Suspected Mysterious Elephant organization uses CHM files to attack many countries in South Asia

Original Red Raindrop Team QiAnXin Threat Intelligence Center

October 16, 2024 10:55

Gang background

Mysterious Elephant is a South Asian APT organization named by the foreign security manufacturer Kaspersky in the APT trend report for the second quarter of 2023 [1]. Domestic merchants have disclosed that the new backdoor ORPCBackdoor belonging to the Bitter organization appeared in the mysterious attack activities [2, 3]. Considering the possible differences in attribution, the merchants also chose to use ORPCBackdoor. The backdoor gang is given a new number different from the Bitter organization for tracking. According to the current public information, the Mysterious Elephant organization is associated with multiple APT organizations in South Asia, especially the attack methods of the Bitter organization are similar. The group's targets include Pakistan and other countries.

Event overview

QiAnXin Threat Intelligence Center recently discovered a batch of special CHM files. The script content of the html file is very simple and only executes an external file (such as "UsoCoreService" in the picture below). Since the CHM script itself does not contain obvious malicious code, the number of reported viruses on VT for these samples is very low.

The CHM sample contains image bait, combined with the ".pdf.chm" double extension in the file name, disguised as a PDF file. The bait content is related to Pakistan, Bangladesh, Myanmar and other South Asian countries, involving government agencies, military, diplomacy, economy, etc. industry. During the sample correlation process, we also found that the attacker imitated the red team’s techniques to create phishing samples, and the bait content indicated that the target of the attack was the Pakistani defense military department.

The external file executed by CHM is actually a backdoor written in C#. The backdoor code is similar to the malicious sample involved in a report [4] that disclosed the Bitter organization's attack arsenal . The server mentioned in this report (libraofficeonline[.]com) used to store attack weapons is also related to Mysterious Elephant. Some of the attack weapons hosted on it are the disclosed Mysterious E

lephant malware [5] (including ORPCBackdoor, WalkerShell, DemoTrySpy etc.).

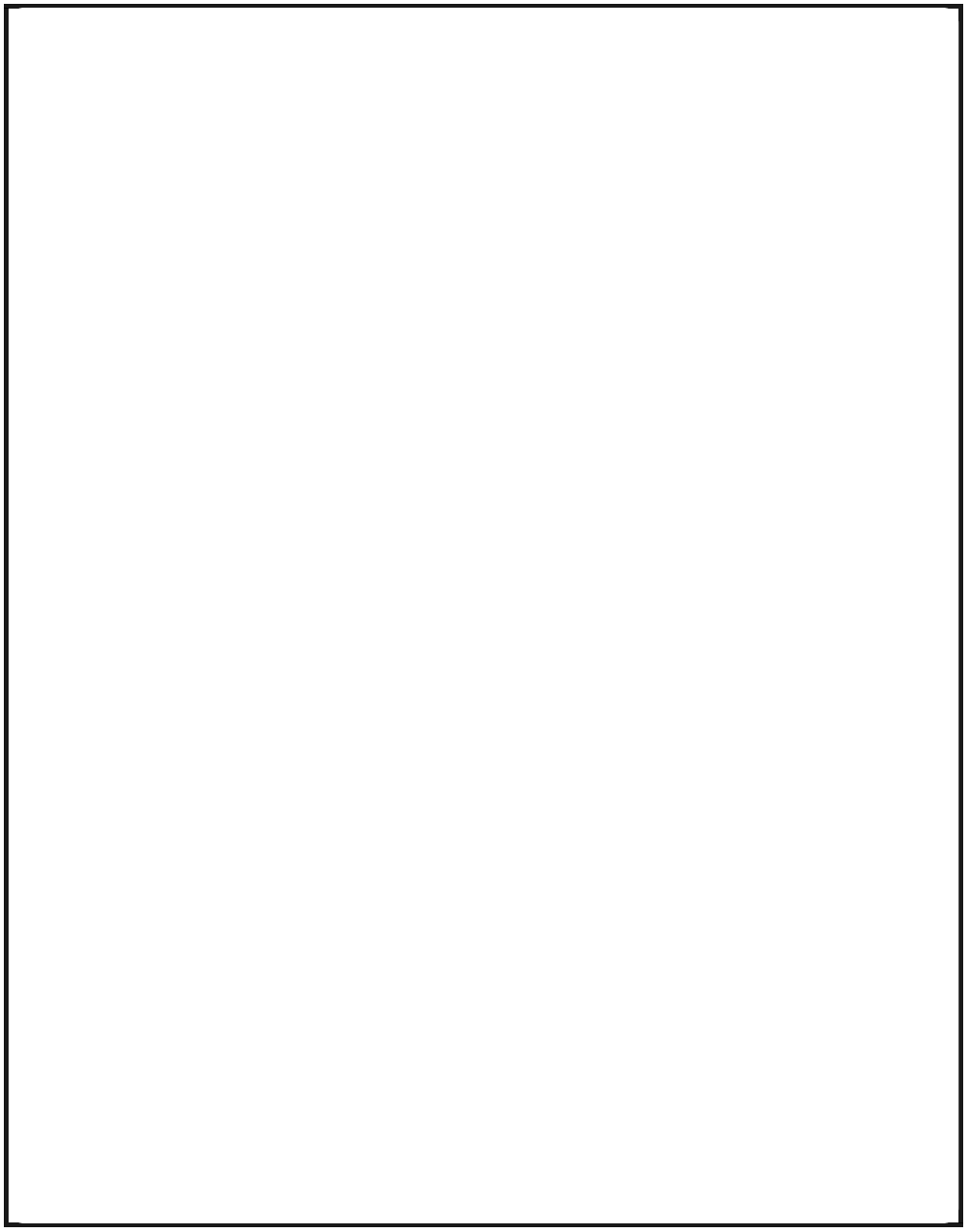
Due to the intricate connections between APT organizations in South Asia and the different tracking perspectives of multiple security researchers, there is currently no consensus in the industry on whether to distinguish Mysterious Elephant from Bitter. In order to avoid introducing more differences, this article believes that these special CHM attack samples and C# backdoors are likely to come from the Mysterious Elephant organization based on the similarity of malicious samples.

