

Fake Tax-Themed Phishing Campaign Delivers Malware

 cyfirma.com/research/fake-tax-themed-phishing-campaign-delivers-malware

Published On : 2026-09-12



EXECUTIVE SUMMARY

CYFIRMA has identified a multi-domain malware distribution campaign abusing the Indian Income Tax Department theme to deliver a malicious payload. The campaign deploys a network of ten fraudulent tax-themed domains designed to impersonate legitimate government communication and trick victims into downloading a malicious archive containing staged malware components.

The threat actors employ social engineering by presenting a fabricated Notice of Assessment u/s 143(3) containing tax-related terminology, legal references, PAN details, demand amounts, compliance requirements, and financial implications to create urgency and increase

victim interaction. The fraudulent portal presents a Download Assessment Order & Workings control that initiates the download of a malicious disk image file (Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx) delivering a PE loader (Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe) and an associated DLL payload (tedutil.dll) loaded from the binary's resource section.

Attackers abuse virtual hard disk containers (VHDX) to distribute malicious content that eludes traditional email security and static detection because of its atypical file type. When mounted, the VHDX reveals the embedded loader and DLL payload, extending the attack into a multi-stage infection chain.

The campaign's modular loader/payload architecture, use of a non-standard container (VHDX), reliance on spoofed government identity, and deployment across multiple disposable domains reflect a deliberate, scalable operation designed to sustain compromise, evade detection, and potentially establish persistent remote access to compromised systems.

INTRODUCTION

This report analyzes a malware distribution campaign that leverages a fraudulent Indian Income Tax Department assessment notice to deliver a RAT-like payload targeting Windows environments. Unlike single-domain campaigns, this operation simultaneously employs ten separate malicious domains to host a fake tax assessment portal designed to resemble official government communication.

The attack chain begins with a social engineering lure that prompts victims to download a malicious VHDX disk image file (Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx) disguised as a legitimate offline utility for ITR-1 to ITR-4 forms for FY2025 – 26. When mounted, the VHDX delivers a loader executable (Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe) and a malicious DLL payload (tedutil.dll) that is loaded as a resource.

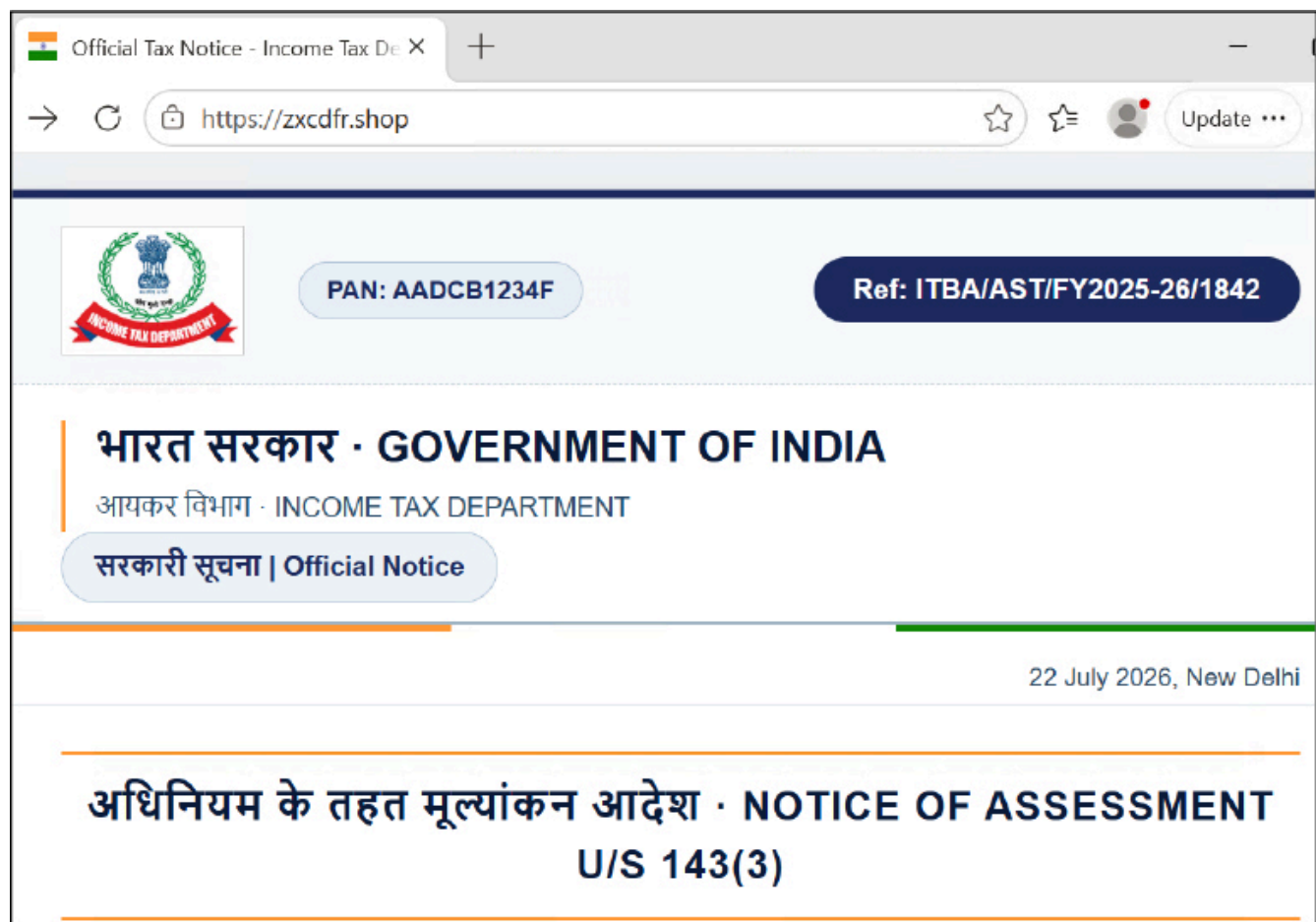
The malware follows a staged execution approach in which the executable acts as a loader, extracting and executing the DLL payload embedded within its resources. Subsequent analysis indicates RAT-like capabilities that enable persistence, host reconnaissance, command execution, and remote communication.

