Operation Cobalt Whisper: Threat Actor Targets Multiple Industries Across Hong Kong and Pakistan.

seqrite.com/blog/operation-cobalt-whisper-targets-industries-hong-kong-pakistan/

Subhajeet Singha October 24, 2024

Estimated reading time: 15 minutes

Contents

Introduction

SEQRITE Labs APT-Team has recently uncovered a campaign targeting various industries such as the Defense Sector in Pakistan and predominantly researchers from Hong Kong. Tracked as **Operation Cobalt Whisper**, the entire campaign heavily leverages the use of a post-exploitation tool Cobalt Strike, which is deployed using obfuscated VBScript. A total of 20 infection chains have been identified so far along with additional individual samples, where 18 of them target Hong Kong and two target Pakistan where over 30 decoy files have been identified.

In this blog, we will explore the technical details of one of the campaigns we encountered during our initial analysis and examine the various stages of the infection chain, starting with a deep dive into the decoy documents. We will then look into the common Tactics, Techniques, and Procedures (TTPs), such as the use of malicious VBScript and LNK payloads employed by this threat actor across most campaigns. These methods facilitate the in-memory execution of the Cobalt Strike implant, which is delivered alongside these lures in an archive file.

Key Targets

Industries Affected

- Defense Industry
- Electrotechnical Engineering
- Energy (Hydropower, Renewable Energy)
- Civil Aviation
- Environmental Engineering
- Academia and Research Institutions
- Medical Science Institutions.
- Cybersecurity Researchers.

Geographical Focus

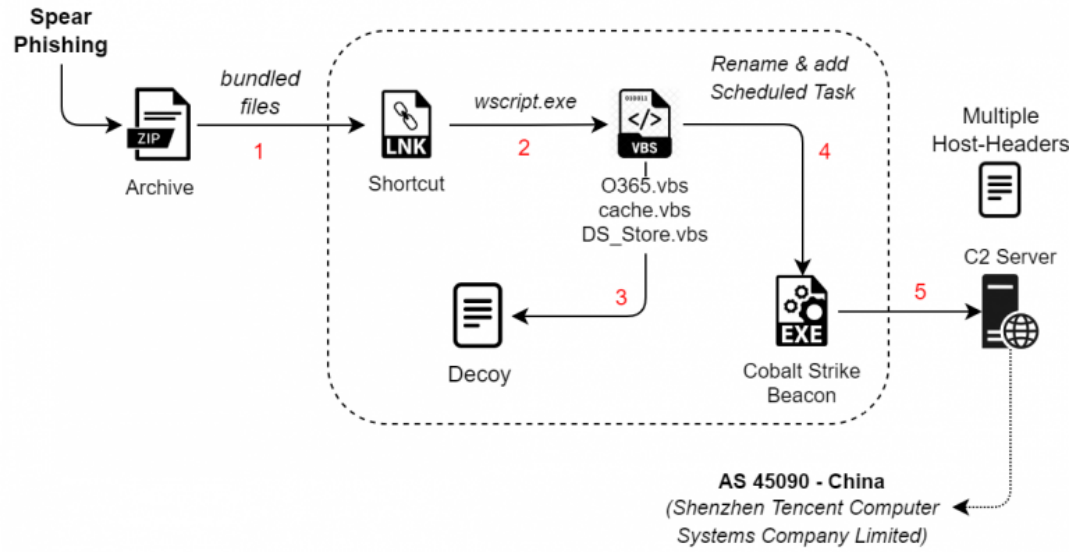
- Hong Kong
- Pakistan

Initial Findings

Recently, on 9th of September 2024, our team found a malicious RAR archive, which surfaced both on various sources like VirusTotal, where the RAR has been used as preliminary source of infection, containing multiple decoys with PDF and LNK extensions and a final Cobalt Strike implant. This was also found by other threat researchers as well.

The RAR archive contains a malicious LNK named, "*附件1：《2024年度中国电工技术学会科学技术奖推荐提名书》（技术发明奖和科技进步奖）填报说明(2024年8月新版).pdf.lnk*", which is responsible for execution of another malicious batch script named as *O365.vbs*. The VBScript is mostly responsible for decoding the Cobalt Strike beacon on disk, known as *cache.bak*, this is further executed, which connects back to the command-and-control server. Let us look into the two decoy documents.

Infection Chain



Looking into the decoy-document – I

Upon looking into the first decoy document known as subscription.db, it turns out that this lure is linked to the Electronic Society of China, focused on nominations for the award ceremony.

中国电工技术学会
China Electrotechnical Society

2024年度中国电工技术学会科学技术奖

推荐/提名书

（技术发明奖和科技进步奖）

2024 Annual China Electrical Society Sciencr and Technology Award

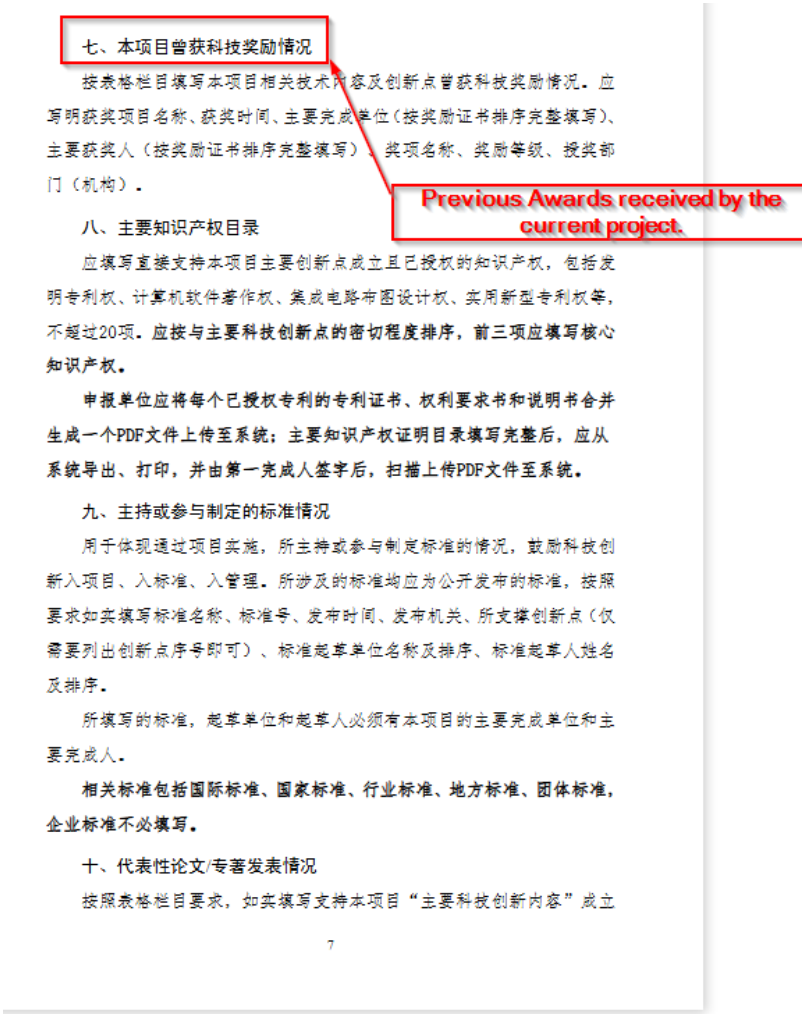
Recommendation / Nomination Form

填报说明

目 录

Contents on Guidelines for Project Submission.

The contents and the entire decoy confirm that this PDF serves as a comprehensive guideline for the application and nomination process for the China Electrical Engineering Society Science and Technology Award. It outlines the necessary documentation, structure, and specific requirements for submitting a project, including details on technological innovations, evaluations, application promotion, and economic and social benefits.

