ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

DoNot (APT-C-35) Cyber-Espionage Campaign Targeting Bangladesh Military and Defence Personnel

TLP: CLEAR
Distribution: Public
Advisory on: DoNot (APT-C-35) Cyber-Espionage Campaign Targeting Bangladesh Military and Defence
Severity: Critical
Threat Type: Advanced Persistent Threat (APT) / Cyber Espionage
Attack Vector: Targeted Spear-Phishing / Weaponized RTF Document
Affected Sectors: Bangladesh Military and Defence Establishment
Date: 16 August 2026

Executive Summary

BGD e-GOV CIRT is issuing this cybersecurity advisory regarding an active and highly targeted cyber-espionage campaign directed against **Bangladesh military and defence personnel**.

The campaign has been attributed with high confidence by security researchers to **DoNot Team (APT-C-35)**, an advanced persistent threat group known for conducting sustained intelligence-gathering operations against government, military, diplomatic, and strategic organizations across South Asia.

The observed intrusion begins with a carefully crafted spear-phishing lure named:

`Biography Air Vice Marshal Sitwat Nayeem.doc`

The document is designed to appear as biographical information concerning a senior Bangladesh Air Force officer, demonstrating deliberate targeting of Bangladesh's defence community.

The malicious RTF does not directly contain the principal malware payload. Instead, it uses **remote template injection** to contact attacker-controlled infrastructure and retrieve a malicious Microsoft Word template. Importantly, the delivery infrastructure performs **server-side victim filtering/geofencing**, allowing the threat actor to selectively deliver malicious content to intended targets while presenting benign content to researchers, sandboxes, VPN users, or other non-target systems.

Once the malicious template is delivered, embedded VBA code executes architecture-specific shellcode and abuses Windows APIs to execute code inside the Microsoft Office process. Subsequent stages use multiple layers of XOR encoding, runtime API resolution, anti-hooking techniques, and payload masquerading using benign-looking `.ico`, `.mp3`, and `.doc` extensions.

The infection ultimately deploys a DLL implant that:

- establishes scheduled-task persistence disguised as Microsoft OneDrive telemetry;
- collects detailed host and software information;
- communicates with attacker-controlled infrastructure over HTTPS;
- encrypts reconnaissance data using AES-128-CBC;

- implements a multi-phase C2 handshake;
- conditionally downloads additional modules based on victim profiling; and
- deletes original artifacts to reduce forensic evidence.

Researchers were able to retrieve a live follow-on module, `ejtest.dll`, directly from active C2 infrastructure, indicating that the infrastructure was actively capable of delivering additional payloads at the time of investigation.

Given the highly targeted lure, regional filtering, active C2 infrastructure, modular payload delivery and focus on military personnel, BGD e-GOV CIRT assesses this activity as presenting **a critical cyber-espionage risk to Bangladesh's defence and government ecosystem**.

Threat Overview

Attribute	Details
Threat Actor	DoNot Team / APT-C-35
Campaign Objective	Cyber espionage / intelligence collection
Target Geography	Bangladesh
Primary Target	Military and defence personnel
Initial Access	Spear-phishing attachment
Initial File	Weaponized RTF disguised with .doc extension
Social Engineering Theme	Biography of Bangladesh Air Force officer
Delivery Technique	Remote Template Injection
Payload Execution	VBA + architecture-aware shellcode
Defense Evasion	Geofencing, obfuscation, anti-hooking, masquerading
Persistence	Scheduled Task
C2	HTTPS / TCP 443
C2 Encryption	AES-128-CBC + Base64
Follow-on Capability	Modular DLL download
Assessed Severity	Critical

Bangladesh-Specific Threat Assessment

This campaign should be treated as particularly significant because the observed intrusion is **not a generic malware distribution campaign**.

The lure itself was customized around Bangladesh's military environment. The malicious document used the biography of a Bangladesh Air Force officer as the social-engineering theme, indicating prior reconnaissance and knowledge of the intended target community. Furthermore, the malicious template infrastructure reportedly evaluates characteristics of incoming requests before deciding whether to deliver malicious content. Researchers observed that direct requests could receive a benign template instead of the malicious VBA-enabled version.

This selective-delivery architecture can significantly reduce detection by automated malware-analysis platforms. Potentially at-risk entities include:

- Bangladesh Armed Forces;
- Ministry of Defence and related organizations;
- defence contractors and suppliers;
- diplomatic missions;
- strategic government organizations;
- military research and educational institutions;
- personnel communicating with defence establishments; and
- organizations maintaining trusted relationships with defence networks.

Compromise of such systems may enable intelligence collection relating to military personnel, internal documents, organizational structures, installed software, operational communications and other sensitive information.

