

# An Income Tax Assessment Notice Phishing Campaign Delivering Malware

 [cyfirma.com/research/an-income-tax-assessment-notice-phishing-campaign-delivering-malware](https://cyfirma.com/research/an-income-tax-assessment-notice-phishing-campaign-delivering-malware)

Published On : 2026-06-23



## EXECUTIVE SUMMARY

CYFIRMA has identified a malware distribution campaign leveraging a fraudulent Indian Income Tax Department-themed lure to deliver a Remote Access Trojan (RAT)-like payload to targeted users. The campaign utilizes a convincing fake tax assessment notification hosted on the domain harivo[.]vip, designed to impersonate legitimate government communication and trick victims into downloading a malicious archive containing staged malware components.

The threat actors employ social engineering techniques by presenting a fake assessment order containing tax-related terminology, legal references, compliance requirements, and

financial implications to create urgency and increase victim interaction. The downloaded archive contains a malicious disk image file (Tax\_Assessment.img) that delivers a PE loader (Tax\_Assessment.exe) and associated payload (libsvcs.dll).

Technical analysis revealed that Tax\_Assessment.exe functions as a loader responsible for initiating execution of libsvcs.dll through .NET reflection mechanisms. Both components were protected using ConfuserEx obfuscation, indicating an attempt to hinder static analysis and evade traditional security detection mechanisms. The malware also employs defense-evasion techniques, including console window hiding, registry modification, spoofed assembly metadata, and misleading file information.

Further analysis of libsvcs.dll identified capabilities consistent with a Remote Access Trojan (RAT), including persistence mechanisms, system information discovery, user activity monitoring, dynamic payload execution, and encrypted Command-and-Control (C2) communication. The malware contains hardcoded C2 infrastructure pointing to 103[.]231[.]12[.]27:4444, along with an embedded encryption key used for socket-based communication.

The observed capabilities—including modular payload loading, encrypted communication, persistence mechanisms, and remote execution functionality—indicate that the campaign is designed to establish unauthorized access to and maintain control over compromised hosts. The activity highlights the continued abuse of trusted government and financial themes to distribute malware targeting users and organizations in India.

## INTRODUCTION

---

This report analyzes a malware campaign leveraging a fraudulent Indian Income Tax Department assessment notification to distribute a RAT-like malware payload targeting Windows environments. The campaign uses the domain harivo[.]vip to host a fake tax assessment portal designed to resemble official government communication.

The attack chain begins with a social engineering lure prompting victims to download a ZIP archive (Tax\_Assessment\_0609.zip) containing a supposed tax assessment document. Upon extraction, the archive delivers a malicious disk image file (Tax\_Assessment.img) containing multiple malware components, including a loader executable (Tax\_Assessment.exe) and a malicious DLL payload (libsvcs.dll).

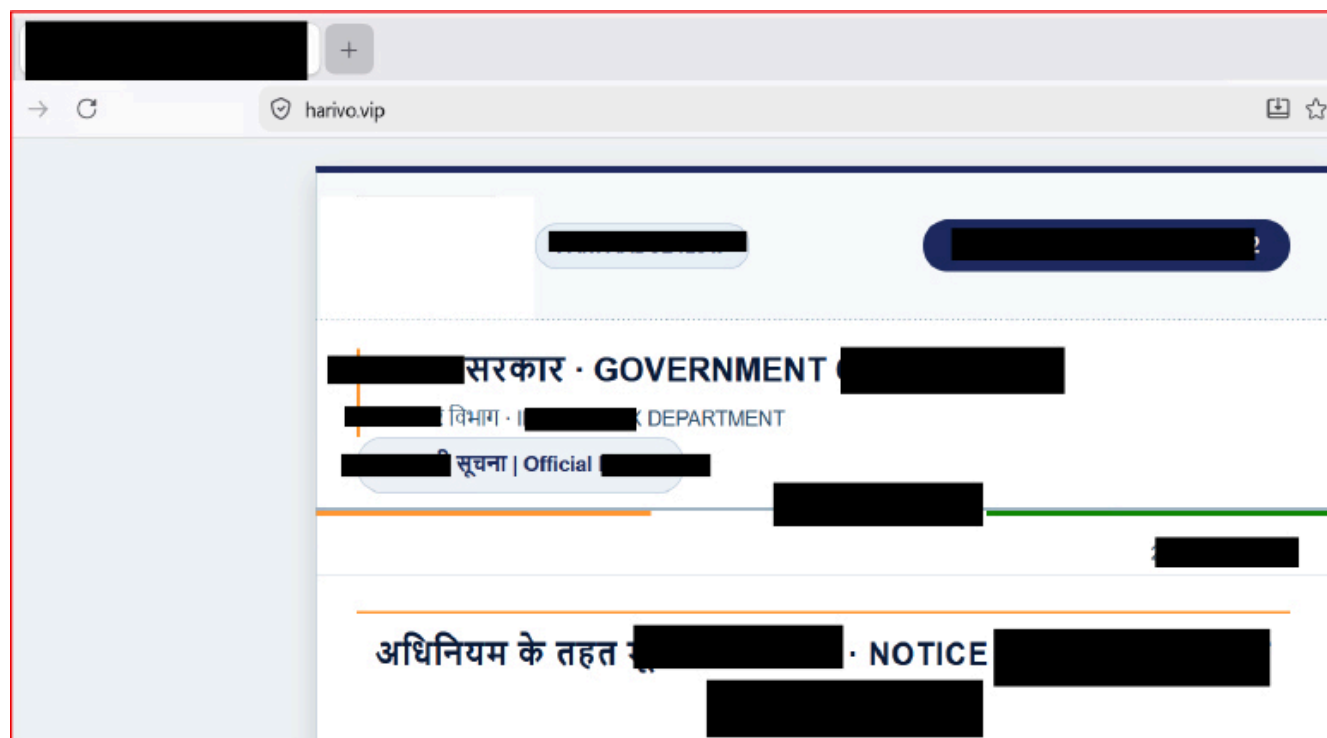
The malware follows a multi-stage execution approach where the initial executable acts as a loader, dynamically loading the DLL payload and transferring execution through reflection-based techniques. Subsequent analysis identified RAT-like capabilities that enable persistence, host reconnaissance, command execution, and encrypted C2 communication.