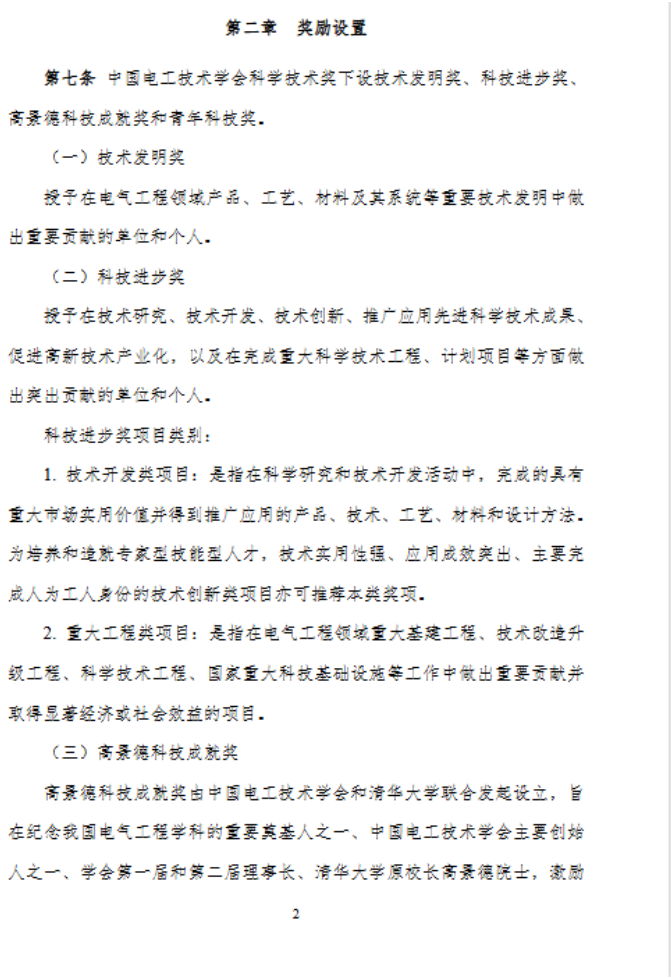


The decoy also mentions some interesting guidelines for the current project for nomination, in case it has received other awards too.

The document concludes with guidelines for researchers on submitting essential documents that validate the legitimacy and credibility of their research. This includes items such as Peer Expert Recommendation Letters, photographs, and other relevant information, including specifications for video format and additional submission guidelines. Now, let us look into the other decoy document.

Looking into the decoy-document – II

The second document, titled 附件2：《中国电工技术学会科学技术奖励办法》（2024年4月修订）.pdf translates to “Attachment 2: Regulations on Scientific and Technological Awards of the China Electrotechnical Society (Revised April 2024),” it is clear that it is closely related to the same theme as the first document. This document also focuses on the purpose of the award ceremony, detailing various awards and emphasizing the overall societal improvement and growth achieved through these award ceremonies.



第二章　奖励设置

第七条 中国电工技术学会科学技术奖下设技术发明奖、科技进步奖、高景德科技成就奖和青年科技奖。

（一）技术发明奖

授予在电气工程领域产品、工艺、材料及其系统等重要技术发明中做出重要贡献的单位和个人。

（二）科技进步奖

授予在技术研究、技术开发、技术创新、推广应用先进科学技术成果、促进高新技术产业化，以及在完成重大科学技术工程、计划项目等方面做出突出贡献的单位和个人。

科技进步奖项目类别：

1. 技术开发类项目：是指在科学研究和技术开发活动中，完成的具有重大市场实用价值并得到推广应用的产品、技术、工艺、材料和设计方法。为培养和造就专家型技能型人才，技术实用性强、应用成效突出、主要完成人为工人身份的技术创新类项目亦可推荐本类奖项。

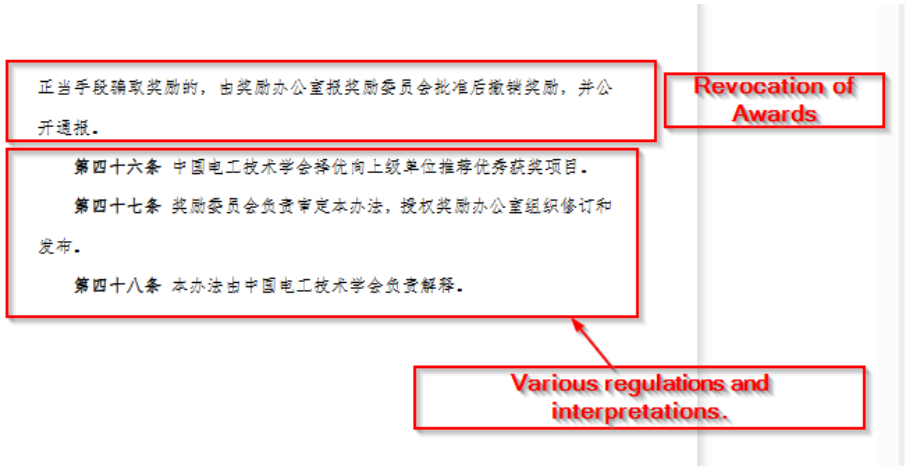
2. 重大工程类项目：是指在电气工程领域重大基建工程、技术改造升级工程、科学技术工程、国家重大科技基础设施等工作中做出重要贡献并取得显著经济或社会效益的项目。

（三）高景德科技成就奖

高景德科技成就奖由中国电工技术学会和清华大学联合发起设立，旨在纪念我国电气工程学科的重要奠基人之一、中国电工技术学会主要创始人之一、学会第一届和第二届理事长、清华大学原校长高景德院士，激励

2

The decoy mentions various awards like the Technology Invention Award, Scientific & Technological Progress Award, and the various criteria like someone building a Major Engineering Project and much more, it also mentions about other award known as Gaojingde Scientific and Technological Achievement Award which aims to inspire and encourage contributions to the Electrical Engineering field.



The document concludes with adhering guidelines on revocation of awards, in case it is found that any improper means have been used to obtain the award, well the last thing which is mentioned in this decoy is about various regulations maintained by Chinese Electrical Engineering Society and they are responsible for the interpretation of the regulations. Overall, this lure document serves as a guideline for the entire process of evaluation, types of awards, and much more under transparency in recognizing the achievements in the electrical engineering domain.

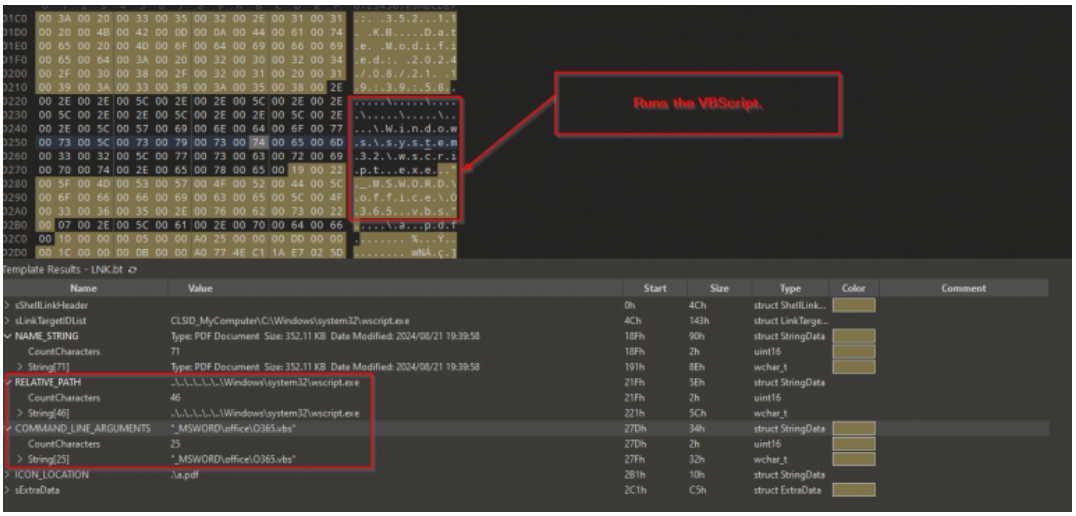
Technical Analysis

We will divide our analysis into two main sections. **First**, we will examine the malicious LNK and VBScript components utilized by the threat actor across the campaigns. **Second**, we will delve into the malicious Cobalt Strike implant and extract its configuration details.

