< Lie to me />

Volt Typhoon II:

A secret Disinformation Campaign targeting U.S. Congress and Taxpayers conducted by U.S. Government agencies

National Computer Virus Emergency Response Center
National Engineering Laboratory for Computer Virus Prevention Technology
360 Digital Security Group

July 8, 2024

Executive summary

After the investigation report of Volt Typhoon is released by National Computer Virus Emergency Response Center of China, manipulated by the U.S. government agencies, all main-stream medias of U.S. remain silence and no comment, take measures of covering up evidence and inside-detection. All these actions reveal the fact of U.S. government agencies hypes up "Volt Typhoon" false narrative for swindling more budgets from the congress. In response to concerns of the international community and cybersecurity research entities, we decide to make full disclosure of the "Volt Typhoon" campaign and reveal the truth behind the scenes. The "Volt Typhoon" is a misinformation campaign targeted U.S. congress and taxpayers. It was planned and conducted by U.S. intelligence agencies. The object of the campaign is to preserve U.S. intelligence agencies' warrantless snooping powers on all people over the world including Americans via FISA Section 702, so that the U.S. government agencies could eliminate the foreign competitors and defend the cyber hegemony and long-term interests of monopolies.

1 Introduction

On April 15, 2024, National Computer Virus Emergency Response Center, National Engineering Laboratory for Computer Virus Prevention Technology and 360 Digital Security Group joint released an investigation report[1] named "Volt Typhoon： A Conspiratorial Swindling Campaign targeting U.S. Congress and Taxpayers conducted by U.S. Intelligence Community" and reveal the fact that the hacker group so-called "Volt Typhoon" is actually a ransomware group. Officials from U.S. intelligence and some corrupt politicians joint manipulated cybersecurity firms to fabricate narratives for exaggerating the cybersecurity threats from abroad and cheat U.S. congress members and taxpayers, who without expertise, to pay the sham budget bill. Medias has reached out to the US Embassy in China and Microsoft for comment on the report, but has no response. It's no surprised that, all main-stream media in the U.S. received gag orders from the U.S. Agency for Global Meida (USAGM), which is a federal propaganda agency.

The response finally come, on April 18, FBI director Christopher Wary take a speech on Nashville's Vanderbilt University. He claimed that the Chinese government-backed hacker group "Volt Typhoon" had compromised lots of U.S. critical infrastructure entities across the telecommunications, energy and water and others. The "speech" soon saturated the U.S.

[1] https://www.cverc.org.cn/head/zhaiyao/news20240415-FTTF.htm

media, which was apparently a successful propaganda operation. Inspired by the speech, we are able to see the whole picture of the "Volt Typhoon" campaign with lots of co-related evidence and tradecrafts.

The "Volt Typhoon" is a misinformation campaign which was initiated no later than the beginning of the year 2023. It was secretly and well planned by NSA, FBI and other agencies belong to the U.S. intelligence community with multiple federal agencies including DOJ, DOD, DOE, DHS getting involved, and supported by intelligence and cybersecurity authorities from other Five Eye countries. It is a typical cognitive warfare operation, but unfortunately, the targets of the operation were U.S. taxpayers, U.S. congress and ex-president Donald Trump and other domestic opponents of current U.S. administration. During the operation, U.S. intelligence abuse their power to manipulate cybersecurity firms and other agencies, intimidate the American people and congress members with hyping the "China threat theory" and silence the domestic opponents. The object of the campaign is to preserve the warrantless snooping powers on all people home and abroad via FISA Section 702 and get more budget for boosting abilities of offensive cyber operation and surveillance.

"Volt Typhoon" is a real case of "HOUSE of CARDS". Although its main targets are U.S. congress and American people, it also attempt to defame China, sow discords between China and other countries, contain China's development, and rob Chinese companies. Apparently, the U.S. government intend to divert the antagonistic problems at home with misinformation operations. In this report, we disclose the evidence and the whole picture of the evil plan including the details of the operation procedures to the world.

2 Self-contradiction and Covering up

Having a hidden agenda, "Volt Typhoon" is well planed by U.S intelligence. However, it is so difficult to coordinate all participants and resistance is inevitable, which give us a chance to have breakthrough in our investigation.

When the first investigation report was released, in order to cover up, U.S. intelligence manipulated ThreatMon to modify their report related to the ransomware group "Dark Power", just like a cat shuts its eyes when stealing cream. Besides that, we also found a lot of contradictions between actions and speeches of U.S. government officials and politicians.

More relationships were found between "Dark Power" and U.S. made "Volt Typhoon"

We have presented the relationship between the ransomware group "Dark Power" and U.S. made "Volt Typhoon" in the first investigation report based on research in the IoCs from the Microsoft's technical analysis report[2] and the alert notifications of the FVE[3]. We quoted

[2] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[3] https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

the report[4] "The Rise of Dark Power: A Close Look at the Group and their Ransomware" published by ThreatMon (a U.S. based cybersecurity firm) and found the IP addresses related to the group which were hidden behind the back cover. It is so absurd that, after we published the first investigation report, ThreatMon modified their report, the new version of report was expanded to 20 pages, but the IP addresses were eliminated from the back cover page. However, the directory remains the same. As Shown in Figure 1, 2, 3 and 4.

Figure 1 Previous back cover of TheatMon's report

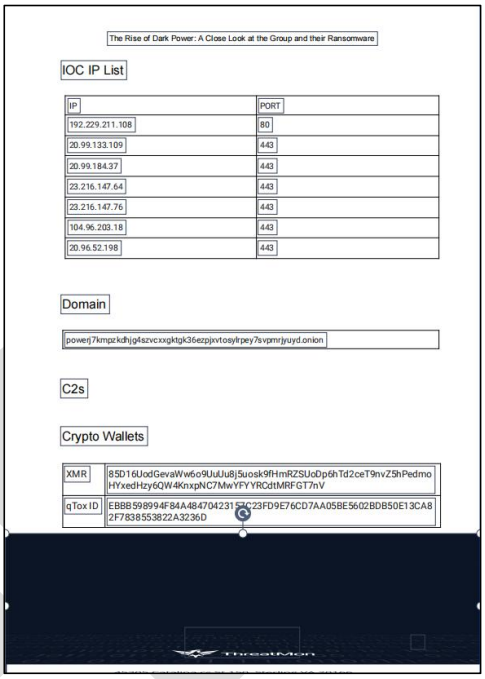


Figure 2 The IoCs hiddden behind the previous back cover picture

[4] https://threatmon.io/the-rise-of-dark-power-a-close-look-at-the-group-and-their-ransomware/ https://threatmon.io/storage/the-rise-of-dark-power-a-close-look-at-the-group-and-their-ransomware.pdf