The use of multiple domains for the same campaign significantly expands the infrastructure footprint, complicates blocking and takedown efforts, and reinforces the resourcefulness of the operators. The campaign demonstrates the continued effectiveness of government-themed impersonation combined with non-standard container formats and modular payload delivery to bypass user awareness and security controls.

CAMPAIGN DETAILS

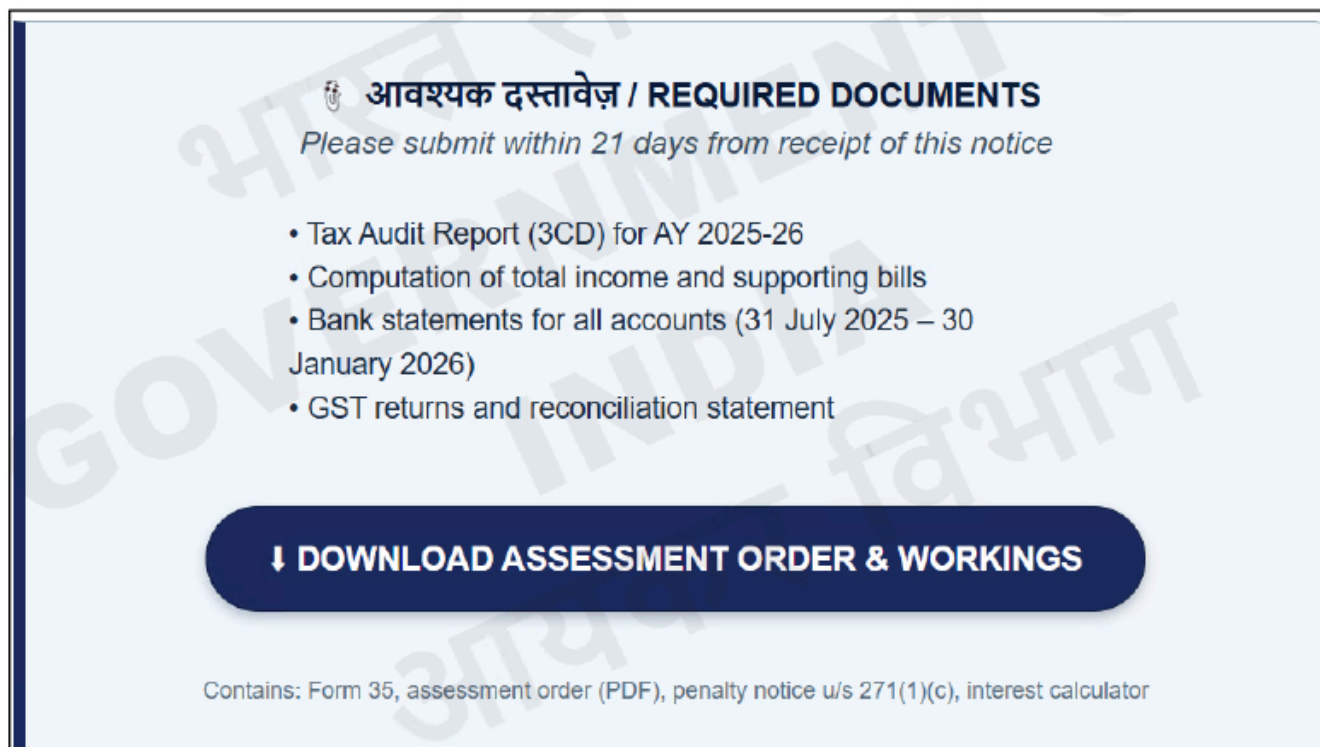
The campaign leverages a counterfeit Income Tax Department Notice of Assessment to target individuals and organizations in India. Threat actors operate a network of ten fraudulent tax-themed domains that closely imitate the appearance, language, and structure of legitimate government tax communications.

