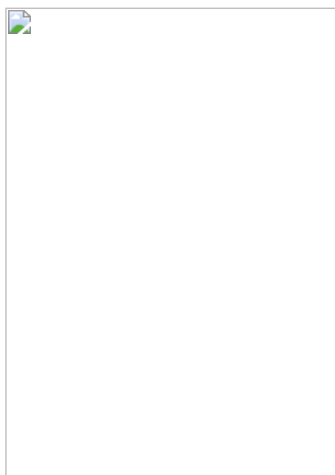


# From Click to Compromise: Unveiling the Sophisticated Attack of DoNot APT Group on Southern European Government Entities

[trellix.com/blogs/research/from-click-to-compromise-unveiling-the-sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/](https://trellix.com/blogs/research/from-click-to-compromise-unveiling-the-sophisticated-attack-of-donot-apt-group-on-southern-european-government-entities/)



## Blogs

---

The latest cybersecurity trends, best practices, security vulnerabilities, and more

By [Aniket Choukde](#), [Aparna Aripirala](#), [Alisha Kadam](#), [Akhil Reddy](#), [Pham Duy Phuc](#) and [Alex Lanstein](#) · July 8, 2025

### Introduction

---

The DoNot APT group, also identified by various security vendors as APT-C-35, Mint Tempest, Origami Elephant, SECTOR02, and Viceroy Tiger, has been active since at least 2016, and has been attributed by several vendors to have links to India. The global cybersecurity landscape is continually challenged by state-sponsored threat actors conducting espionage operations. The DoNot APT group (also known as APT-C-35), is believed to operate with a focus on South Asian geopolitical interests. This threat group typically targets government entities, foreign ministries, defense organizations, and NGOs especially those in South Asia and Europe. DoNot APT is known for using custom-built Windows malware, including backdoors like YTY and GEdit, often delivered through spear-phishing emails or malicious documents. Their operations are marked by persistent surveillance, data exfiltration, and long-term access, suggesting a strong cyber espionage motive. This report provides an analysis of a recent campaign orchestrated by the DoNot APT group.

Trellix Advanced Research Center's ongoing hunting efforts have uncovered a sophisticated campaign attributed to the DoNot APT group targeting a European foreign affairs ministry highlighting the evolving tactics of the group. The attackers impersonated European defense officials mentioning their visit to Bangladesh and lured their targets to click on a malicious Google Drive link. This delivered a malicious RAR archive, ultimately deploying malware consistent with the group's known toolset. This incident underscores the group's persistent focus on governmental and diplomatic entities and their adaptability in using common cloud services for initial infection.

The [Trellix Advanced Research Center](#) discovered this campaign by identifying the initial email chain, which was then blocked from customer inboxes via security signatures. This crucial starting point allowed us to further uncover the Tactics, Techniques, and Procedures (TTPs) and modus operandi (MO) of the campaign through correlation with existing threat intelligence. Other [security organizations](#) and [threat hunting groups](#) have also reported similar DoNot APT group activities, utilizing different initial infection methods.

### Attack summary: A multi-stage intrusion

---

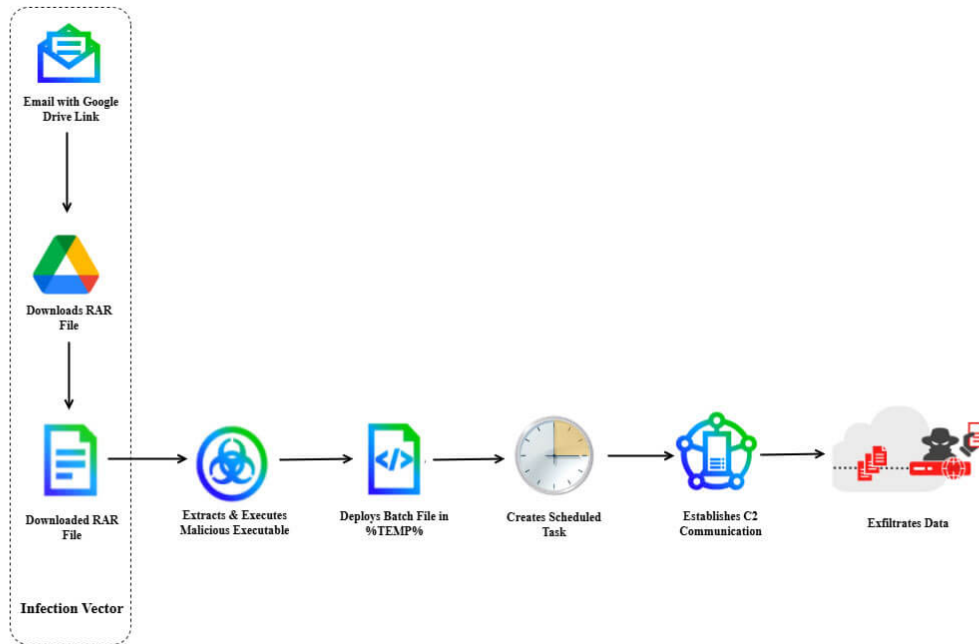


Figure 1: Illustrative representation of the Tactics, Techniques, and Procedures (TTPs) and malware employed by the Advanced Persistent Threat group APT-C-35 (DoNot Team/Mint Tempest) in their cyber espionage campaigns.

The core of the attack involved a multi-stage infection chain designed to establish a foothold within the target's network and exfiltrate sensitive information. Here's a breakdown of the incident:

- **Attack vector:** Spear-phishing email originating from a Gmail address (int.dte.afd.1@gmail[.]com) impersonating official correspondence, with a subject line referencing diplomatic activities.
- **Target:** A European government entity within the diplomatic sector.
- **Delivery method:** The email contained a Google Drive link (drive[.]usercontent[.]google[.]com/download?id=1t-fBZBgVtW\_S81qYGn9IoubWZwIXjl\_T) pointing to a malicious RAR archive named SyClrLtr.rar.
- **Payload and persistence:** The infection chain involved the user execution of notflog.exe from the RAR archive, which then deployed a batch file (djkgnosj.bat) in the %TEMP% directory. Persistence was achieved via a scheduled task named "PerformTaskMaintain," configured to run every 10 minutes, ensuring continued communication with the attackers' command and control (C2) server.
- **Malware implicated:** The telemetry and analysis of the payload associated this attack with "LoptikMod" malware, reportedly used exclusively by DoNot APT since 2018.

