DIGITAL FRONTLINES : INDIA UNDER MULTI-NATION HACKTIVIST ATTACK

Published On : 2025-09-15

DIGITAL FRONTLINES : INDIA UNDER MULTI-NATION HACKTIVIST ATTACK

EXECUTIVE SUMMARY

At CYFIRMA, we are committed to offering up-to-date insights into prevalent threats and tactics employed by malicious actors, targeting both organizations and individuals. In July–August 2025, India faced a surge of

cross-border cyberattacks combining data breaches, DDoS, defacement, phishing, and malware. Pakistani group, Team Insane Pakistan, claimed High Court server breaches; Sylhet Gang-SG disrupted the Defence Ministry site; and Russian-aligned RuskiNet warned of “Operation Trinetara.” Indian groups retaliated under “Operation Vasudev Strike,” hacking Pakistan’s Ibn-e-Sina University. Indonesian group Raizo defaced an Indian transport site, while phishing cloned the eChallan portal, and a fake Income Tax notice spread malware with Chinese indicators—highlighting the growing multinational hacktivism against India’s digital infrastructure.

INTRODUCTION

India’s digital infrastructure has increasingly become a focal point of cross-border cyber hostilities. In July–August 2025, a series of high-impact incidents—including judicial server breaches, government website disruptions, retaliatory defacements, phishing schemes, and malware campaigns—highlighted the growing scale, sophistication, and multinational nature of hacktivist operations targeting Indian entities. These attacks, spanning actors from Pakistan, Bangladesh, Russia, Indonesia, and likely China, underscore a shifting threat landscape where hacktivism and cybercrime blend to challenge national security and public trust.

KEY FINDINGS

- Escalating Hacktivism: Coordinated cross-border campaigns from Pakistan, Bangladesh, Russia, Indonesia, and likely China targeted Indian judicial, defense, and transport systems.
- High-Value Data Breaches: Pakistani group, Team Insane Pakistan, claimed to compromise millions of case records, FIRs, user credentials, and judicial officer databases from Indian High Courts.
- Service Disruptions: DDoS attacks, such as Sylhet Gang-SG’s takedown of the Ministry of Defense website, demonstrated the vulnerability of critical government portals.
- Indian Retaliation: Indian groups under “Operation Vasudev Strike” (Shadow Phantom, Team Red Eagle, Shadow Protocol) launched counterattacks, including hacking Pakistan’s Ibn-e-Sina University website.
- Defacement & Phishing: Raizo defaced an Indian transport website; attackers cloned the eChallan portal to steal citizens’ personal data.
- Malware with Foreign Indicators: A phishing campaign impersonating India’s Income Tax Department distributed malware containing Simplified Chinese resources, pointing to likely Chinese threat actor involvement.
- Multi-Vector Threat Environment: Incidents combined data theft, disruption, propaganda, and malware delivery, signalling a shift from isolated attacks to coordinated, multi-nation campaigns against India’s digital infrastructure.

OPERATIONS AND TACTICS

Targeted Breaches: Team Insane Pakistan allegedly infiltrated High Court servers in Punjab & Haryana and Andhra Pradesh, extracting millions of judicial records, FIRs, and login credentials to publicly embarrass

Indian institutions.

DDoS Campaigns: Sylhet Gang-SG disrupted the Indian Ministry of Defense website on Independence Day using distributed denial-of-service attacks and published check-host proofs to amplify impact.

Strategic Announcements: RuskiNet pre-signaled its “Operation Trinetara,” linking cyber retaliation against India to the Palestine conflict to create psychological pressure before actual attacks.

Retaliatory Hacking: Indian collectives Shadow Phantom, Team Red Eagle, and Shadow Protocol coordinated “Operation Vasudev Strike,” compromising Pakistan’s Ibn-e-Sina University site and exposing admin credentials as a show of offensive capability.

Defacement as Messaging: Indonesian group Raizo defaced India’s transport website with political slogans to broadcast dissent and signal cross-border solidarity among hacktivists.

Phishing & Data Harvesting: Attackers cloned the Ministry of Road Transport’s eChallan portal to collect citizens’ sensitive details (names, PAN, mobile numbers, DOBs) under the guise of official services.

Malware Delivery via Social Engineering: A fake Income Tax “Penalty Notification” ZIP file lured victims into executing a 43 MB malicious installer hosted on a suspicious IP. Metadata with Simplified Chinese resources indicated likely Chinese actor involvement, blending spear-phishing with advanced malware tactics. The payload masqueraded as an official document, and upon execution, established communication with the remote IP 103.97.128.77, performed file and registry operations, created persistence through process injection, and concealed its activity via configuration files. The campaign demonstrates sophisticated use of social engineering—inciting panic to drive users to run the malware—as well as technical tradecraft in evasion, data exfiltration, and multi-stage infection flow, thus posing a significant risk to targeted Indian taxpayers.

ANALYSIS AND EVIDENCE

Data Leaks

On August 14, the Pakistani hacktivist group Team Insane Pakistan claimed to have breached the High Court of Punjab and Haryana’s official servers in India. They shared the targeted government domains and linked the attack with Pakistan’s Independence Day celebration.

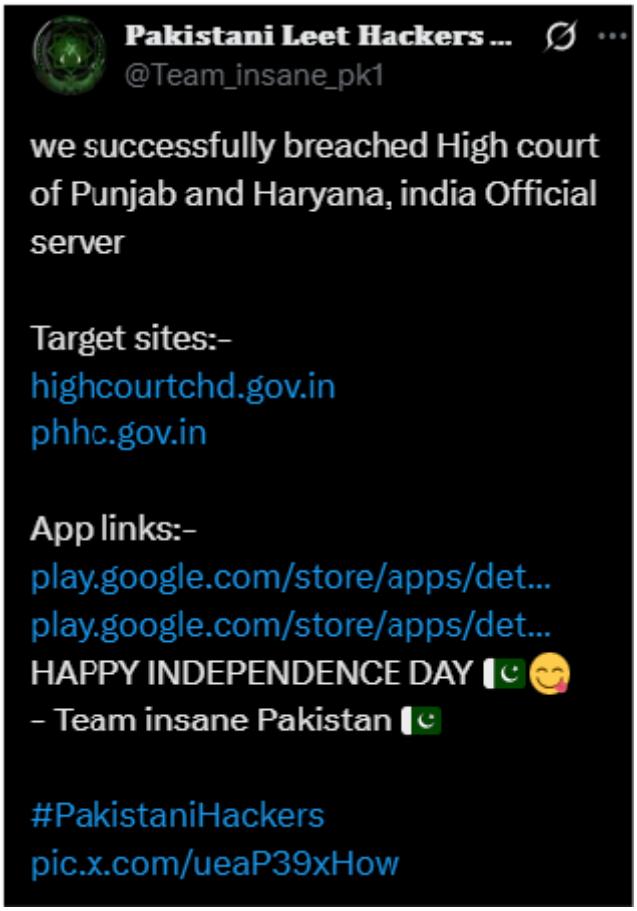


Figure 1. Claimed cyberattack announcement on social media by 'Team Insane Pakistan,' alleging a breach of the High Court of Punjab and Haryana servers, sharing links to targeted domains and apps

On August 14, the Pakistani hacktivist group Team Insane Pakistan claimed to have breached the Andhra Pradesh High Court server in India. They alleged that over 2 million case details, 2 million FIR records, user login data, and judicial officers' databases were compromised. The group also mocked the judiciary by calling it an "uneducated judges whole database."

Figure 2. Social media post by 'Team Insane Pakistan' claiming to have compromised the Andhra Pradesh High Court's entire server database, exposing millions of case records, FIR details, user logins, and judicial officer information.

On 15th August, in retaliation, the Indian cyber hacktivist group Shadow Phantom hacked into Pakistan's Ibn-e-Sina University (isu.edu.pk) website. They exposed the admin panel credentials publicly, allowing unrestricted access to the university's system as part of their cyber campaign.

