose to call it "another country's phone." They hoped that the oblique reference would conceal the real target. China was trying to limit inflammatory information about its hacking capabilities. Besides concealment, Beijing used outright denial, too. When Mandiant released its report on UNC4841's hack of Barracuda products, the Ministry of Foreign Affairs lashed out. The MFA spokesperson called the report "unprofessional" at a press conference. But China did more than simply delete references to US products at its hacking competitions and shout down cybersecurity experts. The jointly issued statement so irked Chinese policy leaders that they pivoted to offense in the hopes of changing global public opinion.

BEFORE MES

The objective of ModifiedElephant is long-term surveillance that at times concludes with the delivery of 'evidence' –files that incriminate the target in specific crimes– prior to conveniently coordinated arrests.

After careful review of the attackers' campaigns over the last decade, we have identified hundreds of groups and individuals targeted by ModifiedElephant phishing campaigns. Activists, human rights defenders, journalists, academics, and law professionals in India are those most highly targeted. Notable targets include individuals associated with the Bhima Koregaon case.

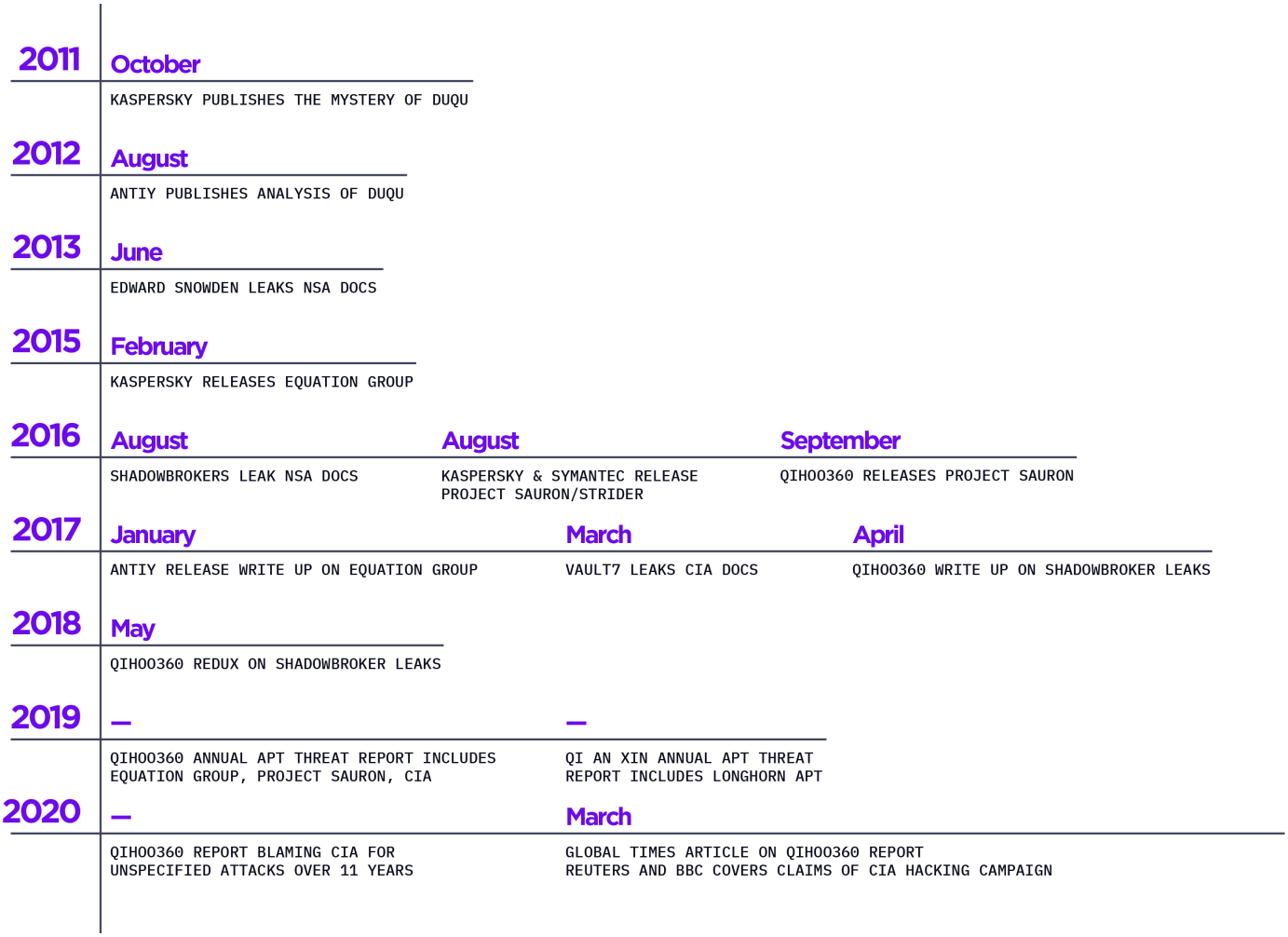


Fig 1: Timeline 2011-2020

Only after Kaspersky released its threat intelligence on Duqu did Chinese cybersecurity firm Antiy release its own analysis of the malware a year later in 2012. Similarly, non-Chinese cybersecurity companies' publications on tools and groups like Regin, Project Sauron, or Equation Group preceded similar reports by Chinese cybersecurity firms. PRC cybersecurity companies' publications were often years behind their international peers.