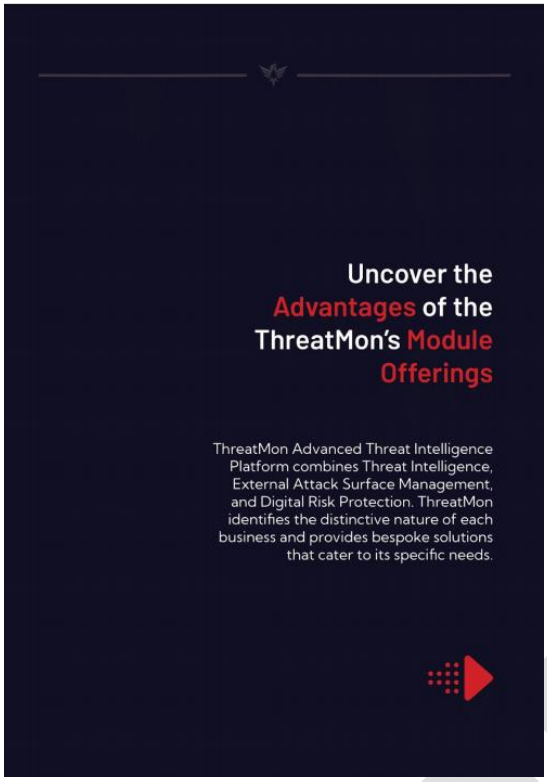


Figure 3 Back cover of new version of the TheatMon's report

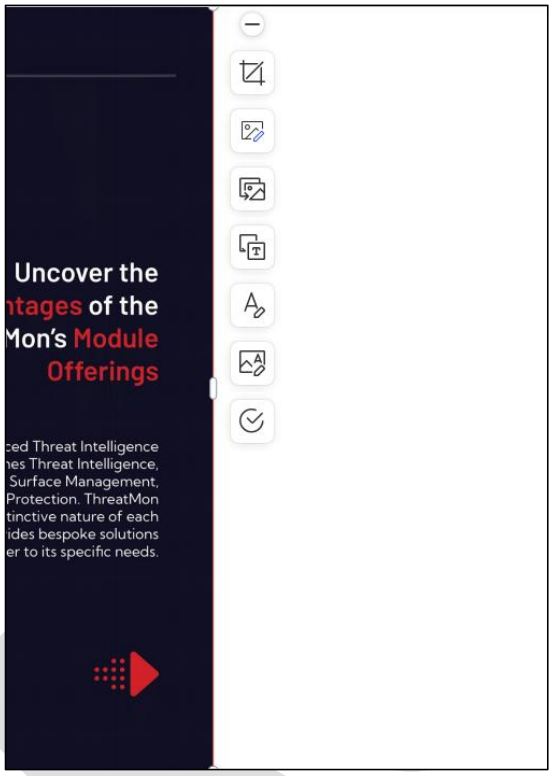


Figure 4 IP list is missing

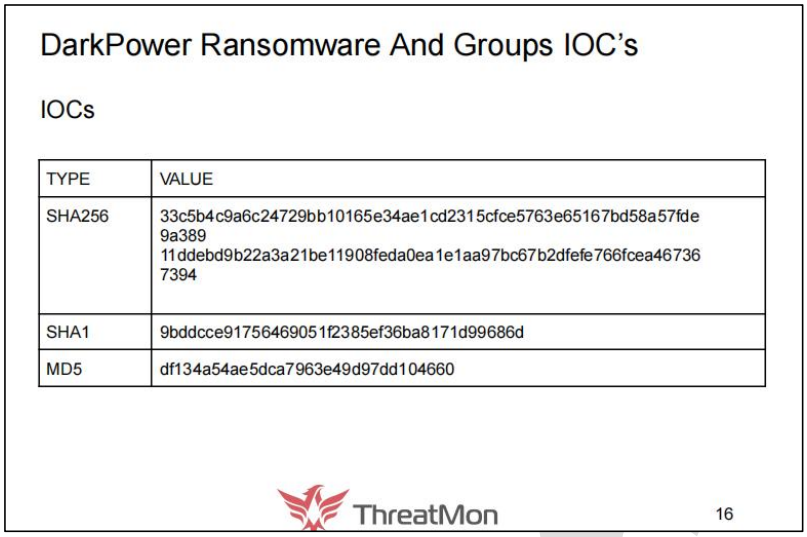
We will attached the latest and original version of ThreatMon's report for the convenience to compare by readers.

Apparently, U.S. intelligence have a guilty conscience and manipulate ThreatMon to falsify the report under desperation. Facts speak louder than words, covering up doesn't work. Actually, ThreatMon is not alone in tracing the "Dark Power". A report[5] named "Shining Light on Dark Power: Yet Another Ransomware Gang" released by Trellix, which is also a U.S. cybersecurity firm merged by McAfee and FireEye, also presents the technical details of ransomware belongs to "Dark Power" group. The conclusion of these two reports are totally the same, including the hashes of the ransomware samples. As shown in Table 1, Figure 5 and Figure 6.

Table 1 Hashes of ransomware samples belong to "DarkPower"

No.	HASH
1	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389
2	11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394

[5] https://www.trellix.com/blogs/research/shining-light-on-dark-power/



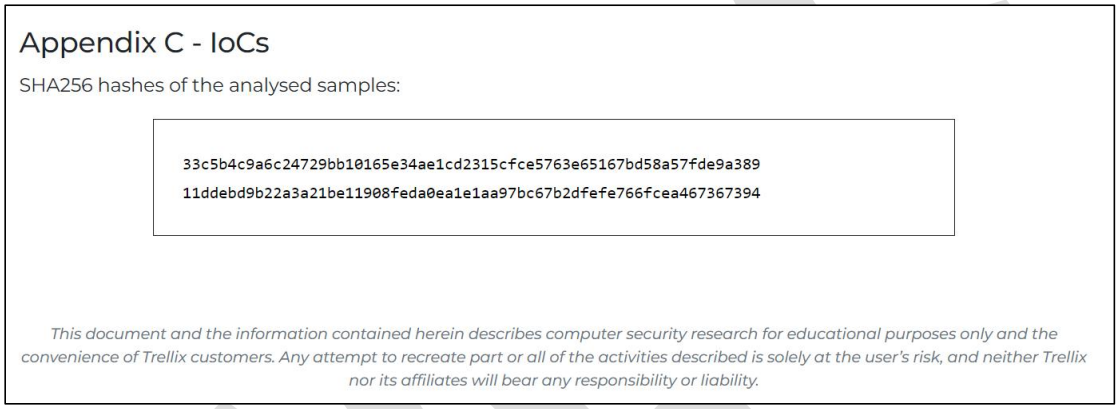
DarkPower Ransomware And Groups IOC's

IOCs

TYPE	VALUE
SHA256	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394
SHA1	9bddcce91756469051f2385ef36ba8171d99686d
MD5	df134a54ae5dca7963e49d97dd104660

ThreatMon 16

Figure 5 Hashes from report of ThreatMon



Appendix C - IoCs

SHA256 hashes of the analysed samples:

33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389
11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.