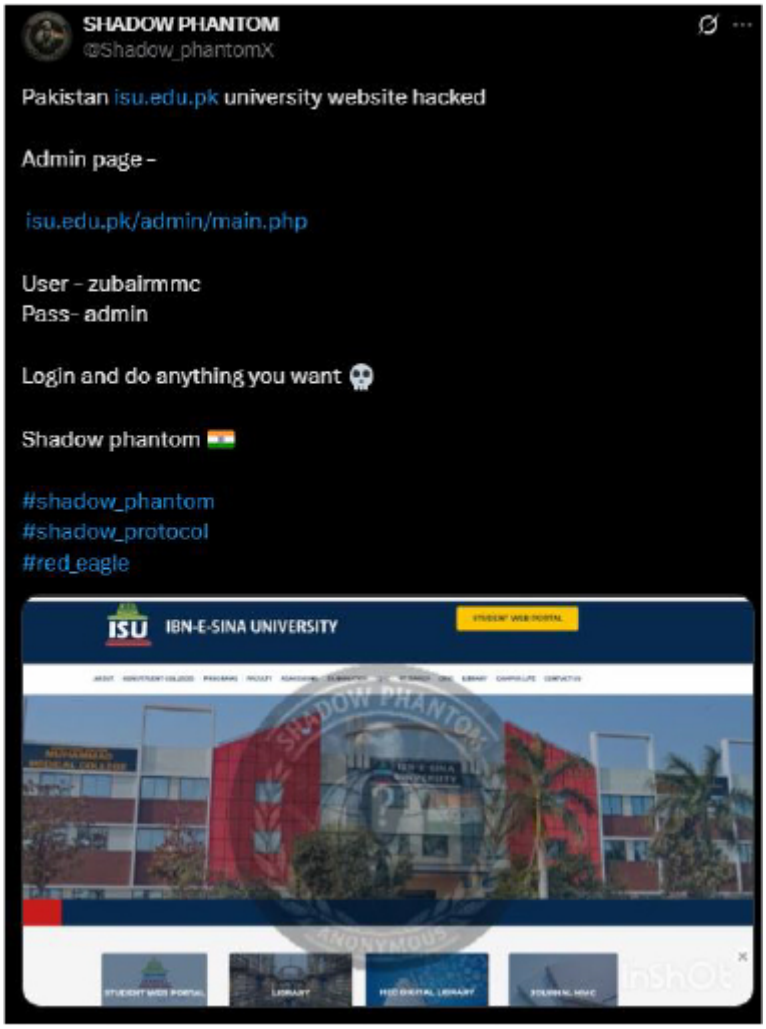


Figure 3. Post by 'Shadow Phantom' claiming to have hacked Pakistan's Ibn-e-Sina University (isu.edu.pk), exposing admin credentials and providing a link to its admin page.

DDoS Attack

On August 15, the hacktivist group Sylhet Gang-SG claimed responsibility for taking down the Indian Ministry of Defense website. They shared a check-host link as proof of the disruption.

Figure 4. Message by 'Sylhet Gang-SG' claiming responsibility for taking down the Indian Ministry of Defense website, accompanied by a masked avatar image.

On 1st August, the hacktivist group RuskiNet announced Operation Trinetara (meaning "Third Eye"), warning India of a large-scale cyber retaliation. They linked the campaign to the Palestine conflict and threatened India's data and infrastructure as part of their coordinated operation.

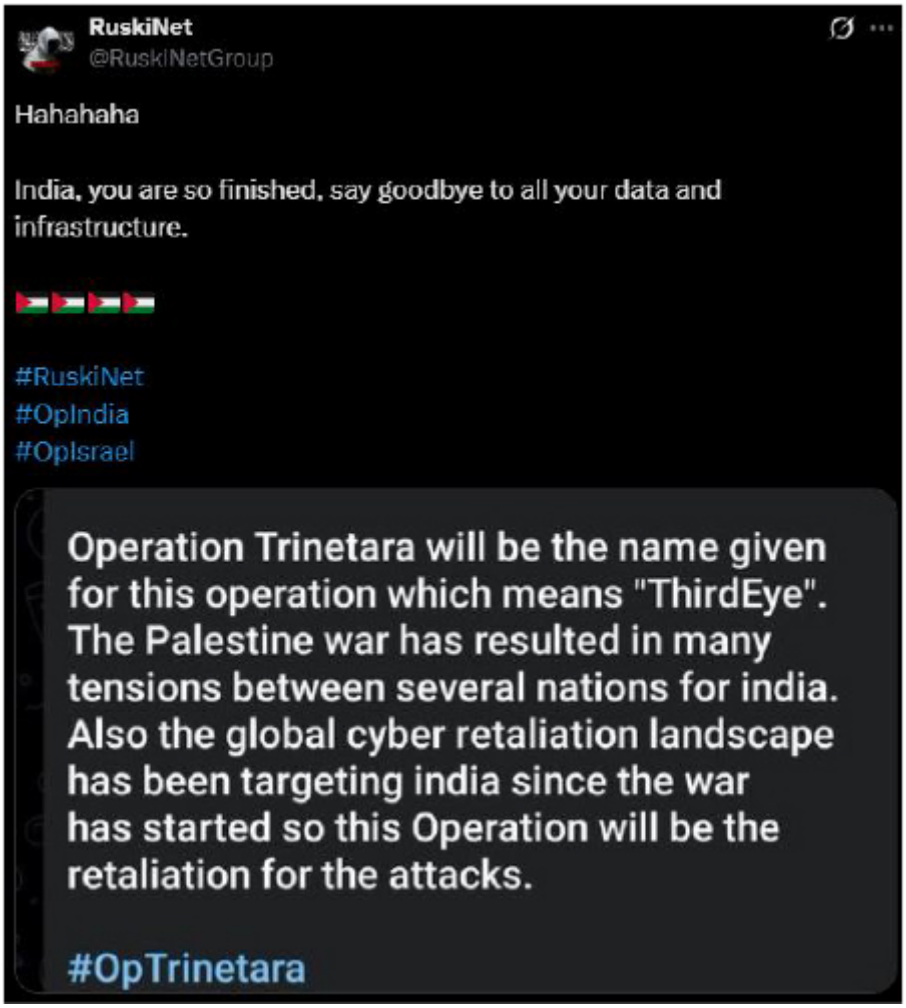


Figure 5. Post by 'RuskiNet' threatening large-scale cyberattacks against India under 'Operation Trinetara,' describing it as retaliation linked to geopolitical tensions.

Hacktivist-Groups Co-Operation

On 12th July 2025, the Indian cyber hacktivist collective Shadow Phantom, Team Red Eagle, and Shadow Protocol announced Operation Vasudev Strike. They declared that on 15th August, the world would witness the power of Indian hackers, positioning the campaign as a retaliation against Pakistan, Bangladesh, Indonesia, and Turkey.

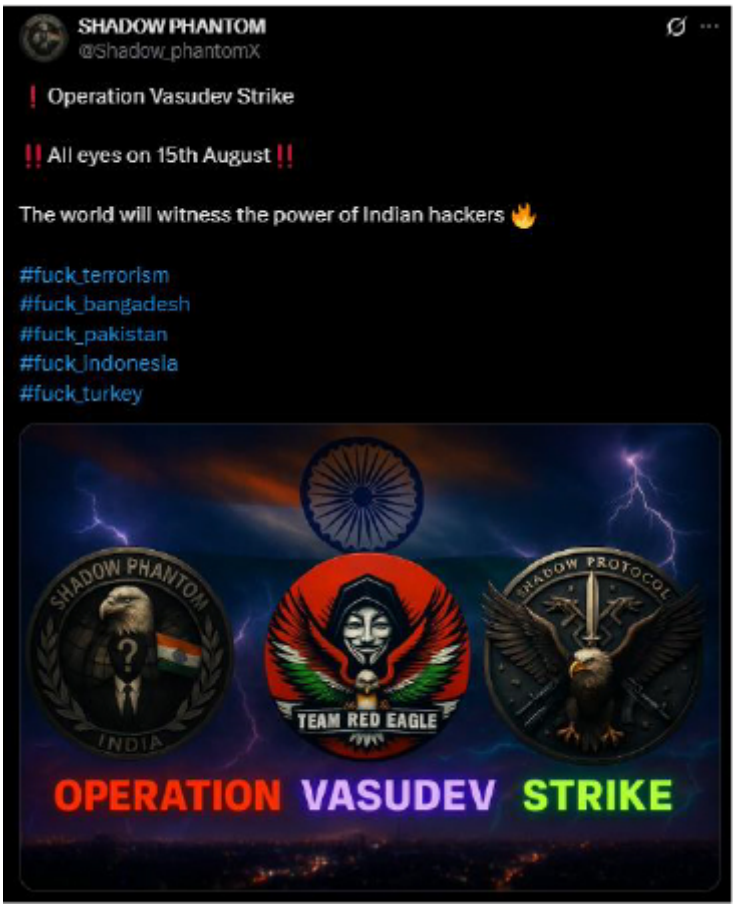


Figure 6. Indian hacker groups announce Operation Vasudev Strike, threatening cyber-attacks on 15th August targeting multiple nations

Defacement

On 30th August 2025, the cyber group Raizo defaced the Indian website rsa.morth.gov.in, leaving a message that read “RAIZO WAS HERE” alongside political slogans in Indonesian, suggesting dissatisfaction with government leadership. The attack highlighted emerging cross-border hacktivism, as the group’s statement and iconography were directed at Indonesian audiences, marking India as a target in ongoing digital conflicts involving multiple countries.