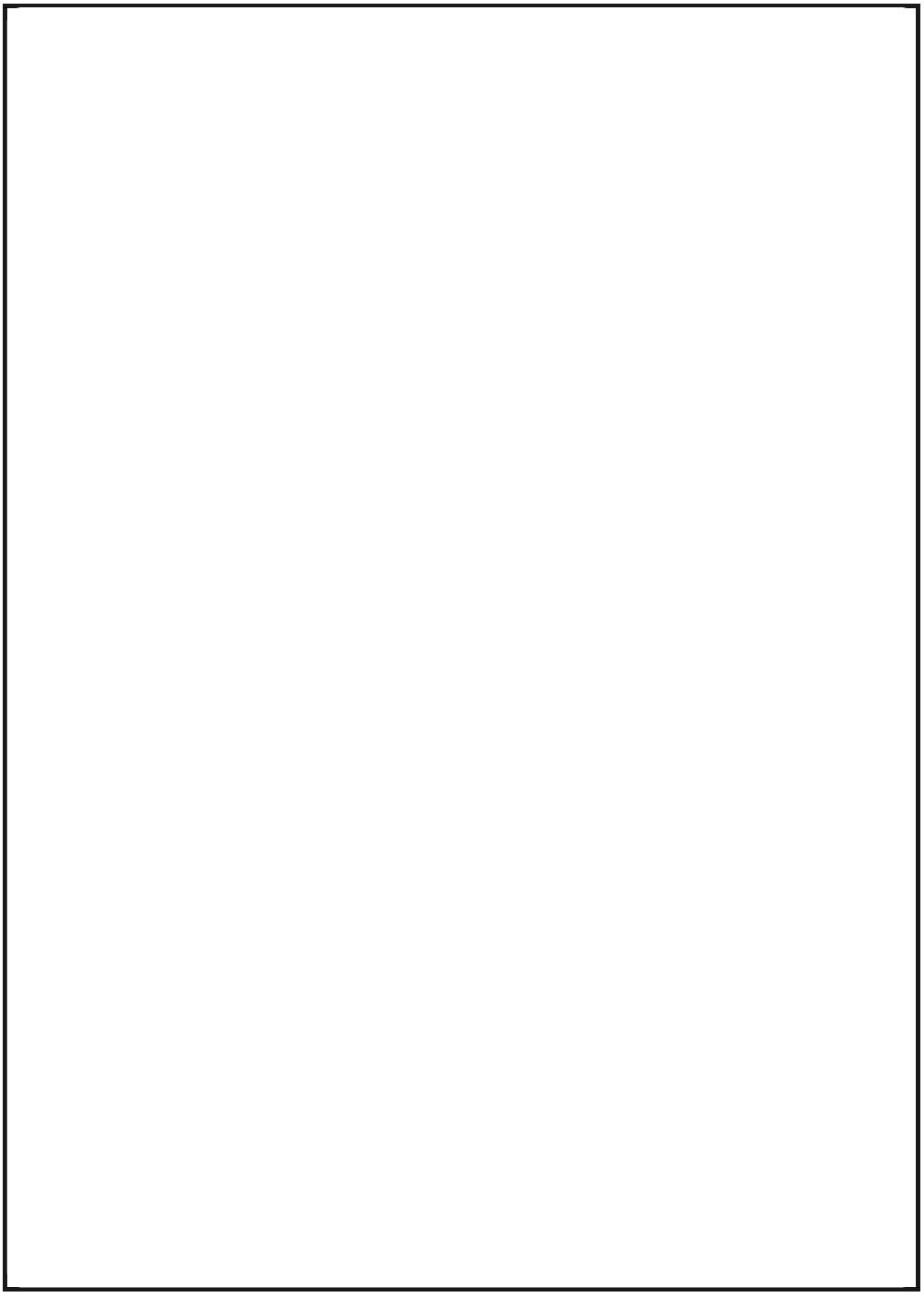
Detailed analysis

The CHM sample information is as follows, some of which have been previously disclosed by other security researchers [6~8].

MD5	file name	bait theme
3df2d899d6d8d827adf2d92c91b3b32b	Upcoming high level visit from China.pdf.chm	Possible outcomes during China’s visit to Pakistan
b38aca4f2d80484d5523f1eada9afe76	STRATEGIC RESTRAINT REGIME IN SOUTH ASIA.pdf.chm	pakistan and india relations
75ee4f79a3ed4137a918888482ded6a1	defoffsetpolicy.pdf.chm	pakistan defense policy
8e2377022b80cdc51d2c98bbf0c9d313	Myanmar Ship Clearance OM-2209.pdf.chm	Myanmar Navy vessel requests access to Bangladesh waters
2f7ee7c1c75fbfdc1d079fcc6e325d19	PM Thanks Letter FAO Xi an Pak.pdf.chm	Thank you letter after visit to Pakistan
19b767974205b66a12a28ccdb69943ed	Talking Points IAEA GC 2024.pdf.chm	Highlights of China - Pakistan Bilateral Meeting
aeb0b7e40f12ba093ff523fc124383ae	Bilateral Cooperation Pakistan China.pdf.chm	Pakistan - China Bilateral Cooperation
1645f406ab4e0d54e477330473c76664	SR ICT 030924.pdf.chm	pakistan military
