Volt Typhoon:

A Conspiratorial Swindling Campaign targets with U.S. Congress and Taxpayers conducted by U.S. Intelligence Community

Apr. 15th, 2024

Executive summary

“Volt Typhoon” was labeled as a People's Republic of China State-Sponsored Cyber Actor by Microsoft and the cybersecurity authorities from The Five Eyes countries. But further analysis shows that the evidence of attribution is so insufficient that the actor has more correlation with ransomware group or other cybercriminals. Multiple cybersecurity authorities of U.S. made this fiction up together just for more budgets from the congress. Meanwhile, Microsoft and other U.S. cybersecurity companies also want more big contracts from U.S. cybersecurity authorities. The truth of “Volt Typhoon” is a conspiratorial swindling campaign which intended to “kill two birds with one stone” by hyping the "China threat theory" and cheating money from the U.S. congress and taxpayers.

1 Introduction

On 11:00 AM E.T. January 31, 2024, the hearing[1] of The CCP Cyber Threat to the American Homeland and National Security was held by the select committee on China of the U.S. House of Representatives in Washington. The hearing was hosted by the chairman of the special committee, the republican Mike Gallgher. The head of Big 4 of U.S. cybersecurity agencies attended the hearing as witnesses, including Paul Nakasong, then Commander of U.S. Cyber Command and Chief of National Security Angency (NSA), Jen Easterly, Director of Cybersecurity and Infrastructure Secruity Angency, Christopher Wray, Director of Federal Bureau of Investigation(FBI), Harry Coker,Jr. ,Director of Office of the National Cyber Director. At the beginning of the hearing, Mike Gallgher claimed that a People's Republic of China State-Sponsored Cyber Actor called "Volt Typhoon", which disclosed by Microsoft in May 2023 and , launched attacks on U.S. critical infrastructure sectors and trying to further damage, posed a serious threat to the U.S. national security. Later, the four witnesses further embellished it, depicting China as a "demon" who could readily subvert U.S. governments and even kill the American people by cyber attack and destroying critical infrastructures. Although we have long been used to the habitual tactics of a thief crying "stop thief" taken by United States politicians, such a spectacle is rare. We can not help wondering, who is "Volt Typhoon"? What is the evidence of its link to the Chinese government? Since the attacks were disclosed in May last year, why did US politicians challenge China again after eight months? This paper will explore the above issues, in order to clarify the truth.

2 Brief History of Volt Typhoon

On May 24th , 2023, the cybersecurity authorities from The Five Eyes countries, U.S., U.K., Australia, Canada and New Zealand, aka FVE, isssued a joint Cybersecurity Advisory[2] (CSA) titled by "People's Republic of China State-Sponsored Cyber Actor Living off the Land to

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

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

Evade Detection". The CSA said that, they had discovered cluster of activity of interest associated with a People's Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon, and this activity affected networks across U.S. critical infrastructure sectors. The CSA used a report from Microsoft as its main reference, which is "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques" written by Microsoft Threat Intelligence[3] and published on the same day of CSA. The report of Microsoft is also the source of the name of "Volt Typhoon", which come from the new threat actor naming taxonomy of Microsoft. Microsoft claimed that the Volt Typhoon is a state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft also introduced the tactics, techniques, and procedures (TTPs) of the actor. It is said that Volt Typhoon achieves initial access to targeted organizations through exploit internet-facing network devices such as firewalls and compromised SOHO network edge devices (including routers), then they rely on living-off-the-land(LOTL) commands for avoid-detection to take lateral-movement and exfiltrate data.

LOTL attack, also called file-less attack, is becoming a popular technique for bypassing AV detection. Unlike traditional malware attacks, LOTL do not require an attacker to install any code or scripts within the target system. Instead, the attacker uses tools that are already present in the environment, such as PowerShell, Windows Management Instrumentation (WMI) or the password-saving tool, Mimikatz, to carry out the attack. And the malicious code can be injected directly into memory without requiring anything to be written to disk.