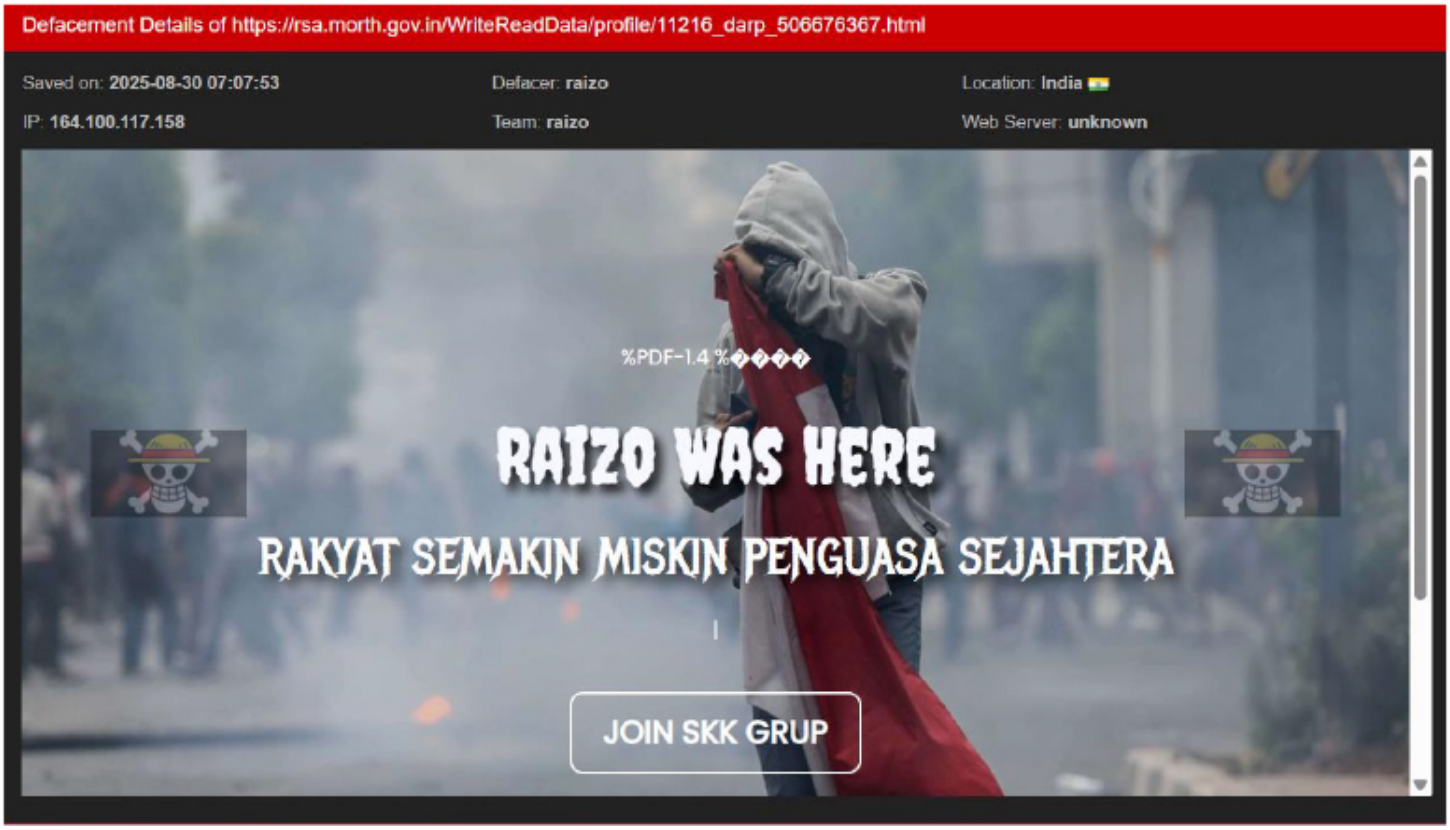


Figure 7 Defacement of an Indian government website by hacker 'Raizo', displaying protest messages and urging visitors to join their group.

Phishing

The Indian Ministry of Road Transport and Highways' eChallan portal was targeted in a cyber incident involving impersonation. Attackers replicated the official interface, likely aiming to deceive users and harvest sensitive details, like names, mobile numbers, PAN card numbers, and dates of birth, demonstrating the serious threat of impersonation and data theft against India's digital infrastructure.

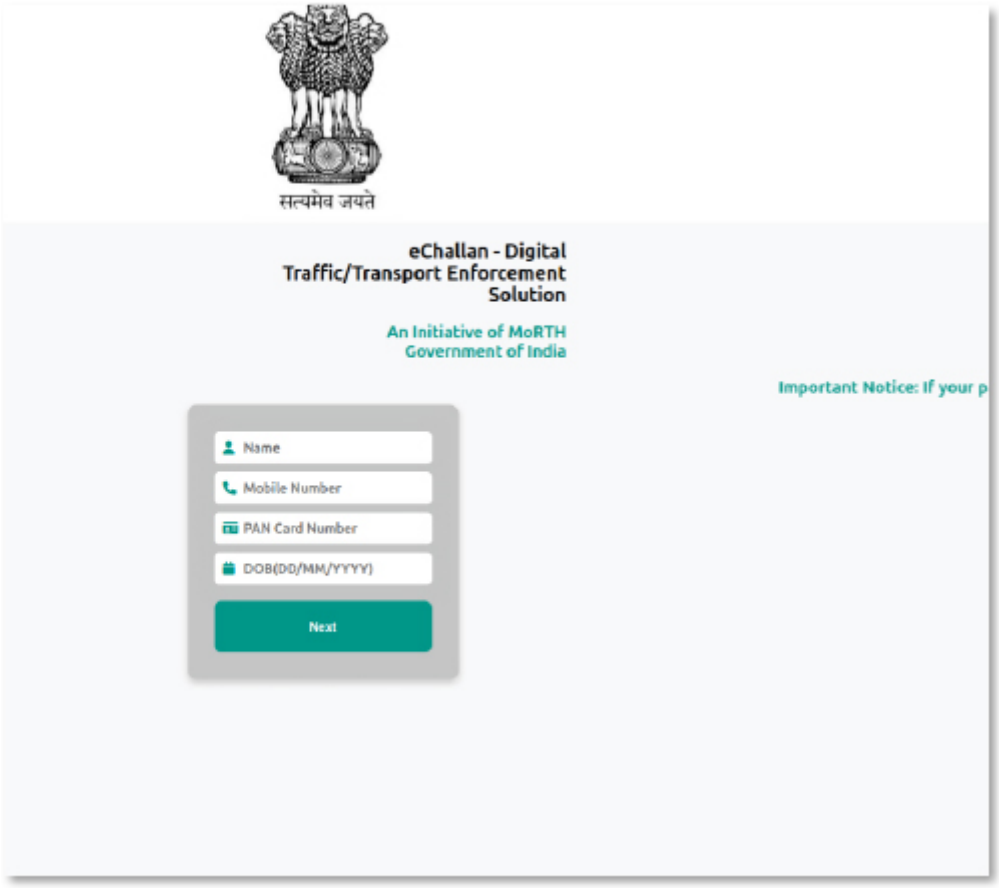


Figure 8. The phishing page impersonating MoRTH's eChallan portal, designed to steal sensitive personal information like PAN and mobile numbers.

Malware

The presented material illustrates a sophisticated phishing campaign impersonating the Income Tax Department of India, emerging prominently in 2025 during the tax filing season. Attackers have crafted convincing fake websites and fraudulent email communications styled with official logos, terminologies, and formats consistent with government-issued tax penalty notices. These deceptive notices warn recipients of alleged tax compliance deficiencies and mandate urgent document submissions through clickable links or downloadable files.

Victims are deceived into downloading a malicious zip archive labeled "Tax Penalty Notification.zip," which contains an executable named "103.97.128.77#ClientSetup.exe." Behavioral and network analysis evidence demonstrates that this payload engages in active communication with a remote IP (103.97.128.77), performs file system manipulations, registry key accesses related to system control, and attempts to conceal itself using configuration files with commands to encrypt, terminate processes, and establishes persistent footholds by creating additional processes, such as "MANC.exe," "svchost.exe," "SMSS.exe," "FSHost64.exe," and "sysaid.exe," some of which evade detection by security vendors. The malware stores configuration and log data in local folders like "install" and "log," utilizes files, such as "YTSysConfig.ini" to set exfiltration parameters (e.g., ServerIP 103.97.128.77), and leverages network activity—including TCP and UDP communications—to receive commands and exfiltrate stolen information. Through these mechanisms,

the campaign blends social engineering with advanced post-exploitation, enabling data theft, evasive persistence, and remote control over compromised systems.

