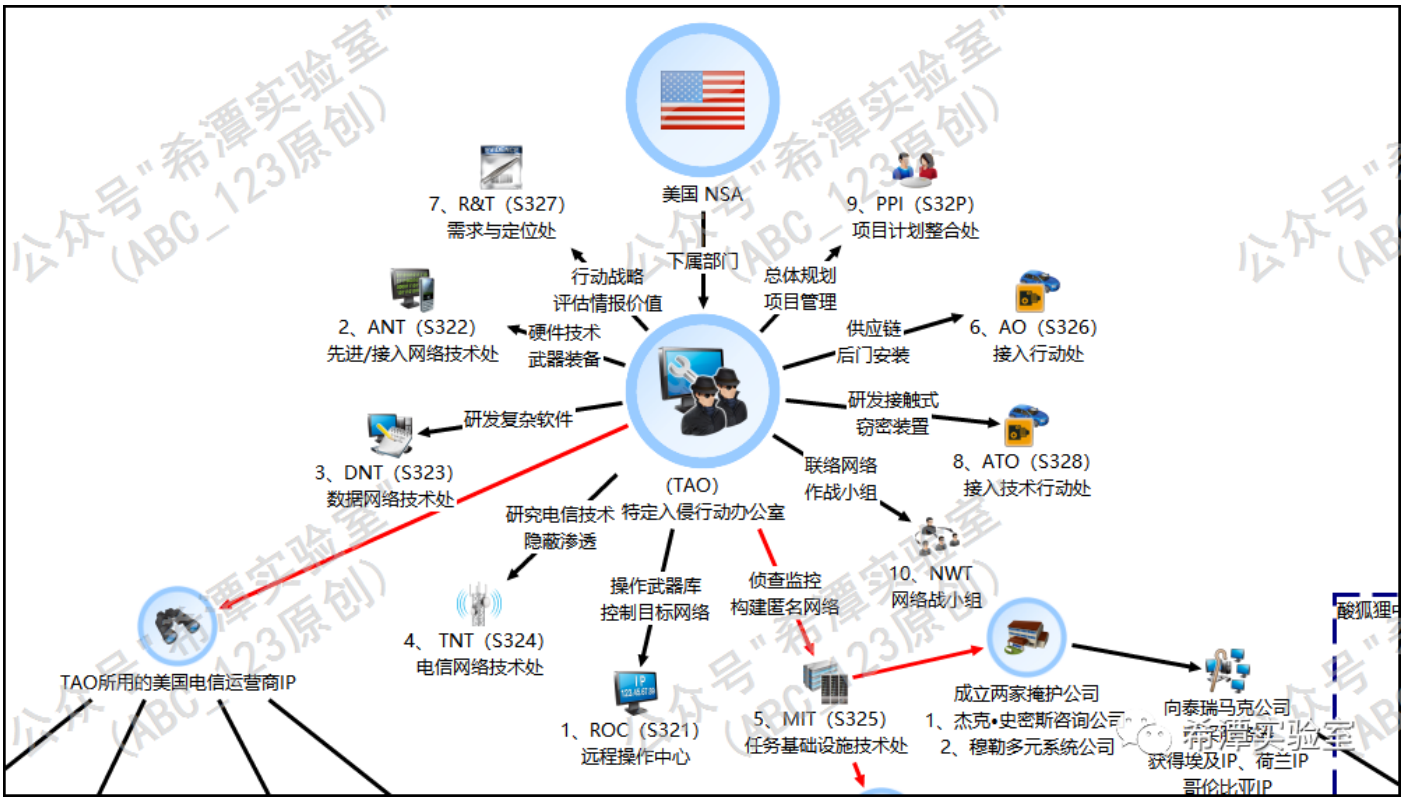
An inside look at NSA (Equation Group) TTPs from China's lense

inversecos



Since I reside in a Five Eyes country (Australia) and have publicly presented four cases I led on China's APT41 attacking organisations in ASEAN, particularly concerning China's cyber and political strategies, I was curious to explore what China publishes about Five Eyes operations. This led me down a rabbit hole of research into TTPs that Chinese cybersecurity entities have attributed to the NSA – or, as they coin "APT-C-40".