Fake Assessment Notice Highlights The fraudulent notice impersonates the Government of India and the Income Tax Department, incorporating official branding and the national emblem to establish credibility. It includes a reference number, PAN details, and assessment year, along with a purported Notice of Assessment under Section 143(3) citing various tax additions, disallowances, and applicable interest provisions. The notice further incorporates urgency indicators, including penalty proceedings, additional interest for delayed payment, and a defined period for submitting supporting documentation, intended to pressure recipients into immediate action.



The website displays a fraudulent assessment order containing purported taxpayer information, legal references, financial penalties, and compliance instructions, thereby creating an appearance of legitimacy and instilling a sense of urgency among potential

victims. To further facilitate user interaction, the page provides a button labeled “Download Assessment Order & Workings.” Clicking this button initiates the download of a malicious VHDX file, which is presented as an official tax-related document but is instead used as the delivery mechanism for the malicious payload.



आवश्यक दस्तावेज़ / REQUIRED DOCUMENTS
Please submit within 21 days from receipt of this notice

- Tax Audit Report (3CD) for AY 2025-26
- Computation of total income and supporting bills
- Bank statements for all accounts (31 July 2025 – 30 January 2026)
- GST returns and reconciliation statement

↓ DOWNLOAD ASSESSMENT ORDER & WORKINGS

Contains: Form 35, assessment order (PDF), penalty notice u/s 271(1)(c), interest calculator

At the time of analysis, the tracking endpoint recorded 1,013 visit events and 48 download events. These values represent observed requests to the tracking endpoint and should not be interpreted as confirmed unique users or victims.



Supporting Domain Infrastructure: The campaign leverages multiple domains exhibiting a consistent naming pattern and serving the same malicious payload, including the following:

- zasxcd[.]shop
- ssefcv[.]shop
- cbvfrd[.]shop
- bvnbyh[.]shop

- bmnjhy[.]shop
- mkjiun[.]shop
- nmhjnu[.]shop
- zxcdfr[.]shop
- sfbnhy[.]shop
- xvbndr[.]shop

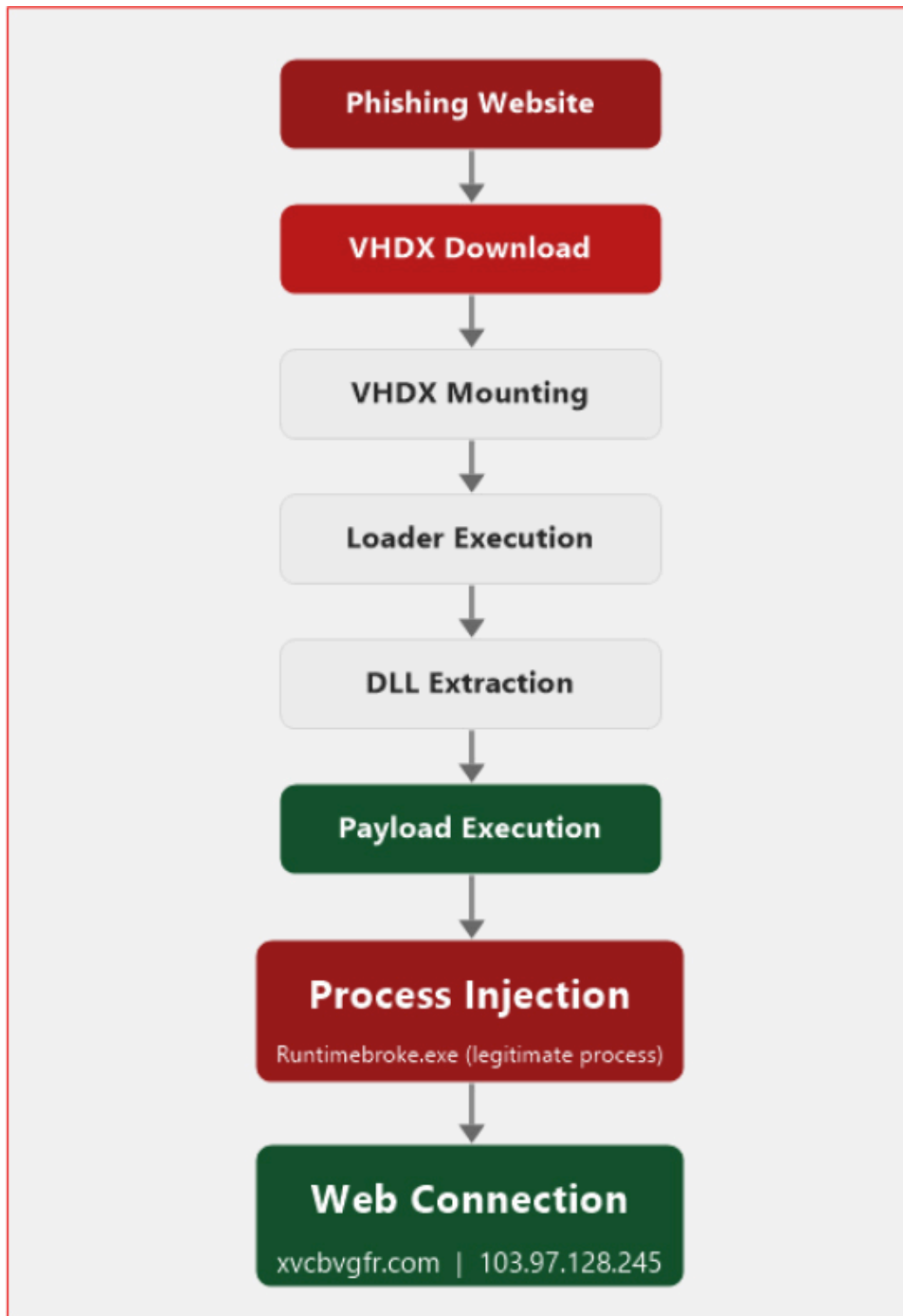
The short keyboard-pattern names and same-day registration on 14 July 2026 suggest bulk registration and support a wide-scale distribution strategy. The use of multiple disposable domains also enables rapid infrastructure rotation, helping the threat actors evade domain-reputation controls, URL filtering, and blocklisting mechanisms.