The fraudulent campaign leverages social engineering to cause panic and urgency, pushing victims toward actions that compromise their systems and potentially lead to data exfiltration or broader compromise. Official warnings from the Income Tax Department and cybersecurity advisories emphasize that authentic tax communications never request passwords, OTPs, sensitive personal information, or file downloads from unverified sources. Taxpayers are urged to verify all notices directly through sanctioned portals (domains ending in @incometax.gov.in), avoid clicking unsolicited links, and report suspected phishing activities to designated authorities.

This case exemplifies the intersection of social engineering, malware deployment, and network operations exploitation within targeted phishing attacks aiming to defraud and compromise Indian taxpayers amid the critical tax filing season in 2025.

A webpage styled in the theme of the Income Tax Department of India prompts the user to download an inspection file in order to cooperate with a tax review. The central message urges clicking “Start Download” to proceed.

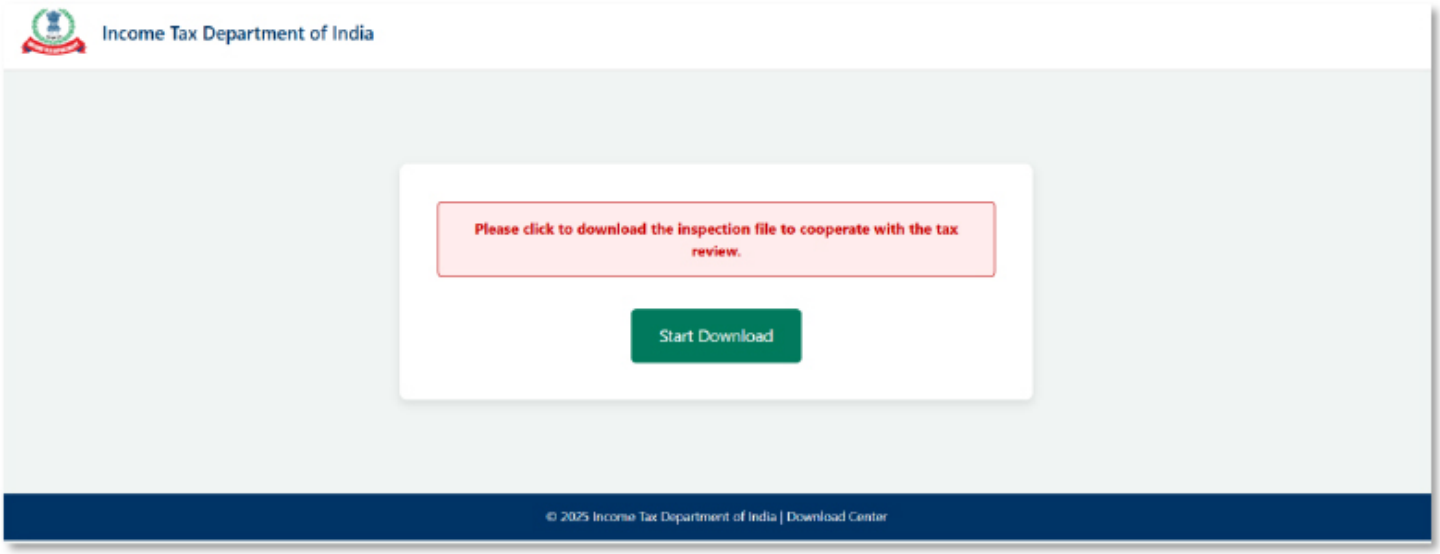
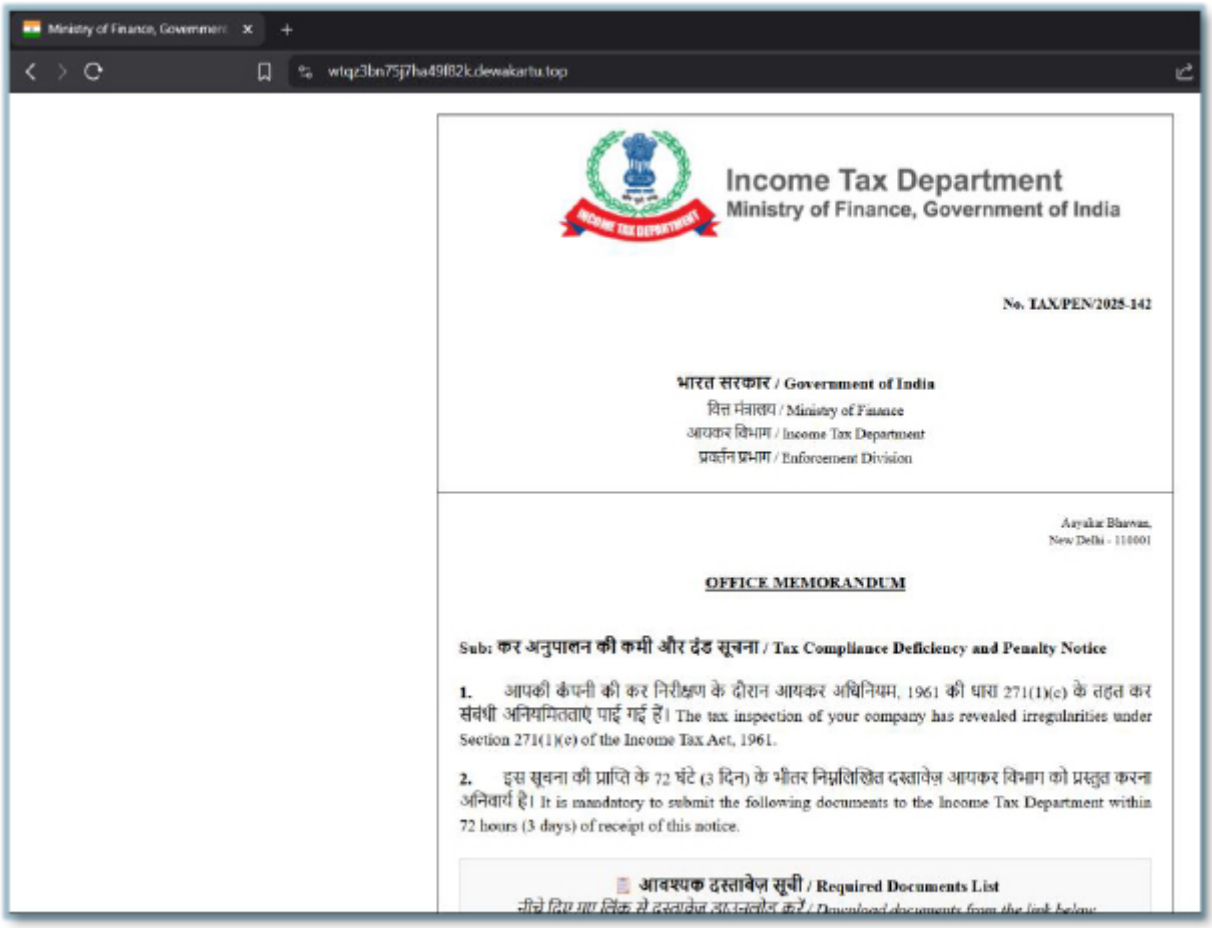


Figure 9. Fake Income Tax Department webpage prompting download of an inspection file.

A browser window displays a fake office memorandum from the Income Tax Department, Government of India, combining both Hindi and English text. The notice cites Section 271(1)(c) and requires submission of documents within 72 hours, providing a “Download Documents” button to obtain the required list.



1. आपकी कंपनी की कर निरीक्षण के दौरान आयकर अधिनियम, 1961 की धारा 271(1)(c) के तहत कर संबंधी अनियमितताएं पाई गई हैं। The tax inspection of your company has revealed irregularities under Section 271(1)(c) of the Income Tax Act, 1961.

2. इस सूचना की प्राप्ति के 72 घंटे (3 दिन) के भीतर निम्नलिखित दस्तावेज़ आयकर विभाग को प्रस्तुत करना अनिवार्य है। It is mandatory to submit the following documents to the Income Tax Department within 72 hours (3 days) of receipt of this notice.

आवश्यक दस्तावेज़ सूची / Required Documents List

नीचे दिए गए लिंक से दस्तावेज़ डाउनलोड करें / Download documents from the link below

दस्तावेज़ डाउनलोड करें / Download Documents

3. निर्धारित समयावधि में दस्तावेज़ प्रस्तुत न करने पर आयकर अधिनियम की धारा 276C के तहत कानूनी कार्रवाई की जाएगी। Legal action will be taken under Section 276C of the Income Tax Act if documents are not submitted within the stipulated time.