Our research has uncovered more than **18 distinct infection chains** linked to this threat actor. In this blog, we will focus specifically on one of these campaigns that targets electrotechnical researchers in Hong Kong. This detailed exploration will shed light on the methodologies employed and provide insights into the threat actor's tactics within this particular campaign.

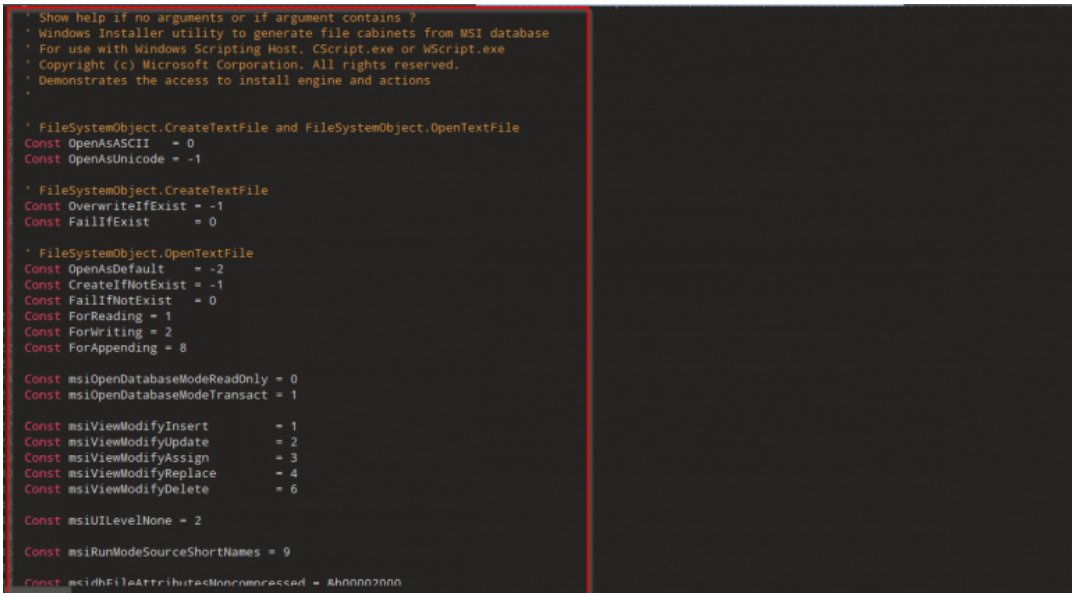
Stage 1 – Malicious LNK Script & VBScript

The RAR contains an LNK known as 附件1：《2024年度中国电工技术学会科学技术奖推荐提名书》（技术发明奖和科技进步奖）填报说明(2024年8月新版).pdf.lnk , upon exploring the it became quite evident that the sole purpose of the LNK is just to run the malicious VBScript O365.vbs using a Windows Utility known as wscript.exe .

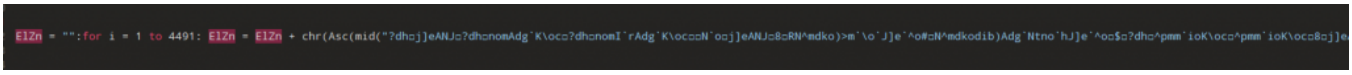


Upon analyzing the malicious VBScript, we found the following.

① The initial part of the script mimics a utility for managing and generating compressed cabinets from an MSI database, which can be useful for software distribution and installation processes.



② Next, there is a variable known as ElZn , which contains the encoded contents, which further on decoding turns out of another VBScript.



③ The decoded VBScript renames the backup cache.bak found in the RAR which was delivered to the target to sigverif.exe and moves subscription.db to a specified destination based on the decoded name. It copies the sigverif.exe to a temporary folder and then deletes the original to remove its presence. The script executes both the renamed executable and the copied version in the temporary folder, indicating an intention to perform actions silently in the background. Additionally, it creates a scheduled task named WpnUserService_x64 to run sigverif.exe every 59 minutes. Finally, the script deletes itself after execution.

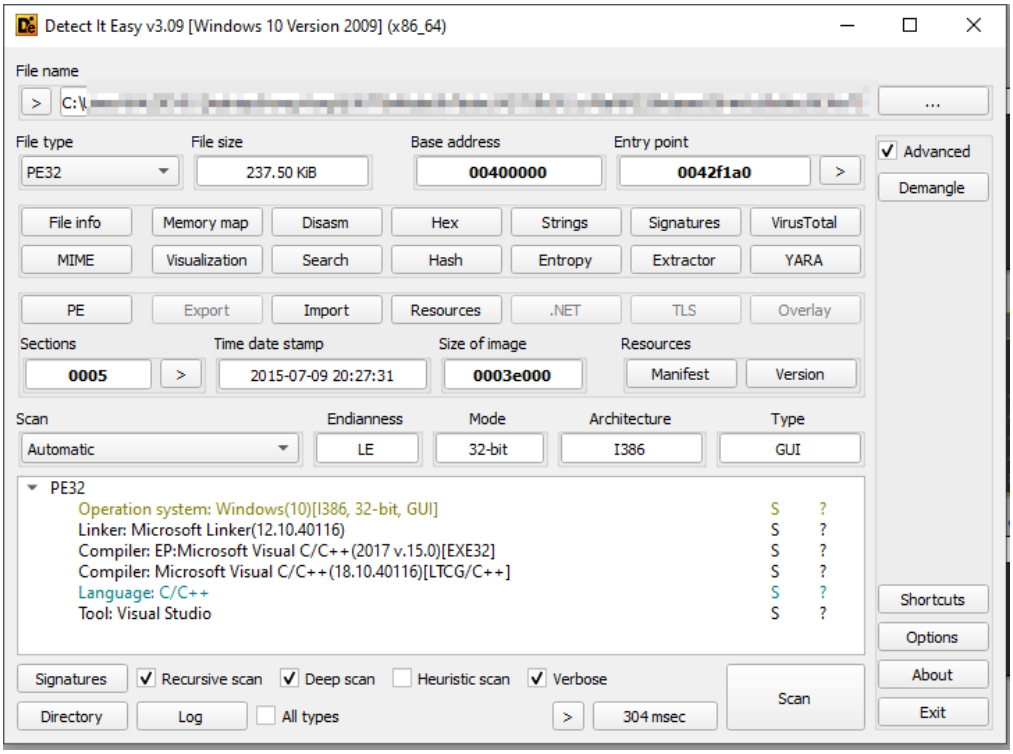
④ Finally, post execution of this VBScript, which performs the persistence, there is some additional garbage code which is completely irrelevant.

```
Dim i, j, k
Dim strMessage
Dim randomValue

' Initialize variables
i = 1
j = 2
k = 3
strMessage = "This is a test string."

' Perform some arithmetic operations
i = i + j
j = j * k
k = k - 1

' Create and use a random number
Randomize
randomValue = Int((100 * Rnd) + 1)

' String manipulation
strMessage = strMessage & " This is an additional message."

' Some loop operations
Dim counter
counter = 0
For i = 1 To 5
    counter = counter + i
Next

' End of script

Sub SafeEcho(message)
    Dim objShell, isCscript

    isCscript = InStr(LCase(WScript.FullName), "cscript.exe") > 0
```