Figure 6 Hashes from report of Trellix

We used VirusTotal[6] again to analyze the samples and find out that those two samples all connected with the five IP addresses which were discussed in the previous investigation report. As shown in Figure 7 and Figure 8, the process can by easily repeated by researchers from all over the world. We have to think about that, is there any possibility of Chinese users will be banned to use VT under the pressure of U.S. government agencies ?

[6] https://www.virustotal.com/gui/graph-overview

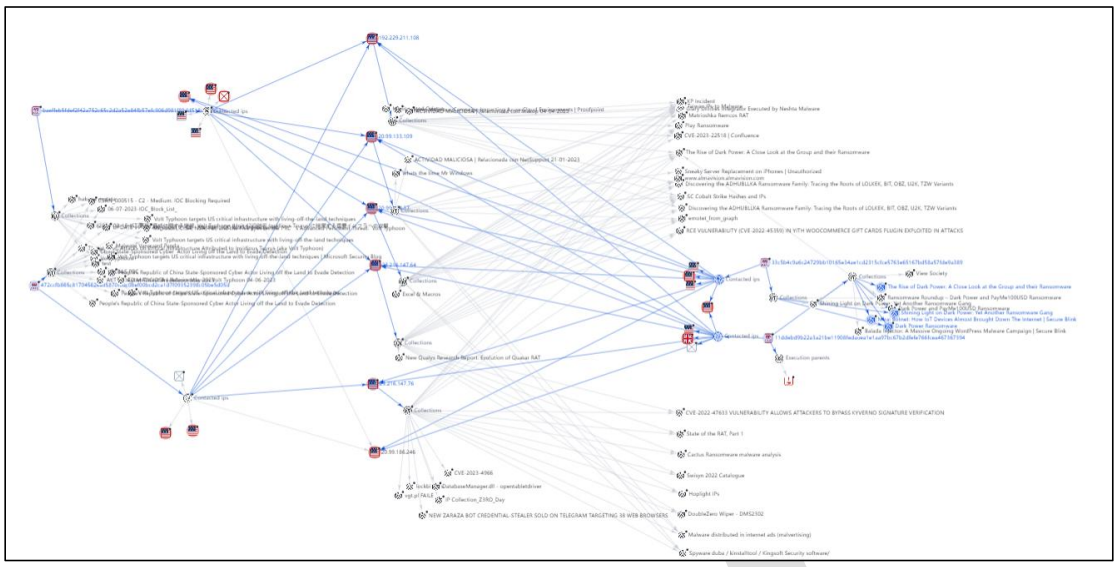


Figure 7 The relationship between malware samples of "Dark Power" and U.S. made "Volt Typhoon" 1 of 2

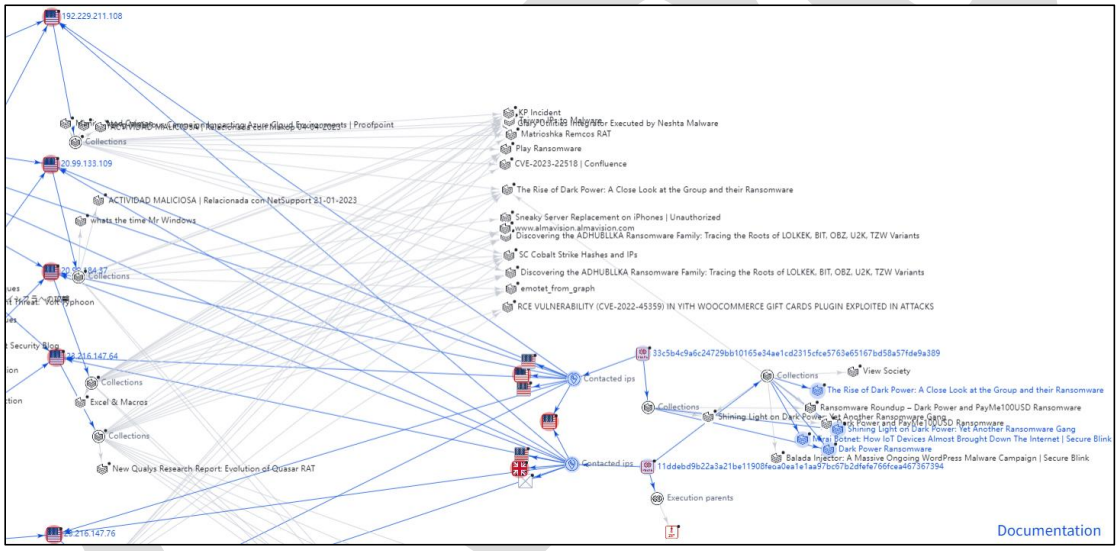


Figure 8 The relationship between malware samples of "Dark Power" and U.S. made "Volt Typhoon" 2 of 2

According to anonymous source from ThreatMon, they had to recall the previous version of the "Dark Power" report and erase the IP list. In fact, as stakeholders, it is very common that cybersecurity firms in U.S. manipulated by intelligence agencies. However, they met some resistance from ThreatMon. "Covering up" the IP list with a "Dark" back cover picture is a good metaphor. We must pay our respects to the honest person, and everyone reading this report should do it as well.

Inconsistency between U.S. government agencies and cybersecurity firms

In the joint Cybersecurity Advisory about "Volt Typhoon", the cybersecurity authorities from Five Eyes countries claimed that "Volt Typhoon" exploited network devices manufactured by

NetGear and other vendors and used them as hops, so did the reports from Microsoft. However, on May 26, 2023, just two days after the reports released, NetGear publish a security advisory[7] regarding "Volt Typhoon", and made a explicit statement that they "are not aware of any NETGEAR product vulnerabilities being exploited by Volt Typhoon", as shown in Figure 9.