(राज कुमार शर्मा)
Raj Kumar Sharma
सहायक आयकर आयुक्त
Assistant Commissioner of Income Tax
Email: hymandibberthfdtgf@gmail.com

To: All concerned taxpayers

Figure 10. Tax penalty and compliance deficiency notice demanding document download within 72 hours.

Copy to: Director (Systems), CBDT, for uploading on Income Tax Department Website

A close-up of a zipped folder labeled “Tax Penalty Notification.zip” is shown, representing the downloaded file referenced on the websites.

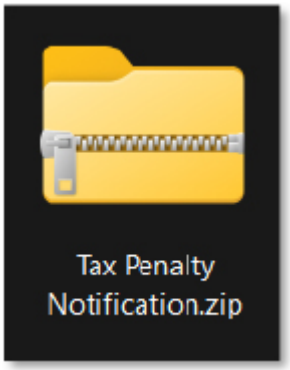


Figure 11. Tax Penalty Notification.zip, purportedly downloaded from the falsified tax notice site

A Windows file explorer window shows the “Tax Penalty Notification” folder within Downloads, displaying the file “103.97.128.77#ClientSetup.exe” with a size of 43,824 KB.

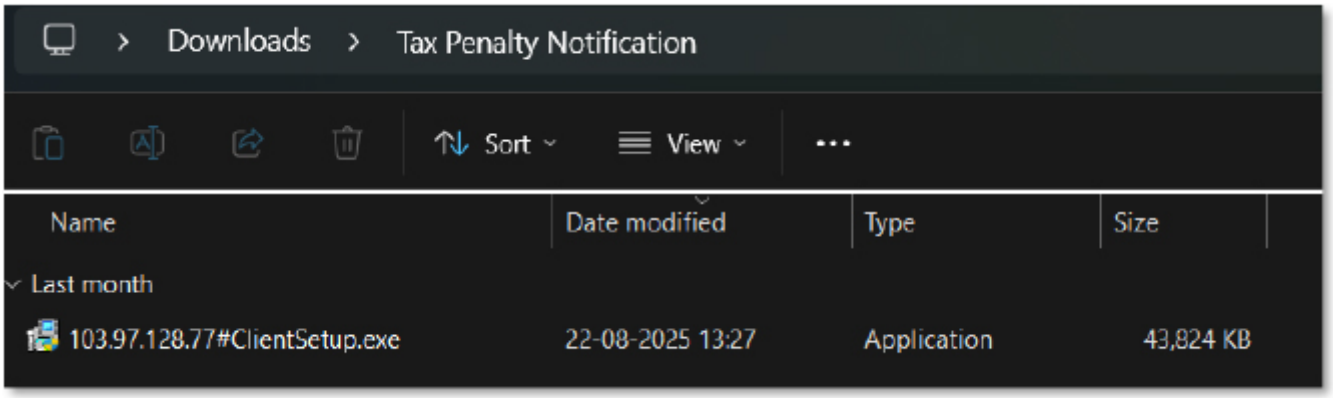


Figure 12. Tax Penalty Notification folder containing 103.97.128.77#ClientSetup.exe application

A diagram illustrates the phishing flow: starting with an Income Tax Department-themed phishing site, leading to the download of Tax Penalty Notification.zip, which contains the malicious file “103.97.128.77#ClientSetup.exe”.

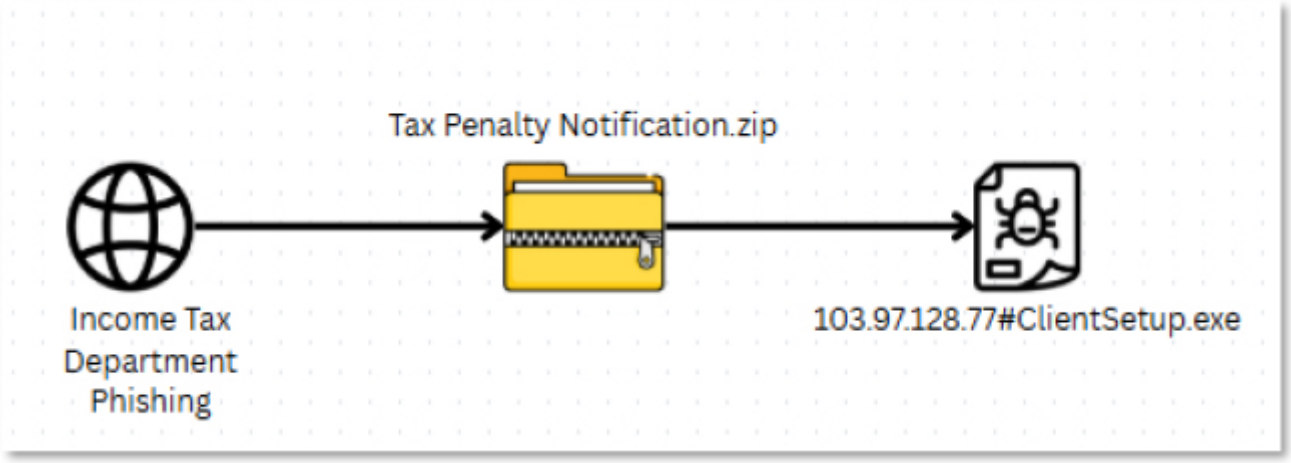


Figure 13. Phishing attack flow from a fake Income Tax site to the delivery of 103.97.128.77#ClientSetup.exe malware.

The metadata shows details of an executable file. The language is specified as Chinese-simplified (code-page 1200, Unicode UTF-16), with the company name listed as “china” and the file version 3.0.0.1. The internal name field contains Chinese characters, “???????”, which translates to “Setup Package Creation Tool”, and the file description/version date is “2023.7.10”.

version > unknown	n/a
first -1 bytes (hex)	88 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00...
first -1 bytes (text)	...4....V..S._..V..E..R..S..I..O..N._..I..N..F..O.....?.....
version > location	0x02AC7C58 - 0x02AC836C
size	0x00000714 (1812 bytes)
file > type	executable
language	0x0804 (chinese-simplified)
code-page	1200 (Unicode UTF-16, little endian)
Comments	n/a
CompanyName	china
FileDescription	2023.7.10
FileVersion	3, 0, 0, 1
InternalName	安装包制作工具
LegalCopyright	n/a
LegalTrademarks	n/a
OriginalFilename	n/a
PrivateBuild	n/a
ProductName	n/a
ProductVersion	2023.7.10
SpecialBuild	n/a

Figure 14. Executable metadata displaying internal name as “Setup Package Creation Tool” and language Chinese-simplified.

Malware contains a code snippet that implements a conditional check (“if (data_427548 == 1)”) and calls TerminateProcess, using GetCurrentProcess() if the condition is met, immediately terminating the current process.

```
if (data_427548 == 1)
    TerminateProcess(hProcess: GetCurrentProcess(), uExitCode: arg1)
    noreturn
```

Figure 15. Code snippet invoking TerminateProcess on the current process upon a specific condition.

The following code snippet shows handling window messages and UI updates by the malware process. It includes a call to WaitForSingleObject, message passing with SendDlgItemMessageA, UpdateWindow, memory setting routines, and a call to GetSystemDirectoryA, and string assignment to “install”.

```
if (WaitForSingleObject(hHandle: wParam_22,
        dwMilliseconds: var_24) != WAIT_OBJECT_0)
    var_24 = 0
    WPARAM wParam_2 = 0x19
    wParam_20 = 0x402
    int32_t nIDDlgItem_2 = 0x3e9
    var_34 = wParam_19
    SendDlgItemMessageA(hDlg: var_34, nIDDlgItem: nIDDlgItem_2,
        Msg: wParam_20, wParam: wParam_2, lParam: var_24)
    var_24 = 0x3e9
    var_24 = GetDlgItem(hDlg: wParam_19, nIDDlgItem: var_24)
    UpdateWindow(hWnd: var_24)
    uint8_t var_958 = 0
    void var_957
    int16_t* edi_22 =
        __builtin_memset(dest: &var_957, ch: 0, count: 0x128)
    *edi_22 = 0
    edi_22[1].b = 0
    var_24 = 0x104
    GetSystemDirectoryA(lpBuffer: &var_958, uSize: var_24)
    char* edi_25 = "install\"
    int32_t i = 0xffffffff
```

Figure 16. Code segment updating window state, messaging UI elements, and referencing “install” directory