Although the CSA and the report of Microsoft described the TTPs and IoCs of Volt Typhoon, they just labeled it a "China State-Sponsored Cyber Actor" without any attribution details. Once released, the reports were widely forwarded by major news media such as Reuters, Wall Street Journal and New York Times. The New York Times also reported[4] that United States intelligence agencies identified cyberattacks against telecom operator in Guam and other U.S. territory, and connected it with the CSA.

Until end of the year 2023, there is no news related. Suddenly in Dec. 13th , 2023 , the Black Lotus Labs team at Lumen Technologies, which is third large fixed network carriers in the U.S., released a report[5] titled with "Routers Roasting On An Open FireWall". In the report, Black Lotus Labs claimed that Volt Typhoon had used the KV-Botnet as hop and covert network, and the attribution was based on similar techniques used against victims based in Guam from August 2022 through May 2023, and both of them exploited NetGear devices. The Lumen's report became a trigger, U.S government then took a series of actions. In Jan 31st , 2024, U.S. Department of Justice released a press[6] titled with "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure", and said that the court-authorized operation had deleted the KV Botnet malware from hundreds

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

[4] https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html?searchResultPosition=1

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

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

of routers nationwide. In the same day of Jan 31st , 2024, CISA and FBI joint published a Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers[7], and pointed out that the guidance based upon "recent and ongoing activity targeting small office/home office (SOHO) routers by malicious cyber actors—particularly the People's Republic of China (PRC)-sponsored Volt Typhoon group". And then, don't forget the hearing held by the select committee on China of the U.S. House of Representatives in the same day also.

As a supplement, the name of "Volt Typhoon" is originated from the new threat actor naming taxonomy of Microsoft published in April 2023[8]. As shown in Figure 1, a weather event or "family name" represents either a nation-state actor attribution[9] , and Typhoon indicates origin or attribution to China. There are only 8 nation-state actors so far, and of course, none of them is FVE country.

Actor category	Type	Family Name
Nation state	China	Typhoon
	Iran	Sandstorm
	Lebanon	Rain
	North Korea	Sleet
	Russia	Blizzard
	South Korea	Hail
	Turkey	Dust
	Vietnam	Cyclone
Financially motivated	Financially motivated	Tempest
Private sector offensive actors	PSOAs	Tsunami
Influence operations	Influence operations	Flood
Groups in development	Groups in development	Storm

Figure 1. Threat actor naming taxonomy of Microsoft (Source: Official website of Microsoft)

From above, we can conclude that, the attribution of Volt Typhoon is mostly based on the report of Microsoft and CSA issued by FVE countries.

3 Is Volt Typhoon really a Nation-State Actor ?

As mentioned above, "Volt Typhoon" is named and attributed from the Microsoft's technical analysis report and the alert notifications of the FVE. Microsoft mentioned "the threat actor puts strong emphasis on stealth in this campaign", which increased the difficulty for

[7] ttps://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
[8] https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/
[9] https://learn.microsoft.com/zh-cn/microsoft-365/security/defender/microsoft-threat-actor-naming?view=o365-worldwide

Obtaining evidence and attribution. Although Microsoft and FVE didn't provide the detail of attribution, the Indicators of Compromise(IoCs) of the attacks were given at the end of both reports, which could lead us to take further analysis.

First of all, we made statistics of the sample information given by both reports. Totally, we got 29 samples after removing duplicates, as shown in Table 1.

Then, we used VirusTotal[10] (a Multi-engine Virus Scanner platform of Google, hereinafter referred to as "VT") to search the samples one by one. As a result, only 13 samples could be found, and each sample is associated with multiple IP addresses. Take sample 1 for example, the search results are shown in Figure 2.