## Deconstructing the attack chain

The attack unfolded in a series of calculated steps:

1. **Initial lure:** The victim receives a carefully crafted spear-phishing email, impersonating defense officials and referencing a legitimate-sounding event to build trust.

The email leveraged diplomatic themes related to defense attaché coordination between Italy and Bangladesh. While the exact body content was not gathered in the findings, the subject line "Italian Defence Attaché Visit to Dhaka, Bangladesh" suggests a lure designed to appear as legitimate diplomatic correspondence that would reasonably contain document attachments or links. The email used HTML formatting with UTF-8 encoding to properly display special characters like "é" in "Attaché," demonstrating attention to detail to increase legitimacy.

2. **Malicious download:** Clicking on the embedded Google Drive link (drive[.]usercontent[.]google[.]com/download?id=1t-fBZBgVtW\_S81qYGn9loubWZwIXjl\_T) downloads the SyClrLtr.rar archive. The archive is protected with a password and the password to extract the archive is provided in the mail itself.

The extracted executable (notflog.exe) mimics a PDF document by displaying a PDF icon, tricking users into believing it's a safe document and prompting them to open it.

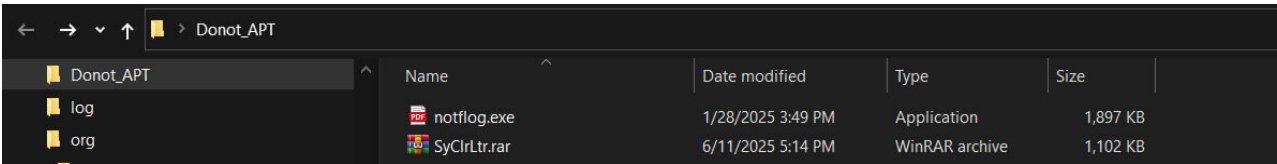


Figure 2: notflog.exe with PDF document icon

The file metadata of the executable contains information associated with a game program and is digitally signed by "Ebo Sky Tech Inc."

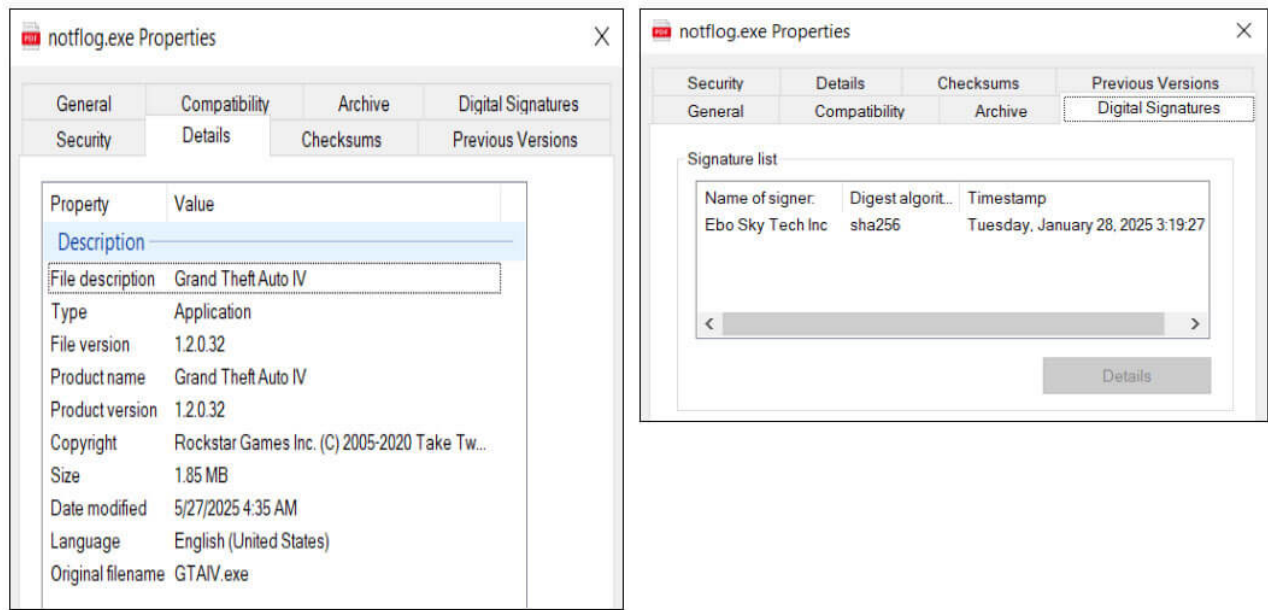


Figure 3: The embedded executable filename corresponds to a legitimate game program digitally signed by "Ebo Sky Tech Inc."

Static analysis of the malware executable also reveals the presence of the string "Loptik" within the strings which is significant because it is identified as being characteristic of the "LoptikMod" malware. This malware is associated exclusively with the DoNot APT group. Other identified string patterns also match previous DoNot APT campaigns, including the use of similar scheduled tasks (sfs.bat and djkfsoj.bat) for persistence. Subsequently, based on ThreatRay code-based analysis, out of 653 functions, there were 590 benign, and 30% of the combined malicious and unknown functions (which totals 63) is 19 malicious functions overlapped with other LoptikMod variants. This identification helped us to attribute the malware to this specific threat actor.