This code snippet shows updates to dialog UI elements, calls to UpdateWindow, setting dialog item texts, string assignment to “SETUP”, and a FindResourceA call. It references a global variable data_423834.

```
if (WaitForSingleObject(hHandle: wParam_22,
        dwMilliseconds: var_24) != WAIT_OBJECT_0)
    var_24 = 0
    WPARAM wParam_3 = 0x32
    wParam_20 = 0x402
    int32_t nIDDlgItem_3 = 0x3e9
    var_34 = wParam_19
    SendDlgItemMessageA(hDlg: var_34,
        nIDDlgItem: nIDDlgItem_3, Msg: wParam_20,
        wParam: wParam_3, lParam: var_24)
    var_24 = 0x3e9
    var_24 = GetDlgItem(hDlg: wParam_19, nIDDlgItem: var_24)
    UpdateWindow(hWnd: var_24)
    var_24 = &data_421b0c
    int32_t nIDDlgItem_19 = 0x3ea
    wParam_20 = wParam_19
    SetDlgItemTextA(hDlg: wParam_20,
        nIDDlgItem: nIDDlgItem_19, lpString: var_24)
    var_24 = 0x3ea
    var_24 = GetDlgItem(hDlg: wParam_19, nIDDlgItem: var_24)
    UpdateWindow(hWnd: var_24)
    uint32_t wParam_29 = data_423834
    var_24 = "SETUP"
    PSTR lpName = 0x7d0
    wParam_20 = wParam_29
    HRSRC eax_16 = FindResourceA(hModule: wParam_20,
```

Figure 17. UI update logic with dialog message handling and resource searching for “SETUP”.

The following displays code performing filename memory initialization, process file name retrieval via GetModuleFileNameA, and conditional assignment between “updatec.exe” and “clientsetup.exe” based on logic checks.

```
void var_b60
void* lpFilename = &var_b60
__builtin_memset(dest: &var_b60, ch: 0,
    count: 0x104)
wParam_20 = 0
GetModuleFileNameA(hModule: wParam_20,
    lpFilename)
var_24 = &var_b60
sub_40a2ca(var_24)
char* var_28_22 = "updatec.exe"
wParam_20 = &var_b60

if (sub_40a020(wParam_20, var_28_22)
        == 0)
    var_24 = "clientsetup.exe"

    if (sub_40a020(&var_b60, var_24) == 0)
        var_20:2.b = 1
else
    lpApplicationName_1 = 1
    *var_1c_1 = 2

var_24 = 0x5c
char* eax_35 =
    sub_409fb0(&var_b60, var_24.b)
```

Figure 18. Conditional logic checking file names for “updatec.exe” and “clientsetup.exe”.

A code snippet shows buffer and memory initialization, string construction for “YTSysConfig.ini”, and assignment of “YTSTATUS” as the application name title in the dialog/property configuration.

```
    void var_131b
    int16_t* edi_37 = __builtin_memset(
        dest: &var_131b, ch: 0, count: 0x128)
    *edi_37 = 0
    edi_37[1].b = 0
    var_24 = &var_b60
    char* var_28_25 = "%s\YTSysConfig.ini"
    wParam_20 = &var_131c
    sub_409b88(wParam_20, var_28_25)
    char var_154c = 0
    void var_154b
    int16_t* edi_40 = __builtin_memset(
        dest: &var_154b, ch: 0, count: 0x100)
    *edi_40 = 0
    edi_40[1].b = 0
    char var_930 = 0
    void var_92f
    int16_t* edi_43 = __builtin_memset(
        dest: &var_92f, ch: 0, count: 0x100)
    var_24 = &var_131c
    uint32_t nSize = 0x104
    *edi_43 = 0
    wParam_20 = &var_154c
    PSTR lpDefault = 0x421a70
    var_34 = "Title"
    lpApplicationName_1.d = "YTSTATUS"
```

Figure 19. String and buffer setup for “YTSysConfig.ini” with dialog title set to “YTSTATUS”.

This displays code that uses GetPrivateProfileStringA to read values from an INI configuration file, specifically looking up keys “Title” and “Secret” with reference to the application name “YTSTATUS”.

```
var_34 = "Title"
lpApplicationName_1.d = "YTSTATUS"
edi_43[1].b = 0
GetPrivateProfileStringA(
    lpAppName: lpApplicationName_1,
    lpKeyName: var_34, lpDefault,
    lpReturnedString: wParam_20, nSize)
var_24 = &var_131c
uint32_t nSize_1 = 0x104
wParam_20 = &var_930
void* lpDefault_1 = &data_4213ac
var_34 = "Secret"
lpApplicationName_1.d = "YTSTATUS"
GetPrivateProfileStringA(
    lpAppName: lpApplicationName_1,
    lpKeyName: var_34,
    lpDefault: lpDefault_1,
    lpReturnedString: wParam_20,
    nSize: nSize_1, lpFileName: var_24)
```

Figure 20. Code querying the “YTSTATUS” INI file for “Title” and “Secret” keys via GetPrivateProfileStringA.

The code performs conditional checks related to “setuptool.exe” and sets application parameters, initializes buffer memory, and assigns the string “/setuptool” under certain conditions.

```
if (var_20:3.b == 0)
    var_24 = "setuptool.exe"

    if (sub_40a020(&var_1448, var_24) != 0)
        char* eax_75
        eax_75.b = lpApplicationName_1

        if (eax_75.b == 0)
            char var_1678 = 0
            void var_1677
            int16_t* edi_77 = __builtin_memset(
                dest: &var_1677, ch: 0, count: 0x128)
            *edi_77 = 0
            edi_77[1].b = 0
            var_24 = "/setuptool"
            void* var_28_55 = &data_4218b0
            wParam_20 = &var_1678
            var_20:3.b = 1
            sub_409b88(wParam_20, var_28_55)
            __builtin_memset(dest: &var_e8, ch: 0,
                count: 0x44)
            hHandle_3 = nullptr
            int32_t var_6c_1 = 0
            var_24 = 0x12c
```

Figure 21. Buffer setup and application parameter assignment for “setuptool.exe”.

Dynamic Analysis

The Windows User Account Control (UAC) prompt displayed the application name as “2023.7.10”, the verified publisher is “SyncFutureTec Company Limited.”

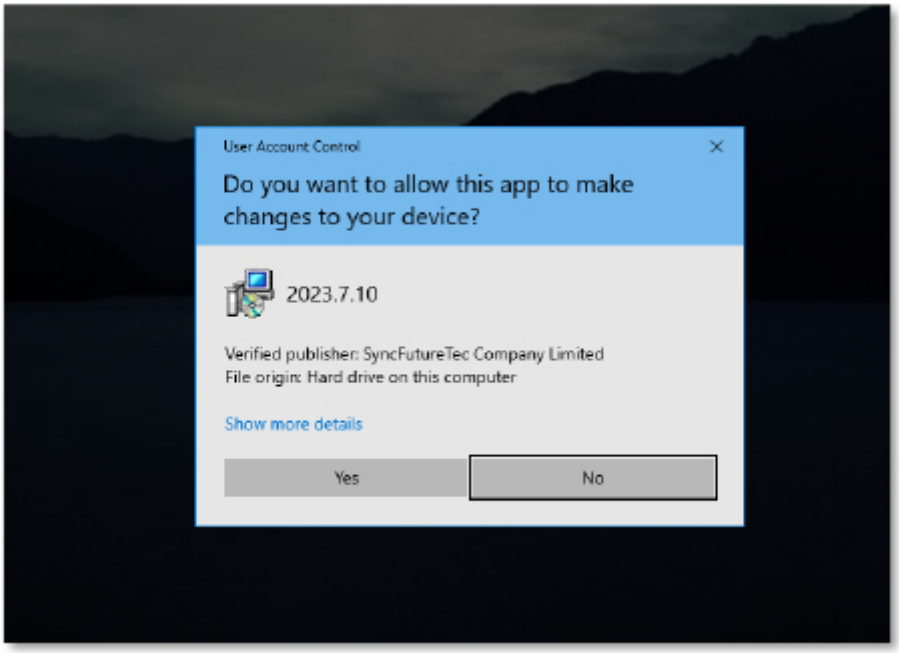


Figure 22. Windows User Account Control (UAC) prompt requesting permission for the application “2023.7.10” from verified publisher “SyncFutureTec Company Limited” to make changes to the device.

The image shows a process tree after executing the file “103.97.128.77#ClientSetup.exe”. It creates another process with persistence, named “MANC.exe”. Under it, there are child processes including “svchost.exe,” “SMSS.exe,” “FSHost64.exe,” and “sysaid.exe.” Some processes use “Microsoft 基础应用程序” (Microsoft Basic Application).