Basic Details:

Target Technologies	Windows Operating System, VHDX Disk Image
Threat Type	Malware Distribution Campaign
File Types	VHDX Virtual Disk (.vhdx), Portable Executable (.exe), Dynamic Link Library (.dll)
Key Malware Identifiers	Tax-themed lure, fraudulent Income Tax Department Notice of Assessment, multi-domain fake assessment portal, VHDX disk image (Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx), PE loader masquerading as offline utility (Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe), DLL payload loaded as a resource (tedutil.dll)
Impact	Potential Unauthorized Remote Access / Data Theft (C2 Not Established)
MD5 Hashes	Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx = 2462c9ca59a40ce04e3f072a95e104f0 Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe = e347d86749a1f9e61c6e3b330c681b50 tedutil.dll = 69c5a70b15c886a7f9ab5449be286779

MALWARE INFECTION LIFECYCLE

Initial Access and Delivery In the initial stage, the victim is directed to one of multiple fraudulent tax-themed domains and prompted to download a malicious VHDX file named Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx, which is presented as an official offline utility for Income Tax Return preparation.



Upon mounting the VHDX image, the malicious content is revealed. The VHDX container can conceal payloads from traditional defenses because disk-image attachments may not be routinely inspected or blocked by email and web security controls.

Name	Date modified	Type	Size
Yesterday			
 Common_Offline_Utility_ITR-1_to_4_AY2026-07-27	9/8/2026 10:47 PM	Hard Disk Image File	18,432 KB

The image contains metadata identifying it as a Virtual Hard Disk v2 (VHDX) container. The metadata indicates creation on Windows 11, version 25H2 (build 10.0.26200.0). Microsoft identifies build 26200 with Windows 11, version 25H2.

Binary

Format: Virtual Hard Disk v2 (VHDX)[CreatorApp:Microsoft Windows 10.0.26200.0]

Region: PE64[Offset=0x00a50000,Size=0x00035000]

Operation system: Windows(10)[AMD64, 64-bit, GUI]

Linker: Microsoft Linker(14.36.33145)

Compiler: Microsoft Visual C/C++ (19.36.33145)[C]

Language: C

Tool: Visual Studio(2022, v17.6)

Region: PE64[Offset=0x01198000,Size=0x9400]

Operation system: Windows(Server 2003)[AMD64, 64-bit, DLL]

(Heur)Language: ASMX64

Region: PE64[Offset=0x011a4000,Size=0x00048000]

Operation system: Windows(10)[AMD64, 64-bit, DLL]

Linker: Microsoft Linker(14.36.33145)

Compiler: Microsoft Visual C/C++ (19.36.33145)[C++]