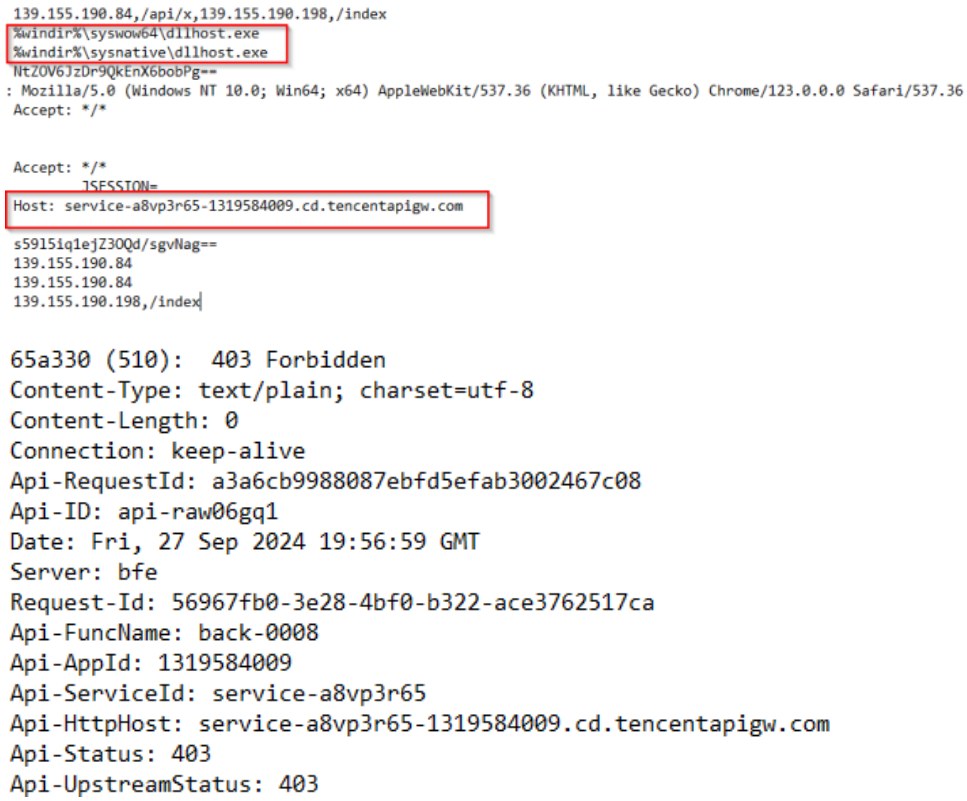
Now, in this section it is clearly evident that this LNK which is responsible for running the VBScript, which was rename the Cobalt Strike Implant and further create a scheduled task. We will look into the Cobalt Strike Beacon in the next section.

Stage 2 – Malicious Cobalt Strike Beacon.

Upon analysis, we found that the cache.bak which was basically renamed as SigVerifier.exe , turns out to be a 32-bit executable.



Now, upon analyzing the binary, we found that this is basically a Cobalt Strike Beacon which is trying to connect to the C2 server. As, there are various research on fundamentals of Cobalt Strike implant, we will not touch into the concepts like Jitter, C2 Uri and other fundamentals. Next, we went ahead and extracted the configurations.



The beacon configuration extracted from the implant are as follows:

Extracted Beacon Configuration:

BeaconType : HTTPS

Port: 443

SleepTime : 60000

Jitter : 10

C2 Server : 139[.]155[.]190[.]84

Malleable_C2_Instructions : Base64 URL-safe decode.

Spawnto_x86: %windir%\\syswow64\\dllhost.exe

Spawnto_x64: %windir%\\sysnative\\dllhost.exe

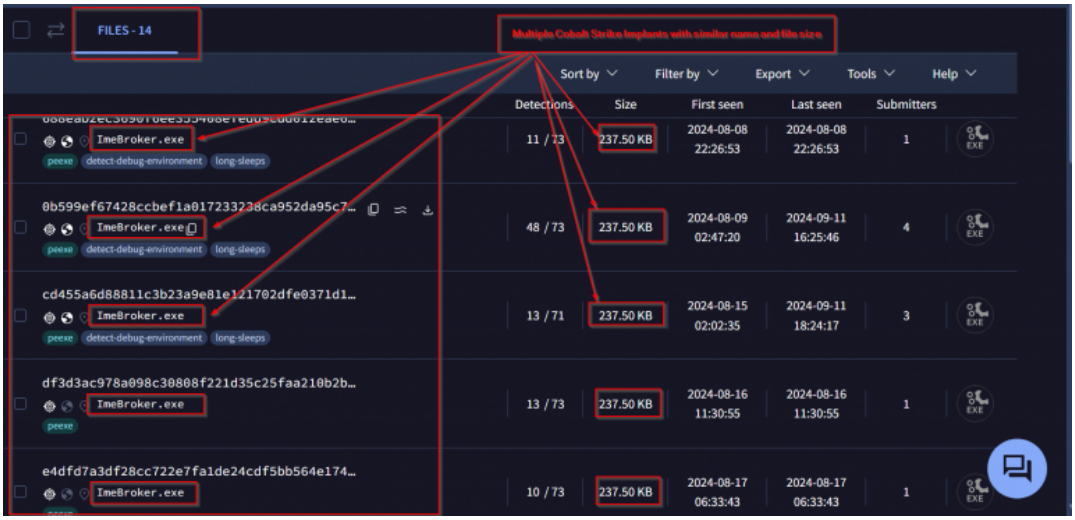
HostHeader : service-a8vp3r65-1319584009[.]cd[.]tencentapigw[.]com

Therefore, above is the extracted configuration from the malicious Cobalt Strike Beacon, next we will look into hunting similar samples and look into similar infrastructure hosted by the threat actor.

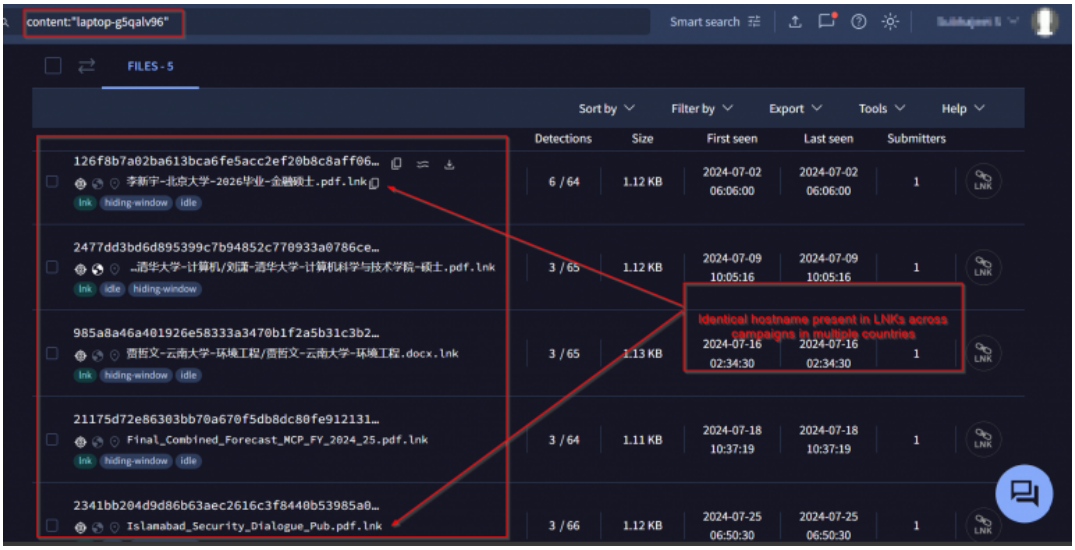
Hunting and Infrastructure

In this section, we will discuss how we uncovered additional campaigns by leveraging a simple artifact: the threat actor's consistent use of the name **ImeBroker.exe** for different Cobalt Strike implants across all campaigns. Originally, **ImeBroker.exe** is a legitimate Windows utility related to language input, specifically managing Input Method Editors (IME) that allow users to type in languages with complex scripts.