The campaign demonstrates the continued effectiveness of government-themed impersonation techniques combined with malware obfuscation and modular payload delivery to bypass user awareness and security controls.

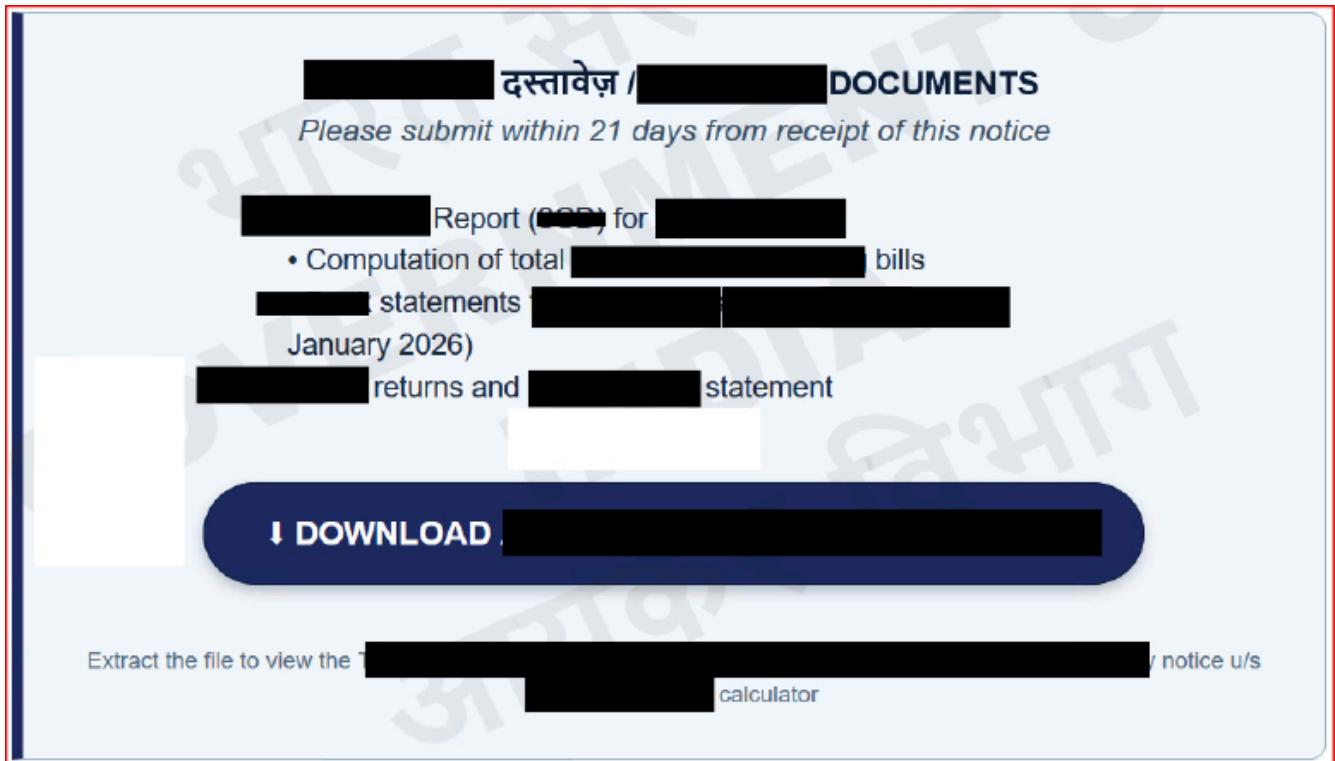
### Campaign Details:

The malware distribution campaign leverages a counterfeit Income Tax Department assessment notice to target individuals and organizations in India. The threat actors host a fraudulent tax-themed website on the domain harivo[.]vip, designed to closely imitate the appearance, language, and structure of legitimate government tax communications.

The fake portal uses official-looking branding, tax-related terminology, assessment references, and compliance instructions to establish credibility and persuade victims to download a malicious archive disguised as official assessment documentation. The campaign relies on social engineering techniques to deliver a staged malware payload, ultimately deploying RAT-like malware capable of persistence, system reconnaissance, and remote communication.



The website presents a fabricated assessment order containing taxpayer information, legal references, financial penalties, and compliance instructions to establish credibility and create a sense of urgency. Victims are encouraged to interact with a button labeled “Download Assessment Order & Workings,” which initiates the download of a malicious ZIP archive under the guise of official tax documentation.



#### Basic Details:

|                         |                                                                                                                                                                                                                                                                            |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target Technologies     | Windows Operating System, ZIP Archive                                                                                                                                                                                                                                      |
| Threat Type             | Social Engineering Campaign                                                                                                                                                                                                                                                |
| File Types              | ZIP Archive (.zip), Portable Executable (.exe disguised as image file), Dynamic Link Library (.dll)                                                                                                                                                                        |
| Key Malware Identifiers | Tax-themed lure, fraudulent Income Tax Department assessment notice, fake assessment portal, PE loader masquerading as image file ( <b>Tax_Assessment.img</b> ), DLL side-loading mechanism ( <b>libsvcs.dll</b> ), staged malware execution ( <b>Tax_Assessment.exe</b> ) |
| Observed First          | 2026-12-06                                                                                                                                                                                                                                                                 |
| Impact                  | Data Exfiltration                                                                                                                                                                                                                                                          |

|                   |                                                                                                                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MD5 Hashes</b> | Tax_Assessment_0609.zip<br>“3adcf5fca3f4fe23a9b73951e20d43bc”<br>Tax_Assessment.img<br>“ba036fbf209b2dbdfec3fd3dee9b1798”<br>libsvcs.dll<br>“c0796f2ee614e1711d5355ee42dcbf62”<br>Tax_Assessment.exe<br>“ac08e8f463e0fa4a431b74fd5d7f01a1” |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Key Capabilities