Language: C++

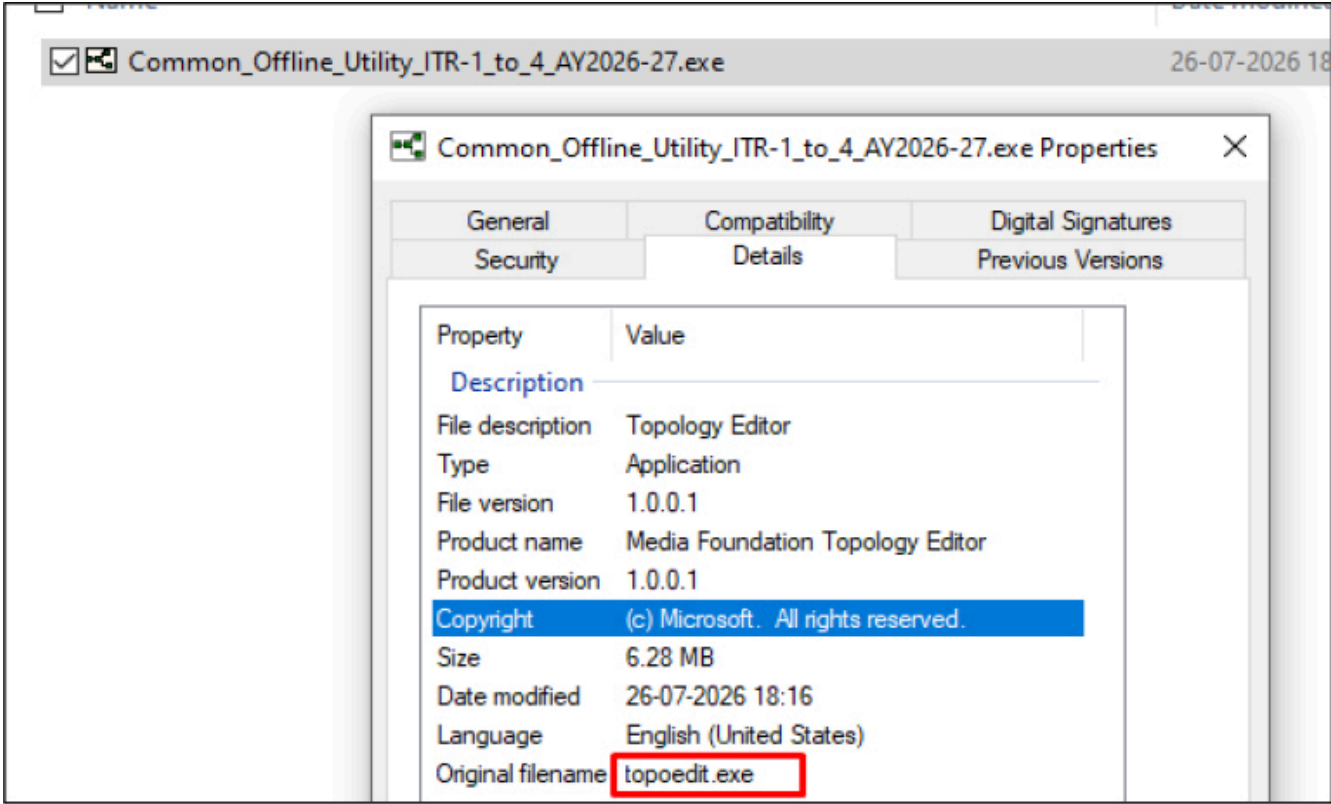
Tool: Visual Studio(2022, v17.6)

Analysis of the VHDX Disk Image Analysis of the VHDX file revealed the presence of two malicious components associated with the next stage of the infection chain. The first component, Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe, is a Portable Executable (PE) file that functions as a loader. The second component, tedutil.dll, is a Dynamic Link Library (DLL) that serves as the primary malware payload and is loaded by the loader from the binary's resource section during the infection process.

Name	Date modified	Type	Size
Earlier this year			
 Common_Offline_Utility_ITR-1_to_4_AY2026-27	7/27/2026 6:46 AM	Application	6,435 KB

Suspicious File Metadata Identified Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx contains an executable whose embedded metadata identifies the original filename as

topoedit.exe, with File Description: Topology Editor, Product Name: Media Foundation Topology Editor, and Product/File Version: 1.0.0.1. The metadata also claims Microsoft copyright, which is inconsistent with the tax-related filename and delivery context. This discrepancy between the presented filename and the embedded Microsoft-related metadata suggests masquerading and potential metadata abuse, likely intended to make the executable appear legitimate and reduce suspicion during execution.



DETAILED ARTIFACT ANALYSIS

Artifact / Attribute	Detail
Malicious container	Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx (Virtual Hard Disk v2)
VHDX creation host	Microsoft Windows 11, version 25H2 (built 10.0.26200.0)
Loader executable	Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe (Portable Executable)
Payload DLL	tedutil.dll (loaded from the loader’s resource section)

Embedded file metadata	Original filename: topoedit.exe; File Description: Topology Editor; Product Name: Media Foundation Topology Editor; Version: 1.0.0.1; Microsoft copyright
Masquerading indicator	Tax-related filenames vs Microsoft Topology Editor metadata (metadata abuse to increase perceived legitimacy)
Observed behavior	Process injection into Runtimebroke.exe during execution
Observed network	Web connection to xvcbvgr.com resolving 103[.]97[.]128[.]245
Campaign engagement	Tracking endpoint: 1,013 visits and 48 downloads

Runtime Process Injection with RuntimeBroke.exe During execution, the malware performs process injection into Runtimebroke.exe, enabling the malicious code to operate within the context of a legitimate process and potentially evade process-based security monitoring and detection mechanisms.

OneDrive.e...	7908	0.0.0.0	51418			TCP	Bound
RuntimeBr...	2508	192.168.88.165	51422	103.97.128.245	443	TCP	SYN sent
RuntimeBr...	2508	0.0.0.0	51422			TCP	Bound
RuntimeBr...	10520	192.168.88.165	51423	103.97.128.245	443	TCP	SYN sent
RuntimeBr...	10520	0.0.0.0	51423			TCP	Bound

Upon execution, the malware attempted to initiate a TCP connection to the external domain xvcbvgr[.]com, which resolves to 103[.]97[.]128[.]245. Network analysis observed a TCP SYN packet sent to the resolved IP address, indicating an attempted connection; however, the TCP handshake was not completed. No successful C2 communication was established or observed during the analysis period.