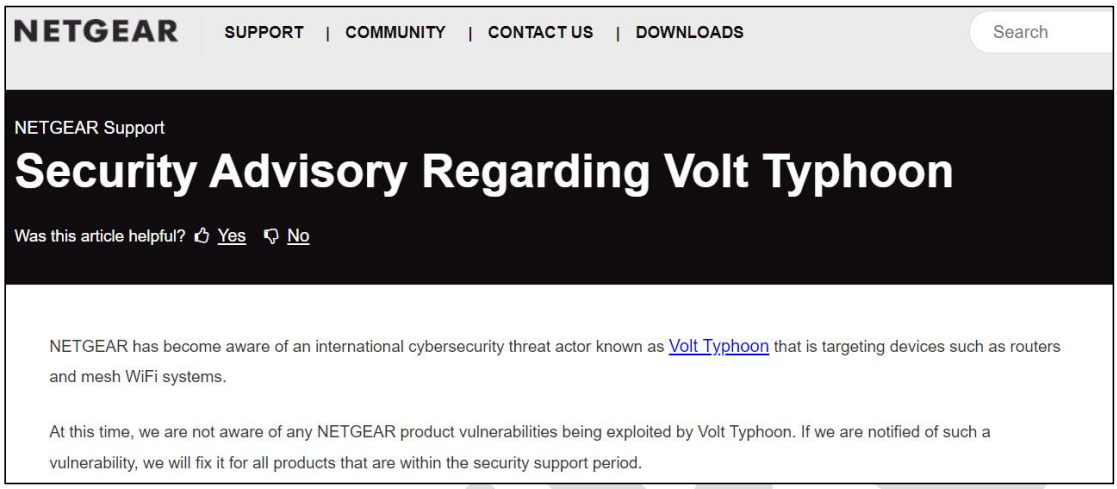


Figure 9 Security Advisory of NetGear

On February 7, 2024, the CISA issued another cybersecurity advisory[8] related to the "Volt Typhoon" named "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure", and declared that the "Volt Typhoon" group has compromised the IT environments of multiple critical infrastructure organizations, including communications, energy, transportation systems, and water and wastewater systems sectors in the continental and non-continental U.S. and its territories. Besides that, more details were provided by the advisory, which said that "Volt Typhoon" exploited the vulnerabilities of Ivanti Connect Secure VPN. But in April 5, another U.S. based cybersecurity firm Mandiant , which belong to Google, released a paper[9] named "Cutting Edge, Part 4:Ivanti Connect Secure VPN Post Exploitation Lateral Movement Case Studies" , and point out that they found and tracked an "uncategorized" threat group called "UNC5291", which they assess with medium confidence to be "Volt Typhoon". In addition, Mandiant said that they has not directly observed Volt Typhoon successfully compromise Ivanti Connect Secure. As shown in Figure 10.

From above, it is not difficult to conclude that, the view of attribution about "Volt Typhoon" hold by Five Eyes and Microsoft were not widely accepted by other U.S. cybersecurity companies, and apparently, the cybersecurity authorities who led the investigation have not share the cases and critical technical details with related companies.

[7] https://kb.netgear.com/000065688/Security-Advisory-Regarding-Volt-Typhoon
[8] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
[9] https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

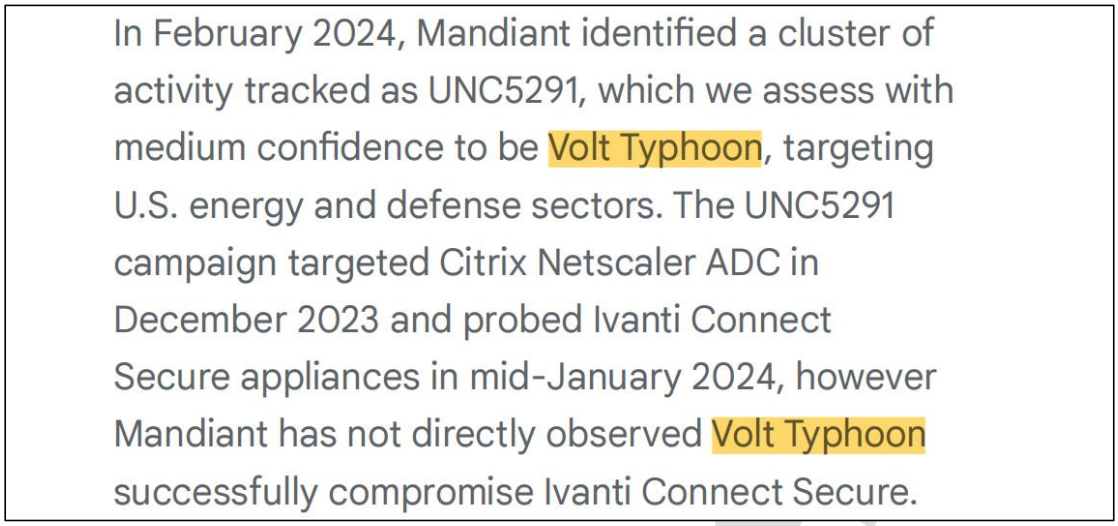


Figure 10 Part of the f Mandiant's paper

Self-contradiction movement of U.S cybersecurity authorities

As mentioned earlier in our previous report, the U.S DOJ released a press[10] titled with " U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure" on January 31, 2024. It is said that, in December 2023, a a court-authorized operation has disrupted a botnet of hundreds of U.S.-based routers hijacked by PRC state-sponsored hackers. In the press conference, officials from DOJ and FBI unanimously expressed that the operation disrupted the efforts of PRC state-sponsored hackers to gain access to U.S. critical infrastructures, including Attorney General Merrick B. Garland, FBI Director Christopher Wray, Assistant Attorney General Matthew G. Olsen of the DOJ's National Security Division. However, on April 18, 2024, FBI director Christopher Wary take a speech[11] on Nashville's Vanderbilt University and claimed that the Chinese government-backed hacker group "Volt Typhoon" had compromised U.S. critical infrastructure entities and waiting "for just the right moment to deal a devastating blow" . Since the so-called the PRC sponsored hackers has been disrupted in December 2023, why did FBI completely negate their own achievements in two months ? Or they just totally forgot it ?

Actually, fabricated by the U.S. government, the "Volt Typhoon" is meant to be a typical "unidentifiable" actor. Although lacks of specificity for attribution, it could be labeled to any actor. It is a good question that why U.S. government agencies desperately made up the so-called "State-Sponsored" hacker group in such ambiguous circumstance. It become clear when U.S. President Joe Biden signed a Act approved by congress.