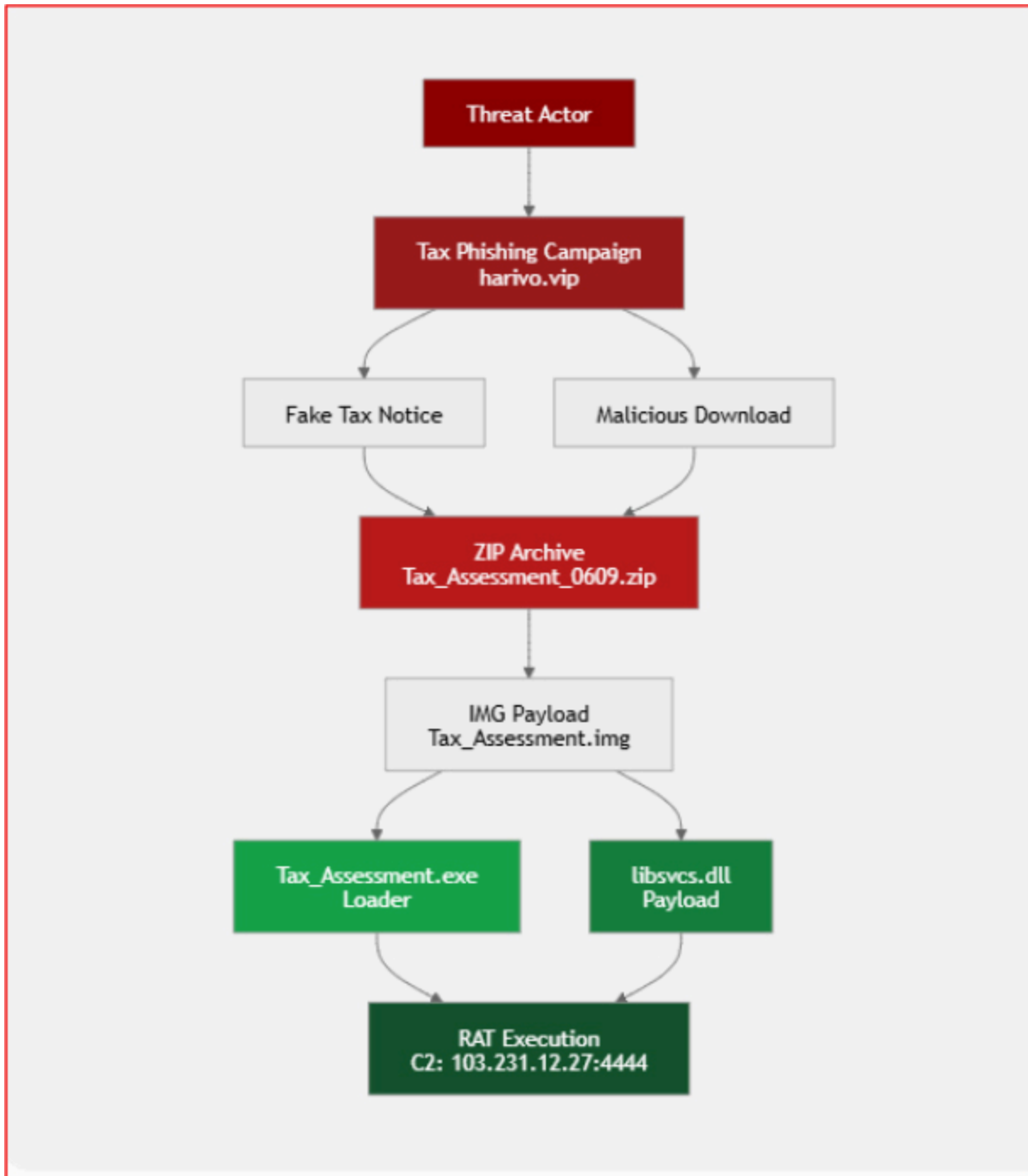
---

### 1. Government-Themed Social Engineering Campaign

- Threat actors used a fake Income Tax Department assessment notice to distribute malware.
- The lure uses tax compliance language, penalties, and legal references to increase victim trust.

### 2. Multi-Stage Malware Delivery Chain Identified

Infection chain:



### 3. Loader and Payload Separation

- Tax\_Assessment.exe operates as a loader.
- The executable dynamically loads libsvcs.dll using:
  - Assembly.LoadFrom()
  - Reflection-based execution
  - client.DllEntry.Run()

### 4. Anti-Analysis and Defense Evasion Techniques

Observed techniques include:

- ConfuserEx-based obfuscation
- Console window hiding
- Registry modification
- Spoofed assembly metadata
- Fake Microsoft-related identification details

## 5. Suspicious Metadata Manipulation

- Original filename identified:  
loader.exe
- Unusual version information:
  - Product Version: 0.0.0
  - File Version: 0.0.0
  - Indicating possible metadata tampering.

## 6. RAT Capabilities Identified

The malware contains functionality for:

- Persistence:
  - Startup registration
  - Auto-run modification
  - Scheduled task creation
- Discovery:
  - System information collection
  - Security product information
  - HWID collection
  - User activity monitoring
- Execution:
  - Dynamic method invocation
  - DLL loading
  - Remote payload execution

## 7. Encrypted C2 Communication

Observed C2 configuration:

IP: 103[.]231[.]12.27

Port: 4444

Location: Hong Kong

Embedded 32-byte encryption key:

03 AC 67 42 16 F3 E1 5C

76 1E E1 A5 E2 55 F0 67

95 36 23 C8 B3 88 B4 45  
9E 13 F9 78 D7 C8 46 F4

## 8. XWorm RAT-Like Behavior Observed

The combination of:

- encrypted socket communication
- RAT utility functions
- persistence mechanisms
- remote execution capability

is consistent with behaviors commonly observed in XWorm RAT-like malware families.