DNS	functional.events.data.microsoft.com A = global.asimov.events.data.trafficman... QUERY	NOER...
DNS	xvcbvgr.com A = 103.97.128.245	QUERY NOER...
DNS	client.wns.windows.com A = wns.notify.trafficmanager.net, 4.213.25.242	QUERY NOER...
DNS	functional.events.data.microsoft.com A = global.asimov.events.data.trafficman... QUERY	NOER...

0x219adaa26e0	28	Peer Address Family Mismatch
0x219adaa2700	24	kernel32.dll
0x219adaa2720	27	SetUnhandledExceptionFilter
0x219adaa2740	30	OVERLORD_SERVER
0x219adaa2760	18	wss://xvcbvgr.com
0x219adaa2780	24	advapi32.dll
0x219adaa27c0	30	OVERLORD_TLS_CA
0x219adaa27e0	28	OVERLORD_MUTEX
0x219adaa2800	24	advapi32.dll
0x219adaa2820	20	2026/09/09 17:35:50
0x219adaa2962	26	EQUEST_METHOD
0x219adaa2980	24	xvcbvgr.com
0x219adaa29a0	24	advapi32.dll

Key Capabilities

1. Government-Themed Social Engineering

- Attackers used a fraudulent Income Tax Department-themed assessment notice to distribute malware.
- The lure included tax terminology, legal references, PAN details, penalties, and assessment information to appear legitimate.
- Multiple malicious domains hosted the same phishing theme, increasing the campaign's infrastructure footprint.

2. VHDX-Based Malware Delivery

- The campaign used a VHDX virtual hard disk file as the malware delivery mechanism.
- The uncommon file format may assist in bypassing conventional email and static security controls.

3. Loader and Payload Separation

- Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe functions as the initial loader.
- The loader extracts tedutil.dll from its embedded resource section.
- The extracted DLL is subsequently loaded to execute malicious functionality.

4. File Masquerading

- The filename Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe mimics legitimate income-tax utility software.
- The tax-related filename and VHDX packaging are designed to reduce user suspicion.

5. Runtime Process Injection

- The malware performs process injection into Runtimebroke.exe during execution.
- This behavior enables the malicious code to execute within the context of another process and may assist in evading process-based detection mechanisms.

6. Command-and-Control Communication

- The malware attempts to connect to xvcbvgrfr[.]com over TCP/443.
- The domain resolves to 103[.]97[.]128[.]245, which serves as the observed network endpoint associated with the malware.

THREAT ACTOR ATTRIBUTION

Based on the observed tactics, techniques, and procedures (TTPs), malware capabilities, delivery mechanism, and associated infrastructure, the activity is assessed as an unattributed malware distribution campaign targeting Indian users and organizations. The use of an Indian Income Tax Department-themed lure, VHDX-based delivery, DLL-based execution, and RAT-like capabilities indicates a deliberate campaign leveraging social engineering and evasive malware-delivery techniques. The observed activity demonstrates TTP overlaps with techniques reported in campaigns associated with China-linked threat activity targeting Indian entities; however, these similarities alone are insufficient to establish attribution to the same actor or activity cluster.

The campaign infrastructure exhibits characteristics consistent with a scalable and potentially disposable distribution model. Multiple similarly structured domains have been identified in association with 103[.]59[.]103[.]170, while the malware also attempted to establish a network connection to xvcbvgrfr[.]com, which resolves to 103[.]97[.]128[.]245 and is assessed as a suspected C2 endpoint based on its association with the analyzed malware. However, during analysis, only a TCP SYN packet was observed, and the connection handshake was not completed; therefore, successful C2 communication with this endpoint was not established. The use of multiple randomly structured domains under the .shop TLD, combined with multiple infrastructure endpoints, is consistent with a low-cost and potentially automated infrastructure model that could facilitate rapid domain rotation and replacement following detection or disruption.

At this stage, no definitive attribution can be established based on the available evidence. The observed TTP similarities with China-associated campaigns should therefore be treated as a supporting analytical lead rather than an attribution indicator. Further correlation of malware configurations, C2 infrastructure, domain-registration patterns, infrastructure reuse, and

additional campaign artifacts would be required to determine whether the activity is connected to any previously identified threat actor or activity cluster.

EXTERNAL THREAT LANDSCAPE MANAGEMENT

The analyzed campaign highlights the continued evolution of government-themed malware distribution operations, in which threat actors impersonate trusted government institutions and regulatory processes to increase victim engagement. By impersonating the Income Tax Department, the operators use realistic tax-related notifications, assessment references, PAN-related information, compliance terminology, and financial implications to create a strong sense of legitimacy and urgency. Such themes can be particularly effective during tax and assessment periods, increasing the likelihood of users interacting with malicious links, downloading files, or executing seemingly legitimate utilities.