These insights stem from extensive research I did on Weixin containing intelligence reports published by China's Qihoo 360, Pangu Lab, and the National Computer Virus Emergency Response Center (CVERC). It is important to note that the authenticity and extent of these allegations remain unverified by independent sources. My goal in writing this blog is simply to aggregate and share what Chinese sources are publishing about NSA's cyber operations (APT-C-40) to see if I could learn any new detection techniques or offensive techniques to research for fun.

As I did this research, I had a realisation that the Chinese methodology of Incident Response appears very different to how we perform IR in the West and had me thinking more about how I could modify some of my own methodologies to include some of the learnings. Maybe I will write a blog on this in the future. Ultimately, depending on the reception of this blog, I may continue this

series by sharing my other findings on Chinese reports regarding CIA (APT-C-39) cyber operations and a third North American group (not NSA or CIA) that Chinese firms are tracking named APT-C-57.

How the NSA Allegedly Hacked China's Northwestern Polytechnical University

This is how China's Northwestern Polytechnical University, a leading institution specializing in aerospace and defence, allegedly became the target of a sophisticated cyberattack attributed to the NSA's APT-C-40 group **back in 2022**. Reports claim that the attack was executed by Tailored Access Operations (TAO), a division within the NSA, which allegedly deployed over 40 unique malware strains to conduct data theft and espionage.

All the information regarding this breach is publicly disclosed on the internet by Chinese cyber companies Qihoo 360 and National Computer Virus Emergency Response Centre on Weixin.

The attack was publicly announced by the University in a public bulletin post on June 2022 (below). Saying the University suffered a series of phishing emails to staff and employees.

公开声明

西北工业大学 西北工业大学 2022-06-22 11:08 发表于陕西

西北工业大学
NORTHWESTERN POLYTECHNICAL UNIVE

近期，我校电子邮件系统遭受网络攻击，对学校正常教学生活造成负面影响。我校第一时间报警，经公安机关初步判定，是境外黑客组织和不法分子发起的网络攻击行为。现公开声明如下：

此次网络攻击事件中，有来自境外的黑客组织和不法分子向我校师生发送包含木马程序的钓鱼邮件，企图窃取相关师生邮件数据和公民个人信息，给学校正常工作和生活秩序造成重大风险隐患。长期以来，我校高度重视网络安全工作，经常性开展网络安全宣传教育，定期开展网络安全检查和技术监测，明确主动防御策略，全面采取技术防护措施。全校师生网络安全意识和敏锐性逐年提高，来自境外的钓鱼邮件暂未造成重要数据泄露，暂未引发重大网络安全事件，校园网络安全和广大师生的个人信息安全得到有效维护。

为进一步查明事实，依法处理相关黑客组织和不法分子的网络攻击行为，采取有力措施筑牢校园网络安全屏障，维护广大师生合法权益，我校已就遭受境外网络攻击情况向公安机关报案，并保留进一步追诉的权利。

在此，我校提醒广大互联网用户：网络空间不是法外之地，发送钓鱼邮件、侵犯公民个人信息属于犯罪行为。请广大网民文明用网、规范用网，严格遵守《中华人民共和国网络安全法》，共同营造清朗网络空间。

How did China perform the attribution?Through the joint investigation and forensics on the University, CVERC and 360 identified 4 IPs that the NSA supposedly purchased through two cover companies “Jackson Smith Consultants” and “Mueller Diversified Systems”. The four IPs identified are listed at the end of this report. CVERC and 360 alleged a TAO employee with the pseudonym “Amanda Ramirez” anonymously purchased these for the NSA’s FoxAcid platform which was later used in the attack on the University.