## MALWARE INFECTION LIFECYCLE

### Initial Access and Delivery

In the initial stage, download a malicious ZIP archive file named “Tax\_Assessment\_0609.zip” from the fraudulent website.

| Name                                                                                                        | Date modified      | Type                    | Size   |
|-------------------------------------------------------------------------------------------------------------|--------------------|-------------------------|--------|
| ▼ Today                                                                                                     |                    |                         |        |
|  Tax_Assessment_0609.zip | 6/17/2026 11:03 PM | Compressed (zipped) ... | 126 KB |

Upon extraction of the ZIP archive, a malicious disk image file named “Tax\_Assessment.img” is revealed. This IMG file acts as a container for multiple malware-related components and serves as the next-stage package responsible for delivering and facilitating the execution of the malicious payloads on the victim’s system.

| Name                                                                                                   | Date modified     | Type            | Size   |
|--------------------------------------------------------------------------------------------------------|-------------------|-----------------|--------|
| ▼ Last week                                                                                            |                   |                 |        |
|  Tax_Assessment.img | 6/8/2026 10:56 PM | Disc Image File | 366 KB |

### Analysis of the Disk Image File

Analysis of the “Tax\_Assessment.img” file revealed the presence of two malicious components associated with the next stage of the infection chain. The first component, “Tax\_Assessment.exe”, is a Portable Executable (PE) file that functions as a loader,

facilitating the execution of subsequent malicious payloads. The second component, “libsvcs.dll”, is a Dynamic Link Library (DLL) that serves as the primary malware payload and is loaded and executed by the loader component during the infection process.

|                                                                                                      |                   |                       |        |
|------------------------------------------------------------------------------------------------------|-------------------|-----------------------|--------|
| Last week                                                                                            |                   |                       |        |
|  libsvcs.dll        | 6/8/2026 10:56 PM | Application extension | 209 KB |
|  Tax_Assessment.exe | 6/8/2026 10:56 PM | Application           | 96 KB  |

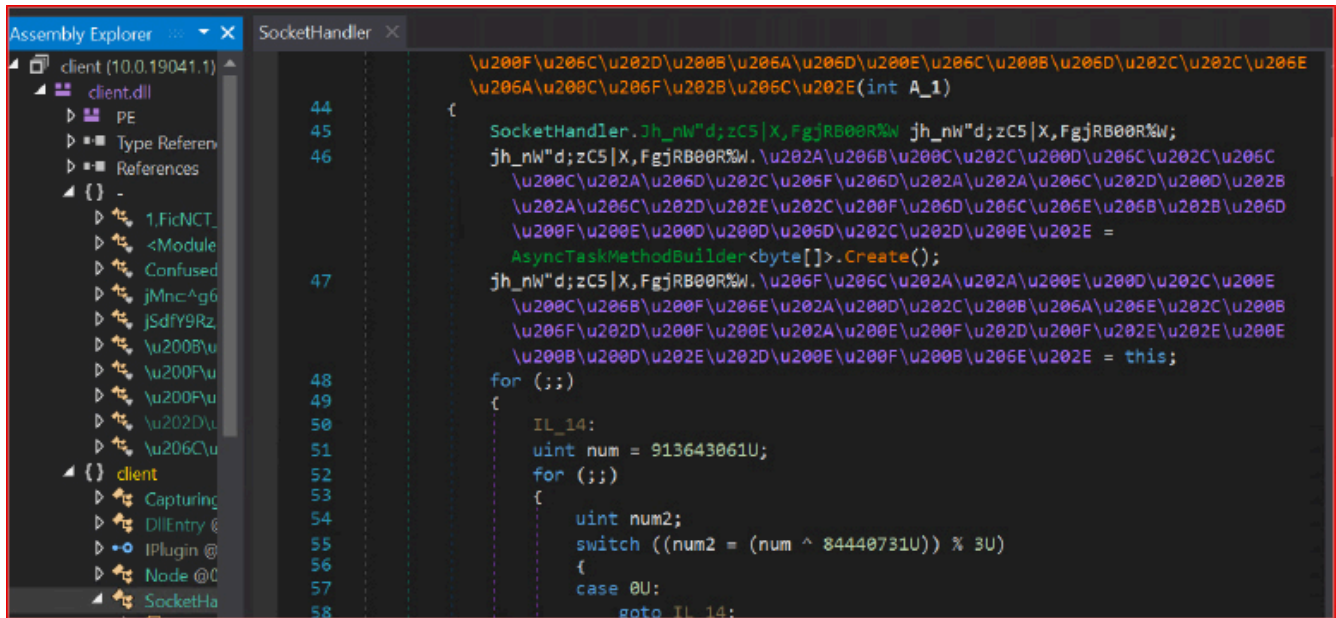
**Suspicious File Metadata Identified**

Tax\_Assessment.exe revealed the original filename loader.exe. The binary contains an unusual version of metadata with Product Version/File Version: 0.0.0.0, which may indicate metadata tampering or incomplete build information.

| Property          | Value             |
|-------------------|-------------------|
| Description       |                   |
| File description  |                   |
| Type              | Application       |
| File version      | 0.0.0.0           |
| Product name      |                   |
| Product version   | 0.0.0.0           |
| Copyright         |                   |
| Size              | 95.9 KB           |
| Date modified     | 6/8/2026 10:56 PM |
| Language          | Language Neutral  |
| Original filename | loader.exe        |