The campaign demonstrates a structured multi-stage infection framework that begins with fraudulent tax-themed domains distributing a malicious VHDX file disguised as an official offline ITR utility. The infection chain incorporates a VHDX container, executable loader, and DLL-based payload, separating the initial delivery mechanism from the subsequent malicious functionality. This modular approach provides operational flexibility and can reduce the visibility of malicious components during the initial stages of compromise. The combination of deceptive filenames, process injections, and remote communications demonstrates an emphasis on maintaining execution and access after initial compromise.

The campaign also aligns with the broader pattern of Income Tax-themed malware activity previously documented by CYFIRMA, including An Income Tax Assessment Notice Phishing Campaign Delivering Malware (23 June 2026) and Operation TaxShadow (June 2026). The timing is also notable, with the identified domains registered on 14 July 2026, shortly before the 31 July ITR-1/ITR-2 filing deadline. This timing suggests that the campaign leveraged a period when tax-related communications and filing activity were particularly relevant to potential victims. The combination of a familiar government theme, time-sensitive tax context, and an apparently legitimate offline utility increases the credibility of the delivery lure.

MITRE ATT&CK FRAMEWORK

Tactic	ID	Technique Name
Execution	T1204.002	User Execution: Malicious File

Stealth	T1055	Process Injection
	T1036	Masquerading
	T1036.005	Masquerading: Match Legitimate Resource Name or Location
Discovery	T1082	System Information Discovery
Command & Control	T1071.001	Application Layer Protocol: Web Protocols

CONCLUSION

The analysis identifies a multi-domain malware campaign leveraging a fraudulent Income Tax Department-themed lure to distribute a malicious payload through a staged infection chain involving a VHDX file, the executable loader (Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe), and the DLL payload (tedutil.dll). The campaign uses deceptive tax-related naming, resource-based payload extraction, VHDX-based delivery, and multiple disposable domains to facilitate malware delivery. Observed activity includes process injection and an attempted command-and-control (C2) connection. Based on analysis of the identified payload family, the malware is assessed to have capabilities related to persistence, system discovery, and remote command execution.

The identified phishing domains share an association with 103[.]59[.]103[.]170, while the malware attempted to communicate with xvcbvgr[.]com, which resolves to 103[.]97[.]128[.]245; however, successful C2 communication was not established during analysis. These infrastructure relationships are consistent with coordinated campaign infrastructure; however, IP geolocation alone is insufficient to establish attribution to a specific threat actor or geographic origin. The campaign's use of tax-themed lures and disposable infrastructure indicates a deliberate malware distribution operation with potential for sustained unauthorized access.

RECOMMENDATIONS AND MITIGATION

1. Email and Web Security Controls

- Implement advanced email security controls to detect and block phishing campaigns using tax-themed lures, suspicious attachments, and newly registered domains.

- Monitor and restrict access to newly registered, low-reputation, or suspicious domains, particularly those impersonating government or financial institutions.
- Enable URL filtering, reputation-based blocking, and sandboxing for suspicious links and downloaded files.
- Monitor and flag downloads of VHDX, IMG, and ISO disk-image files originating from untrusted external sources.

2. File and Disk-Image Execution Restrictions

- Restrict the mounting and execution of unknown disk-image files received through email, web downloads, or removable media.
- Restrict execution of .exe, .dll, and script-based files from user-writable and temporary locations, including:
 - %AppData%
 - %Temp%
 - %USERPROFILE%\Downloads
 - Mounted disk-image locations
- Disable automatic execution of content originating from downloaded archives and mounted disk images.

3. Malware Detection and Endpoint Protection

- Deploy EDR detections for topoedit.exe executing outside the expected Windows SDK path or from a mounted volume, particularly when it loads tedutil.dll from the same non-standard location.
- Monitor RuntimeBroker.exe for unusual outbound TCP/443 connections to non-Microsoft IP addresses and detect WebSocket upgrades involving newly registered or suspicious domains.
- Implement behavioral detection for process injections, abnormal DLL loading, resource-based payload extraction, and execution from mounted disk images or user-writable directories.
- Restrict standard users from double-click mounting .vhd/.vhdx files through appropriate endpoint policies or file-association controls and keep EDR/antivirus signatures and campaign-specific threat indicators updated.

4. Network and Web Communication Monitoring

- Monitor outbound web traffic for communication with the identified infrastructure, including xvcbvgrfr[.]com, which resolves to 103[.]97[.]128[.]245, and the associated campaign infrastructure at 103[.]59[.]103[.]170.

- Create detection rules for suspicious or anomalous outbound web connections from applications that do not normally require external communication.
- Monitor unusual or persistent web connections originating from newly executed or unsigned binaries.
- Correlate DNS, proxy, firewall, and endpoint telemetry to identify additional domains and infrastructure associated with the campaign.

5. Persistence Monitoring

- Monitor commonly abused Windows persistence locations, including:
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - Startup folders
 - Scheduled Tasks
- Alert on unauthorized modifications to registry autorun locations, startup mechanisms, or other persistence-related configurations.