CVERC and 360 also alleged that the NSA had used anonymous protection services of a Registrar in the US to anonymize domain names and certificates to prevent them from being queried by public channels.

Investigators from CVERC and 360 were able to trace the attack back to NSA's TAO unit through a mix of human error, patterns in their analysis and tool overlap.

1. Attack Times

One of the frameworks used by TAO that was forensically uncovered during the incident named “NOPEN” requires human operation. As such, a lot of the attack required hands-on-keyboard and data analysis of the incident timeline showed 98% of all the attacks occurred during 9am – 4pm EST (US working hours).

There were zero cyber-attacks on Saturdays and Sundays with all attacks centralised between Mon-Fri.

No attacks occurred during Memorial Day and Independence Day holidays which were unique American holidays.

No attacks occurred during Christmas.

2. Keyboard Inputs

Attacker used American English.

All devices used by the attacker had English OS and English applications.

American keyboard was utilised.

3. Human Errors

Due to the length and scale of the incident, when one of the alleged NSA “attackers” tried to upload and run a Pyscript tool, they forgot to modify the parameters. This returned an error – the error message exposed the working directory and file name of the attacker’s internet terminal.

This was then used to identify that they were running on a Linux system and the directory “etc/autoutils” was known to be the special name of the TAO network attack tool directory.

*The error message is as follows: Quantifier follows nothing in regex; marked by <-- HERE in m/ * <-- HERE .log/ at .. /etc/autoutils line 4569*

4. Tools Were Found Prior to Shadow Brokers Leak

The Northwestern Polytechnical University had allegedly suffered multiple breaches throughout the years where several pieces of malware uncovered in prior investigations (prior to Shadow Broker's leak) were allegedly the same tools described in the Shadow Broker's leak. They did not provide further information on this.

5. Toolkits related to NSA

41 different tools and malware samples were identified as a part of the investigation in the forensic analysis.

16 of these tools were consistent with the TAO weapons exposed by the Shadow Brokers leak.

23 of the tools had around 97% similarity to the tools in the Shadow Brokers leak.

2 of these tools were not found in Shadow Brokers but were seen used by TAO in other cyber-attacks (according to 360).

Inside the Attack: Alleged NSA TTPs

1. Pre Attack Preparation

One of the NSA's primary strategies in breaching the university was the use of zero-days. However, to begin the attack the attackers first conducted a pre-attack preparation phase with extensive work. Two zero-days were used to breach any company with SunOS-exposed systems in neighbouring countries to China. 360 and CVERC did not specify which vulnerabilities were targeted in their reports.

Specifically, the NSA would target any server with large network traffic (i.e. educational institutions and commercial organisations). Once the attack was successful, they would install NOPEN (more on this later) to establish a foothold. By deploying zero-days on these systems, they established access on these systems that would later be used as springboards for the main attack on the University.

In total, 54 jump servers and 5 proxy servers were used to perform the attack coming from 17 different countries including Japan, South Korea, Sweden, Poland and Ukraine with 70% of the attacks coming from China's neighbouring countries.