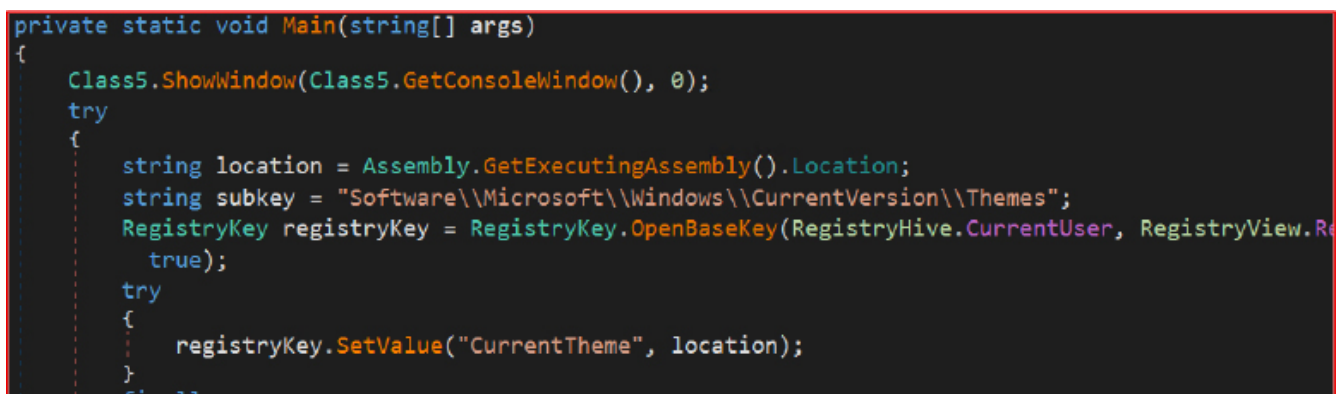
**Obfuscation in Tax\_Assessment.exe and libsvcs.dll**

The threat actor leveraged ConfuserEx to obfuscate Tax\_Assessment.exe and libsvcs.dll, introducing additional complexity for analysis and obscuring malicious code paths from analysts and automated security tools.



## Deobfuscated:

After deobfuscation, Tax\_Assessment.exe was observed hiding its console window and modifying user registry settings. This behavior suggests defense-evasion techniques aimed at reducing visibility and supporting malicious execution.



## Tax\_Assessment.exe Loads libsvcs.dll via Reflection

During entry-point analysis, Tax\_Assessment.exe was observed loading libsvcs.dll through Assembly.LoadFrom(). After successfully loading the assembly, the executable uses reflection to resolve the client.DllEntry class and invoke the Run method. This behavior indicates that Tax\_Assessment.exe functions primarily as a loader, while the core malicious functionality resides within libsvcs.dll. The use of reflection adds an additional layer of obfuscation, making automated analysis and detection more challenging.

```

case 2U:
    Assembly.LoadFrom(text).GetType("client.DllEntry").GetMethod("Run", BindingFlags.Static |
        BindingFlags.Public).Invoke(null, null);
    num3 = 2294105343U;
    continue;
case 3U:
    num3 = ((File.Exists(text) ? 2029637159U : 195690076U) ^ num2 * 3174451044U);
    continue;

```

```

string[] array = new string[]
{
    "libsvcs.dll"
};

```

## DLL Analysis:

Analysis of the DLL revealed modified assembly metadata intended to appear as a legitimate software component. The binary uses misleading identification details, such as “Runtime Service Host” and “Microsoft Corporation,” to blend with trusted Windows components, potentially reducing suspicion and increasing the chance of bypassing security detections.

```

[assembly: AssemblyVersion("10.0.19041.1")]
[assembly: AssemblyTrademark("")]
[assembly: AssemblyCopyright("Copyright (C) Microsoft Corporation")]
[assembly: AssemblyProduct("Runtime Service Host")]
[assembly: ComVisible(false)]
[assembly: TargetFramework(".NETFramework,Version=v4.7.2", FrameworkDisplayName = ".NET Framework 4.7.2")]
[assembly: AssemblyFileVersion("10.0.19041.1")]
[assembly: Guid("a2ebdf12-12c8-487a-90a6-31f2f5ddb1cc")]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: CompilationRelaxations(8)]
[assembly: AssemblyTitle("Runtime Service Host")]
[assembly: AssemblyCompany("Microsoft Corporation")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyDescription("Runtime Service Host")]

```

## Hardcoded C2 Infrastructure and Encrypted Communication Identified

Further analysis of the DLL revealed hardcoded Command-and-Control (C2) infrastructure, including the IP address 103[.]231[.]12[.]27 and port 4444. Additionally, the binary contains an embedded 32-byte constant likely used as a cryptographic key for socket communication, indicating the use of encrypted command-and-control (C2) traffic. The embedded encryption key identified within the binary is:

### Encryption Key (32 bytes):

```

03 AC 67 42 16 F3 E1 5C 76 1E E1 A5 E2 55 F0 67
95 36 23 C8 B3 88 B4 45 9E 13 F9 78 D7 C8 46 F4

```

The combination of a hardcoded C2 endpoint, custom encrypted socket communication, and RAT-like communication patterns is consistent with behavior commonly observed in XWorm RAT-like malware families.

```

// Token: 0x040000DE RID: 222
private static string string_0 = "103.231.12.27";

// Token: 0x040000DF RID: 223
private static int int_0 = 4444;

// Token: 0x040000E0 RID: 224
private static byte[] byte_0 = new byte[]
{
    3,
    172,
    103,
    66,
    22,
    243,
    225,
    92,
    118,
};