3 Review "Operation Volt Typhoon"

[10] https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[11] https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/

In previous report, we had disclosed the truth of "Volt Typhoon" , which is a conspiratorial swindling campaign intended to "kill two birds with one stone" by hyping the "China threat theory" and cheating money from the U.S. congress and taxpayers. However, as known to all, trade power for money is the nature of the U.S. money-oriented politics, and budget application must be compliance with the department's functions, in hence, the power of the U.S. intelligent authorized by law is their lifeblood.

Date back to the beginning of the year 2023, as a major leader of the U.S. intelligence community, General Paul M. Nakasone, the then-commander of U.S. Cyber Command and Director and the Chief of National Security Agency, was worrying two major issues which going in a negative direction.

The first issue is the upcoming expiration of Section 702 of the Foreign Intelligence Surveillance Act[12], or FISA. Section 702 of FISA was about to expire at the end of the year 2023, which is the critical legal basis of the massive internet surveillance program target citizens from all countries and regions, including U.S, implemented by U.S. intelligence agencies. FISA is enacted by the U.S. congress in 1978, and it provides a statutory framework for U.S. intelligence agencies to obtain authorization to gather foreign intelligence. Section 702[13] was added to the FISA in 2008. It is widely recognized as a "Warrantless Surveillance Act" because of it authorized U.S. intelligence to engage in surveillance on non-American overseas without any court approval. It also force the internet giants, such as Google, Microsoft, Apple, Meta etc. , to hand in the private data of non-American users to the U.S. government agencies. The most notorious internet surveillance programme "Prism" which disclosed by Edward Snowden has been operating by U.S. NSA with the approval of FISA Section 702.

Nevertheless, FISA Section 702 has always been misusing by U.S. intelligence agencies, hence Although rather controversial, it was approved to renew in 2018, and continued to be valid until the end of 2023, under the request of U.S. intelligence agencies for the reason of counter-terrorism.

As is known to all, there has been great changes taken placed in the international and domestic situation of the U.S. since 2018. The terrorism is not the biggest threat of U.S. any more. In the National Security Strategy of the U.S., China, Russia, DPRK, and Iran has been recognized as major foreign adversaries. In addition, "Black Lives Matters" movement happened during the prevalence of COVID-19, and Capitol Hill riot happened after the president election on January 6, 2021. Under the circumstances, U.S. intelligence agencies has to face great challenges and pressure, especially in the domestic escalating political conflict. In hence, the misusing of FISA Section 702 is becoming increasingly serious. According to the Annual Statistical Transparency Report[14] Regarding the Intelligence

[12] https://crsreports.congress.gov/product/pdf/IF/IF11451
[13] https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf
[14] https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf#page=24

Community's Use of National Security Surveillance Authorities published by the Office of the U.S. Director of National Intelligence, FISA Section 702 has been misused over 200,000 times annually on Americans. U.S. intelligence agencies are also criticized by ex-president Donald Trump and his supporters for misusing the FISA Section 702 to help Democratic and Biden's administration spying on his election campaign. Meanwhile, lots of human right groups in the U.S. continue to call for repeal the Section 702. As a result, renewal of the Section 702 became uncertain.

If the Section 702 failed to be extended, the legal basis of U.S. intelligence agencies' internet surveillance and cyber warfare programs would be lost, and those programs had to go underground. The agencies' budgets and purchase orders would be reduced accordingly, which means a great unacceptable regression for the U.S. intelligence agencies, cybersecurity firms , military-industrial complex, and the capitals. The Five Eyes would become "Myopic Eyes".

The second issue is about the persecution on Chinese-funded firms. Nowadays, the productes and services of Chinese IT companies continues to gain popularity around the world, but have long been recognized as serious threats to the U.S. national security "theoretically" by the U.S. intelligence community. It is also unacceptable for the U.S. intelligence agencies leaving such lots of internet firms remains out of their control. Even if the FISA Section 702 renewal get approved, they most likely won't be as meek as U.S. firms, such as Google, Microsoft, Apple and Meta, etc. In hence, from the perspective of the U.S. government and intelligence agencies, it's urgent to kick Chinese IT firms out by any kinds of means as precaution.

January 12, 2023, General Paul M. Nakasone, the then-commander of U.S. Cyber Command and Director and the Chief of National Security Agency, took a public speech[15] and urged U.S. Congress for renewal of Section 702 and granting more power of surveillance to the intelligence agencies. He said that Section 702 has played an "irreplaceable" role in helping the agency fend off ransomware attacks and prevent weapons components from reaching adversaries, as well as being used to identify threats to U.S. troops. Not surprisingly, the main subject of the speech is cyber security. Nakasone is very clear that keep pushing the counter-terrorism theory does not work any more for the Congress. As an expedient measure, exaggerating cyber threats from abroad become the only option for conducting the social engineering attack against the Congress and American people.

Of course, it is not enough to earn trust from the members of congress only with verbal trick. "Great job" performance is essential as well. Under the circumstance, the U.S. intelligence community must united to defend their interests, and find a "one stone two birds" plan to deal with the problems mentioned above.

We named the plan and campaign "Operation Volt Typhoon" because the narrative about the "Volt Typhoon" hacker group is the crucial part of the plan. Based on the known

[15] https://therecord.media/nakasone-foreign-surveillance-program-helped-fend-off-cyber-attacks

information, "Operation Volt Typhoon" has been activated since the beginning of 2023 or even earlier. Such a massive operation which involved with multiple countries, departments, and private-owned firms must cost lots of time and resources. There are three stages so far as we observed.

Stage I: Preparation (from Jan 2023 to May 2023 approximately)

The priority job in the first stage is to "find" a cyber attack source from other countries, especially from China, Russia, DPRK and Iran, with victims in U.S. territory. In order to facilitates the operation, the attacker "should" be China State-Sponsored. Then, as victim, a critical infrastructure located in the U.S. territory or military bases "would be better". Furthermore, it would be the best if the victim's location is far away from public eye and full-controlled by U.S. Intelligence agencies. Follow the lines above, Guam must be the perfect victim. As a overseas territory, Guam has the largest U.S air force and navy base in the western pacific region, the location is extremely important to deter China in strategic. Half succeed would be achieved by just public announce that the facilities and communication of U.S military base located in Guam is under cyber attack by China. The cyber threat awareness and prevention solutions, which cost a lot of money, deployed in the military base would meet a failure at any suitable time, and let the critical infrastructures suffered real cyber attacks. As to the threat actor, an "unidentifiable" actorwould be the perfect scapegoat, and technical details should be given while the attribution should not be serious.