d0030f5411698bb65f1cd281c5d302bc	26082024_DSR_No.pdf.chm	Pakistan Islamabad Police Report
232bb5b436c0836370fde34ca7b7138a	A Letter of China Development Bank.pdf.chm	Letter from China Development Bank
f26435785dd856ddb1fbcc682547aab0	CAPSTONE Course 2024.pdf.chm	Bangladesh government documents
68d458d1df36eaf885116a1b6801ab42	Notice EC10 Power.pdf.chm	Pakistan Special Investment Promotion Council (SIFC) meeting on power sector

Some bait pictures are shown below:





The relevant C# backdoor information is as follows:

MD5	file name
27ac8eb519679530999e786281e9a578	FileViewer.exe
115fb536e981c87873b0f35cb0059d93	STRATEGIC_RESTRAINT_REGIME_DETAILS.exe
4e8e1339f9754d8d2c5f74cb03f44fbb	Guidelines_on_Offset_Program.exe
00f2df1829893caa85f3968961b6e736	UsoCoreService.exe
a59fe2c89b0000a360a8468f2b990c73	IAEA_GC_2024.exe ; Bilateral_Cooperation.exe
a3a06d50438681fc9917e22c41bd2cab	SR_ICT.exe
316e8d798f7db625c207532e2f7a5d38	Annexure.exe
616b29bd9e20fc032bc54acd5ed8aff0	RuntimeIndexer.exe
ee64e70388e422dd9a620c3d18613268	RuntimeIndexer.exe