Table 1. Samples related to"Volt Typhoon"

	SHA-256	**Source**
1	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	Microsoft
2	b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74	Microsoft
3	4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349	Microsoft
4	c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	Microsoft
5	d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af	Microsoft
6	9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a	Microsoft
7	450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267	Microsoft
8	93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066	Microsoft
9	7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5	Microsoft
10	389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	Microsoft
11	c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	Microsoft
12	e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	Microsoft
13	6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	Microsoft

[10] https://www.virustotal.com/

	SHA-256	Source
14	cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	Microsoft
15	17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4	Microsoft
16	8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	Microsoft
17	d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295	Microsoft
18	472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	Microsoft, FVE
19	3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	Microsoft
20	f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	FVE
21	ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872eb1d427ee27d31	FVE
22	d6ebde42457fe4b2a927ce53fc36f465f0000da931cfab9b79a36083e914ceca	FVE
23	66a19f7d2547a8a85cee7a62d0b6114fd31afdee090bd43f36b89470238393d7	FVE
24	3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	FVE
25	41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	FVE
26	c7fee7a3ffaf0732f42d89c4399cbff219459ae04a81fc6eff7050d53bd69b99	FVE
27	3a9d8bb85fbcfe92bae79d5ab18e4bca9eaf36cea70086e8d1ab85336c83945f	FVE
28	fe95a382b4f879830e2666473d662a24b34fccf34b6b3505ee1b62b32adafa15	FVE
29	ee8df354503a56c62719656fae71b3502acf9f87951c55ffd955feec90a11484	FVE

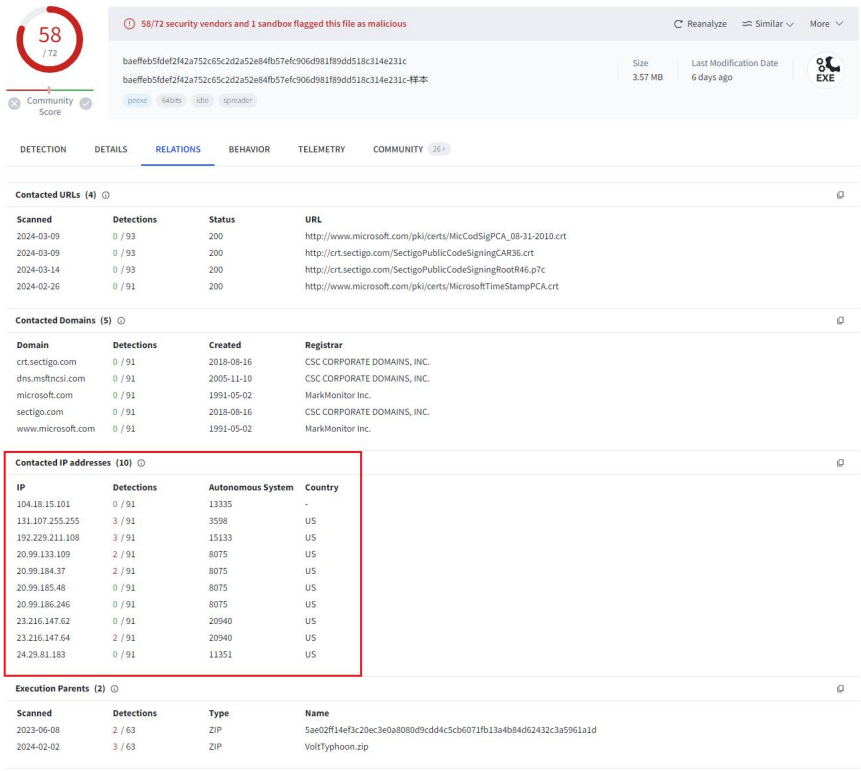


Figure 2. Search results of sample on VT

Repeating the above process, we found 13 samples link to multiple IP addresses, and each IP address links to multiple samples. The statistical results are shown in Table 2.

Table 2. IP addresses associated with samples

	IP	SHA-256	Source
1	192.229.211[.]108	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	Microsoft
2		c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	Microsoft
3		389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	Microsoft
4		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	Microsoft
5		e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	Microsoft
6		6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	Microsoft
7		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	Microsoft
8		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	Microsoft

	IP	SHA-256	Source
9		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	Microsoft、FVE
10		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	Microsoft
11		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	FVE
12		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	FVE
13		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	FVE
14	20.99.133[.]109	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	Microsoft
15		c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	Microsoft
16		389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	Microsoft
17		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	Microsoft
18		6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	Microsoft
19		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	Microsoft
20		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	Microsoft
21		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	Microsoft,FVE
22		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	Microsoft
23		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	FVE
24		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	FVE
25		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	FVE
26	20.99.184[.]37	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	Microsoft
27		c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d	Microsoft
28		389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61	Microsoft
29		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	Microsoft