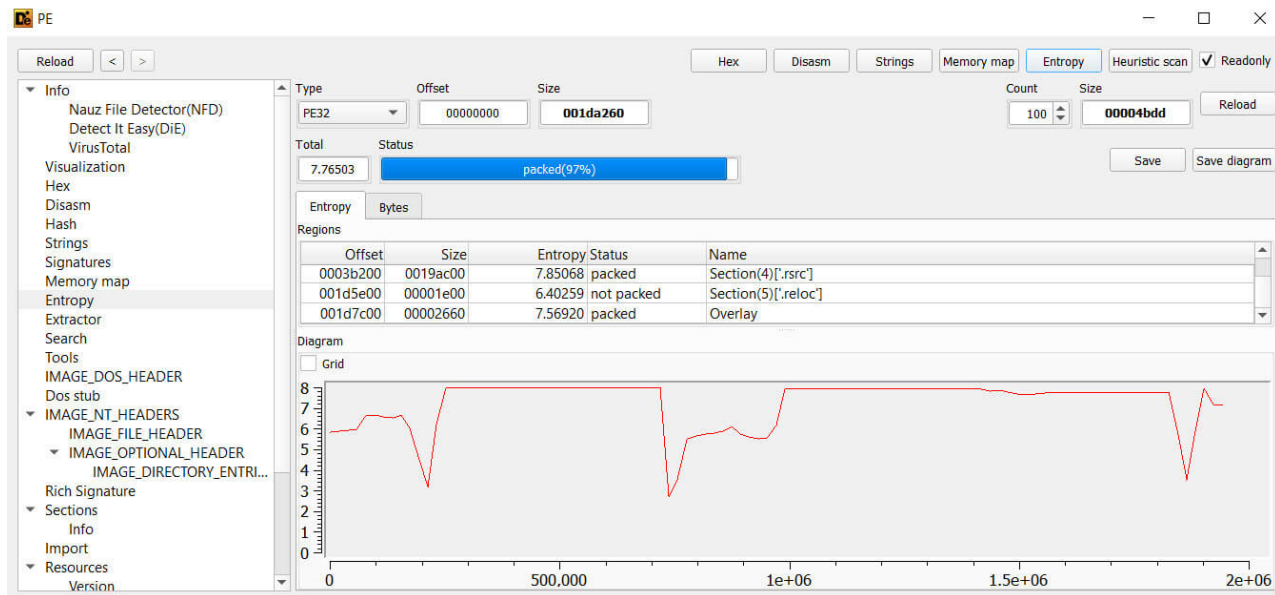


Figure 7: Selective Obfuscation via Section Packing in Malware Binary.

The file has less number of imports and the APIs required for the functionality of malware are loaded at runtime. Malware authors sometimes minimize the number of listed imports. This makes it harder for static analysis tools to quickly understand what the malware does just by looking at its imports. A low number of imports can make the file appear less suspicious at a glance.

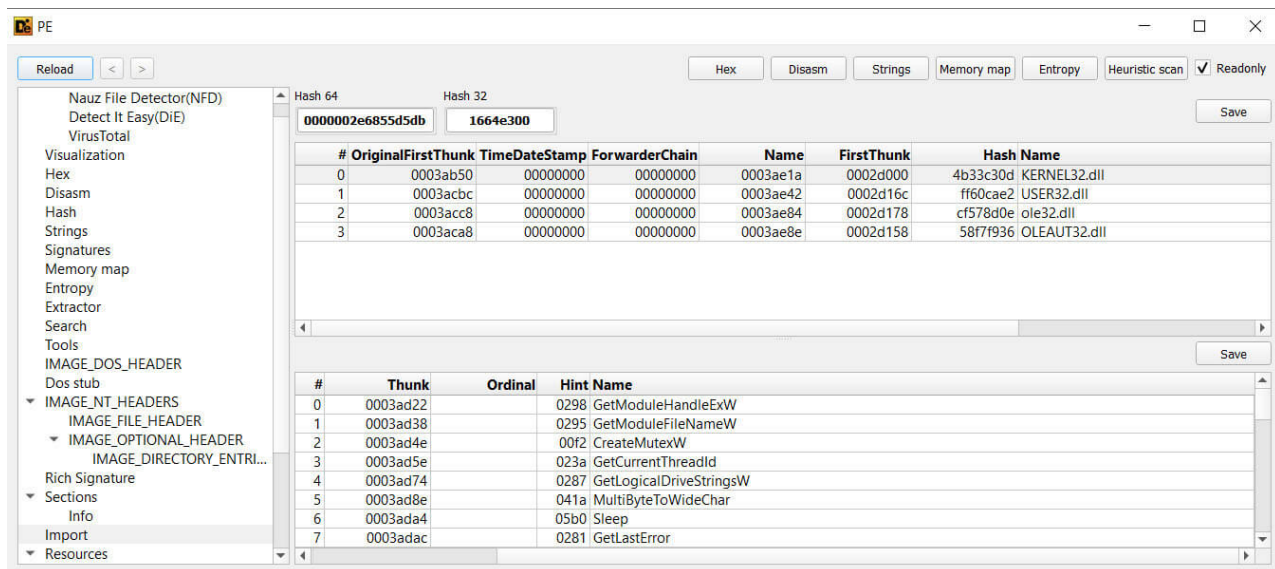


Figure 8: Minimal Import Table - API Obfuscation

Instead of directly importing APIs, malware can load them dynamically at runtime. This is done using functions like 'LoadLibrary' (to load a DLL) and 'GetProcAddress' (to retrieve the address of a specific function within that DLL).

The screenshot shows two windows from the IDA Pro disassembler. The left window, titled 'IDA View-A', displays assembly code. The right window, titled 'Pseudocode-A', displays the corresponding pseudocode.

```

IDA View-A:
cmova ecx, [ebp+lpProcName]
cmp [ebp+var_54], 7
push ecx
cmova eax, [ebp+lpModuleName]
push eax
call ds:GetModuleHandleW
push eax
push int
call ds:GetProcAddress
cmp [ebp+var_84], 0Fh
mov [ebp+var_BC], eax
lea eax, [ebp+lpLibFileName]
cmova eax, [ebp+lpLibFileName]
push eax
push int
call ds:LoadLibraryA
mov [ebp+var_B8], eax
test eax, eax
jnz loc_4037FA

Pseudocode-A:
if ( v81 > 7 )
    v2 = lpModuleName[0];
    ModuleHandleW = GetModuleHandleW(v2);
    ProcAddress = GetProcAddress(ModuleHandleW, v65);
    v4 = (const CHAR *)lpLibFileName;
    if ( v75 > 0xF )
        v4 = lpLibFileName[0];
    LibraryA = LoadLibraryA(v4);
    if ( LibraryA )
    {
        v68 = &v60;
        sub_409E50(v71 + 168);
        sub_40D2B0(&v60, v28, v34, v40, v46, v52, v58);
        LOBYTE(v87) = 5;
        sub_409E50(v71 + 912);
        LOBYTE(v87) = 4;
        sub_40D520((int)Block, v29, v35, v41, v47, v53, v59, v60, v61, v62, v63, (int)
        LOBYTE(v87) = 6;
    }

```

Figure 9: Import Address Table Evasion via Runtime API Lookup

Loading APIs at runtime means that these function calls are not visible in the static import table of the executable. This further hinders static analysis. Dynamic API loading adds an extra layer of obfuscation.