While reverse-engineering the implant, we discovered a suspicious code segment. Using this segment we identified a total of **14 samples** with similar names and identical binary sizes, all deployed by the threat actor as Cobalt Strike beacons with compilation timestamp "Compilation Timestamp: 2015-07-10 03:27:31" and delivered via different lures. Additionally, going by configurations, we found **21 more Cobalt Strike beacons** with similar configurations. This pattern highlights the threat actor's widespread use of consistent naming and configurations across multiple campaigns.



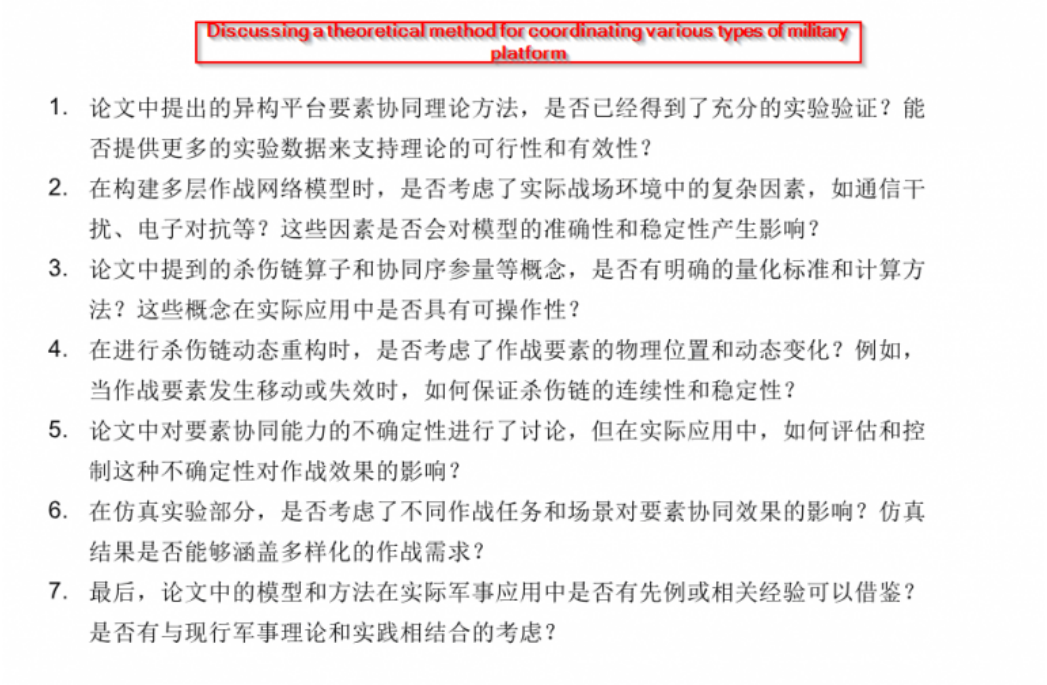
Another artefact, we used while hunting this threat actor was machine IDs present in multiple LNKs, which were common across campaigns targeting Hong Kong & Islamabad. The ID **laptop-g5qalv96** triggers cscript.exe unlike the others that uses wscript.exe to execute the VBS. Based on this ID, two campaigns with Pakistan-based lures have been found.



Another related ID **desktop-727otfd** triggers explorer.exe to open “PressMe.pdf” which is found in multiple archive files of this campaign. An interesting file path is present as well: “C:\LLVM\bin\LnkFishing\.asset\.asset.pdf“.

We, will look into some set of interesting campaigns and their decoys linked to the Cobalt Strike beacons, that we have found.

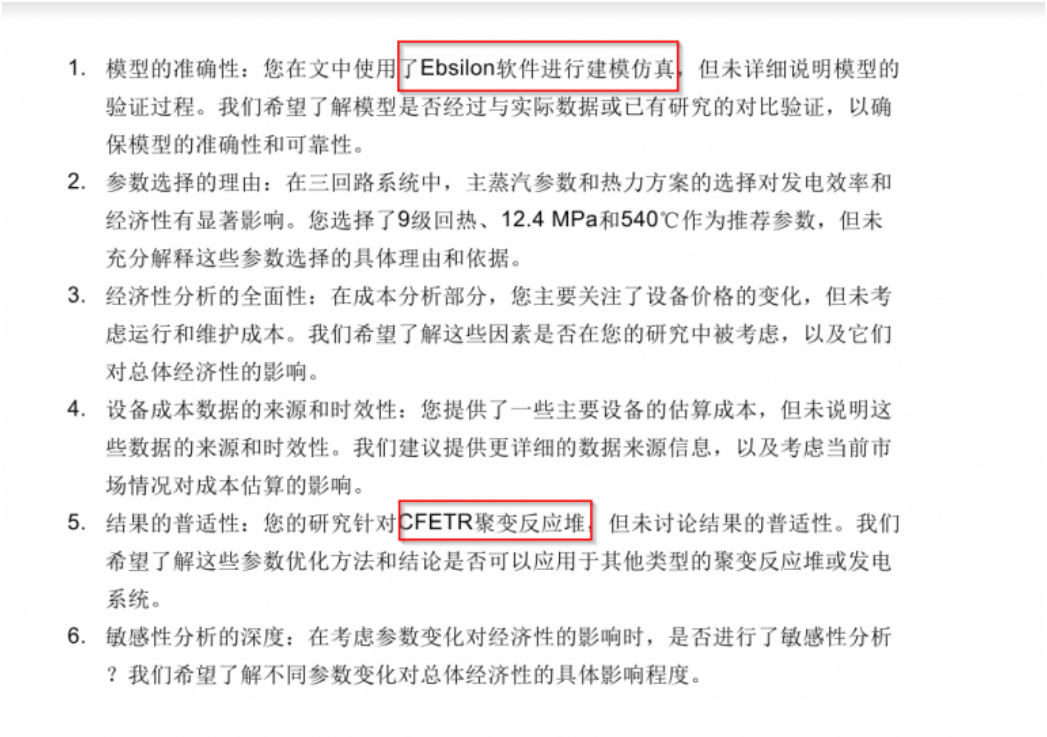
Campaign 1: Targeting Defense industry.


Discussing a theoretical method for coordinating various types of military platform

1. 论文中提出的异构平台要素协同理论方法，是否已经得到了充分的实验验证？能否提供更多的实验数据来支持理论的可行性和有效性？
2. 在构建多层作战网络模型时，是否考虑了实际战场环境中的复杂因素，如通信干扰、电子对抗等？这些因素是否会对模型的准确性和稳定性产生影响？
3. 论文中提到的杀伤链算子和协同序参量等概念，是否有明确的量化标准和计算方法？这些概念在实际应用中是否具有可操作性？
4. 在进行杀伤链动态重构时，是否考虑了作战要素的物理位置和动态变化？例如，当作战要素发生移动或失效时，如何保证杀伤链的连续性和稳定性？
5. 论文中对要素协同能力的不确定性进行了讨论，但在实际应用中，如何评估和控制这种不确定性对作战效果的影响？
6. 在仿真实验部分，是否考虑了不同作战任务和场景对要素协同效果的影响？仿真结果是否能够涵盖多样化的作战需求？
7. 最后，论文中的模型和方法在实际军事应用中是否有先例或相关经验可以借鉴？是否有与现行军事理论和实践相结合的考虑？

We found this lure along with one of the Cobalt Strike beacons, which seems to be an evaluation of a research paper focusing on proposed theoretical framework in military operations.

Campaign 2: Targeting Electro-technical Researchers.