```

IP

PORT

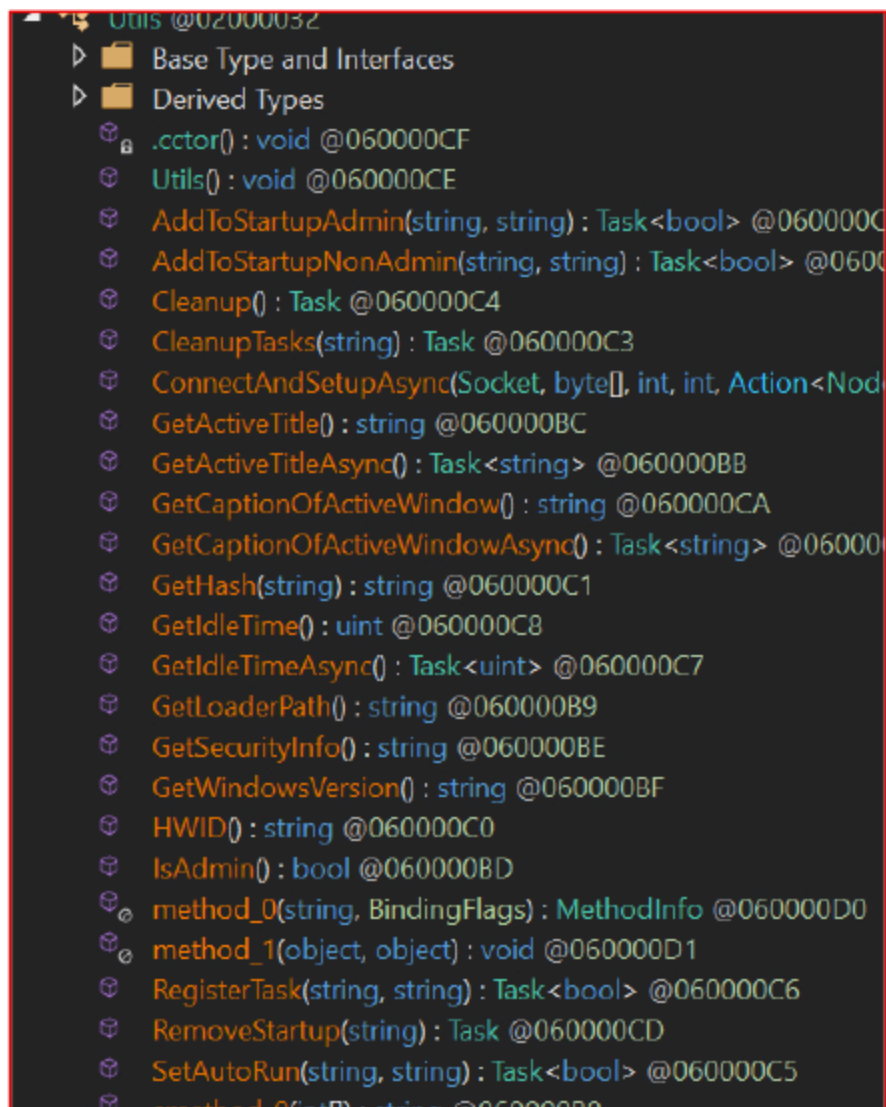
ENCRYPTION KEY

**Note:** The IP address 103[.]231[.]12[.]27 was identified as the RAT's hardcoded C2 server, geolocated to Hong Kong.

### RAT-Like Capabilities Identified Through Utility Function Analysis

Further analysis of the Utils class revealed multiple functions associated with Remote Access Trojan (RAT) functionality. The binary contains capabilities for persistence, system information gathering, remote communication setup, and payload execution. Functions such as AddToStartupAdmin, AddToStartupNonAdmin, and SetAutoRun indicate startup persistence mechanisms, while GetWindowsVersion, GetSecurityInfo, HWID, IsAdmin, and GetIdleTime support host reconnaissance.

The presence of ConnectAndSetupAsync, socket-related handling, and dynamic method invocation functionality indicates the ability to establish remote communication and execute additional code/components, including potential DLL loading. These capabilities align with behavior commonly observed in RAT malware families.



## Domain Analysis

The domain harivo[.]vip, registered on 25 September 2025 through Gname.com Pte. Ltd., is hosted on 38[.]76[.]161[.]218 and uses the name servers A6.SHARE-DNS.COM and B6.SHARE-DNS.NET. The domain is geolocated in Kwai Chung, New Territories, Hong Kong, and is assessed as potentially malicious due to its recent registration.

# Whois Record for Harivo.vip

## — Domain Profile

|                  |                                                                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registrar        | Gname.com Pte. Ltd.<br>IANA ID: 1923<br>URL: <a href="https://www.gname.com/">https://www.gname.com/</a><br>Whois Server: <a href="https://whois.gathernames.com">whois.gathernames.com</a><br><a href="mailto:complaint@gname.com">complaint@gname.com</a> |
| Registrar Status | clientTransferProhibited                                                                                                                                                                                                                                    |
| Dates            | 265 days old<br>Created on 2025-09-25<br>Expires on 2026-09-25<br>Updated on 2026-05-12                                                                                                                                                                     |
| Name Servers     | A6.SHARE-DNS.COM (has 4,137,157 domains)<br>B6.SHARE-DNS.NET (has 25 domains)                                                                                                                                                                               |
| IP Address       | 38.76.161.218 - 5 other sites hosted on this server                                                                                                                                                                                                         |
| IP Location      |  - New Territories - Kwai Chung - Cogent Communications Llc                                                                                                               |

## THREAT ACTOR HYPOTHESIS

Based on the observed tactics, techniques, and procedures (TTPs), the activity is assessed to be associated with a financially motivated threat actor or malware distribution group leveraging social engineering techniques to target users and organizations.

The use of an Income Tax Department-themed lure indicates an attempt to exploit regional trust, regulatory concerns, and tax compliance activities to increase victim interaction. The campaign demonstrates a preference for establishing unauthorized remote access, potential data theft, and long-term control over compromised systems rather than immediate destructive operations.

The adoption of a modular loader-payload architecture, ConfuserEx obfuscation, spoofed assembly metadata, encrypted C2 communication, and persistence mechanisms indicates deliberate efforts to maintain operational stealth and evade security detection.

The observed infrastructure shows a potential China/Hong Kong linkage, as both the identified C2 infrastructure (103[.]231[.]12[.]27:4444) and the malware distribution domain (harivo[.]vip) were associated with Hong Kong-based hosting/geolocation data during analysis. However, infrastructure location alone does not confirm the threat actor's origin, as

adversaries frequently use third-party hosting, compromised infrastructure, or regional services to obscure attribution.