Key modules that have been loaded by malware are described below.

DLL name	Description
wininet.dll	Provides high-level functions for accessing the internet (HTTP, FTP) used by browsers and applications.
advapi32.dll	Provides access to advanced Windows functions like the Windows Registry, service control manager, and security APIs.
winhttp.dll	Provides low-level access to HTTP protocols for sending/receiving HTTP requests.
urlmon.dll	Handles URLs and protocols for downloading and linking content, used by Internet Explorer and other apps.
ws2_32.dll	Provides the core WinSock (TCP/IP) networking API used by nearly all network-enabled applications.

General	Statistics	Performance	Threads	Token	Modules	Memory	Environment	Handles	GPU	Disk and Network	Comment
Name	Base address	Size	Description								
<b>notflog...</b>	<b>0x400000</b>	<b>1.86 MB</b>	<b>Grand Theft Auto IV</b>								
advapi3...	0x75e70000	484 kB	Advanced Windows 32 Base API								
bcryptpr...	0x75050000	380 kB	Windows Cryptographic Primiti...								
combas...	0x751a0000	2.46 MB	Microsoft COM for Windows								
cryptbas...	0x74df0000	40 kB	Base cryptographic API DLL								
gdi32.dll	0x75bc0000	132 kB	GDI Client DLL								
gdi32full...	0x76a70000	1.36 MB	GDI Client DLL								
iertutil.dll	0x732d0000	2.16 MB	Run time utility for Internet Ex...								
imm32.dll	0x759e0000	148 kB	Multi-User Windows IMM32 AP...								
IPHLPAP...	0x74b50000	200 kB	IP Helper API								
kernel.a...	0x775c0000	60 kB	AppModel API Host								
kernel3...	0x75770000	896 kB	Windows NT BASE API Client ...								
KernelB...	0x772d0000	2 MB	Windows NT BASE API Client ...								
locale.nls	0x6e0000	796 kB									
msvcpr...	0x74fd0000	496 kB	Microsoft® C Runtime Library								
msvcrt.dll	0x75450000	764 kB	Windows NT CRT DLL								
mswsoc...	0x74d30000	328 kB	Microsoft Windows Sockets 2....								
mswsoc...	0x2520000	12 kB	Microsoft Windows Sockets 2....								
nsi.dll	0x775d0000	28 kB	NSI User-mode interface DLL								
ntdll.dll	0x77640000	1.6 MB	NT Layer DLL								
ntdll.dll	0x7ff9c1b600...	1.94 MB	NT Layer DLL								
ole32.dll	0x76970000	988 kB	Microsoft OLE for Windows								
oleaut3...	0x750b0000	584 kB	OLEAUT32.DLL								
OnDem...	0x746c0000	72 kB	On Demand Connctiond Route ...								
powrpro...	0x75150000	268 kB	Power Profile Helper DLL								
profapi.dll	0x756b0000	108 kB	User Profile Basic API								
rpcrt4.dll	0x75bf0000	748 kB	Remote Procedure Call Runtime								
sechost.dll	0x75960000	472 kB	Host for SCM/SDDL/LSA Looku...								
SHCore.dll	0x756d0000	528 kB	SHCORE								
shlwapi.dll	0x775e0000	272 kB	Shell Light-weight Utility Library								
SortDef...	0x2540000	3.21 MB									
sspicli.dll	0x74e00000	148 kB	Security Support Provider Inte...								
ucrthas...	0x74e30000	1.13 MB	Microsoft® C Runtime Library								
umpdc.dll	0x75850000	52 kB									
urlmon.dll	0x74020000	1.67 MB	OLE32 Extensions for Win32								
user32.dll	0x75510000	1.59 MB	Multi-User Windows USER API ...								
uxthem...	0x73b10000	488 kB	Microsoft UxTheme Library								
win32u.dll	0x75860000	92 kB	Win32u								
window...	0x76340000	5.75 MB	Microsoft WinRT Storage API								
winhttp.dll	0x73a10000	756 kB	Windows HTTP Services								
wininet.dll	0x74250000	4.36 MB	Internet Extensions for Win32								
winpr...	0x74750000	22 kB	Network Store Information PR...								

Figure 10: Modules loaded by the executable at runtime

- Execution and deployment:** Upon extraction and execution of notflog.exe, the payload creates a mutex with name "08808" to ensure that only one instance of the malware is active on the compromised system, preventing conflicts or interference with its operations.

Figure 11: Mutex Creation for Single Instance Control.

Figure 12: Malware Mutex Check for Instance and Infection Status.



Figure 13: Malware Mutex Object Creation.

The malware employs anti-VM techniques, specifically the "IN" assembly instruction, to hinder execution in virtual environments and evade analysis.

Figure 14: Anti-VM Check (Virtualization/Sandbox Evasion)

```

0040EDBA . 64:A3 00 mov dword ptr fs:[0],eax
0040EDC0 . 8965 E8 mov dword ptr ss:[ebp-18],esp
0040EDC3 . C645 E7 mov byte ptr ss:[ebp-19],1
0040EDC7 . C745 FC mov dword ptr ss:[ebp-4],0
0040EDCE . 52 push edx
0040EDCF . 51 push ecx
0040EDD0 . 53 push ebx
0040EDD1 . B8 685840 mov eax,564D5868 ; Load magic value 'VMXh' (reversed: 'hVMX' - known VMware magic)
0040EDD6 . BB 000000 mov ebx,0
0040EDDB . B9 0A0000 mov ecx,A ; I/O port 0x5658 (commonly used in VMware backdoor)
0040EDE0 . BA 585600 mov edx,5658 ; Read from port 0x5658 - triggers VMware behavior if present
0040EDE5 . ED in eax,edx ; Compare EBX to 'VMXh' magic value
0040EDE6 . 81FB 6858 cmp ebx,564D5868 ; Set byte if EBX == 'VMXh' - true if running under VMware
EIP->0040EDE7 . 0F9445 EB sete byte ptr ss:[ebp-19]
0040EDF0 . 5B pop ebx
0040EDF1 . 59 pop ecx
0040EDF2 . 5A pop edx
0040EDF3 . C745 FC mov dword ptr ss:[ebp-4],FFFFFFF
0040EDFA . 8A45 E7 mov al,byte ptr ss:[ebp-19] ; Move the byte to al
0040EDFD . 8B4D F0 mov ecx,dword ptr ss:[ebp-10]
0040EE00 . 64:890D mov dword ptr fs:[0],ecx
0040EE07 . 59 pop ecx
0040EE08 . 5F pop edi
0040EE09 . 5E pop esi
0040EE0A . 5B pop ebx
0040EE0B . 8BE5 mov esp,ebp
0040EE0D . 5D pop ebp
0040EE0E . C3 ret
0040EE0F . B8 010000 mov eax,1
0040EE14 . C3 ret
0040EE15 . 8B65 E8 mov esp,dword ptr ss:[ebp-18]
0040EE18 . 32C0 xor al,al
0040EE1A . C745 FC mov dword ptr ss:[ebp-4],FFFFFFF
0040EE21 . 8B4D F0 mov ecx,dword ptr ss:[ebp-10]

byte ptr ss:[byte ptr ss:[ebp-19]]=0019F92F=1

.text:0040EDEC .notflag_log_aslr_disabled.exe:$EDEC #E1EC <: Set byte if EBX == 'VMXh' - true if running under VMware>
Set flag if EBX == 'VMXh'