When they did publish, these companies rarely added new analysis. It was not until 2017 that Qihoo360 first mentioned the NSA in relation to attacks on the PRC. Still, the company did not add new information to public discussion, instead pointing to the recently leaked ShadowBrokers documents. In a nod to their ability to track but their inability to publish technical details of US operations, Qihoo360 claimed to have tracked the CIA's operations tied to tooling disclosed in the Vault7 leaks as far back as 2008. At least two major outlets covered the report. But the company's report underscores the problem with the integrity of China's claims. Most of the Qihoo360's report focused on the Vault7 leaker, as well as the structure and purpose of the CIA.

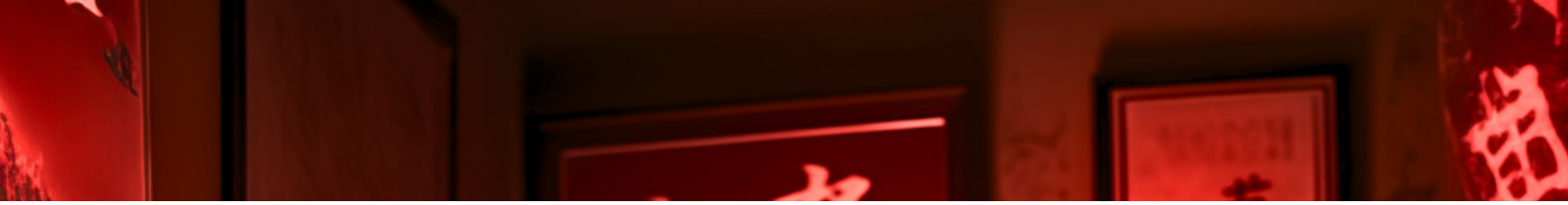
This was the state of affairs until the July 2021 joint statement condemned China's behavior.

CHINA PIVOTS TO REHASHING OLD QUARRELS

Qi An Xin published the first report in the new year and fired the starting gun on China's new media strategy. The February 2022 report analyzed yet another leaked tool of US operators, one disclosed by an intelligence leak. This time, however, the company's report was released alongside a slew of state media coverage. Importantly, the coverage included a corresponding, English-language article from Global Times–a nationalist state media outlet. From then on, a Global Times article has accompanied each cyber threat intel publication about US hacking.

Qihoo360 re-released its March 2020 report claiming US hacked unspecified targets in the country just one month later. In March 2022, the spokesperson for the Ministry of Foreign Affairs announced Qihoo360's two-year old report during a press conference. It was momentous for the PRC. The coordination marked a new era in China's approach to talking about spying by other nations. The PRC so desperately wanted to talk about US hacking that the MFA spokesperson dragged out a two-year-old report.