Next step, there must be someone push it to the public. Microsoft stepped up. Microsoft has been not going very well in business for the last a couple of years. In July 2021, under Biden's administration, U.S. Department of Defense canceled[16] a 10 billion contract of cloud computing program called Joint Enterprise Defense Infrastructure, aka. JEDI, which Microsoft has won it from Amazon and other competitors in 2019. Then, the U.S. DoD initiated a substitution program called Joint Warfighting Cloud Capability, aka. JWCC on Dec. 7 2022. The new program became a multi-vendor program, and the contract amount has been reduced to 9 billion. Microsoft has to compete with Amazon, Oracle and Google for more share of contract. Of course, Microsoft was not willing to lose the game that it had won before. Plus, Microsoft was aware of that, the main objective of JWCC is intelligence gathering and analysis. If Section 702 failed to be renewed, the following contract including the JWCC will be cut off. Microsoft must defend the budget and contract of the programs together with U.S. intelligence community.

Beside that, apparently an one-sided story can't be bought by the old hands of U.S. Congress. For more reliable, diverse sources are necessary. The intelligence agencies from Five Eyes countries are allies of interests. It is reasonable for conduct a joint action with each other.

On May 8, 2023, General Nakasone attended the Vanderbilt University Summit on Modern

[16] https://edition.cnn.com/2021/07/06/tech/defense-department-cancels-jedi-contract-amazon-microsoft/index.html

Conflict and Emerging Threats and said[17] that the U.S. will stick to strategy of "Defend Forward". He also pointed out that "U.S. clandestine community would suffer if Congress fails to renew Section 702 of the Foreign Intelligence Surveillance Act before the end of the year".

However, on May 19 2023, the U.S. Foreign intelligence Surveillance Court released a "Memorandum Opinion and Order"[18] which indicated that U.S. intelligence agencies had conduct surveillance operations violate the Section 702 during the chaos in Capitol Hill happened on Jan 6 2021 and the BLM movements in 2020.In order to ease the pressure from the court order, the U.S. intelligence agencies had to activate Operation Volt Typhoon immediately

On May 24 2023, after half-year planning, the highlight of the Operation Volt Typhoon arrived. The CSA[19] of Five Eyes and report[20] of Microsoft released to the public on the same day, then the medias, which controlled by U.S. intelligence community and the related Capitals, craft an elaborate narrative . It was successful diversion of the public's attention on the topic of misusing the Section 702.

Overall, the first stage of the operation had been going well and get off a good start for the next stage.

Stage II: Breakthrough (from June 2023 to January 2024 approximately)

More jobs were about to be done in the second stage, but two of them were critical. The first one would be making sure the Section 702 renewal get approved, the other one would be acquiring more budget in FY 2025. Inspired by Microsoft's showing off, Google[21], BlackBerry[22], CrowdStrike[23], Dragos[24] and Fortinet[25] join the operation and vie with each other for the next several months, which kept the topic hot. The reports from those firms were so multifarious that "Volt Typhoon" could be comparable to superheroes on the movie. It is thanks to the "unidentifiable" actor that so much imagination were given.

As the end of 2023 is getting closer and closer, the renewal of Section 702 is imminent. On December 5,2023, In a contentious Senate hearing, FBI director Christopher Wray personally

[17] https://therecord.media/nakasone-cyber-strategy-section-702-hunt-forward-russia-ukraine-nato
[18] https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf
[19] https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF
[20] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[21] https://cloud.google.com/blog/topics/threat-intelligence/chinese-espionage-tactics
[22] https://blogs.blackberry.com/en/2023/08/bb-protects-from-volt-typhoon
[23] https://www.crowdstrike.com/blog/falcon-complete-thwarts-vanguard-panda-tradecraft/
[24] https://hub.dragos.com/report/voltzite-espionage-operations-targeting-u.s.-critical-systems
[25] https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

to defend[26] Section 702, questioned by senators about abuses of spying on Americans, Christopher Wray repeatedly claimed that "section 702" is crucial to combat cyber crime and terrorism. But he didn't win the trust from all senators. Sen. Mike Lee said "We have no reason to trust you because you haven't behaved in a way that is trustworthy".

On December 8,2023, at an event[27] of the an Intelligence and National Security Alliance held in Arlington, Virginia, Nakasone again stood out and publicly urged for the US Congress to reauthorize Section 702.

On December 13,2023, Another vendor of the U.S. DoD, Lumen Technology stepped up and released a report[28] and claimed that the hacker group used the Internet of Things botnet named "KV-Botnet" as a hop in its cyber attack activities. At the request of the U.S. Agency for Global Meida (USAGM), the report once again sparked heated debate and a new round of "China threat theory" hype.

But that is still not enough, and opposition to the renewal of Section 702 remained high in the U.S. The U.S. intelligence agencies play a trick which was inclusion of Section 702 re-authorization in the National Defense Authorization Act (NDAA) which was a must-pass legislation. Although more than 30 social organizations in the United States signed a letter[29] to Congress requesting the removal of the Section 702 from NDAA, the bill was finally passed[30] on December 22, 2023, and Section 702 was extended to April 19, 2024. For the U. S. intelligence agencies, although they had not achieve the goal of long-term extension for Section 702, it was kind of a relief for a moment.

Another big challenge is to increase the budget for the next fiscal year. It must be fully prepared before the president submits the budget for the next fiscal year on February 5,2024. Therefore, on January 31,2024, when the US Department of Justice announced that it had successfully cleared KV-Botnets[31] from hundreds of routers across the country by organizing special operations. CISA and FBI jointly issued[32] "Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers", which claimed that, including the Chinese government sponsored "Volt Typhoon" group, hackers were targeting small commercial and home network equipment attacks, the U.S. government urged all related equipment manufacturers to strengthen security design and fix vulnerabilities.