```

Address	Hex	ASCII
0019F92F	01 1C F9 19	..u.....pu..poA

Figure 15: VM/Sandbox evasion capabilities using x86 "IN" instruction

Initially, the sample generates the "%LocalAppdata%\TEMP\FROX\\" folder and drops "djkggosj.bat" into that location. This script likely handles the next stage of the infection.

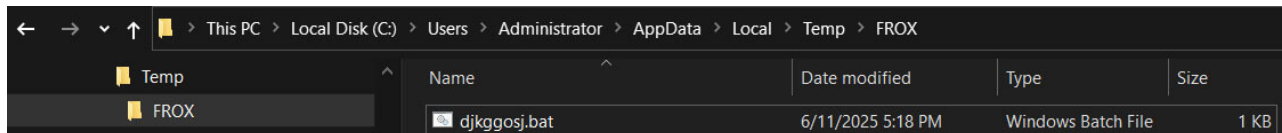
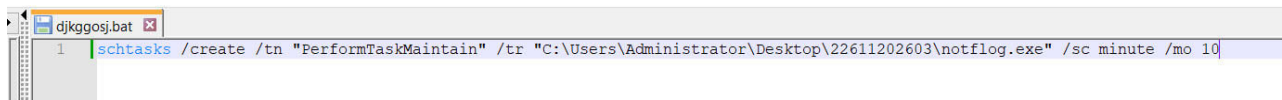


Figure 16: Temporary folder and .bat file creation for next stage infection.

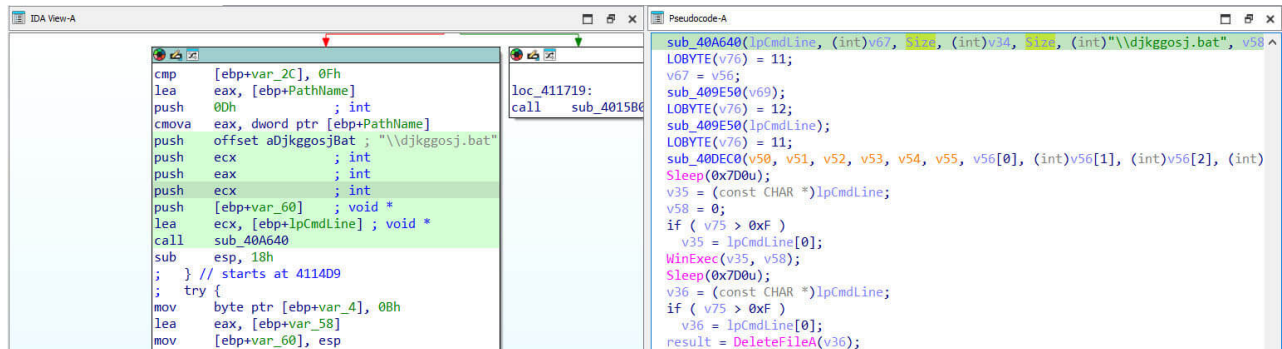
4. **Establishing persistence:** The batch script or the initial executable creates a scheduled task named "PerformTaskMaintain." This task is set to run every 10 minutes, ensuring the malware remains active and can re-establish connections even if interrupted.



```
schtasks /create /tn "PerformTaskMaintain" /tr "C:\Users\Administrator\Desktop\22611202603\noflog.exe" /sc minute /mo 10
```

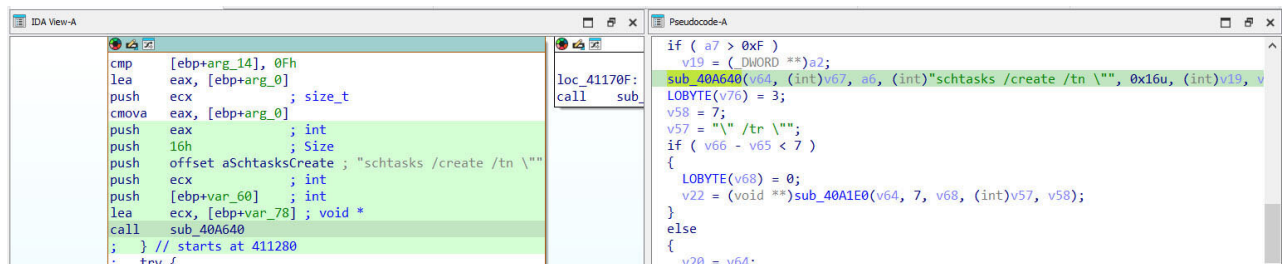
Figure 17: To ensure its continued operation on the compromised system even after reboots, the malware establishes persistence using schtasks.