Fishing sample structure

According to disclosed samples[8, 9], attackers deliver phishing samples in encrypted compressed packages. Both the CHM file and the C# backdoor exist in the compressed package, but the C# backdoor sets the file hidden attribute, causing the victim to only see the CHM file after decompression. Even if some security-conscious victims will use anti-virus software to scan CHM files, since the CHM files themselves do not carry too many malicious scripts, they are likely to be judged as safe, causing the victims to directly open the bait CHM files and start the hidden C# back door.

C# backdoor

The C# backdoor uses Task asynchronous programming, part of which is packed with ConfuserEx. The function is relatively simple, mainly executing cmd commands issued by the C2 server. Some backdoors also support other attack commands.

Get C2

There are different ways for C# backdoors to obtain C2 server information, including the following.

(1) C2 server information is directly hard-coded in the code.

(2) Decrypt from the configuration file.

For example, 00f2df1829893caa85f3968961b6e736 and 316e8d798f7db625c207532e2f7a5d38 both read the SysConfig.enc file in the same directory, and then use AES to decrypt to obtain the C2 server information.

(3) Disguised as a seemingly legitimate network service access request, parsed from the response content of the remote server.

Taking a3a06d50438681fc9917e22c41bd2cab as an example, the GetIpInfo function requests "hxxp://easyiplookup.com:5080/main/get_ip_data?userId=zqlCYqgp4f&ip=8.8.8.8"

Extract the content from the RequestId field of the response content, and base64 decode it to obtain the C2 information "91.132.92.231:5959". In addition to port 5959, port 6060 of the same IP (91.132.92.231) was also found to be passed as C2 information to the C# backdoor. This way, the attacker has the flexibility to change the C2 server IP address and port to which the backdoor actually connects.

Port 80 of the easyiplookup.com domain name seems to be running an IP query service. The website script custom.js calls the fetchIpInfo function to obtain the visitor's IP information from ip-api.com and displays it on the page. After clicking the IP lookup button "Lookup" on the web page and submitting the form, the same URL as the backdoor requesting C2 information ("hxxp://easyiplookup.com:5080/main/get_ip_data") will be accessed, indicating that the website is under the control of the attacker. Down.

Other C# backdoors that use the same method to obtain C2 information include:

MD5	4e8e1339f9754d8d2c5f74cb03f44fbb
Request URL	hxxp://winfreecloud.net:6396/athena/identification?name=f0inqMaHra&addr=6.5.6.2
Obtained C2 information	162.252.175.131:8246

MD5	115fb536e981c87873b0f35cb0059d93
Request URL	hxxp://winfreecloud.net:6396/athena/identification?name=9az1g3qdYp&addr=9.9.9.9
Obtained C2 information	46.183.186.208:6060

Both winfreecloud.net and easyiplookup.com resolve to the same IPs (151.236.9.75 and 84.32.84.32).

Backdoor functionality

The backdoor uses the hostname and username of the infected device as victim identification information after connecting to the C2 server.

The function of most backdoors is only to execute remote commands or creat e a cmd.exe shell for attackers to perform subsequent operations.

Some backdoors also support other C2 commands.

The C2 instructions supported by sample a59fe2c89b0000a360a8468f2b990c73 are as follows.

C2 command code	Function
dir	List file names and subdirectory names in the specified directory
cat	Read file contents
copy	Copy files
whoami	Show username
upload	Upload files
tasklist	List all process information and corresponding executable file paths
schtasks	List the names and descriptions of all scheduled tasks
download	Download file
systeminfo	Obtain system information, including system version, serial number, and free physical memory size

other	command execution

The C2 instructions supported by sample 27ac8eb519679530999e786281e9a578 are as follows.