The RAT-like capabilities, encrypted communication, and similarities to XWorm-like malware families suggest the possible use of a commodity RAT or a customized variant derived from publicly available malware frameworks. Based on current evidence, attribution to a specific threat actor remains unconfirmed.

## EXTERNAL THREAT LANDSCAPE MANAGEMENT

---

The analyzed campaign highlights the continued evolution of government-themed malware distribution operations, where threat actors abuse trusted institutions and regulatory processes to increase victim engagement. By impersonating the Income Tax Department, the operators leverage realistic tax-related communication, assessment references, compliance language, and financial pressure tactics to create urgency and convince victims to interact with malicious content.

The campaign demonstrates a structured multi-stage infection framework beginning with a fraudulent tax notification website (`harivo[.]vip`) that distributes a malicious archive disguised as official assessment documentation. The infection chain utilizes a staged payload delivery mechanism involving a ZIP archive, disk image container, executable loader (`Tax_Assessment.exe`), and DLL-based payload (`libsvcs.dll`). This modular approach allows the operators to separate delivery, execution, and payload functionality, increasing operational flexibility and reducing visibility during initial compromise.

Technical analysis identified multiple defense-evasion techniques, including ConfuserEx obfuscation, spoofed assembly metadata, hidden execution behavior, and reflection-based DLL loading. These mechanisms indicate a deliberate attempt to complicate reverse engineering, bypass static detection, and delay security analysis. The malware further demonstrates RAT-like functionality, including persistence mechanisms, host reconnaissance, remote execution capability, and encrypted Command-and-Control (C2) communication.

The identified C2 infrastructure (`103[.]231[.]12[.]27:4444`) and associated domain infrastructure show Hong Kong-based geolocation characteristics, indicating possible regional infrastructure overlap. However, such infrastructure usage alone does not establish attribution, as threat actors commonly rely on third-party hosting providers, rented infrastructure, or compromised systems to conceal their operational origin.

From a broader threat landscape perspective, this activity reflects the increasing adoption of commodity RATs and customized malware variants distributed through highly targeted social engineering campaigns. The combination of trusted-brand impersonation, malware

obfuscation, encrypted communication, and persistence capabilities increases the likelihood of successful compromise and prolonged unauthorized access.

Organizations should maintain heightened monitoring of tax-related phishing activity, strengthen controls around externally sourced archives and executable files, and improve detection coverage for suspicious loader behavior, DLL execution chains, unusual registry modifications, and outbound communication to newly observed infrastructure.

## MITRE ATT&CK FRAMEWORK

| Tactic         | ID        | Technique Name                             | Compacted Description                                         |
|----------------|-----------|--------------------------------------------|---------------------------------------------------------------|
| Initial Access | T1566.002 | Phishing: Spear phishing Link              | Fraudulent Income Tax website → malicious archive download    |
| Initial Access | T1189     | Drive-by Compromise                        | ZIP archive with malware delivered via fake portal            |
| Execution      | T1204.002 | User Execution: Malicious File             | User downloads/executes Tax_Assessment.exe                    |
| Execution      | T1218     | System Binary Proxy Execution              | Mounted disk image (Tax_Assessment.img) stages execution      |
| Execution      | T1059     | Command and Scripting Interpreter          | Reflection-based .NET dynamic execution                       |
| Execution      | T1620     | Reflective Code Loading                    | Assembly.LoadFrom() loads libsvcs.dll                         |
| Stealth        | T1027     | Obfuscated/Compressed Files                | ConfuserEx obfuscation on EXE/DLL                             |
| Stealth        | T1036     | Masquerading                               | Deceptive filenames/metadata impersonating tax docs           |
| Stealth        | T1036.005 | Match Legitimate Resource Name or Location | DLL metadata: "Runtime Service Host", "Microsoft Corporation" |

|                              |           |                                           |                                                       |
|------------------------------|-----------|-------------------------------------------|-------------------------------------------------------|
| <b>Stealth</b>               | T1140     | Deobfuscate/Decode Files                  | Runtime decoding of protected assemblies              |
| <b>Stealth</b>               | T1564.003 | Hide Artifacts: Hidden Window             | Console window hidden during execution                |
| <b>Stealth</b>               | T1112     | Modify Registry                           | Registry mods for execution/persistence               |
| <b>Persistence</b>           | T1547.001 | Registry Run Keys / Startup Folder        | SetAutoRun, AddToStartupAdmin/NonAdmin                |
| <b>Persistence</b>           | T1053.005 | Scheduled Task                            | Scheduled-task persistence functionality              |
| <b>Discovery</b>             | T1082     | System Information Discovery              | GetWindowsVersion() collects OS/host details          |
| <b>Discovery</b>             | T1518.001 | Security Software Discovery               | GetSecurityInfo() enumerates security products        |
| <b>Discovery</b>             | T1033     | System Owner/User Discovery               | User info collection during reconnaissance            |
| <b>Discovery</b>             | T1497.001 | Virtualization/Sandbox Evasion            | Anti-analysis checks before execution                 |
| <b>Command &amp; Control</b> | T1071.001 | Application Layer Protocol: Web Protocols | C2 via application-layer web communications           |
| <b>Command &amp; Control</b> | T1573     | Encrypted Channel                         | 32-byte embedded encryption key for C2                |
| <b>Command &amp; Control</b> | T1105     | Ingress Tool Transfer                     | Dynamic payload loading/execution                     |
| <b>Command &amp; Control</b> | T1219     | Remote Access Software                    | RAT functionality for remote access/command execution |

## CONCLUSION

---

The analysis identifies a malware campaign leveraging a fake Income Tax Department-themed lure to distribute a RAT-like payload through a staged infection chain involving a malicious ZIP archive, disk image, loader (Tax\_Assessment.exe), and DLL payload (libsvcs.dll).

The malware employs multiple evasion techniques, including ConfuserEx obfuscation, spoofed metadata, hidden execution, registry modification, and reflection-based DLL loading to hinder detection and analysis. The payload demonstrates RAT capabilities such as persistence, system discovery, remote execution, and encrypted C2 communication.