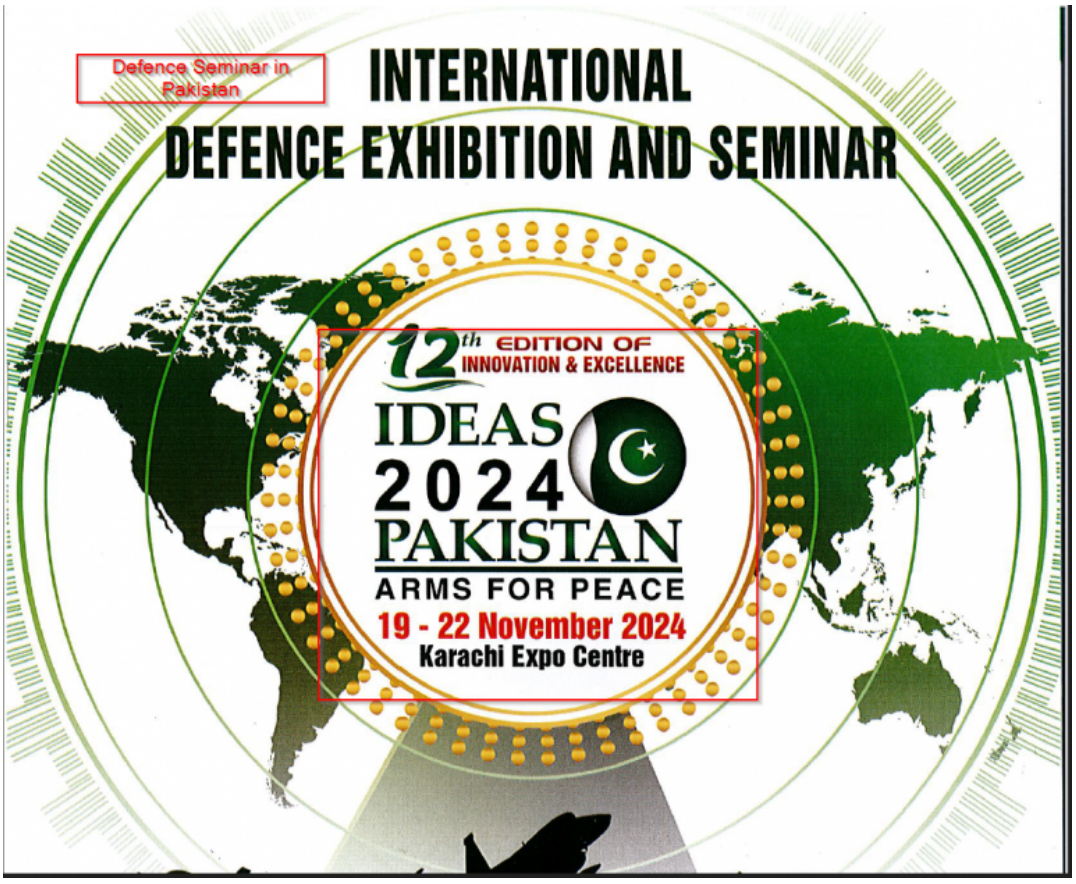

1. 模型的准确性：您在文中使用了Ebsilon软件进行建模仿真，但未详细说明模型的验证过程。我们希望了解模型是否经过与实际数据或已有研究的对比验证，以确保模型的准确性和可靠性。
2. 参数选择的理由：在三回路系统中，主蒸汽参数和热力方案的选择对发电效率和经济性有显著影响。您选择了9级回热、12.4 MPa和540℃作为推荐参数，但未充分解释这些参数选择的具体理由和依据。
3. 经济性分析的全面性：在成本分析部分，您主要关注了设备价格的变化，但未考虑运行和维护成本。我们希望了解这些因素是否在您的研究中被考虑，以及它们对总体经济性的影响。
4. 设备成本数据的来源和时效性：您提供了一些主要设备的估算成本，但未说明这些数据的来源和时效性。我们建议提供更详细的数据来源信息，以及考虑当前市场情况对成本估算的影响。
5. 结果的普适性：您的研究针对CFETR聚变反应堆，但未讨论结果的普适性。我们希望了解这些参数优化方法和结论是否可以应用于其他类型的聚变反应堆或发电系统。
6. 敏感性分析的深度：在考虑参数变化对经济性的影响时，是否进行了敏感性分析？我们希望了解不同参数变化对总体经济性的具体影响程度。

We found another lure which discusses about critics on a research paper, which focuses on modeling and simulation of a power generation system, mentioning Ebsilon software and CFETR [China Fusion Engineering Test Reactor].

Campaign 3: Targeting Electronic Engineering Education Industry.

Well, upon extracting a RAR based on our hunting known as 博士后申请-王玉玺-华中科技大学-电气与电子工程-博士 which translates to Postdoctoral Application – Wang Yuxi – Huazhong University of Science and Technology – Electrical and Electronic Engineering – PhD in English, we found that the threat actor had been targeting the victim by using lures of postdoctoral application pro s of individuals.

Campaign 4: Targeting Defense Industry of Pakistan.



Upon looking into this lure, we found out that the lure is basically targeting Pakistani Defense Industry, the lure contains data on information about the upcoming exhibition in Pakistan in November 2024.

Other interesting campaigns

ylodes lancea

AO Ye[1], ZHANG Yi-feng[1] ✉,

r Chinese Materia Medica, China
b Medicine, Ministry of

t *Atractylodes lancea*, and it
ing cold, and brightening the
in clinical practice, including
and hepatoprotective effects.
oportion of the main active
e research progress of genes
cting their biosynthesis, so as
terpenoids in *A. lancea* and

Medical Research

燥根茎入药，具有燥湿
重要的药用价值[2,3]。同
[4,5]。苍术作为我国大宗
类化合物是苍术重要的
成分含量和组成变化大
物合成途径尚未完全解
文系统整理了苍术倍半

FORECAST OF PAKISTAN ARM

2024 - 2025 (GRAT

Targeting Pakistani Military Academy

TRAINING INSTITUTIONS
PAKISTAN MILITARY ACADEMY
SCHOOL OF ARMOUR AND MECHANIZED WARFARE, NOWS
SCHOOL OF ARTILLERY, NOWSHERA
SCHOOL OF ARMY AIR DEFENCE, MALIR KARACHI

We also found these interesting lures from campaigns targeting Pakistani Military Academy & Chinese Cybersecurity Researchers mimicking CNCERT, well last but not the least, we also found that the threat actor also targets medical institutes based out of China.

Based on the beacons of all these similar implants, we found most of this samples connect to the similar Command & Control server with exactly the same ASN5090 registered with Tencent as shown below:

IP	ASN	Geolocation
139.155.190..84	AS45090 (Shenzhen Tencent Computer Systems Company Limited)	China
43.137.69.76		
139.155.190.198		
106.55.77.71		
129.204.98.221		
119.45.2.30		
119.45.67.241		
119.45.2.56		

A huge set of host headers have been identified that are linked to Tencent (*tencentapigw.com or *tencentcs.com), of which few are:

Host Headers
service-a8vp3r65-1319584009.cd.tencentapigw.com
service-c2y0jtba-1319584009.gz.tencentapigw.com.cn
service-qgezbin5-1319584009.sh.tencentapigw.com

service-h87kxr41-1319584009.bj.tencentapigw.com.cn
service-cyuasu6k-1319584009.nj.tencentapigw.com
service-3z1ebnpd-1319584009.sh.tencentapigw.com
service-b4ibcyjt-1325935989.sh.tencentapigw.com
service-k6iylaqt-1319584009.bj.tencentapigw.com.cn
service-7wu3p58s-1319584009.nj.tencentapigw.com

Conclusion

A new threat actor campaign has been uncovered that primarily focuses on the Defence and research sectors in South Asian nations, particularly targeting Pakistan and Hong Kong, with an increasing interest in India. Our analysis indicates a significant focus on engineering researchers, professors, and key entities in **Hong Kong, Mainland China, and Pakistan**. Leveraging sophisticated lures—such as decoy documents related to electrotechnical societies, energy infrastructure, civil aviation, and environmental engineering—this campaign strategically targets professionals in technical fields. The actor heavily relies on the post-exploitation tool Cobalt Strike to execute their operations, suggesting a methodical approach to cyber-espionage.