C2 command code	Function
dir	List file names and subdirectory names in the specified directory
copy	Copy files
upload	Upload files
download	Download file
other	command execution

Traceability association

Related samples

The backdoor sample 316e8d798f7db625c207532e2f7a5d38 also appears in another compressed package, and the C2 information 46.183.187.42:443 is decrypted from the configuration file SysConfig.enc.

MD5	b28bb7cabfb12e9bc5b87692b065c83a
file name	Islamabad_Security_Dialogue_Pub.rar

According to a file filename.lnk (MD5: ae55cb4988f2f45197132631f5a86632) in the compressed package that does not seem to work, it can be associated with a phishing sample with a similar directory structure of the compressed package.

serial number	MD5	VT upload time	File timestamp in compressed package
1	3b669279c534987d6d7cab08d85df55a	2024-06-19 04:59:57 UTC	2024-06-18
2	432230af1d59dac7dfb47e0684807240	2024-07-02 06:04:24 UTC	2024-06-28
3	865483fea76242e687aa9e76b1a37f28	2024-07-09 10:04:58 UTC	2024-07-09
4	af669dfa074eb9b6fda3fd258f58e2d2	2024-07-16 02:34:10 UTC	2024-07-10
5	7728fee377137e83e9bd1c609cc166c0	2024-07-19 10:45:35 UTC	2024-07-11
6	dad7d9528e9506ebd0524b3ebd89ddf2	2024-07-18 10:36:13 UTC	2024-07-18

The above-mentioned related samples can be divided into two categories. Samples 1 to 4 use resume documents as bait, the backdoor is written in C++, and uses Tencent Cloud services as C2. They are attack samples of domestic red teams.

The decoy PDF content of Samples 5 and 6 is related to the Pakistan Defense Military. The C# backdoor (MD5: 5e7dba4aafb8176ab026e2f4aa3211dd) code is consistent with the backdoor related to the CHM file mentioned earlier. The connected C2 server information is also decrypted from the configuration file "license" through AES. ” obtained from . The configuration files of the two compressed packages are the same, and the C2 is 158.255.215.115:443.

Based on the upload time of these samples on VT and the file timestamp in the compressed package, we believe that the attacker imitated the attack samples targeting Pakistan based on the public red team phishing samples.

Attack attribution

The C# backdoor is similar to the malicious sample hosted in the op directory on the libraofficeonline[.]com server mentioned in the report [4] .

Taking the backdoor a59fe2c89b0000a360a8468f2b990c73 as an example, malware similar to this sample in the op directory is shown in the table below. The similarities include: using Task asynchronous programming, sending the machine name and user name to the C2 server as the victim identification, using similar function names and Output information string.

Similar file names	MD5	illustrate
figlio.exe	25e5d1790f61e6a45720da0a500be131	C# backdoor, cmd command execution
SearchApp.jpg	16c33dbd1d7f6f98827e14f9d6d918e7	C# backdoor, cmd command execution
sparrow.jpg	b7289c3f37a4305b4d6898f2e71fbb2c	C# backdoor supports multiple commands

The report[4] attributes libraofficeonline[.]com to the Bitter group, and some of the malware hosted on this server are attack weapons of the Mysterious Elephant group disclosed by other security vendors[5].

file name	MD5	illustrate
page/MicrosoftEdge.msi	6ff3f0a2f7f1ec8a71bed37496e2e6fa	Contains ORPCBackdoor

msas.msi	7dc1d21554dce36958614817e3f531e6	Contains ORPCBackdoor
msws.msi	c13c4c025c5c779d5dc8848ef160d5da	Contains ORPCBackdoor
Hazel.exe	1ad818406f06d1cb728b5d0f324fb3b5	WalkerShell
Pro-CLA.exe	79ed88fa92f87bf8f36ed98c44436472	WalkerShell
GOG.exe	36edd4fe5ee415f81e2ef8da75f23734	DemoTrySpy
Gogo.exe	4b6b8135c2d48891c68cc66cd9934c40	DemoTrySpy
Nix.exe	eb9cd31960e3bc9da5a3a03cd0055180	NixBackdoor

Since ORPCBackdoor was initially considered to be a new backdoor of the Bitter organization, some domestic and foreign security vendors later used ORPCBackdoor's group to track the new organization Mysterious Elephant. This may be the reason for the above attribution inconsistency. This article is consistent with previous open source reports disclosing ORPCBackdoor attack activities and avoid introducing more differences. Therefore, it is believed that the CHM files and C# backdoors targeting many South Asian countries are likely to originate from the Mysterious Elephant organization.