The most important "show time" was also presented on January 31,2023, when the select

---

[26] https://www.usatoday.com/story/news/politics/2023/12/05/fbi-director-christopher-wray-702-surveillance-senate-judiciary/71813997007/

[27] https://www.c4isrnet.com/battlefield-tech/it-networks/2023/12/08/cyber-commands-nakasone-urges-enewal-of-foreign-spy-law/

[28] https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

[29] https://www.brennancenter.org/our-work/research-reports/coalition-letter-urges-congressional-leaders-keep-reauthorization-section

[30] https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=974

[31] https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[32] https://www.cisa.gov/resources-tools/resources/secure-design-alert-security-design-improvements-soho-device-manufacturers?utm_source=FBI&utm_medium=press_release&utm_campaign=SbD_SOHO

committee on the CCP of the U.S. House of Representatives held a hearing[33] titled "CCP Cyber Threat to the American Homeland and National Security" at the office building of the House of Representatives in Washington. The chairman of the special committee on China, Mike Gallagher chaired the meeting, The head of Big 4 of U.S. cybersecurity agencies attended the hearing as witnesses. By hyping the threats from so-called "China-sponsored" hacker group for gaining the resonance of congress. It was the highlight moment of the Operation Volt Typhoon. Christopher Wray, director of the FBI, declared[34] publicly at the hearing that "Section 702 is the most powerful tool for the FBI to combat Chinese hackers." It fully exposes the real purpose of the hearing, which is to seek the renewal of Section 702 under the guise of the so-called Chinese hacker cyber attacks, in order to keep the power of U.S. intelligence agencies to conduct "warrant-less surveillance" on global Internet users and related financial guarantee. It was embodied in the U.S. Federal government budget[35] for fiscal year 2025. This part has been detailed in our previous Volt Typhoon report.

At this point, the goal of the Operation Volt Typhoon was partially achieved, because the authorization period of Section 702 was only extended to April 19,2024, far from meeting expectations.

Stage III: Persistence (from February 2024 to April 2024 approximately)

As the deadline approaching again, the sounds of domestic opposition became louder and louder, the former President of the United States Donald Trump also claimed[36] that he has become the victim of Section 702 directly. American democracy fighter Snowden and Wikileak also called for the American people to oppose Section 702 being renewed again through the X platform.

At the same time, the U.S. intelligence agencies continued to hype the "China cyber threat theory" with the "Volt Typhoon" narrative according to the established plan, and once again took advantage of the "Five Eyes" intelligence cooperation mechanism to mislead public opinion for the renewal of the Section 702.

On February 7th, 2024, The U.S. Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security, together with the Department of Energy, the Environmental Protection Agency and other federal agencies, and other Five Eyes countries' cybersecurity authorities, jointly issued a security advisory[37] called "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure". The advisory hyped Volt Typhoon again, trying to divert attentions of the members of Congress

[33] http://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-ccp-cyber-threat-american- homeland-and-national-security

[34] https://selectcommitteeontheccp.house.gov/media/press-releases/chairman-gallaghers-opening-remarks-and-witness-testimony-2

[35] https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf

[36] https://thehill.com/policy/national-security/4584988-trump-on-warrantless-surveillance-reauthorization-kill-fisa/

[37] https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental -living-land

and the public, continue to render the false alarm about threat of Chinese cyber attacks. And at the relevant press conference held on February 7, according to Cynthia Kaiser[38], deputy assistant director for the FBI's cybersecurity division, FBI investigators used the Section 702 as a tool in monitoring and collecting data from the so-called hacker group from China against the key infrastructure attacks, but declined to give further details. This is further proof that the Operation Volt Typhoon is an important bargaining chip owned by U.S. intelligence agencies fighting for the renewal of Section 702. Moreover, the U.S. intelligence agencies can refuse to disclose the details of the attribution investigation on the grounds of confidentiality. and the current members of the U.S. Congress, as non-professionals, cannot make a correct judgment even if they see the so-called evidence.

The CISA keep playing the game, on March 19th, 2024, another cybersecurity alert[39] tiltled "PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders" was published. In the tone of an executive order, CISA have asked American critical infrastructure authorities to take precautions against the so-called "Volt Typhoon" attacks. Literally, the alert is a sequel of the previous cybersecurity advisor published by the Five Eyes Alliance, but in fact it was clearly a "warn" on critical infrastructures owned by private operators in the United States. It is well known that many of the U.S. critical infrastructure operators are private sectors, which have long been reluctant to add unnecessary investment in cybersecurity for their own interests. The CISA has been so bitter about it. For many American cybersecurity vendors such as Microsoft, the critical infrastructure cybersecurity solutions are "big cakes", and it should also be the reasonable reward for playing a big role of Operation Volt Typhoon. Therefore, the CISA did not hesitate to use its administrative power to "intimidate" these private units, forcing the private sector to increase their investment in cybersecurity, so as to win greater interests for the American cybersecurity enterprises and the capitalists behind them.

On April 9, 2024, a bill titled "Reforming Intelligence and Securing America Act", aka. RISAA, was submitted to the house of representatives, the bill proposed Section 702 extension for another two years, and further expand the Section 702 in the "electronic communication service provider" (ECSP) definition, which also means that Section 702 would authorize U.S. intelligence agencies to conduct surveillance program in a broader scope.

On April 12,2024, just before the voting of RISAA bill in U.S. House of Representatives, General Timothy Haugh, who has took over General Nakasone's position[40], made Posture Statement[41] on behalf of U.S. Cyber Command, which once again criticized that the cyber activities of China, Russia, Iran and DPRK were top threats to national security of U.S. and allies, and pointed out they are "particularly focused on defending against PRC's persistent access and pre-positioning for attack on U.S. critical infrastructures. Finally, after a tight vote, the U.S. House of Representatives approved the RISAA bill by 273-147 on April 12,2024.

---

[38] https://www.theregister.com/2024/02/09/fbi_volt_typhoon_section_702/

[39] https://www.cisa.gov/resources-tools/resources/prc-state-sponsored-cyber-activity-actions-critical-infrastructure-leaders

[40] https://defensescoop.com/2024/02/02/timothy-haugh-takes-over-cyber-command-nakasone/

[41] https://www.cybercom.mil/Media/News/Article/3739700/posture-statement-of-general-timothy-d-haugh-2024/

After the RISAA bill passed the House of Representatives, Americans have not stopped their efforts to veto it. On April 16,2024, more than 70 private organizations, including the Electronic Privacy Information Center (EPIC), signed a letter[42] to members of the U.S. Senate, asking the Senate to veto the bill. The U.S. intelligence agencies had to take it seriously.

On April 18,2024, the day before voting Section 702 extension bill in the senate, In order to manipulate public opinion and put more pressure on the senators, FBI director Christopher Wray took a speech again in Tennessee Vanderbilt University, and claimed that the China sponsored "Volt Typhoon" has successfully compromised many American companies, including 23 firms in pipeline transportation sector.

Finally, on the deadline of April 19,2024, the U.S. Senate passed the bill by 60-34 votes, which was quickly signed after it was submitted to U.S. President Joe Biden on April 20.

Meanwhile, another battle of beating Chinese IT firms has made a progess as well. Thanks to hyping "Volt typhoon" narrative, all the so-called cybersecurity threats related to China have been highly valued by the U.S. politicians.