	IP	SHA-256	Source
30		e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	Microsoft
31		6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	Microsoft
32		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	Microsoft
33		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	Microsoft
34		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	Microsoft,FVE
35		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	Microsoft
36		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	FVE
37		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	FVE
38		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	FVE
39	23.216.147[.]64	baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c	Microsoft
40		c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b	Microsoft
41		e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95	Microsoft
42		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	Microsoft
43		8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2	Microsoft
44		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	Microsoft、FVE
45		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	Microsoft
46		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	FVE
47		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	FVE
48		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	FVE
49	23.216.147[.]76	6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff	Microsoft
50		cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984	Microsoft

	IP	SHA-256	Source
51		472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d	Microsoft, FVE
52		3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642	Microsoft
53		f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd	FVE
54		3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	FVE
55		41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597	FVE

Whereafter, we used VT again to analyze the 5 IP addresses in the set, further discovered that these addresses are related to a lot of cyber attack events, and there are multiple IP addresses associated with the same cyber attack event or cybersecurity risk. One of them with connection of all 5 IP addresses is a Ransomware Group named Dark Power. And it is related to a report[11] "The Rise of Dark Power: A Close Look at the Group and their Ransomware" published by ThreatMon(a U.S. cybersecurity vendor located in VA) on April 11, 2023. Shown in Figure 3 and Figure 4.