China's National Computer Virus Emergency Response Center, a self-described "national cyber defense agency", moved quickly to provide more content. Immediately following the March press conference, CVERC issued a report detailing previously leaked US backdoors and tools, like NOPEN. Weeks later in April 2022 CVERC detailed another US tool, HIVE. The bevy of reports continued to provide fodder to PRC



state media. A third CVERC piece focused on old, leaked tools was released in June, this one delving into ACIDFOX. The Ministry of Foreign Affairs again took care to highlight the ACIDFOX reporting at a press conference that month. The shoutout by MFA spokespersons at the press conference was another effort to again push US hacking into public discourse. In 2021, Global Times had only twice mentioned the NSA–both in the context of railing against global capitalists. The publication mentioned the NSA in connection to hackings tools or operations 24 times the following year. But it wouldn't be until late June that the PRC named its first victim of US hacking, a notable feature missing from public discourse and one that caught the attention of western press.

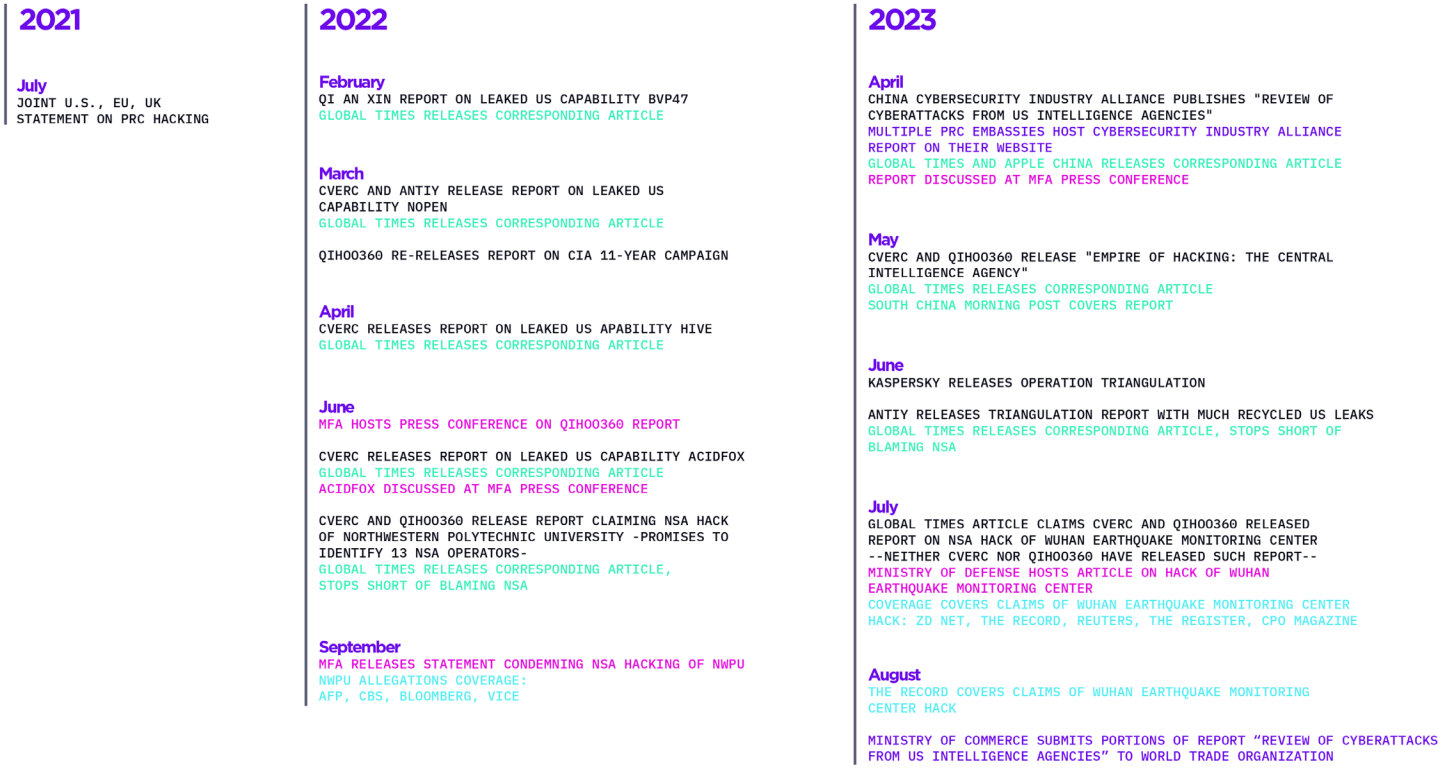


Fig 2: Timeline 2021-2023

CVERC and Qihoo360 jointly released a report in June 2022 claiming the NSA's Office of Tailored Access Operations had penetrated the networks of Northwestern Polytechnical University. Although the report was again based on leaked intelligence, it was the first report that identified a victim of US hacking in the PRC. It's unclear why it took so long for any company or state media to identify targets of the US. It may be that naming an organization that fell victim to US hacking

is bad politics. In competition between Party factions and aspirational leaders, having your organization named as a victim NSA would be an undesirable blemish, even if for propaganda purposes. Regardless of the reasons such details had been withheld, naming NWPU helped the story gain traction.

The authors offered a second lurid detail that foreign press would later grab hold of. The last sentence of the report claimed that CVERC and Qihoo360 had identified 13 US operators tasked with the mission, promising to reveal their identities. To help promulgate the content of the report, the State Council Information Office released an English language piece on the report, which was quickly picked up by other foreign-focused state media. The gambit worked. Western press flocked to cover the allegations.

Despite all this, the report still failed to publish verifiable details. The authors redacted half of each IP number and the last two digits of each calendar date in the report. The first bit of erasure was likely to comply with state secrecy laws; the second half to hide that the alleged operation would have been more than a decade old at the time of the report's publication.