The bat file is launched via the WinExec API and subsequently erased. This is a common tactic used by malware authors to evade forensic analysis and detection. Removing the file makes it more difficult for investigators to reconstruct the infection chain and understand the malware's actions.



```
cmp     [ebp+var_2C], 0Fh
lea     eax, [ebp+PathName]
push    0Dh ; int
cmova   eax, dword ptr [ebp+PathName]
push    offset aDjkggosjBat ; "\\djkggosj.bat"
push    ecx ; int
push    eax ; int
push    ecx ; int
push    [ebp+var_60] ; void *
lea     ecx, [ebp+lpCmdLine] ; void *
call    sub_40A640
sub     esp, 18h
; } // starts at 4114D9
; try {
mov     byte ptr [ebp+var_4], 0Bh
lea     eax, [ebp+var_58]
mov     [ebp+var_60], esp
```

Figure 18: Batch File Execution and Deletion - Evasion of Forensic Analysis



```
cmp     [ebp+arg_14], 0Fh
lea     eax, [ebp+arg_0]
push    ecx ; size_t
cmova   eax, [ebp+arg_0]
push    eax ; int
push    16h ; Size
push    offset aSchtasksCreate ; "schtasks /create /tn \"
push    ecx ; int
push    [ebp+var_60] ; int
lea     ecx, [ebp+var_78] ; void *
call    sub_40A640
; } // starts at 411280
; try {
```

Figure 19: Creating Persistence via Scheduled Task

5. **Command and control (C2) communication:** The malware gathers system details, including the CPU model, operating system name and build, username, hostname, CPU ProcessorID, and a list of installed software.

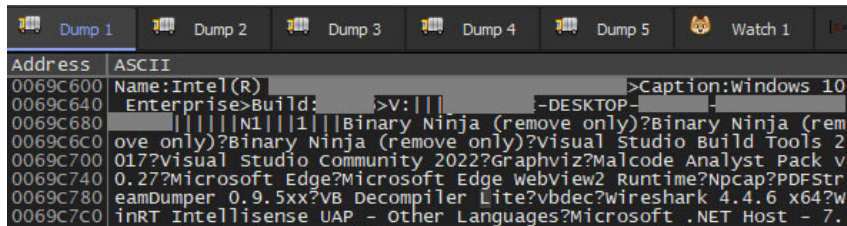


Figure 20: System Information Discovery - Data Collection by Malware.

The malware encrypts the gathered data using AES and then encodes it with Base64. This encoded data is appended to the 'batac=' parameter and sent via an HTTP POST request to 'https://totalservices[.]info/WxporesjaTexopManor/ptomekasresdkolerts'

The malware then attempts to establish communication with the command and control (C2) server located at totalservices[.]info, which resolves to the IP address 64[.]52[.]80[.]252. This communication uses HTTPS, and the malware sends POST requests to the C2 server.

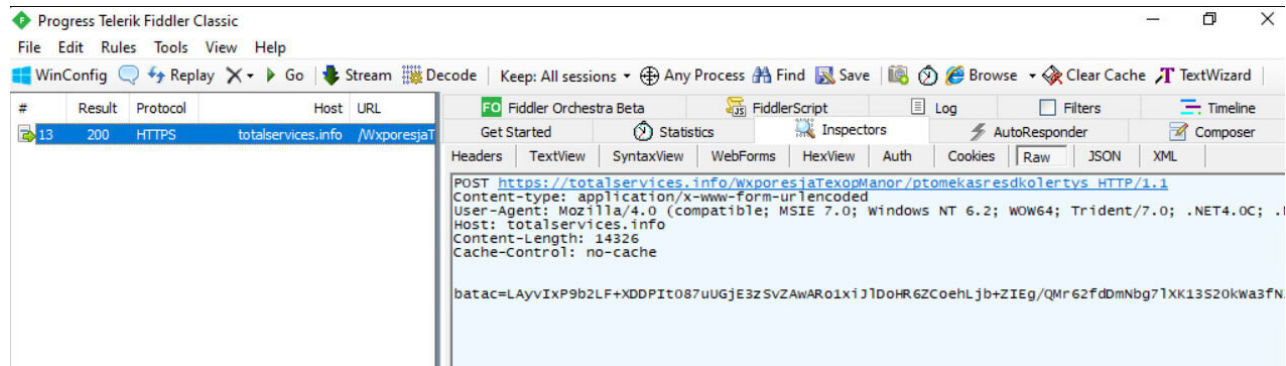


Figure 21: C2 Communication - HTTPS POST to totalservices[.]info (64[.]52[.]80[.]252) - Mimicking Legitimate Services

The command and control domain (totalservices[.]info) follows the actor's typical pattern of using legitimate-sounding service domains.

Once the connection is established, the malware can receive further commands, download additional modules, and exfiltrate sensitive data from the compromised system to likely target MFA credentials and diplomatic communications.

However, during our analysis of this malware, the C2 server appeared to be inactive. This made it challenging to observe the full range of commands the malware might receive or the extent of data it intended to exfiltrate. The inactive state of the C2 server at the time of analysis could mean that the attackers have temporarily disabled it, switched to a different server, or the infrastructure is no longer functional.

Based on the C2 server's response, the malware determines whether to download a follow-on payload, 'socket.dll'. Prior to this determination, the malware collects and exfiltrates system information such as username, hostname, and ProcessorID.

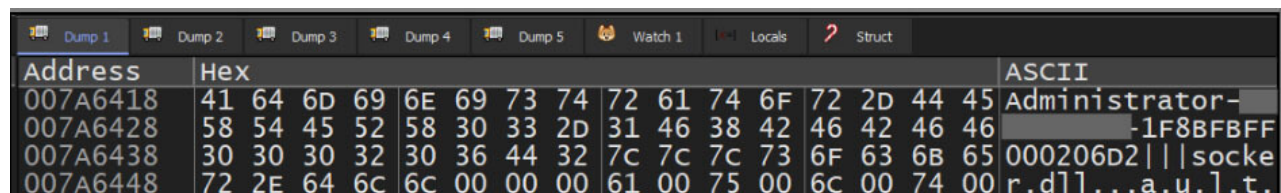


Figure 22: Victim Identification Data Collection (Username, Hostname, ProcessorID).

This payload is encrypted, combined with a victim ID (derived from username, hostname, and ProcessorID), and sent in the 'data' field of a POST request to : 'https://totalservices[.]info/WxporesjaTexopManor/vrtpvabkokamekastra/N1/SA'.