Based on the tactics, techniques, and procedures (TTPs) employed in the campaign, including the consistent use of malicious **LNKs**, **VBScript**, and **Cobalt Strike** payloads, we can conclude that this threat actor has specifically targeted this group of victims since **May 2024** based on timestamps. The scope and complexity of the campaign, coupled with the tailored lures, strongly suggest a targeted effort by an APT group to compromise sensitive research and intellectual property in these industries.

It is recommended to take necessary precautions to stay protected – don't click any unknown links or download suspicious attachments, update your anti-virus solutions and software systems, backup your data regularly and enable multi-factor authentication.

SEQRITE Protection

- Whisper.49086.GC
- Whisper.49085
- CobaltStrike

IOCs

Archive

MD5	Filename
86543a984e604430fb7685a1e707b2c4	科学技术奖填报说明和奖励办法修订版.rar
95557088474250a9749b958c3935dee4	最新停车场收费标准调整方案.rar
95f05674e4cb18a363346b488b67fd38	╒δ╢ ╘í╢│Θ╥«╨ε─▄╡ⁿ ╒╡ ╨Σ╥«╖ó╡ⁿ╤╡═│╖╜░╕ ╒Φ╜ ╞▒╚╥í╥╨╛┐ í╖╡─╨ █╡─╜¿╥Θ.zip
b8c94d2f66481cc52b30948f65fed761	╢╥╕ µ═╢╖┼╥¬╟≤╨Θ.zip
4cf9bd6af64c3937e156ffb20537a6c1	预加油航班管理方法研究与软件实现（修改意见）.rar
b2649134fbf0520222263d73b7e985d8	aaa.zip
af669dfa074eb9b6fda3fd258f58e2d2	贾哲文-云南大学-环境工程.rar
865483fea76242e687aa9e76b1a37f28	刘潇-清华大学-计算机.rar
432230af1d59dac7dfb47e0684807240	李新宇-北京大学-2026毕业-金融硕士.rar
b9d04a61b30ddf53b28bf58a86fc28f5	热核聚变发电岛三回路参数优化研究（修改意见）.rar
2d478e4527486d85932254c7a7413951	国家互联网应急中心CCSC认证邀请函_海关信息中心.rar
e08dcbbd3e2ab9bcc2c02c44b6a97870	异构平台要素协同理论方法研究(修改意见).rar
fe4c575abf70ad11cdbce0b0821ee681	博士后申请-王玉玺-华中科技大学-电气与电子工程-博士.rar

68278e47f36a44d9a8bbd46b74422bbe	企业资质材料.zip
58f5ff5be4e765e62758b1f3e679a2ac	针对《苍术倍半萜类化合物生物合成的研究进展》的修改建议.rar
955841a4d2315422818b47aec6ce51fb	中债数据无法使用情况.rar
75def3a25b1d355c9163d3c247990867	参编《人工智能通用大模型合规管理体系 指南》申请表.rar
343a3944218a040089fa7131112c1681	中国外汇交易中心信息产品许可表.rar
b28bb7cabfb12e9bc5b87692b065c83a	Islamabad_Security_Dialogue_Pub.rar
7728fee377137e83e9bd1c609cc166c0	IDEAS_2024_Calling_Letter.zip
dad7d9528e9506ebd0524b3ebd89ddf2	Final_Combined_Forecast_MCP_FY_2024_25.zip

LNK

MD5	Filename
22c07c76020f9311385cfaa97a2d6adb	附件1：《2024年度中国电工技术学会科学技术奖推荐提名书》（技术发明奖和科技进步奖）填报说明(2024年8月新版).pdf.lnk
7a494f7448bc350bb46fb7f21450d1d9	最新停车场收费标准调整方案.lnk
3c3986899bdb4890ea6d44c00538e2fd	╒δ╢ ╘í╢│Θ╤«╨ε─▄┤ⁿ╒╛╧Σ╤«╖ó┤ⁿ╧┤═│╖╜░┐╓Φ╜╞▒╚╓í╤╨╛┐í╖┤─╨▐╚─╜¿╖Θ.docx.lnk
74ca14032a93be59098d607ba7039660	预加油航班管理方法研究与软件实现（修改意见）.docx.lnk
cd14d51d27f294c2e60d1bc3ef907160	电影宣传要求.pdf.lnk
db08274efb374e2196a9f46961c8d8f8	需使用中债数据.jpg.lnk
62eb90df5ee3a3b443c277d12b893141	贾哲文-云南大学-环境工程.docx.lnk
41b5d5a04cf4534550e6ac3fc9a8f42d	刘潇-清华大学-计算机科学与技术学院-硕士.pdf.lnk
ae55cb4988f2f45197132631f5a86632	filename.lnk
5ae488083403cd69002c29ef6326cca7	李新宇-北京大学-2026毕业-金融硕士.pdf.lnk
72011305317d7e9d38a0e75650f22e34	修改建议.docx.lnk
d73a5c11423923d8a8c483cf6172f7e2	<NA>
473adee7068573fd01862b4bf43979e6	Islamabad_Security_Dialogue_Pub.pdf.lnk
a02a664f80d9011e38c45762683771c0	Final_Combined_Forecast_MCP_FY_2024_25.pdf.lnk 12th_Edition_Of_Innovation_&_Excellence_IDEAS_2024.pdf.lnk
10d0a351df1bfe57494ac18a7f2edec1	热核聚变发电岛三回路参数优化研究（修改意见）.docx.lnk
10d6fb6ab395001a4424058a52c3c69f	国家互联网应急中心CCSC认证邀请函_海关信息中心.pdf.lnk
1070fc4a998cb7515842fb1b647340be	异构平台要素协同理论方法研究(修改意见).docx.lnk
1b538fef54102fd36e83e4fc549f960e	博士后申请-王玉玺-华中科技大学-电气与电子工程博士-简历.pdf.lnk
c8231c5709ca548f1fe70f3b61d3537a	针对《苍术倍半萜类化合物生物合成的研究进展》的修改建议.docx.lnk
955a8b63723eb35686ddce6cbfe890cf	中债数据无法使用情况.jpg.lnk
da623c5ca61e25c6205904a5cb91bd55	参编《人工智能通用大模型合规管理体系 指南》申请表.pdf.lnk
afc805006390b00713898c09d50343b6	中国外汇交易中心信息产品许可表.doc.lnk

VBS

MD5	Filename

0a34cc8983fb581a59308135868b75d0	O365.vbs
5d18995193465c618844949f0ff9c786	cache.vbs
4c409d7201ec5dccf55a8ea54b0de101	DS_Store.vbs
39ab2053406493b9a0d81ed40212ffa8	O365.vbs
4711d0d163c00158abd4b20177d68b9a	DS_Store.vbs
3dce8d8f9664c755448413cbfe1bc08f	DS_Store.vbs
3b573c2229b43bde50f998f6cba17f2f	DS_Store.vbs
318a1a18df75b49f72fbcc020384cc24	DS_Store.vbs
a0d760492c0193d14114792f0c3fff7a	cache.vbs
cafdc03dcbe06ac43ec25fb38c1e013f	cache.vbs
d13828ae89a7dab34d2f380eef518332	cache.vbs
7e98bb7ffba4cf12d29132a2c71973eb	cache.vbs
c3d460ac3a93e86782c2bc374aa5ecd2	Anx.vbs
93eafad827126a9d12fc1d0e6e21aaef	cal.vbs
a4a47dd08cf59f8b6a7c907cf0e39029	cal.vbs
b2c882f6121d758cfcd4ece31834f497	O365.vbs
86e4c5d39dda20eee4dd8f794be04c80	DS_Store.vbs
e7f3c33a5cd569ebf4b57381f03c5337	cache.vbs
7ac5daaa5fe4e59137271eaf97c9e692	O365.vbs
a2f64bafeafbeb303d24fd6ed1f5a89a	DS_Store.vbs
8ba5b61454a29e09e7f536e85c951f53	DS_Store.vbs
4eeeb2b40e7189c271098c515b8f91d8	DS_Store.vbs
3711e1913f2ae74c4fc765bc28dbc60f	DS_Store.vbs
e112698125e67a1a6f26597371cae502	DS_Store.vbs
67dc90468327a0c733ca48881084593b	cache.vbs
d68fb3502e63ef3ca91c45f508d146b9	cache.vbs
91b7328a6064706fa9f125621a09f648	cache.vbs
bfd61e5e133b2cd592d42ecdbc0eaee2	cache.vbs
e5e709be4584031aefdc2a0782017f8f	cache.vbs
cf59916d271dce7f44bbf349464a31e2	cache.vbs
5d18995193465c618844949f0ff9c786	cache.vbs
e213dc8060794bb97c5f94f563107e88	cache.vbs
d01e7c41140aeff82ad87a558ae96587	DS_Store.vbs
de3a0ff11c7645f5d0ac717b0eb98e52	cache.vbs