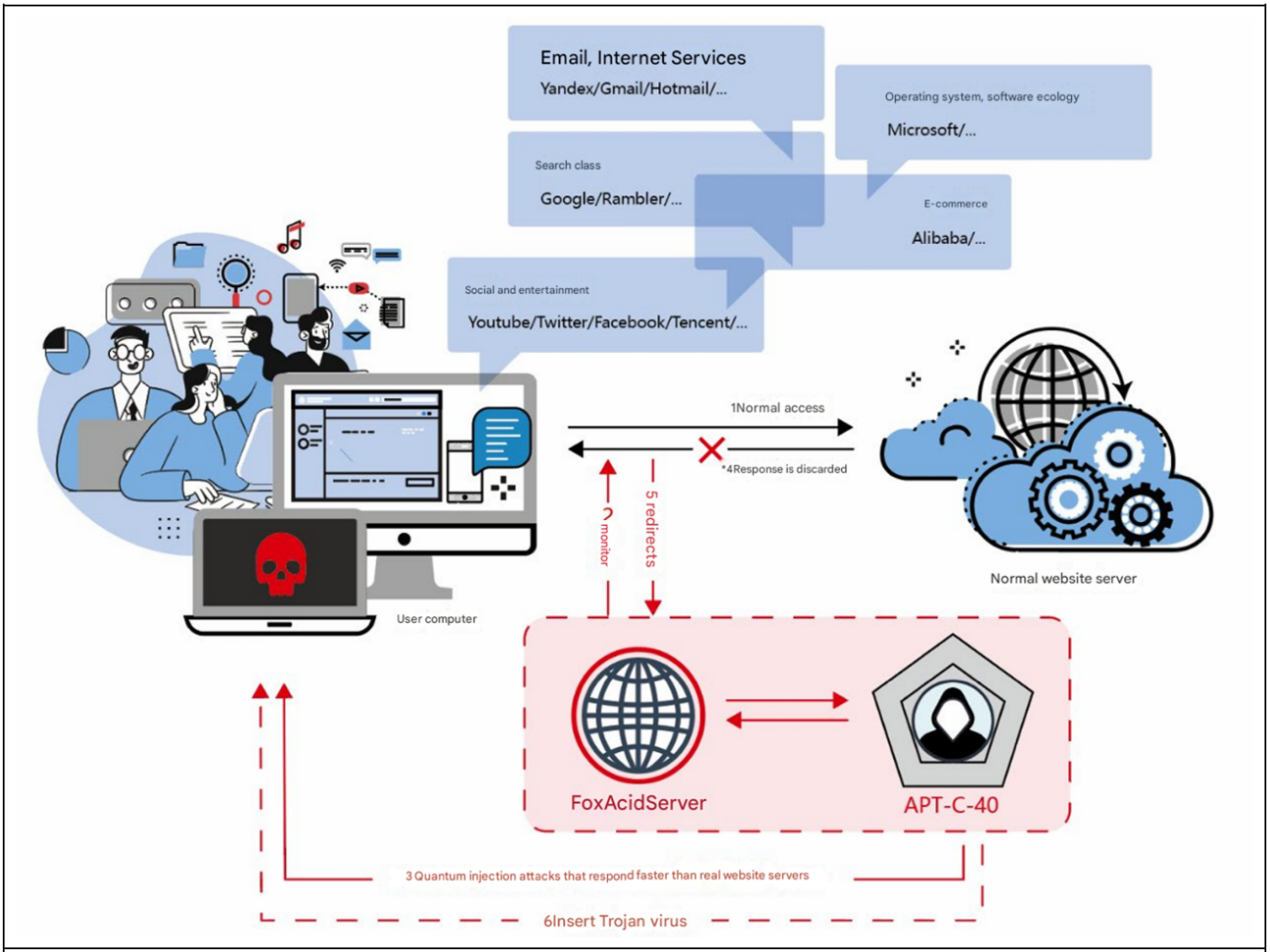
The proprietary tool that was alleged to be run:

SHAVER: This tool was used to attack the SunOS exposed servers that were used for the jump servers. This was identified as an automated exploitation tool designed for x86 and SPARC architectures with RPC services enabled.

2. Initial Access into the University

To gain access into the network, they leveraged MiTM and spear phishing emails. Around April, there were phishing emails identified with references to “scientific research review” targeted towards members of the University (students and teachers). These phishing emails contained malware embedded in them and some were designed to steal credentials from these users.

Aside from this, 360 and CVERC also reported that one of the platforms used was a platform coined as [“FOXACID” which was a part of the Snowden leaks](). This platform according to Wikileaks, 360 and CVERC is a 0-day vulnerability attack platform designed by the NSA to automate delivery of browser (IE, Chrome, FireFox, Safari, Android Webkit etc) exploits to workstations, servers and mobile devices. When a user tries to access a website like Gmail, BiliBili (Chinese YouTube) instead of the normal server response, the response is hijacked to redirect to APT-C-40 (NSA) controlled server which injects malware onto the user’s browser. Below is a diagram 360 drew of how it works (I translated it into English with Google).