By now, cybersecurity companies in the PRC were regularly including references to US-based APTs in their annual reports—none of which offered technical analysis besides what had been leaked in the preceding decade.

China expanded its efforts in 2023. In April of that year, the China Cybersecurity Industry Alliance, a group formed in 2016, released its *Review of Cyberattacks from US Intelligence Agencies*. The nearly 100-page report summarized past publications and intelligence leaks, and added no new evidence or allegations. Of the nearly 150 citations in the report, less than one-third are attributed to PRC vendors. Still, the document provides a tool to those in search of evidence of US operations in cyberspace. The report neatly condenses more than a decade of disparate research into an easily accessible report. Anyone searching for evidence of the US's malfeasance in cyberspace would now have something, in English, at the top of their search results.

CVERC released a similar report the following month focused on CIA operations and organization structure. Again, drawing on leaked intelligence, Empire of Hacking: The U.S. Central Intelligence Agency rehashed old Vault7 files and added no new claims or technical evidence for readers. The report did, however, claim that the CIA had conducted attacks against targets in the PRC—a still new phenomenon following the July 2021 joint statement. Some press picked up on the piece, which was even hosted on some Chinese embassies' websites.

A NEW ERA

In July 2023, China did something it hadn't done before—it spread new allegations of US hacking apparently unrelated to past US intelligence leaks and, as of this report, entirely unsubstantiated. In a series of publications by Global Times, the CEO of Antiy claimed the United States had hacked into seismic censors of the Wuhan Earthquake Monitoring Center. His claims, along with those of the Global Times, were ostensibly based on a report from CVERC and Qihoo360. But this report is not yet public, if it exists. Neither CVERC nor Qihoo360 host such a report on their respective websites, nor does any PRC government agency. Qihoo360's only mention of the Wuhan Center is a community board post by an anonymous user referencing state media.

According to Antiy's CEO, seismic monitoring data would provide US military analysts insights into weapons testing happening in Wuhan. The allegations must have tasted sweet in his mouth—years earlier, leaked NSA documents identified his company as a collection target.