Cobalt Strike (EXE)

MD5	Filename
d29980f768aafdcf102cf1b3741c8a2b	ImeBroker.exe / cache.bak

2acfad6fd814b02683038d21ba3eccbe	ImeBroker.exe / cache.bak
1aa1f12d26d3a34265d0b99705bdf283	DevicesFlow.EXE / DS_Store
e7550dd2db4dbe1a2cc1dadc47846cd0	ImeBroker.exe / cache.bak
1d109c8bb9e6ad16cd5f6813db39c21a	Microsoft IME / DS_Store
d8c348a2f27097d8689dba4452bb76eb	charmap.exe / DS_Store
14df06539b72837adb9f8d13cfcea6db	CTTUNE.EXE / DS_Store
6388625810652f0767be13b43363c10d	ImeBroker.exe / cache.bak
e8d3540212384d45ba9d7135c5bf8d8e	ImeBroker.exe / cache.bak
352e299fc3f2327bfad5026b4a56b7cb	ImeBroker.exe / cache.bak
73fa6149e68dd7842f7cfce78dd732c5	ImeBroker.exe / cache.bak / sigverif.exe
3813e4ebddd87615c1adc9c05888341d	企业资质材料/企业签名解密专用解密工具.exe D:\MyPrograms\vs2022\vt01\vt\x64\Release\vt.pdb
316e8d798f7db625c207532e2f7a5d38	keycongif.exe / Anx
5e7dba4aafb8176ab026e2f4aa3211dd	Adobbee.exe / cal
33b3e322679f1500a9f3c162e4b25040	ImeBroker.exe / cache.bak
2694553347f23e250ed70a8c23096d8f	BioEnrollmentHost.exe / DS_Store
800be8a4989d4b7ed07ddd068c6469f1	DevicesFlow.EXE / DS_Store
bfd6c2f0787865ecb1604439ea9a5f15	imecfmui.exe / cache.bak
49c5553995f032195890b5bfc2abcb00	ImeBroker.exe / cache.bak
ae9d676e4eda5cfa18a061e4bc2b1637	ImeBroker.exe / cache.bak
008255c14420420e9a53c9959d0d08b8	ImeBroker.exe / cache.bak
49a9c56fab34795b7e6e4c0b6185ca3e	ImeBroker.exe / cache.bak
d901fa81a4b3d83219440b80a1c338bc	ImeBroker.exe / cache.bak
88b8bbe04b53e4af857cd1c032968c94	ImeBroker.exe / cache.bak / sigverif.exe
1d065492e7b5d118e31e571cc53dfe65	ImeBroker.exe / cache.bak / sigverif.exe

Decoys

MD5	Filename
98b85b474c02ce8c0a33ad7507abbf2a	subscription.db
5368f0b6ff56cce0de42165f14067427	附件2：《中国电工技术学会科学技术奖励办法》（2024年4月修订）.pdf
22ce60653860fe33bdfc47ce60deb681	│Θ╥«╨ε─▄┤τ╒╜╨Σ╥«╖ó┤τ╧═┤═│╖╜░╕╔Φ╝╞▓╙╞í╤╨┤┐_╥╤╫╚╞µ.pdf
b69c075caff565528bf42705d936a066	cache.db
477c5abea7299891b7f7c487f8636613	╡τ╙░╨√┤½╥¬╟≤.pdf / 电影宣传要求.pdf
298a27e24e4ca917020fa5a230fe6c8f	subscription.db
820485d456ce6bfab933a1b662ff590a	贾哲文-云南大学-环境工程.docx
55467fcb1b51477104442e74d7baf3df	cache.db
ab1bc05e7f110042d7eacda5724918e0	cache.db
8423873a0eee6139c1eb6d5a9919121b	企业资质证明（请先解密）.pptx
6833e934c675717a0581472e00cb6d93	12th_Edition_Of_Innovation_&_Excellence_IDEAS_2024.pdf

9294dd350f921745602f745e501e8e43	预加油航班管理方法研究与软件实现.pdf
43bed053851e7a182b99835bcd1d2d16	需使用中债数据.jpg
154bf965c1c8e54540179b2d01c4202e	刘潇-清华大学-计算机科学与技术学院-硕士.pdf
1fbffdc19d3cfee158558e266206f46f	李新宇-北京大学-2026毕业-金融硕士.pdf
8bdd5587b9863bdb154d9db85c67037b	热核聚变发电岛三回路参数优化研究.pdf
05770b4da4f87150f2faf6c4e821f727	cache.db
c5b2970e227e311abb5acf480bc48934	异构平台要素协同理论方法研究.pdf
edd1a870a0eea3bf9dcbd88ece487920	cache.db
1c2126ea78d3430ce04bf96b0d1c524e	JPCS-2021-A_novel_current_differential_protection_for_MMC-HV.pdf
13097891c790fbd3df75a2aebf993b16	论文及荣誉证书/电力系统自动化-2024-逆变型新能源场站送出线时域方向元件.pdf
23bd40035a9a9fd1d31a1c7aceda1727	IET-2022-A simplified model of Type-4 wind turbine for short-circuit currents simulation analysis.pdf
7763e73dd2e877c4770c0f10e4d3a1dd	论文及荣誉证书/教育部学籍在线验证报告-王玉玺.png
162a9b9aee469b8de10c37c6311906cd	Islamabad_Security_Dialogue_Pub.pdf
e8db7191c84a84717bffd0f1af9de36c	Final_Combined_Forecast_MCP_FY_2024_25.pdf
91611a155d4722d178f7697cd4ddd95f	苍术倍半萜类化合物生物合成的研究进展_冯铃芳.pdf
75c1403abfbe9f5c92625a1baf8b22f5	subscription.db
d967a709472775c118ec339963c1d940	中债数据无法使用情况.jpg
154141caa12b828ace18fd4b3fda77e0	参编《人工智能通用大模型合规管理体系 指南》申请表.pdf
c116a1971593a3a5468eb972b505fb57	cache.db
63d4015195c5006d81e14a85aa2459c4	联系方式.txt
a3df3505d89c15bb3940062f7abd786b	联系方式.txt
041d01a5495cdede35f4ad8e1fe437f7	清华通知.txt

MITRE ATT&CK

Tactic	Technique ID	Name
Initial Access	T1566.001	Phishing: Spear phishing Attachment
Execution	T1204.002 T1059.005	User Execution: Malicious File Command and Scripting Interpreter: Visual Basic
Persistence	T1053.005	Scheduled Task
Defense Evasion	T1055.002	Process Injection: Portable Executable Injection
Discovery	T1033	System Owner/User Discovery
Command and Control	T1071.001	Application Layer Protocol: Web Protocols

Authors

- **Sathwik Ram Prakki**
- **Subhajeet Singha**