On February 28,2024, president Joe Biden signed an Executive Order[43] to protect Americans' sensitive personal data from exploitation by "countries of concern", which intend to restrict China and other foreign strategic rivals access to sensitive personal data of U.S. The executive order requires the Department of Justice to issue regulations that establish clear protections for Americans' sensitive personal data from access and exploitation by countries of concern.

On the 13th day of March, 2024, The U. S. House of Representatives suddenly voted 352-65 to pass the H.R.7521 bill, called Protecting Americans from Foreign Adversary Controlled Applications Act, proposed by Mike Gallagher, then chairman of the U. S. Special Committee on China, which prohibits distributing, maintaining, or providing internet hosting services for a foreign adversary controlled application. Gallagher said he had been secretly preparing with his colleagues for eight months to prevent the bill from being leaked to the media in advance. According to the media, the main reason for the bill is that both Democratic and Republican lawmakers believe that Chinese IT companies pose risks to the national security of the US, which is also due to the Operation Volt Typhoon. On April 23,2024, Speaker of the House of Representatives Bill Johnson tied the bill into a series of emergency supplementary funding bills totaling $95 billion to aid Ukraine and Israel, before passing a Senate vote. Before the Senate vote, Mark Warner, chairman of the Senate Intelligence Committee and a famous anti-China politician, also delivered a speech to the Senate and claimed that the ordinary Americans could not know the "secret intelligence" provided by the US intelligence agencies, so they did not understand the Chinese IT products' risks "to the US national security". And advocated that those products "should not be owned or controlled by an

[42] https://epic.org/epic-coalition-urge-opposition-to-risaa-terrifying-expansion-of-fisa-section-702/

[43] https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/

'adversary' country recognized by American law." The so-called "secret intelligence" is bound to be the "result" of Section 702, and apparently a set-up on China, which is just a piece of cake for the US intelligence agencies with "warrant-less surveillance rights".

On April 24,2024, the bill was signed by U.S. President Joe Biden.

TikTok Immediately said it would use legal means to protect its rights, but facing the joint striking of the U.S. Congress, the U.S. government, intelligence agencies and monopoly capital, TikTok must be in a very difficult situation.

At this point, despite the process of difficulties and twists and turns, the U.S. intelligence agencies finally satisfied with Operation Volt Typhoon's overall victory. Over the next two years, American intelligence agencies will not only retain their power, secure higher budgets, expand surveillance, but also gain a great hope for getting rid of ByteDance.

At last, General Nakasone, who made great contribution to the Operation Volt Typhoon, retired in February 2024, but the U.S. government, intelligence community, cybersecurity firms and the capitalists behind them certainly know the truth of "not forgetting the people who dug the well". On June 13, 2024, OpenAI, the famous artificial intelligence innovation company and the founder of the "ChatGPT", announced the hiring of Nakasone as a member of the company's board of directors[44]. As we all know, OpenAI's largest shareholder is Microsoft. Obviously, Nakasone, as an executive of the company, will "help" OpenAI to better comply with the Section 702, while enjoying high salary. Moreover, on June 10, 2024, OpenAI announced a cooperation with Apple[45] to further integrate ChatGPT with Apple iOS, iPadOS and MacOS, including the Siri assistant and other writing tools that come with Apple's operating systems. The activities conducted by U.S. government entities and intelligence agencies has exposed their objective obliviously and also means the massive surveillance program of the "Empire of Hacking" has entered the "Era of AI".

As the principal indirect victim, China has not only suffered a grievance but also cyber attacks lunched by U.S. intelligence. On June 22, 2022, Northwestern Pyrotechnical University, which known for its education and research programs inf the fields of aeronautics, astronautics and marine technology engineering and located in Xi'an, Shaanxi province, China, called the police and made a statement that its internal servers had been suffered cyber attack in April, 2022. In September, 2022, China's National Computer Virus Emergency Response Center and cybersecurity company 360 released the investigate report which indicated that the cyber attack was conducted by U.S. NSA's Office of Tailored Access Operation, and also provided the whole picture, technical details, cyber warfare and TTPs(Tactic, Technique, Procedure). Beside that, on July 26, 2023, the Wuhan Municipal Emergency Management Bureau from Hubei province in China said in a statement that some of the network equipment of the front-end station collection points of the Wuhan Earthquake Monitoring Center, were subjected to a cyber attack by a overseas actor, the joint-investigate team of China identified

[44] https://www.theverge.com/2024/6/13/24178079/openai-board-paul-nakasone-nsa-safety

[45] https://openai.com/index/openai-and-apple-announce-partnership/

the actor as a state-sponsored group came from the U.S..

In addition, according to analysis on existing data, there has been more than 45 million cyber attacks activities from U.S. government sponsored hackers against to the Chinese government, universities, research institutions, large enterprises, and critical infrastructure, and the number of victims is more than 140. Tradecrafts collected from the victims' network have been proved to be related to cyber warfare program operated by U.S. Central Intelligence Agency (CIA), the National Security Agency and the Federal Bureau of Investigation departments with the Section 702 authorization.

4 Conclusion

The Operation Volt Typhoon once again exposed the essence of "money politics" in the United States, which is inevitable with the background of intensifying conflict in political and interests of the U.S. and the global hegemony that the United States is trying to maintain. The conspiracy, which the U.S. politicians intend to export their own problems for their own interests, is seriously harming China's interests and intolerable to all Chinese people.

In the next few years, we expect that, under the control of the U.S. intelligence agencies, more false "foreign government sponsored cyber attacks" narrative will be made by the cybersecurity companies, constantly cheat the U.S. congress approval more budget and increase the debt burden of American taxpayers. In fact, U.S. intelligence agencies and military agencies have long been colluding with related suppliers, fabricating false budgets, and wasting government funds from American taxpayers in buying high price but low quality products for their own benefits. Since the United States describes itself as the international "model of the rule of law" and a "Lighthouse of human rights", these politicians, officials and private enterprises involved in the collusion and fraud should pay the price for their illegal act. At the same time, we also advise U.S. politicians should mind their own business when dealing with domestic political issues, don't always take China as a "cover" for their own dirty jobs. They are better to abandon the ideas of isolate China and curb the development of China.

Finally, we also warn all countries and people who are pursuing peaceful development around the world that the U.S. Section 702 of FISA is an important legal basis for the U.S. to build the "Empire of Hacking". It is a serious threat not only to the American people, but also to the privacy of all ordinary people and sovereign security of all countries in the world, including China. We call on the governments and people of all countries to oppose and resist the hegemonism of the U.S. who taking the advantages of technology to undermine the sovereignty of other countries and the legitimate interests of its people.