6. User Awareness

- Educate users to verify tax-related communications through official government portals rather than interacting with links or attachments received through email or messaging platforms.
- Train employees to identify:
 - Urgent tax and compliance notifications
 - Suspicious software or utility downloads
 - Fake government notifications
 - Unexpected VHDX or disk-image files
 - Requests to install or execute tax-related applications from unofficial sources

7. Threat Hunting Activities

- Hunt for identified malware artifacts, including:
 - Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe
 - tedutil.dll
 - Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx
- Search for suspicious executable and DLL files originating from mounted disk images, temporary directories, and user-writable locations.
- Monitor for execution chains involving VHDX mounting followed by executable and DLL execution.
- Hunt for abnormal process-injection activity associated with the identified execution chain.
- Use the provided IOCs and YARA rules to identify related samples and potential variants.

8. Incident Response Readiness

- Immediately isolate affected systems when suspicious malware execution or abnormal process-injection activity is identified.
- Collect relevant forensic artefacts, including:
 - Process execution logs
 - Registry modifications
 - DNS and network connection records
 - Mounted disk-image activity
 - Dropped or extracted files
 - Persistence mechanisms
- Reset potentially compromised credentials and investigate possible data exposure, lateral movement, and unauthorized access following confirmed compromise.

9. Application Control

- Implement application allowlisting to prevent execution of unauthorized or unknown binaries.
- Apply least privilege principles and restrict administrative privileges for standard users.
- Where operationally feasible, restrict execution of unsigned or untrusted binaries from temporary, download, and mounted disk-image locations.

10. Continuous Threat Intelligence Monitoring

- Continuously monitor emerging domains, IP addresses, malware variants, and infrastructure associated with:
 - Tax-themed phishing campaigns
 - Government impersonation activity
 - VHDX-based malware delivery
 - Process-injection activity
 - Similar domain-registration and infrastructure patterns
- Track the identified domains, 103[.]59[.]103[.]170, and xvcbvgr[.]com / 103[.]97[.]128[.]245 for infrastructure changes, additional DNS associations, and potential campaign expansion.
- Correlate newly identified indicators with existing threat intelligence to identify related campaigns, malware variants, and infrastructure reuse.

INDICATORS OF COMPROMISE

Kindly refer to the IOCs section, applying relevant security controls.

S. No	Indicator	Remarks
1	zasxcd[.]shop	Block
2	ssefcv[.]shop	Block
3	cbvfrd[.]shop	Block
4	bvnbhy[.]shop	Block
5	bmnjhy[.]shop	Block
6	mkjiun[.]shop	Block
7	nmhjnu[.]shop	Block
8	zxcdfr[.]shop	Block
9	sfbnhy[.]shop	Block
10	xvbndr[.]shop	Block
11	Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx	Monitor
12	Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe	Monitor
13	518ee4c9ae0321bd4fe8616e4f195f0079c6503109d2710e80e09d1a0f1dc98f	Monitor
14	f4ae0f7c0c663e41dab28b2992f1afa9b97fe13a52f2d1fa26156554a23b99a7	Block
15	71d15f3c13f5b11866cf65d9cf014236a47d221155ae992d9992abccedb66cf2	Monitor
16	103[.]59[.]103[.]170	Block
17	xvcbvgr[.]com	Monitor
18	103[.]97[.]128[.]245	Monitor

YARA Rules

```
rule IncomeTax_Themed_VHDX_Malware_Campaign { meta: description = "Detection rule for the multi-domain Income Tax themed VHDX malware distribution campaign" author = "CYFIRMA" date = "2026-09-09"
```

strings: // File name indicators \$file1 = "Common_Offline_Utility_ITR-1_to_4_AY2026-07-27.vhdx" \$file2 = "Common_Offline_Utility_ITR-1_to_4_AY2026-27.exe"

// Domain indicators \$dom1 = "zasxcd.shop" \$dom2 = "ssefcv.shop" \$dom3 = "cbvfrd.shop" \$dom4 = "bvnbyh.shop" \$dom5 = "bmnhjy.shop" \$dom6 = "mkjiun.shop" \$dom7 = "nmhjnu.shop" \$dom8 = "zxcdfr.shop" \$dom9 = "sfbnhy.shop" \$dom10 = "xvbndr.shop" \$dom11 = "xvcbvgr.com"

// IP address indicator \$ip1 = "103.59.103.170" \$ip2 = "103.97.128.245"

// SHA-256 hash indicators \$hash1 = "518ee4c9ae0321bd4fe8616e4f195f0079c6503109d2710e80e09d1a0f1dc98f" \$hash2 = "f4ae0f7c0c663e41dab28b2992f1afa9b97fe13a52f2d1fa26156554a23b99a7" \$hash3 = "71d15f3c13f5b11866cf65d9cf014236a47d221155ae992d9992abccedb66cf2"

condition: any of (\$file*) or any of (\$dom*) or any of (\$ip*) or any of (\$hash*) }

Copyright CYFIRMA. All rights reserved.