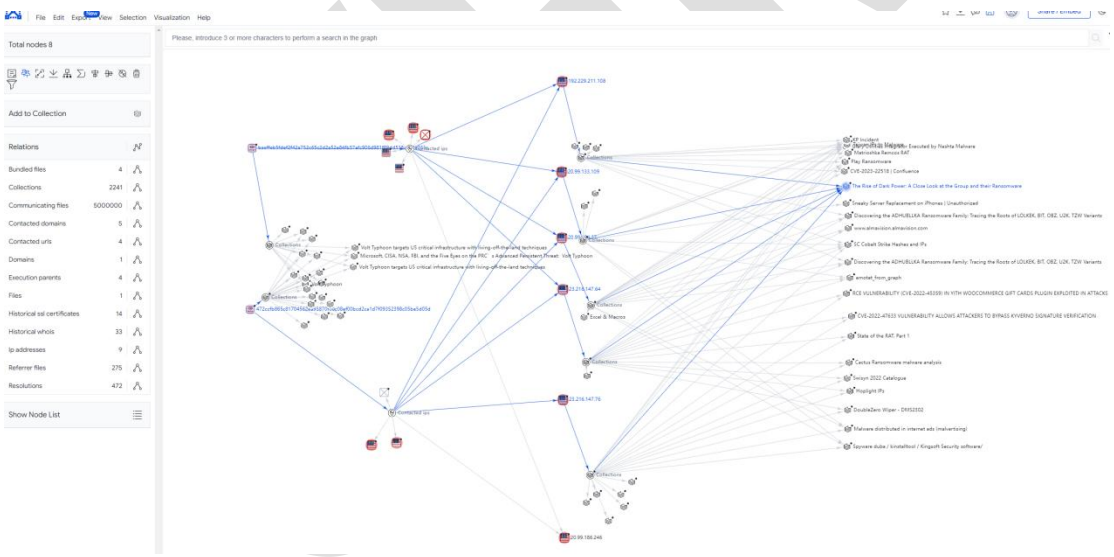


Figure 3. The relationship between malware samples and IP addresses

[11] 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

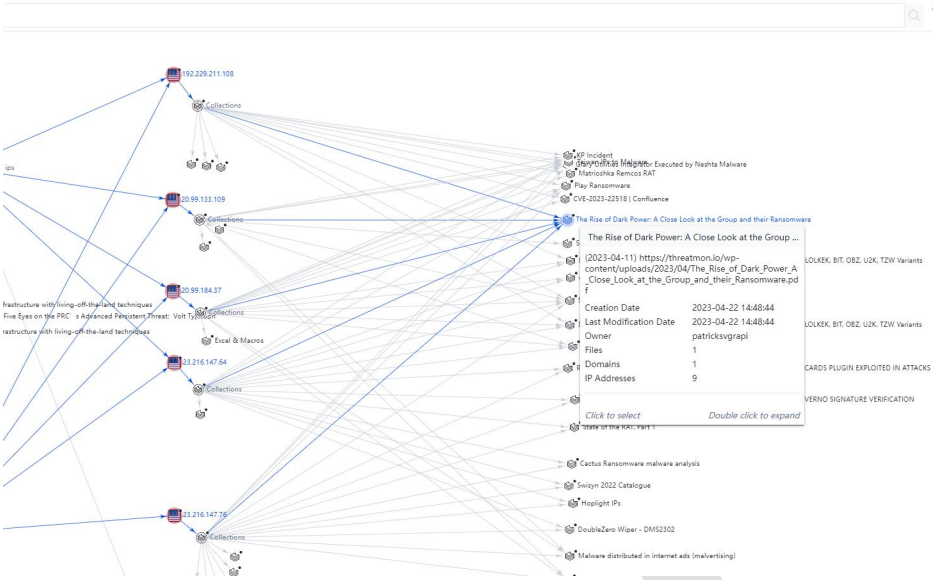
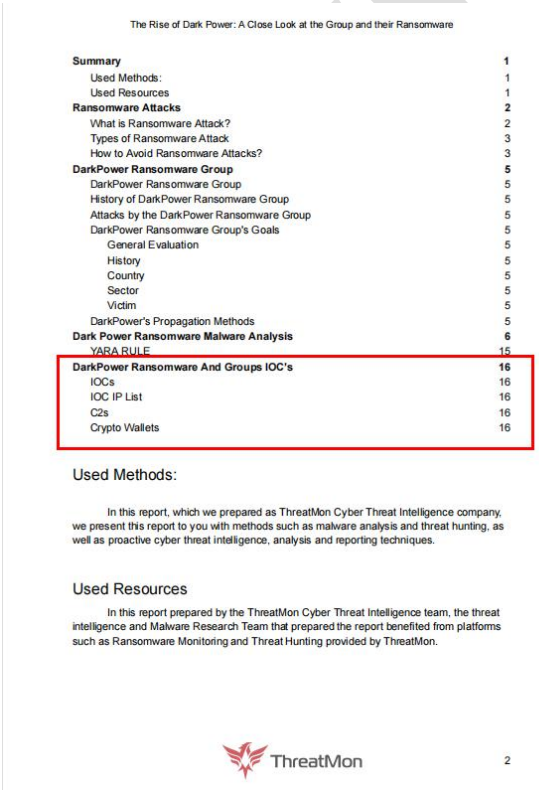


Figure 4. Related event information

We downloaded the report from the link, and expected to find those IP addresses in it. Strangely, although the report table of contents shows that the list of IP is on page 16, there is no relevant information on page 16 as the last page of report. Shown in Figure 5 and Figure 6.



The Rise of Dark Power: A Close Look at the Group and their Ransomware

Used Methods:

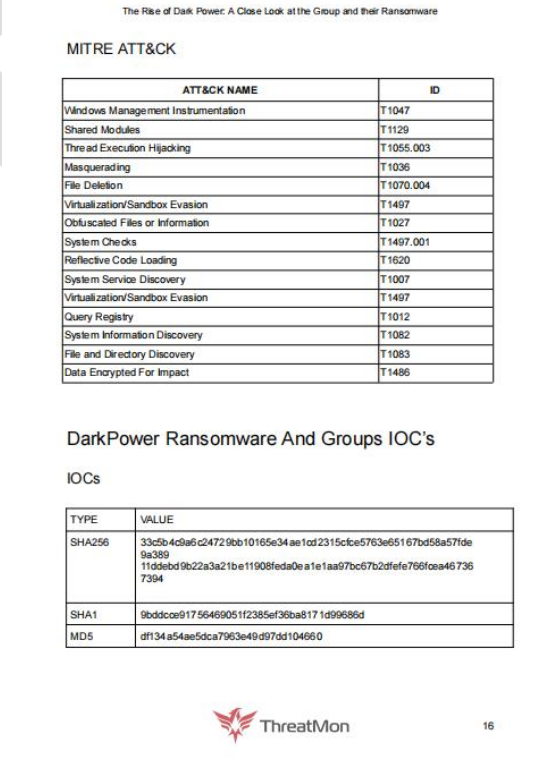
In this report, which we prepared as ThreatMon Cyber Threat Intelligence company, we present this report to you with methods such as malware analysis and threat hunting, as well as proactive cyber threat intelligence, analysis and reporting techniques.