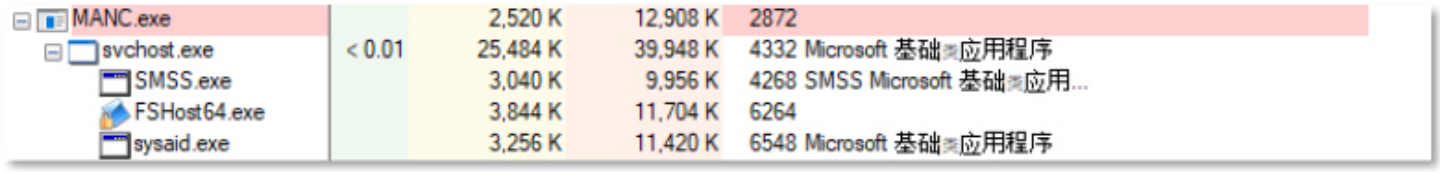


Figure 23. Process tree showing “MANC.exe” running (triggered after executing “103.97.128.77#ClientSetup.exe”) with child processes “svchost.exe,” “SMSS.exe,” “FSHost64.exe,” and “sysaid.exe,” along with memory usage and process IDs.

The executables (MANC.exe, svchost.exe, sysaid.exe) have lower detection by the security vendors, while SMSS.exe and FS… have no detection yet.

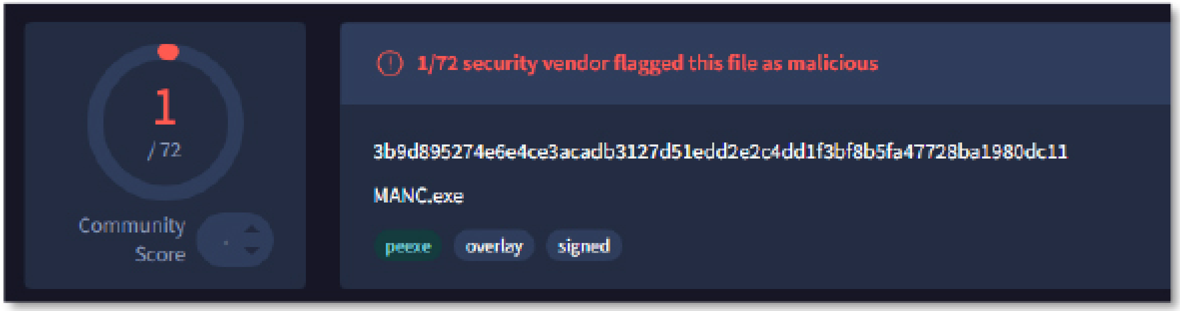


Figure 24. MANC.exe flagged as malicious by 1/72 security vendors

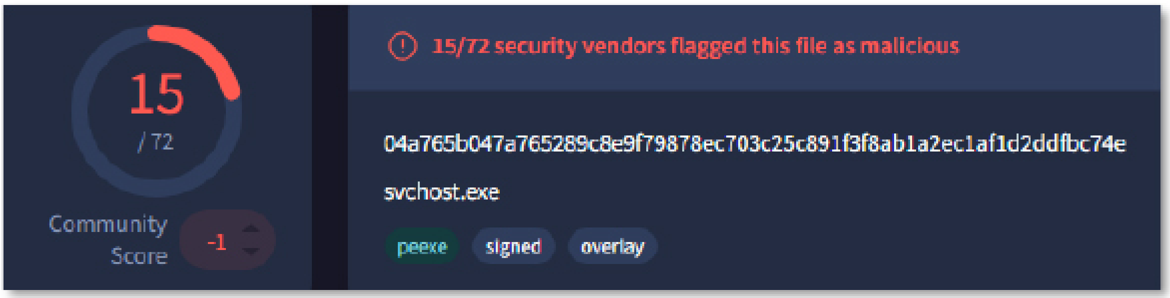


Figure 25. svchost.exe flagged as malicious by 15/72 security vendors.

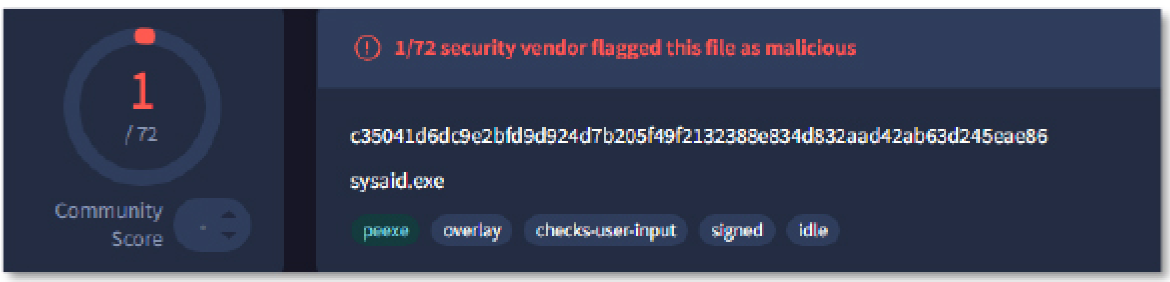
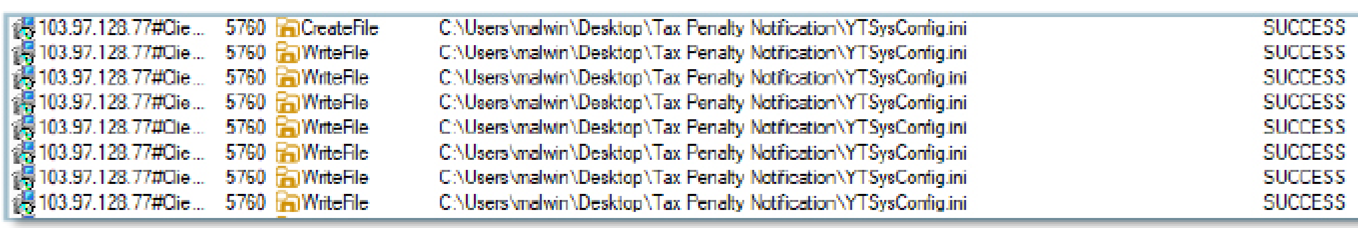


Figure 26. sysaid.exe flagged as malicious by 1/72 security vendors.

A process activity log shows file operations performed on the file "YTSysConfig.ini" located in "C:\Users\malwin\Desktop\Tax Penalty Notification". The listed actions include CreateFile, WriteFile, and CloseFile APIs, all executed successfully by a process with PID 5760.



103.97.128.77#Clie...	5760	CreateFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS
103.97.128.77#Clie...	5760	WriteFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS
103.97.128.77#Clie...	5760	WriteFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS
103.97.128.77#Clie...	5760	WriteFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS
103.97.128.77#Clie...	5760	WriteFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS
103.97.128.77#Clie...	5760	WriteFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS
103.97.128.77#Clie...	5760	WriteFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS
103.97.128.77#Clie...	5760	WriteFile	C:\Users\malwin\Desktop\Tax Penalty Notification\YTSysConfig.ini	SUCCESS

Figure 27. File system operations on YTSysConfig.ini

The configuration file "YTSysConfig.ini". includes several parameters under the header [YTSTATUS], notably specifying ServerIP as 103.97.128.77. This IP address is associated with data exfiltration activity.

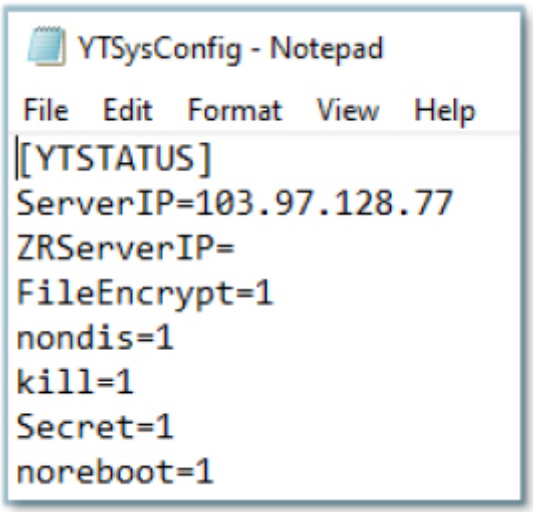


Figure 28. YTSysConfig configuration file in Notepad, containing directives for system behavior and setting ServerIP (103.97.128.77) for data exfiltration activity.

A process activity log records CreateFile and WriteFile operations involving the folder “C:\install” and its contents. Several filenames (e.g., C:\install\0001DB86) are referenced.