Qihoo 360 - Diagram

The question would be “how did they use FOXACID” without having compromised systems? Based on the reports it seems like this is a logical sequence of events:

External servers of the University were compromised giving APT-C-40 foothold into the environment using a tool called ISLAND (manual exploitation of Solaris systems)

APT-C-40 installed a framework called SECONDDATE an espionage software designed to be installed on network devices (gateways, border routers and firewalls). There is a server and control side to the tool. The server is run on the network edge device and the traffic is monitored/ tampered through a driver. The communication back to controller is encrypted and the port used is randomised. Second date has capabilities of network eavesdropping, MiTM, and code injection. It can be used with other malware to perform espionage activities. It's primarily used to hijack mass amounts of data traffic, tampering and misdirection.

SECONDDATE redirects traffic from users within the University network accessing popular sites like BiliBili to FOXACID platform which performs the browser exploitation on the student/staff devices to gain control.

Using this MiTM platform, they allegedly hijacked internal hosts and servers of the University before deploying further tools for remote control of the systems. This allowed them access into core network equipment, servers and terminals relating to ops and maintenance of the University network. Of interest (and this appears to be a pattern), APT-C-40 (according to 360 and CVERC) had a keen interest on network devices like routers and switches.

The proprietary tools that were alleged to be run include:

ISLAND: This tool was allegedly run against the University's external servers to gain control. It is a manual exploitation tool used to breach Solaris-based systems.

FOXACID: Browser exploitation framework that fingerprints the browser and deploys a 0-day.

SECONDDATE: This tool was allegedly used by TAO (NSA) to hack into the office intranet of the University. Attribution of SECONDDATE was discovered through collaboration with other industry partners. They found thousands of network devices running this spyware – where the communications went back to NSA servers located in Germany, Japan, South Korea and Taiwan. This tool was used to redirect user traffic to the FOXACID platform.

3. Persistence and Lateral Movement

After securing initial access, APT-C-40 focused on long-term persistence and lateral movement across the university's network. To avoid detection, they allegedly deployed a combination of backdoors and credential theft techniques.

SECONDDATE – Backdoor installed on network edge devices such as gateways and border routers to filter, and hijack mass amounts of data in a MiTM. This was placed on the border routers of the University to hijack traffic to redirect to NSA's FOXACID platform.

NOPEN: A remote-controlled malware that provided NSA operators with ongoing access to compromised systems. It allowed for file execution, process management, system command execution, and privilege escalation. TAO used this to gain persistent control over core business servers and key network equipment.

FLAME SPRAY - Windows-based remote-controlled malware with strong anti-analysis features. Can be customized to generate different types of servers. Works with the "Acid Fox" platform to control personal office network hosts. It has strong anti-analysis/anti debug capabilities.

CUNNING HERETICS: A lightweight implant that established encrypted communication channels for NSA to remotely reactivate access points even after clean up attempts.

STOIC SURGEON: A stealthy backdoor targeting Linux, Solaris, JunOS, and FreeBSD systems, enabling the NSA to maintain control while avoiding security audits.

4. Lateral Movement Techniques:

There was a keen focus from APT-C-40 on targeting edge network devices. From the IR perspective this makes complete sense (lack of EDR, lack of logs, lack of visibility and differing OS's makes investigation at scale incredible difficult and very manual). At this stage of the attack, they used legitimate credentials to access firewall appliances and focused a portion of the attacks on the telecom operators of the University. This was highlighted by 360 and CVERC as their method of fingerprinting and accessing personal data related to key researchers.