Used Resources

In this report prepared by the ThreatMon Cyber Threat Intelligence team, the threat intelligence and Malware Research Team that prepared the report benefited from platforms such as Ransomware Monitoring and Threat Hunting provided by ThreatMon.

ThreatMon 2

Figure 5. IoC of the report



The Rise of Dark Power: A Close Look at the Group and their Ransomware

MITRE ATT&CK

ATT&CK NAME	ID
Windows Management Instrumentation	T1047
Shared Modules	T1129
Thread Execution Hijacking	T1055.003
Masquerading	T1036
File Deletion	T1070.004
Virtualization/Sandbox Evasion	T1497
Obfuscated Files or Information	T1027
System Checks	T1497.001
Reflective Code Loading	T1620
System Service Discovery	T1007
Virtualization/Sandbox Evasion	T1497
Query Registry	T1012
System Information Discovery	T1082
File and Directory Discovery	T1083
Data Encrypted For Impact	T1486

DarkPower Ransomware And Groups IOC's

IOCs

TYPE	VALUE
SHA256	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394
SHA1	9bddcce917564690511f2385ef36ba8171d99686d
MD5	df134a54ae5dca7963e49d97dd104660

ThreatMon 16

Figure 6. IP list could not be found in IoC

At first, we thought the report maybe contained a textual error, and we tried to find the file of IoCs on the GitHub repository of ThreatMon. However, we just found the file hashes of the report[12] but did not find the IPs , as shown in Figure 7. Moreover, the upload date is May 8th , 2023, not April 11th or near.

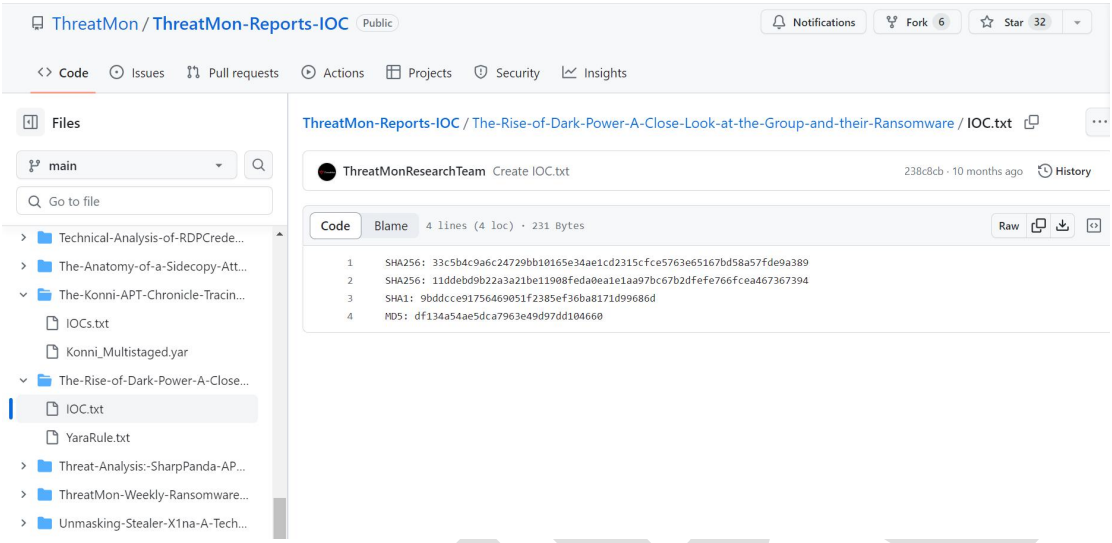


Figure 7. GitHub repository of ThreatMon

However, we were so lucky to find out that the back cover of report is not just a picture, after moving the picture, we found the IP list, which contains all 5 IP addresses as mentioned above. Shown in Figure 8 and Figure 9.