Fig 3: A slide from Antiy regarding attacks on the PRC

The lack of technical details–or in this case, a report at all–did not stop the story from getting attention. A handful of cybersecurity industry outlets in the U.S. picked up the story and ran it in July and August after the Global Times published another report covering the allegations. This time, state media claimed that "Chinese authorities will publicly disclose a highly secretive global reconnaissance system of the US government…" Yet another report that has not been released.

The allegations of US hacking without technical evidence coincided with China's Ministry of State Security launching its public WeChat account. Since the middle of 2023, the MSS has published four accounts of foreign spies operating in China and being caught. Three are alleged to have been working for the U.S., a fourth was alleged to have worked for the UK and was tied to office raids of foreign due diligence firms. Off-the-record American officials confirmed one of the US cases to press later in the year.

CONCLUSION

In both domains of alleged spying, cyber and human, China has not yet published detailed accounts that analysts have come to expect from cybersecurity firms or western prosecutors' indictment of foreign spies. Accepting this asymmetry in data sharing benefits China, allowing the country to publish claims of foreign hacking without the requisite information. If analysts do not actively challenge the CCP's claims, the government can lie with impunity.

Repeating China's allegations helps the PRC shape global public opinion of the U.S. China wants to see the world recognize the U.S. as the "empire of hacking." But outright ignoring China's claims undermines public knowledge and discourse. The fact that China is lodging allegations of US espionage operations is still notable, providing insight into the relationship between the US and China, even if China does not support its claims. CTI analysts and intelligence consumers would be wise to differentiate between the claims made by China across domains, however.

Human intelligence collection will always be subject to highly secretive practice, prosecution, and use. Few governments willingly talk about the operations of hostile nations, much less confirm their own operations alleged by foreign intelligence. For allegations of human intelligence, the path forward is unlikely to change–it will remain secretive. China will make claims of foreign spying without ever releasing public indictments, and those allegations may be periodically confirmed or denied by other governments.

But claims of cyber espionage are subject to different standards of integrity and openness. Intelligence consumers would be negligent to trust claims of cybersecurity companies that were unable to provide technical details supporting their analysis. To date, China has provided no reasonable evidence to support any of its claims besides wantonly recycling leaked US intelligence. In western cybersecurity industry circles, claims of US hacking without supporting technical evidence are derided—and rightfully so.

State secrecy laws are the likely culprit stopping PRC-based cybersecurity companies from publishing technical data. With their hands tied, the CCP's political mandate to support narratives of western espionage operations leaves its companies hamstrung. Analysts should not lower their standards to help the PRC achieve its objective of changing global public opinion on Chinese and US hacking. Instead, claims made by Chinese firms and the government should be held to the same, rigorous analytical standards the global cybersecurity community has self-imposed. As one expert said at Labscon 2022 regarding China's claims of US hacking, "PCAPs or fuck off."

FIGURE 1 REFERENCES

2011 Kaspersky Duqu The Mystery of Duqu: Part One | Securelist

2012: Antiy report on Duqu 探索Duqu木马身世之谜-安天 智者安天下 (archive.org)

2013 June: Edward Snowden: Timeline - BBC News

2014: First CAC mention of US attacks on PRC 2014 after Snowden, references to PRISM and some data.
https://web.archive.org/web/20220705194209/https://www.gov.cn/xinwen/2014-05/20/content_2682440.htm
https://web.archive.org/web/20150606043314/http://www.cac.gov.cn/2014-05/20/c_126522072.htm

2015 February Equation Group report Equation Group: The Crown Creator of Cyber-Espionage | Kaspersky

2016 August Shadowbrokers 'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked? - The New York Times (nytimes.com)

2016 August Project Sauron ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms | Securelist

2016 Eye of Sauron by Qihoo360
https://web.archive.org/web/20231001211033/https://apt.360.net/orgDetail/70

2017 January Antiy diagram of EQG

2017 March Vault7 - Home (wikileaks.org)

April 2017 qihoo360 First mention of NSA is after Shadowbrokers:
https://web.archive.org/web/20231001192726/http://www.360.cn/weishi/news.html?i=news0421p No claim of attack on PRC