Legitimate Credentials: NSA allegedly used legitimate credentials for the Cisco PIX firewall, Tianrongxin firewall and other equipment to scope out the intranet, monitor data, control the SMS gateway and telecom operators. They then relied on other tools like MAGIC SCHOOL to query sensitive personnel, encrypted the information and exfiltrated it. The result of the queried data was saved to: var/tmp/.2e434fd8aeae73e1/erf/out/f/ before being encrypted and exfiltrated.

Hijacking Intranet Upgrade Programs: The NSA allegedly compromised software update mechanisms to distribute malware disguised as legitimate updates.

Credential Harvesting via the tool DRINKING TEA: This tool sniffed SSH, Telnet, and Rlogin passwords used by university IT administrators, granting NSA full access to internal systems. NSA allegedly used this to capture command-line logs, passwords generated by University staff during their operation and maintenance work. This data was them compressed and encrypted for exfil by NOPEN. These credentials then gave them more access to edge devices and business devices.

Hijacking Border Routers: NSA installed Second Date spyware on university routers, allowing them to intercept, manipulate, and reroute network traffic.

5. Data Exfiltration: Stealing Critical Research and Credentials

Once inside, NSA operatives allegedly systematically stole classified research data, network infrastructure details, and sensitive operational documents.

Exfiltration Methods Used:

OPERATION BEHIND ENEMY LINES: A suite of tools used to query, package, and encrypt stolen data before transmitting it to NSA-controlled servers.

School of Magic, Clown Food, and Cursed Fire: These NSA tools were specifically designed for extracting sensitive files from telecom and defense research systems.

Use of Proxy Servers & VPNs: To avoid detection, stolen data was routed through 54 jump servers and proxy nodes in 17 countries, masking the true origin of the attackers.

6. Evasion and Anti-Forensic Measures

To minimize the risk of detection and forensic investigation, the NSA employed several anti-forensic techniques (but most of these are inbuilt in the tools and frameworks they leveraged):

TOAST BREAD: A log manipulation tool that erased evidence of unauthorized access, including UTMP, WTMP, and LASTLOG files.

Encrypted Communications: All NSA tools leveraged encryption, ensuring that traffic to their command-and-control (C2) servers remained undetectable.

What did I learn from this?

There is a clear and structured collaboration amongst Chinese cybersecurity organizations during casework. While industry collaboration exists in the West through closed invite-only groups, Chinese cyber organizations openly acknowledge and publicize their partnerships. This openness was particularly interesting to observe and may be influenced by cultural factors, such as the Confucian emphasis on shared knowledge and a political framework that encourages collective efforts. Additionally, this collaboration extends across borders, involving cybersecurity entities from multiple countries.

In the Incident Response process, Western methodologies typically focus on constructing a super timeline of an attack, detailing events in chronological order. We compile timelines, document indicators of compromise (IoCs), and hand off reports to intelligence teams, often accompanied by a verbal debrief. However, large-scale data analysis using AI across multiple cases—or even on a single case—is not a standard practice. A key observation from the Chinese case notes was the extensive use of big data analysis, particularly in tracking “hands-on keyboard” activity. This approach enabled Qihoo 360 to identify patterns, such as the alleged absence of activity on Memorial Day, and precisely documenting the operational hours of the attackers, allowing 360 to isolate activity to Monday-Friday, EST working hours.

Attacks on edge devices, IoT, and network appliances appear to be becoming the norm. From a threat actor’s perspective, this makes complete sense. Most adversaries are aware that XDR/EDR solutions are deployed on traditional endpoints, making edge devices an attractive target for initial access and persistence. Defending and detecting such threats is particularly challenging due to the variety of operating systems, proprietary encoding methods, and the extensive manual forensic analysis required. The focus on edge devices is not unique to the NSA—it is an emerging trend that is likely to escalate. We have already seen Chinese APTs and Russian actors adopting similar techniques, including firmware manipulation. It will be interesting to see how this space evolves.