Figure 8. The original back cover of report

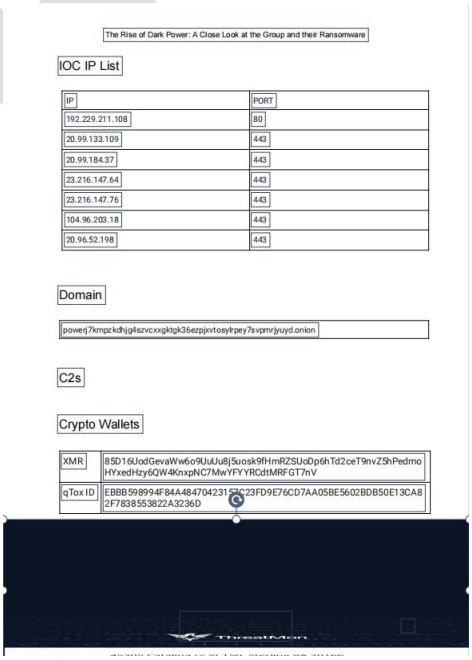


Figure 9. ThreatMon's report after moving the back cover picture

[12] https://github.com/ThreatMon/ThreatMon-Reports-IOC/commits/main/The-Rise-of-Dark-Power-A-Close-Look-at-the-Group-and-their-Ransomware/IOC.txt

Although we were puzzled by what ThreatMon did, we read the report carefully. In this report, ThreatMon Threat Intelligence team revealed a ransomware group who claimed themself "Dark Power". According to ThreatMon, Dark Power was first observed to have started its attacks in January 2023, which means the group was active before 2023. And at least 10 institutions worldwide were attacked and blackmailed by Dark Power in March 2023 alone, and "there was no country and sectoral connection". The victims were from Algeria, Egypt, the Czech Republic, Turkey, Israel, Peru, France and the US. The Dark Power uses the typical "double extortion" technique, that is, first hacking into the victim's internal network to steal data and then encrypt them, in addition to crypto extortion, the victim is threatened with the disclosure of sensitive internal data on the internet if the ransom is not paid on time. The report described the Tactics, Techniques, and Procedures (TTPs) of Dark Power in detail, which indicated that Dark Power also used the living-off-the-land techniques. They used the Windows Management tool (WMI) to shut down the system process and clear the footprint by deleting system log generated during the attack before the end of the attack, and finally leave a ransom note to inform the victim. As shown in Figure 10.

Figure 10. The ransom note of Dark Power

It's worth noting that, according to a report[13] of TheRecord.media, which owned by another U.S. cybersecurity company Recorded Future, published on March 21, 2023, Guam's largest telecommunications company, DOCOMO PACIFIC (a wholly owned subsidiary of Japan's NTT DOCOMO), was hit by a cyber attack on March 16, 2023, resulting in service disruptions. It pointed out that several Pacific island countries, including Tonga and Vanuatu, have been attacked by ransomware groups. DOCOMO PACIFIC also acknowledged the incident[14].

In addition, we used VT to search the malware samples and IP address in the report published by Lumen Technologies about the KV-Botnet, but could not find any link to the IoCs of the Microsoft's technical analysis report and the CSA of FVE.

[13] https://therecord.media/guam-telecom-cyberattack-restore
[14] https://bettertogether.pr.co/224192-docomo-pacific-responds-to-multiple-service-outage

At this point, based on analysis result above, we found that the actor is more likely a cybercrime group, and obviously, the attribution of Microsoft and FVE was very hasty. Obviously , that is abnormal, but we believe everything happens for a reason, so we dig a little deeper and found some interest things.

4 Money, Money, Money

As above mentioned, it is easy to find out that Jan 31st, 2024, was a crucial time node for the U.S. Congress, U.S. government cybersecurity authorities, and U.S. cybersecurity enterprises. On the same day, U.S. Congress, U.S. Department of Justice, and U.S. Department of Homeland Security jointly take a combination of actions against Volt Typhoon.