May 2018: Analysis of NSA tool from shadowbroker, no claim of attack on PRC
https://web.archive.org/web/20231001193520/http://www.360.cn/newslist/zxzx/gnzNSASrvanyMinnerwkmmgjbdlywrbwjqfwz.html

Qihoo 2019 annual report:
https://archive.org/details/2020-apt/page/n33/mode/2up
https://archive.org/details/2020-apt

2019 equation group after kaspersky
https://web.archive.org/web/20231001210543/https://apt.360.net/report/apts/85.html

2019 Annual Report QAX 全球高级持续性威胁（APT）2019-23年度报告: Free Download, Borrow, and Streaming : Internet Archive

2020 Annual Report QAX 全球高级持续性威胁（APT）2019-23年度报告: Free Download, Borrow, and Streaming : Internet Archive

APT-C-39 2020
https://web.archive.org/web/20230420151007/https://apt.360.net/orgDetail/12

March 2020: First Qihoo360 report claiming US CIA attacks (vague) PRC. https://web.archive.org/web/20230420151334/https://www.360.cn/n/11563.html

Based on vault7 leaks. Bottom of page introduces the 360 APT Threat Intelligence Center and claims they have been tracking APTs since 2007, a nod to the fact that they may have been capable of such reporting for a long time. 披露美国中央情报局CIA攻击组织（APT-C-39）对中国关键领域长达十一年的网络渗透攻击 (archive.ph)
https://world.huanqiu.com/article/3xGuuRGwKVW

2020 March CIA 11 year campaign claim
https://www.reuters.com/article/idUSKBN20Q2SG/
https://www.bbc.com/news/technology-51736410

FIGURE 2 REFERENCES

July 2021 Joint US, EU, UK statement on PRC The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China | The White House

Feb 2022 Qianxin report on bvp47
https://web.archive.org/web/20220223060134/http://www.pangulab.cn/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/

Feb 2022
https://www.globaltimes.cn/page/202202/1252952.shtml

March 2022 Qihoo360 co-release with govt on US attacking PRC: https://web.archive.org/web/20230520211935/https://www.360.cn/n/12330.html

Post claims that Qihoo360 identified an 11-year long campaign of US APT-C-39 (CIA) attacking PRC.

March 2022 NOPEN report CVERC:
https://archive.org/details/20220314_202310

https://archive.ph/aNT9S

https://web.archive.org/web/20220828222100/https://www.antiy.cn/research/notice&report/research_report/20220315.html

April 2022: CIA HIVE report CVERC:
https://archive.org/details/hive_20231001

June 2022: ACIDFOX report CVERC:
https://archive.org/details/ACIDFOX
https://archive.ph/AuPCc

June 2022 ACIDFOX comes up at MFA Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on June 30, 2022 (archive.org)

June 2022 NWPT (NPU) Announced by CVERC. Threaten to name 13 NSA operators responsible for the hack. Didn't release names. 信息安全摘要 (archive.ph)

June 2022 GT piece
https://www.globaltimes.cn/page/202206/1268801.shtml

Sept 2022: NWPT piece MFA
http://english.scio.gov.cn/pressroom/2022-09/06/content_78406151.htm

Sept 2022: Coverage of NWPT report
https://english.news.cn/20220913/c0160cc560a7443db81ca77a5a7b5481/c.html

Sept 2022 2022: AFP picks up NWPT piece
https://www.france24.com/en/live-news/20220905-china-accuses-us-of-tens-of-thousands-of-cyberattacks

https://gizmodo.com/china-nsa-northwestern-polytechnical-university-hack-1849530364

https://www.cbsnews.com/news/china-accuses-us-nsa-cyberattack-spying-northwestern-polytechnical-university-military-research/

https://www.vice.com/en/article/k7b3bz/china-accuses-nsa-hacking-military-research-university

https://www.bloomberg.com/news/articles/2022-09-05/china-accuses-us-of-repeated-hacks-on-polytechnic-university