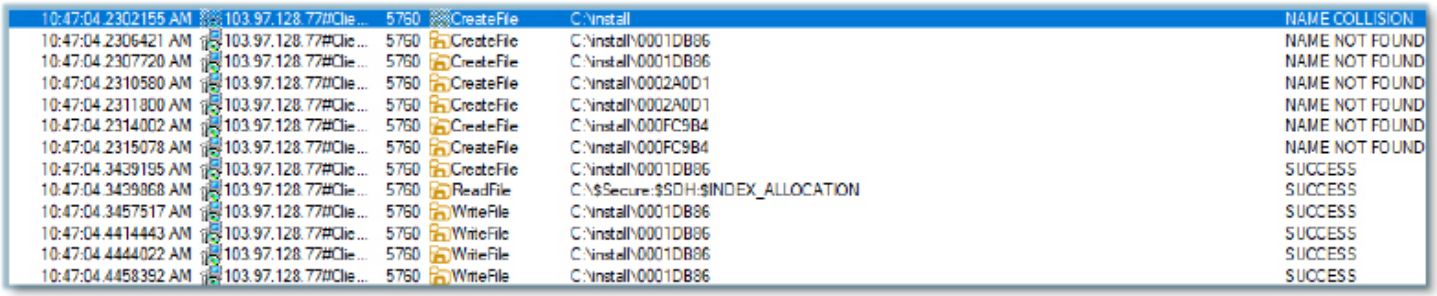


Figure 29. File operations on C:\install and its subfiles.

A directory listing displays the contents of the install folder:

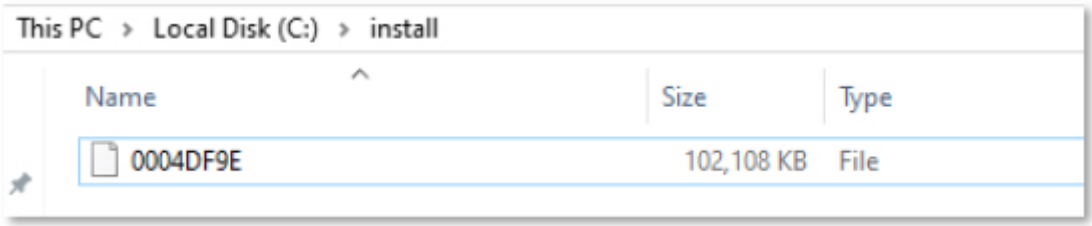


Figure 30. Contents of C:\install folder showing a text document

The contents of the “log” folder reveal multiple text documents, such as “AdoBase”, “AssistantThC”, “FSHost32”, “installok”, and others, along with file sizes and modification times.

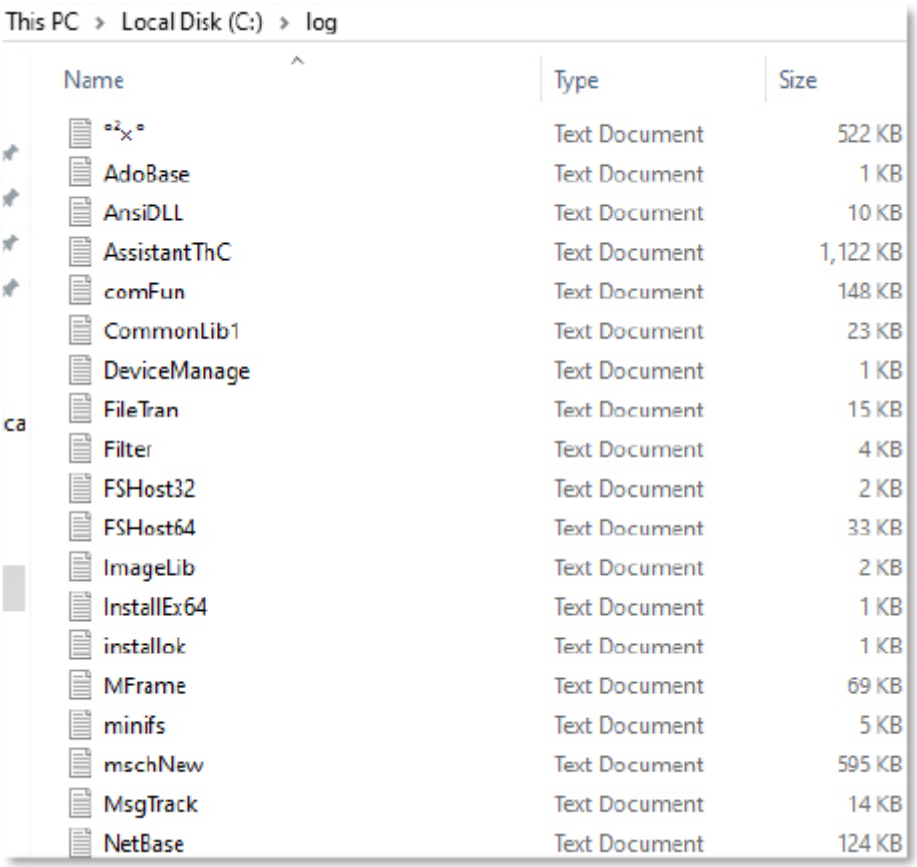


Figure 31. Contents of C:\log folder showing various log text documents.

The contents of the “UfsdCrypt” file (C:\log folder) include entries for UD_Initialize, MyQueryDosDevice, and StartFilter, with time stamps and device references, containing both English and Chinese text.

Figure 32. UfsdCrypt log file contents showing device and filter initialization events.

The process svchost.exe (PID 4332) established TCP connections to the remote address 103.97.128.77, using ports 6671 and 6681, respectively, and listening on UDP port 6677, indicating command receiving capability of the malware.

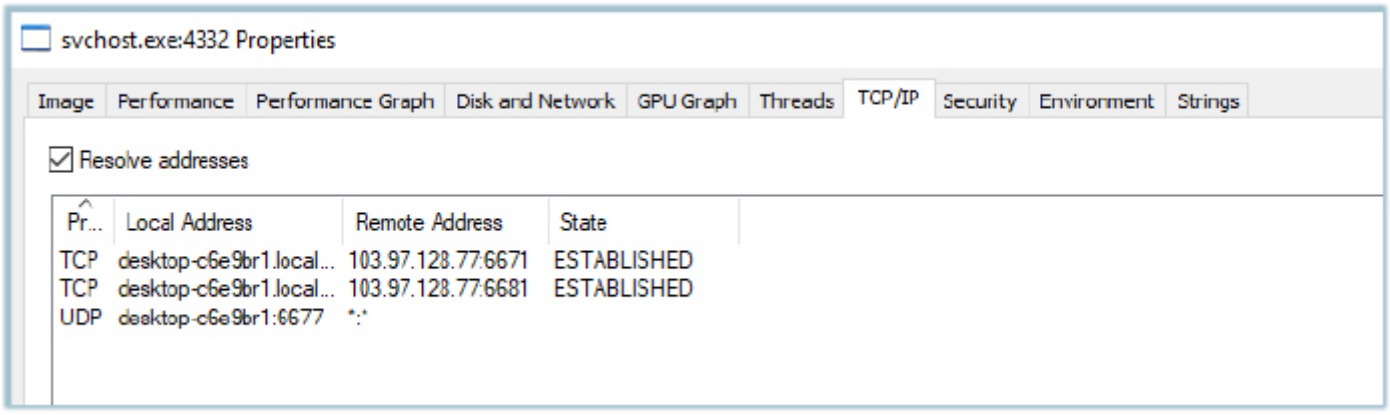


Figure 33. svchost.exe process with established TCP connections to 103.97.128.77.

CONCLUSION

The events of July–August 2025 highlight a significant escalation in hacktivist-driven cyber operations against India, with coordinated attacks spanning data breaches, DDoS disruptions, defacements, phishing schemes, and malware campaigns. The involvement of multiple foreign actors—including groups from Pakistan, Bangladesh, Russia, Indonesia, and likely China—illustrates a shift from isolated incidents to organized, multinational campaigns targeting critical institutions and public-facing services. India's retaliatory actions signal a growing cycle of offensive and defensive cyber activity in the region. Together, these incidents underscore the urgent need for stronger threat intelligence, proactive defense measures, and cross-agency coordination to protect national security and public trust in digital infrastructure.

IOCs(Indicators of Compromise)

No	Indicator (SHA-256)	Remarks
1	https://rto[.]dc7[.]live	URL
2	https://wtqz3bn75j7ha49f82k[.]dewakartu[.]top/	URL
3	https://fhauifhyileydhfl[.]com/	URL
4	https://yunvxi[.]com/	URL
5	https://enzedi[.]com/	URL
6	54660fd2ff160f70a3ae5d8e54fca990562e4bfee1f8fdc882261e35420d209b	SHA256
7	b75dec6f19a3dec025862a0d6e7dd565ad49c327cd85c21d5135ccffef60e68f	SHA256
8	103.97.128.77	IP
9	202.189.10.112	IP

Back to Listing