Summarize

The CHM samples related to this attack targeted Pakistan, Bangladesh and other places in South Asia, involving government agencies, national defense and military, diplomatic and other departments. The attacker used a less common attack method using CHM samples, that is, the CHM file directly launches an external file without other malicious code. External files related to CHM are all C# backdoors. Some C# backdoors disguise requests to obtain C2 address information as access to seemingly legitimate network services, and then parse the C2 address from the response results. The attackers also imitated red team attack samples and used the same C# backdoor. The above signs indicate that the attack group has been trying different attack methods and working hard to disguise the attack activities.

Protection recommendations

QiAnXin Threat Intelligence Center reminds users to beware of phishing attacks. Do not open links from unknown sources shared on social media, do not click to execute email attachments from unknown sources, do not run unknown files with exaggerated titles, and do not install apps from informal sources. . Back up important files in a timely manner and update and install patches.

If you need to run and install applications from unknown sources, you can first identify them through the Qianxin Threat Intelligence File In-depth Analysis Platform (https://sandbox.ti.qianxin.com/sandbox/page). Currently, it supports in-dep

th analysis of files in multiple formats including Windows and Android platforms.

Currently, all products based on the threat intelligence data of QiAnXin Threat Intelligence Center, including QiAnXin Threat Intelligence Platform (TIP), Tianqing, Tianyan Advanced Threat Detection System, QiAnXin NGSOC, QiAnXin Situational Awareness, etc., all support this Accurate detection of similar attacks.

IOC

MD5

(CHM)

3df2d899d6d8d827adf2d92c91b3b32b

b38aca4f2d80484d5523f1eada9afe76

75ee4f79a3ed4137a918888482ded6a1

8e2377022b80cdc51d2c98bbf0c9d313

2f7ee7c1c75fbfdc1d079fcc6e325d19

19b767974205b66a12a28ccdb69943ed

aeb0b7e40f12ba093ff523fc124383ae

1645f406ab4e0d54e477330473c76664

d0030f5411698bb65f1cd281c5d302bc

232bb5b436c0836370fde34ca7b7138a

f26435785dd856ddb1fbcc682547aab0

68d458d1df36eaf885116a1b6801ab42

(C# backdoor)

27ac8eb519679530999e786281e9a578

115fb536e981c87873b0f35cb0059d93

4e8e1339f9754d8d2c5f74cb03f44fbb

00f2df1829893caa85f3968961b6e736

a59fe2c89b0000a360a8468f2b990c73

a3a06d50438681fc9917e22c41bd2cab

316e8d798f7db625c207532e2f7a5d38

616b29bd9e20fc032bc54acd5ed8aff0

ee64e70388e422dd9a620c3d18613268

(compressed package)

b28bb7cabfb12e9bc5b87692b065c83a

7728fee377137e83e9bd1c609cc166c0

dad7d9528e9506ebd0524b3ebd89ddf2

C&C

162.252.172.67:443

95.156.206.105:443

46.183.187.42:443

158.255.215.115:443

91.132.92.231:5959|6060

162.252.175.131:8246

46.183.186.208:6060

URL

hxxp://easyiplookup.com:5080/main/get_ip_data

hxxp://winfreecloud.net:6396/athena/identification

Reference link

[1].https://securelist.com/apt-trends-report-q2-2023/110231/

[2].https://paper.seebug.org/2075/

[3].https://paper.seebug.org/3000/

[4].https://strikeready.com/blog/open-sesame/

[5].https://mp.weixin.qq.com/s/Uf708Khax2rJaUhNo1Mz1Q

[6].https://www.securonix.com/blog/analysis-of-phantomspike-attackers-leveraging-chm-files-to-run-custom-csharp-backdoors-likely-targeting-victims-associated-with- pakistan/

[7].https://x.com/StrikeReadyLabs/status/1834599289391108556

[8].https://x.com/__0XYC__/status/1843593304010813479

[9].https://x.com/__0XYC__/status/1800129922054447220