Why Jan 31st? In fact, under the Budget and Accounting Act[15] issued by 1921, the U.S. president must submit a budget report, including the federal government's budget request for the next fiscal year, to Congress by the first Monday in February, which is Feb 5th of this year. This explains why the hearing held by the House Select Committee on China on that day fulfilled with "Begging for Money".

Firstly, witnesses who attended the hearing, the heads of the NSA, the CISA, the FBI, and the ONCD hyped the "China threat theory" again and again, asked Congress to further increase more funds in the field of cybersecurity.

Secondly, the 2024 presidential election is attracting worldwide attention, and both the Republican and Democratic parties do not want to "lose votes" on the issue of China, by openly "denouncing" China, members of Congress can also improve their exposure and gain good political capital, and some lawmakers even clamor to counter China and ban TikTok.

Finally, network security companies certainly hope that the U.S.federal government, the most affluent major clients, will have a bigger and bigger wallet, and the "China threat theory" has become the best marketing advertisement for these companies to explore the European and American markets.

Eventually, in the 2025 fiscal year budget[16] request announced by the Biden administration on March 11, 2024, the federal government's cybersecurity budget in the civil administrative departments and agencies reached a record $13 billion, a 10% increase from the 2024 fiscal year. Among them, the budget for the CISA reached $3 billion, an increase of $103 million from the previous year. The budgets of the U.S. Department of Justice and the FBI increased by $25 million specifically for the "cyber and counterintelligence investigative capabilities." Of course, as a subordinate unit of the U.S. Department of Defense with a total budget of $850 billion, the National Security Agency has never worried about budget issues.

[15] https://www.govinfo.gov/help/budget#about
[16] https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf

Furthermore, we also observed some details. Just two months before Microsoft released its report, on March 24, 2023, Microsoft received the first batch of task orders[17] for the $9 billion Joint Warfighting Cloud (JWCC) project from the U.S. Department of Defense. And one month before Lumen Technologies released an analysis report linking the KV-Botnet to the Volt Typhoon, on November 7, 2023, Lumen Technologies had just won a five-year contract[18] order worth $110 million from the U.S. Defense Information Systems Agency (DISA).

In short, U.S. politicians, officials, and entrepreneurs are all making a fortune from the Volt Typhoon. And the essence of above is to vainly attempt to defame China, disrupt relationships between China and partner countries, delay the pace of economic development of China, which should be exposed to whole world.

5 Conclusion

We acknowledged that the attribution of cyber attacks is an international stubborn problem. The leak of cyber weapons and the rapid proliferation of offensive and defensive technologies have led to a significant increase in the technical level of cyber criminals. As early as 2016, Mirai, the first generation of the IoT botnet, caused a wide range of Internet outages in the United States, while the Colonial Pipeline attacked by ransomware, which led to a state of emergency in parts of the United States and the battle between Pro-Russian and pro-Ukrainian hacker groups in the Russia-Ukraine conflict have fully demonstrated that, some ransomware groups and botnet operators have more resources and technical capabilities than the average state, and have even been able to reach the level of cyber warfare. At the same time, ransomware organizations and botnet operators have long established a mature underground eco-system, driven by interests, these cyber criminal gangs are increasingly rampant. These Internet hazards are a common threat to all countries in the world, including China and the United States. However, the U.S. government and politicians always keep "few banding together" and "small yard and high fence" policies, and even politicizing cyber attacks origin-tracing, manipulating Microsoft and other companies to conduct media smear campaign against China, and just for filling their own pockets. These "Volt Typhoon" narratives won't be any beneficial to the normal order of the international public cyberspace but only undermine China-US relations, and finally eat their own bitter fruit.

At last, we would like to express our appreciation to 360 Digital Security Group for providing technical support on attribution.

[17] https://defensescoop.com/2023/03/29/defense-department-has-awarded-first-jwcc-cloud-task-order/
[18] https://ir.lumen.com/news/news-details/2023/Lumen-wins-110-million-contract-from-Defense-Information-Systems-Agency/default.aspx