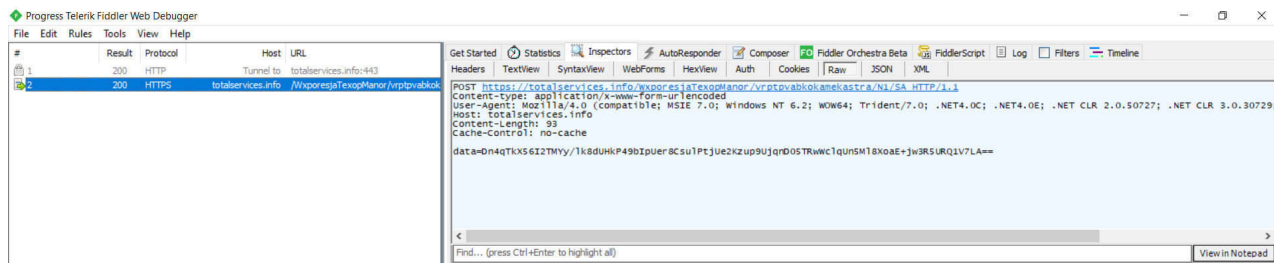


Figure 23: Data Exfiltration via Encrypted POST Request to C2 Server

Following the download of the payload, the malicious actor saves the dynamic link library, "socket.dll," to the location "%LocalAppdata%\moshtmlclip\socket.dll."

Address	Hex	ASCII
009FCD50	43 3A 5C 55 73 65 72 73 5C 41 64 6D 69 6E 69 73	C:\Users\Adminis
009FCD60	74 72 61 74 6F 72 5C 41 70 70 44 61 74 61 5C 4C	trator\AppData\L
009FCD70	6F 63 61 6C 5C 6D 6F 73 68 74 6D 6C 63 6C 69 70	ocal\moshtmlclip
009FCD80	5C 73 6F 63 6B 65 72 2E 64 6C 6C 00 00 00 00 00	\socket.dll.....

Figure 24: Destination Path for 'socket.dll' Delivery

Subsequently, another batch file, named "sfs.bat," is dropped into the "%LocalAppdata%\Temp\FROX\" directory.

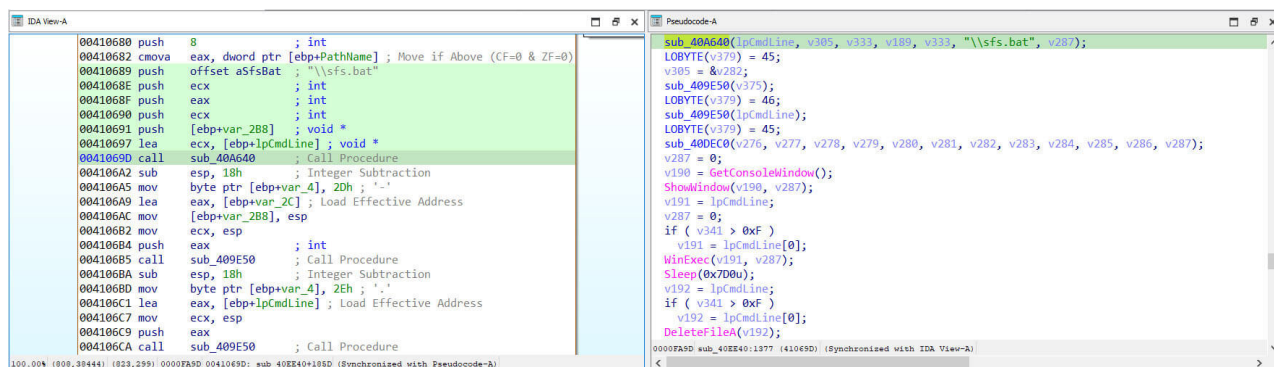


Figure 25: Staging of "sfs.bat" for Scheduled Task Setup

← → ↕ This PC > Local Disk (C:) > Users > Administrator > AppData > Local > Temp > FROX				
Temp	FROX	sfs.bat	6/11/2025 5:20 PM	Windows Batch File 1 KB

Figure 26: "sfs.bat" Batch File Drop Location

This batch file is designed to create a scheduled task named "MicorsoftVelocity." The purpose of this scheduled task is to ensure the execution of "socket.dll," specifically triggering the export function "?ejjwed@@YAHXZ." This sequence of actions ensures the persistence and subsequent activation of the downloaded payload on the compromised system.

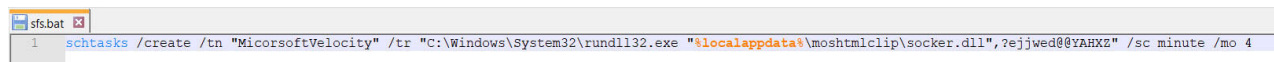


Figure 27: 'MicorsoftVelocity' scheduled task - Execution of 'socket.dll' export function '?ejjwed@@YAHXZ'.

As "socket.dll" was not obtained during analysis, a detailed examination of its loading behavior and subsequent loading functions are currently not possible. Due to this unavailability and lack of a captured sample, the investigation into how it loads and operates is presently limited.

The DoNot APT group is a persistent cyber-espionage threat, active since at least 2016, targeting government, military, and diplomatic entities primarily in South Asia, but with increasing reach to other regions.

They employ sophisticated malware frameworks like "YTY" and use various infection methods, including spear-phishing and malicious archives, demonstrating adaptability in their tactics.

The recent targeting of a European foreign affairs ministry highlights their expanding scope and persistent interest in gathering sensitive information, underscoring the need for heightened vigilance and robust cybersecurity measures.

## European diplomatic interests in the crosshairs

---

Trellix Advanced Research Center's proactive threat hunting efforts highlighted a significant development which has been observed with the targeting of a European foreign affairs ministry by the DoNot APT group. While historically focused on South Asia, this incident targeting South Asian embassies in Europe, indicates a clear expansion of their interests towards European diplomatic communications and intelligence. These operations underscore DoNot APT's persistent and broadening efforts to gather sensitive political, military, and economic information, a threat that Trellix is actively tracking and analyzing through its advanced intelligence initiatives.