2022 Annual Report QAX 全球高级持续性威胁（APT）2019-23年度报告 : Free Download, Borrow, and Streaming : Internet Archive

Qianxin
https://archive.org/details/apt-2022

Qihoo 2022
https://web.archive.org/web/20231001204555/http://pub1-bjyt.s3.360.cn/bcms/2022%E5%B9%B4%E5%85%A8%E7%90 %83%E9%AB%98%E7%BA%A7%E6%8C%81%E7%BB%AD%E6%80%A7%E5%A8%81%E8%83%81%EF%BC%88APT%EF%BC%89%E7%A0%94%E7%A9%B6%E6%8A%A5%E5%91%8A.pdf

2023 March China CIA report Wayback Machine (archive.org)

2023 April China Daily boosts China CIA report CCIA report exposes malicious behavior and threat of US cyber hegemony - Opinion - Chinadaily.com.cn (archive.ph)

GT May 2023 https://archive.ph/fU6mh

embassies https://archive.ph/MyQik https://archive.ph/V5hcc

MOFCOM to WTO August 2023
https://web.archive.org/web/20230811163549/http://images.mofcom.gov.cn/sms/202308/20230811165019325.pdf

27) May 2023: CVERC Report on US activity May 2023.
(Part 1, Part 2 in word doc already and is website CVERC)
https://web.archive.org/web/20230530221200/http://gb.china-embassy.gov.cn/eng/PressandMedia/Spokepersons/202305/P020230508664391507653.pdf

CVERC & Qihoo360 on Empire CIA Global Times
https://archive.ph/esx1O

May 2023 SCMP pick up report:
https://www.scmp.com/news/china/science/article/3219414/us-controlled-empire-hackers-attacking-china-other-countries-report

June 2023: Kaspersky Operation Triangulation
https://archive.ph/ZPPKr

Antiy follow-on:
https://archive.ph/0Y3T1

GT follow-on of Antiy:
https://archive.ph/VDg2V

July 2023: NSA hacking of Wuhan Seismic Devices. (CVERC and 360) Exclusive: Wuhan Earthquake Monitoring Center suffers cyberattack from the US; investigation underway - Global Times (archive.ph)

2023 July The Record runs with Seismic
therecord.media/china-accuses-us-global-reconnaissance-system-wuhan

https://www.reuters.com/world/china/china-says-wuhan-earthquake-centre-attacked-by-overseas-hackers-2023-07-26/

SCMP
https://archive.ph/AXhs2

Aug The register
https://www.theregister.com/2023/08/15/china_seismic_us_spying_expose/

Aug ZD NET
https://www.zdnet.com/article/china-accuses-us-intelligence-agencies-as-source-behind-wuhan-cybersecurity-attack/

https://www.chinadaily.com.cn/a/202307/26/WS64c070dda31035260b81887f.html

PRC MOD
https://archive.ph/2mFbB

2023 August The Record again on Seismic
therecord.media/china-accuses-us-hacking-earthquake-monitoring-wuhan

2023 August
https://www.globaltimes.cn/page/202308/1296226.shtml
Claims of future relase “Chinese authorities will publicly disclose a highly secretive global reconnaissance system of the US government, which poses a serious security threat to China’s national security and world peace.” “hacker empire”

Aug 2023 CPO Mag picks up Wuhan
https://www.cpomagazine.com/cyber-security/china-blames-us-intelligence-agencies-for-cyber-attack-on-wuhan-emergency-system-claims-spies-were-probing-for-underground-facilities/

2023 September GT
https://www.globaltimes.cn/page/202309/1298520.shtml

ABOUT SENTINELLABS

InfoSec works on a rapid iterative cycle where new discoveries occur daily and authoritative sources are easily drowned in the noise of partial information. SentinelLabs is an open venue for our threat researchers and vetted contributors to reliably share their latest findings with a wider community of defenders. No sales pitches, no nonsense. We are hunters, reversers, exploit developers, and tinkerers shedding light on the world of malware, exploits, APTs, and cybercrime across all platforms. SentinelLabs embodies our commitment to sharing openly –providing tools, context, and insights to strengthen our collective mission of a safer digital life for all. In addition to Microsoft operating systems, we also provide coverage and guidance on the evolving landscape that lives on Apple and macOS devices. https://labs.sentinelone.com/