The presence of hardcoded C2 infrastructure (103[.]231[.]12[.]27:4444) and RAT-like functionality suggests the use of a commodity RAT or customized variant similar to XWorm RAT. Although Hong Kong-based infrastructure was identified, available evidence is insufficient for definitive threat actor attribution.

Organizations should strengthen phishing awareness, restrict suspicious file execution, monitor abnormal network activity, and apply endpoint detection controls to mitigate similar threats.

## RECOMMENDATIONS AND MITIGATION

---

### 1. Email and Web Security Controls

- Implement advanced email security controls to detect and block phishing campaigns containing tax-themed lures, suspicious attachments, and newly registered domains.
- Monitor and restrict access to newly created or low-reputation domains, especially those impersonating government or financial institutions.
- Enable URL filtering and sandboxing for suspicious web links and downloaded files.

### 2. File Execution Restrictions

- Block execution of unknown executable files delivered through archives, disk images, or removable media.
- Restrict execution of .exe, .dll, and script-based files from user-writable locations such as:
  - %AppData%
  - %Temp%
  - %Downloads%
  - mounted disk image locations
- Disable automatic execution behavior for downloaded archive contents.

### **3. Malware Detection and Endpoint Protection**

- Deploy endpoint detection solutions capable of identifying:
  - DLL side-loading behavior
  - Reflection-based assembly loading
  - Suspicious PowerShell or process execution chains
  - Abnormal registry modifications
  - Persistence mechanisms
- Ensure antivirus and EDR solutions are updated with the latest detection signatures and behavioral rules.

### **4. Network Monitoring and C2 Detection**

- Monitor outbound traffic for communication with suspicious external infrastructure, including:
  - 103[.]231[.]12[.]27:4444
  - Associated malicious domains and indicators
- Create detection rules for unusual encrypted socket communication from user endpoints.
- Inspect anomalous outbound connections from applications that normally do not require external communication.

### **5. Persistence Monitoring**

- Monitor registry locations commonly abused for persistence:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - Startup folders
  - Scheduled Tasks
- Alert on unauthorized modifications to autorun mechanisms.

### **6. User Awareness**

- Educate users to verify tax-related communications through official government portals instead of interacting with links or attachments received through email or messaging platforms.
- Train employees to identify:
  - Urgent compliance messages
  - Suspicious document downloads
  - Fake government notifications

### **7. Threat Hunting Activities**

- Hunt for:
  - Tax\_Assessment.exe
  - libsvcs.dll
  - Suspicious loader-style executables
  - ConfuserEx-obfuscated .NET binaries
  - Reflection-based DLL loading behavior
- Search for similar RAT activity using the IOCs and YARA rules provided.

## 8. Incident Response Readiness

- Isolate affected systems immediately if RAT activity is detected.
- Collect forensic artifacts including:
  - Process execution logs
  - Registry changes
  - Network connections
  - Dropped files
- Reset credentials and investigate potential data exposure after a confirmed compromise.

## 9. Application Control

- Implement application allowlisting policies to prevent execution of unknown binaries.
- Apply least-privilege principles and avoid running daily user activities with administrative privileges.

## 10. Continuous Threat Intelligence Monitoring

Monitor emerging infrastructure, domains, and malware variants related to:

- Tax-themed phishing campaigns
- RAT distribution activity
- Similar C2 infrastructure patterns

## INDICATORS OF COMPROMISE

---

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

| S. No | Indicator                                                        | Remarks |
|-------|------------------------------------------------------------------|---------|
| 1     | 372d7d8ca222e03afa5970848cf88efa6a3bc5146d20398601285fc7eaea6735 | Block   |
| 2     | f5dc1016679f54f2be22da0ff6642046f7a943410c188514b96c28d8a3b95e12 | Block   |

|   |                                                                  |         |
|---|------------------------------------------------------------------|---------|
| 3 | 4b5405d9acd00dd9225ffcec840a1752951be801d20ee1cab4ebde9ccd96916a | Monitor |
| 4 | 3fe29bf7e2c391d5405f8c6947cc42a6ec356fcf8455ce705dc23a156f5b450a | Block   |
| 5 | harivo[.]vip                                                     | Monitor |
| 6 | 103.231.12[.]27                                                  | Monitor |

## YARA Rules

---

```
rule Tax_Assessment_Malware_Campaign_IOC
```

```
{
```

```
meta:
```

```
description = "Detection rule for Tax Assessment themed malware campaign based on  
observed IOCs"
```

```
author = "CYFIRMA"
```

```
date = "2026-06-19"
```

```
strings:
```

```
// SHA-256 hashes
```

```
$hash1 = "372d7d8ca222e03afa5970848cf88efa6a3bc5146d20398601285fc7eaea6735"
```

```
$hash2 = "f5dc1016679f54f2be22da0ff6642046f7a943410c188514b96c28d8a3b95e12"
```

```
$hash3 = "4b5405d9acd00dd9225ffcec840a1752951be801d20ee1cab4ebde9ccd96916a"
```

```
$hash4 = "3fe29bf7e2c391d5405f8c6947cc42a6ec356fcf8455ce705dc23a156f5b450a"
```

```
// Domain IOC
```

```
$domain = "harivo.vip"
```

```
// IP IOC
```

```
$ip = "103.231.12.27"
```

```
// File Names
```

```
$file1 = "Tax_Assessment_0609.zip"
```

```
$file2 = "Tax_Assessment.img"
```

```
$file3 = "libsvcs.dll"
```

```
$file4 = "Tax_Assessment.exe"
```

```
// Campaign-specific strings
```

```
$str1 = "Download Assessment Order & Workings"
```

```
$str2 = "NOTICE OF ASSESSMENT"
```

\$str3 = "Income Tax Department"

\$str4 = "Assessment Order for AY 2025-26"

condition:

any of (\$hash\*) or

\$domain or

\$ip or

any of (\$file\*) or

3 of (\$str\*)

}

Copyright CYFIRMA. All rights reserved.