## MITRE ATT&CK TTPs and Indicators of Compromise:

---

This campaign showcases several Tactics, Techniques, and Procedures (TTPs) commonly associated with APT operations, mapped to the MITRE ATT&CK® framework:

Initial Access	Phishing: Spearphishing Link	T1566.002	Email URL: drive[.]usercontent.google[.]com/download?id=1t-fBZBgVtW_S81qYGn9loubWZwlXjl_T
Execution	User Execution: Malicious File	T1204.002	Victim opens SyClrLtr.rar → runs notflog.exe
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	Executes Djkggosj.bat, sfs.bat
Persistence	Scheduled Task/Job: Scheduled Task	T1053.005	Creates scheduled tasks: "PerformTaskMaintain" "MicorsoftVelocity"
Defense Evasion	Virtualization/Sandbox Evasion: System Checks	T1497.001	"IN" x86 assembly instruction used for evading virtual environment
Defense Evasion	Obfuscated Files or Information: Encrypted/Encoded File	T1027.013	Encoded ASCII strings in file Notflog.exe
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	C2 communication: totalservices[.]info
Discovery	System Information Discovery	T1082	Collecting username, hostname, and ProcessorID etc.
Discovery	File and Directory Discovery	T1083	Search for %localappdata% in user environment

Exfiltration	Exfiltration Over C2 Channel	T1041	HTTPS POST request: hxxps://totalservices[.]info/WxporesjaTexopManor/vrptpvabkokamekastra/N1/SA'.
--------------	------------------------------	-------	--

### Key Indicators of Compromise (IoCs) from this campaign include:

Email Sender Address	int[.]dte[.]afd[.]1@gmail[.]com
Email Subject	Italian Defence Attaché Visit to Dhaka, Bangladesh
URL – stage-0	drive.usercontent.google[.]com/download?id=1t-fBZBgVtW_S81qYGn9IoubWZwlXjI_T
URL – RAR file	SyClrLtr.rar
SyClrLtr.rar (SHA256)	5317f22c60a4e08c4caa28bc84f653b1902fa082d2d1d7fcf2cd0ce1d29798d6
Initial Executable	notflog.exe
notflog.exe (SHA256)	4d036e0a517774ba8bd31df522a8d9e327202548a5753e5de068190582758680
C2 Domain	totalservices[.]info
C2 IP Address	64[.]52[.]80[.]252
Scheduled Task Name	PerformTaskMaintain, MicorsoftVelocity

*Note: While these IoCs were reported in this specific campaign, public corroboration for the hashes on platforms like VirusTotal or the C2 domain in widely indexed threat feeds was not available at the time of this analysis. The malware name "LoptikMod" and specific file names like notflog.exe and djkggosj.bat are also not broadly documented in public threat intelligence regarding DoNot APT.*

### Strategic implications

Attacks targeting foreign ministries and diplomatic entities are classic espionage operations. The goal is to gain illicit access to sensitive state communications, policy documents, negotiation strategies, and intelligence reports. For an actor like DoNot APT, such information can provide significant strategic advantages to their sponsors. The use of a trusted platform like Google Drive for initial malware delivery also highlights the attackers' efforts to bypass initial security filters.

### Defending against DoNot APT: Detection and mitigation

Organizations, especially government and diplomatic entities, should consider the following measures:

- Enhanced email security:** Implement robust email filtering solutions to detect and block spear-phishing attempts. Train employees to identify suspicious emails, especially those containing links or attachments, even if they appear to come from known or official sources.
- Network traffic analysis:** Monitor network traffic for unusual outbound connections, especially to known malicious domains/IPs or those not typically associated with your organization's activities. Look for beaconing patterns consistent with C2 communication.
- Endpoint detection and response (EDR):** Deploy EDR solutions to monitor endpoint activity for suspicious processes, file modifications (especially in %TEMP%), and the creation of scheduled tasks.  
Specifically, hunt for scheduled tasks with unusual names or frequent execution intervals (e.g., "PerformTaskMaintain" running every 10 minutes).
- Application whitelisting and script control:** Restrict the execution of unauthorized applications and scripts (e.g., PowerShell, batch files) where possible.
- Cloud service monitoring:** While challenging, monitor or restrict downloads from personal or untrusted cloud storage links if feasible within your organization's policy.
- IoC blocking:** Block the known IoCs (domains, IPs) associated with this and other DoNot APT campaigns at your firewall and proxy levels.
- Regular patching:** Keep operating systems and applications, particularly Microsoft Office, updated to prevent exploitation of known vulnerabilities.

8. **Threat intelligence sharing:** Participate in threat intelligence sharing communities to stay informed about the latest TTPs and IoCs from groups like DoNot APT.

## Trellix product detection:

---

Trellix Endpoint Security (HX)	<ul style="list-style-type: none"><li>• DONOT APT (FAMILY)</li><li>• Gen:Variant.Fragtor.831285</li></ul>
Trellix ENS	Trojan-Donot!893561FF6D17
Trellix EDR	<ul style="list-style-type: none"><li>• Created batch file [T1059.003]</li><li>• Created Scheduled Task via Schtasks.exe [T1053.005]</li><li>• Suspicious scheduled task creation (runs a binary from uncommon location) [T1053.005]</li><li>• Suspicious scheduled task was created [T1053.005]</li></ul>
Trellix Network Security Trellix VX Trellix Cloud MVX Trellix Malware Analysis Trellix Email Security Trellix Detection As A Service Trellix NX	<ul style="list-style-type: none"><li>• FE_Backdoor_Win_LoptikMod_1</li><li>• FE_Backdoor_Win_LoptikMod_2</li><li>• Backdoor.Win.LoptikMod</li><li>• Backdoor.Win.LoptikMod.MVX</li></ul>

## Conclusion:

---

The DoNot APT group remains an active and evolving threat, particularly to governmental and diplomatic organizations in South Asia and, increasingly, their interests in other regions like Europe. Their use of common platforms like Google Drive for malware delivery, combined with their established multi-stage infection tactics and custom malware, underscores the need for a defense-in-depth security posture. Vigilance, robust security controls, and employee awareness are crucial in mitigating the risk posed by such sophisticated state-sponsored actors.

Trellix offers a robust and integrated security solution designed to protect various aspects of an organization's digital environment. It covers endpoints, networks, data, email, cloud, and security operations with different security technologies and features. By integrating AI, real-time intelligence, behavioral analysis, and cloud-based detection, Trellix ensures that its security platform remains adaptable and resilient in the face of evolving cyber threats. The continuous learning and dynamic threat response capabilities make Trellix a proactive solution, helping organizations stay ahead of emerging challenges in the ever-changing cybersecurity landscape.

Discover the latest cybersecurity research from the Trellix Advanced Research Center: <https://www.trellix.com/advanced-research-center/>

## RECENT NEWS

---

## RECENT STORIES

---

## Get the latest

---

Stay up to date with the latest cybersecurity trends, best practices, security vulnerabilities, and so much more.

Please enter a valid email address.

Zero spam. Unsubscribe at any time.