Finally, across the reports, there were sporadic mentions that most of the attack frameworks operated in-memory, with no files written to disk. This is not abnormal to see – however, it is interesting always to observe how the investigation and forensics was done. One area I wish had been covered in more detail was the methodology used to investigate these attacks, particularly how IR teams conducted forensic analysis on edge devices and routers.

Alleged NSA IoCs

The IPs are redacted by 360 and CVERC (not me).

NSA IPs (Purchased through cover companies):

209.59.36.xx
69.165.54.xx
207.195.240.xx
209.118.143.xx

Weapon Platform IPs (C2 Servers):

192.242.xx.xx (Colombia)
81.31.xx.xx (Czech Republic)
80.77.xx.xx (Egypt)
83.98.xx.xx (Netherlands)
82.103.xx.xx (Denmark)

IPs Used to Launch Attacks:

211.119.xx.xx (Korea)
210.143.xx.xx (Japan)
211.119.xx.xx (Korea)
210.143.xx.xx (Japan)
211.233.xx.xx (Korea)
143.248.xx.xx (Korea - Daejeon Institute of Science and Technology)
210.143.xx.xx (Japan)
211.233.xx.xx (Korea)
210.143.xx.xx (Japan)
210.143.xx.xx (Japan)
210.143.xx.xx (Korea - Korea National Open University)
211.233.xx.xx (Korea - KT Telecom)
89.96.xx.xx (Italy - Milan)
210.143.xx.xx (Japan - Tokyo)
147.32.xx.xx (Czech Republic - Brno)
132.248.xx.xx (Mexico - UNAM)
195.162.xx.xx (Sweden)

210.143.xx.xx (Japan - Tokyo)
210.228.xx.xx (Japan)
211.233.xx.xx (Korea)
212.187.xx.xx (Germany - Nuremberg)
222.187.xx.xx (Germany - Bremen)
210.143.xx.xx (Japan)
91.217.xx.xx (Finland)
211.233.xx.xx (Korea)
84.88.xx.xx (Spain - Barcelona)
210.143.xx.xx (Japan - Kyoto University)
132.248.xx.xx (Mexico)
148.208.xx.xx (Mexico)
192.162.xx.xx (Italy)
211.233.xx.xx (Korea)
218.232.xx.xx (Korea)
148.208.xx.xx (Mexico)
61.115.xx.xx (Japan)
130.241.xx.xx (Sweden)
210.143.xx.xx (India)
210.143.xx.xx (Japan)
202.30.xx.xx (Australia)
220.66.xx.xx (Korea)
222.122.xx.xx (Korea)
141.57.xx.xx (Germany - Leipzig Institute of Economics and Culture)
212.109.xx.xx (Poland)
210.135.xx.xx (Japan - Tokyo)
148.208.xx.xx (Mexico)
82.148.xx.xx (Qatar)
46.29.xx.xx (UAE)
143.248.xx.xx (Korea - Daejeon Institute of Science and Technology)

SecondDate CnC

MD5: 485a83b9175b50df214519d875b2ec93
SHA-1: 0a7830ff10a02c80dee8ddf1ceb13076d12b7d83
SHA-256: d799ab9b616be179f24dbe8af6ff76ff9e56874f298dab9096854ea228fc0aeb

SOURCES

https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm

https://mp.weixin.qq.com/s/CfkLGhqLB3hyVcDzqUQwJQ

https://www.secrss.com/articles/54025

https://www.cverc.org.cn/head/zhaiyao/news20220629-FoxAcid.htm

https://www.aclu.org/documents/foxacid-sop-operational-management-foxacid-infrastructure

https://nsarchive.gwu.edu/document/22069-document-01

https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

https://m.thepaper.cn/wifiKey_detail.jsp?contid=20362635&from=wifiKey

http://www.ce.cn/xwzx/gnsz/gdxw/202209/27/t20220927_38130496.shtml

https://world.huanqiu.com/article/4EX89Zq6zNg