Technical Attack Chain

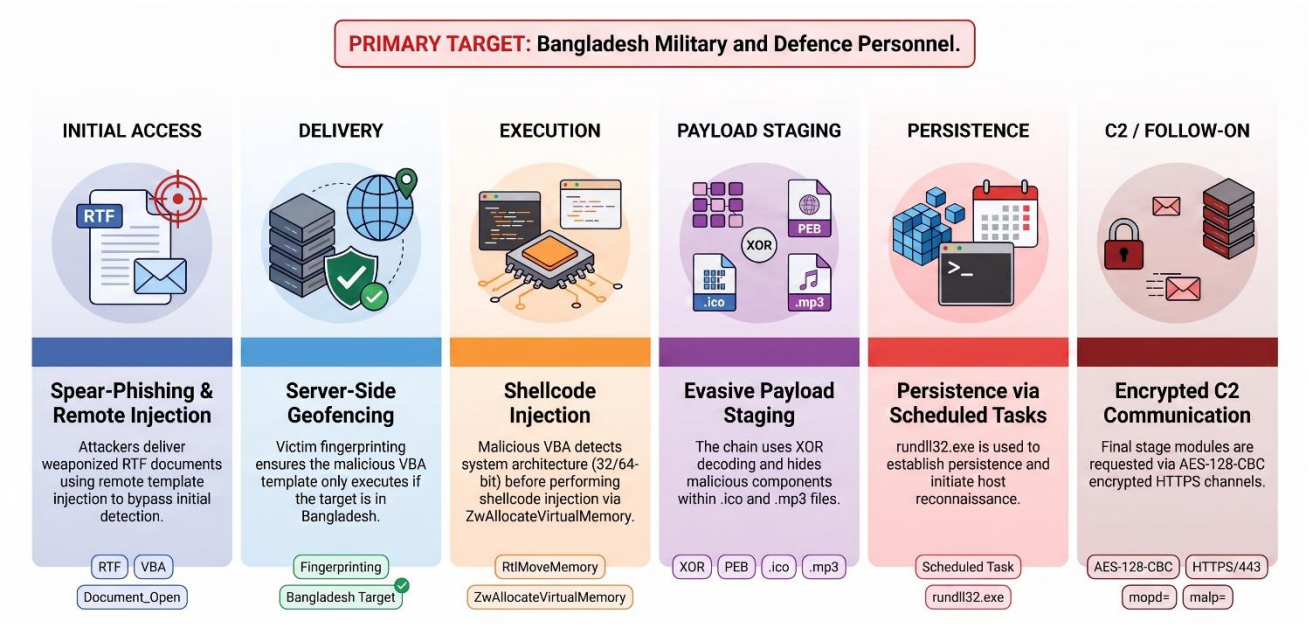

Figure: Complete DoNot (APT-C-35) Attack Chain Targeting Bangladesh Military Personnel

Initial Access – Targeted RTF Spear-Phishing

The observed initial-access artifact was:

`Biography Air Vice Marshal Sitwat Nayeem.doc`

Despite the `.doc` extension, the file is a weaponized RTF document. The lure presents a fake Microsoft Office Protected View-style message instructing the recipient to enable editing and active content. This social-engineering mechanism attempts to convince the target that normal Microsoft Office security controls are preventing legitimate content from being displayed.

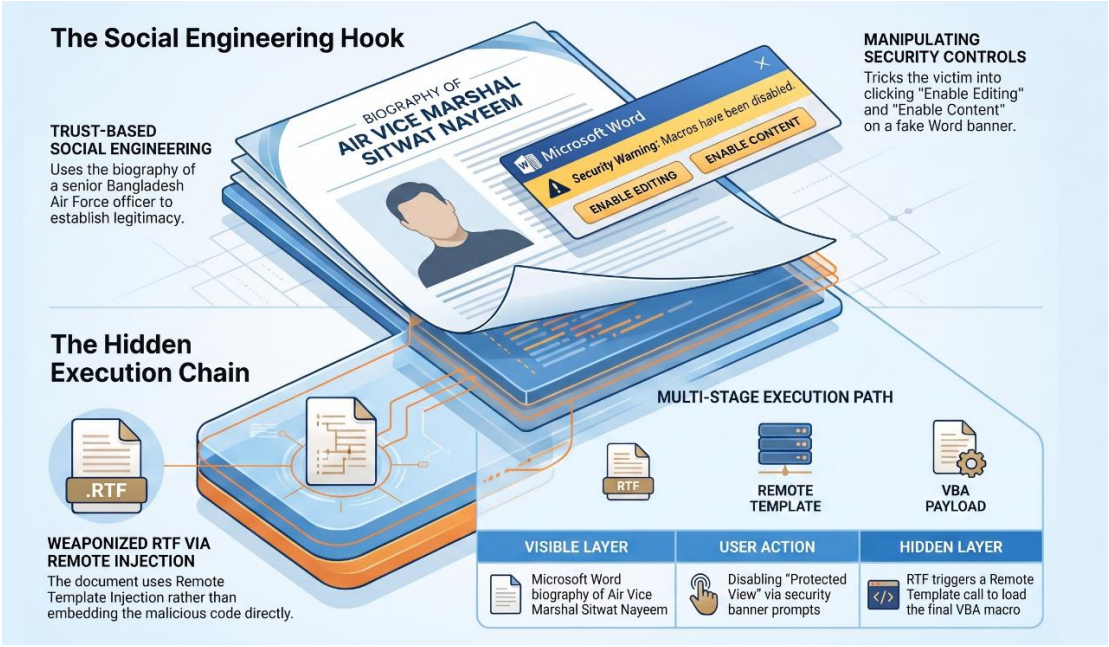

Figure: Weaponized Biography-Themed RTF Lure Used Against Bangladesh Military Personnel

The use of military-specific information is important from a threat-intelligence perspective because it suggests deliberate target selection rather than mass phishing.

Remote Template Injection

The RTF does not directly embed the main malicious VBA payload. Instead, it contains an external template reference. Analysis of the RTF template destination reveals an obfuscated remote URL using Unicode escape sequences.

The decoded infrastructure included:

`hxxp[://]greezupdto[.]info/5IrzalAfHEUM9Tg6/5zbnrP5Dj2BLtwQm[.]php`

Microsoft Word attempts to retrieve the external template when the document is opened.

Encoding the URL using Unicode escape sequences helps conceal the network indicator from basic static analysis and security controls searching documents for plaintext URLs.

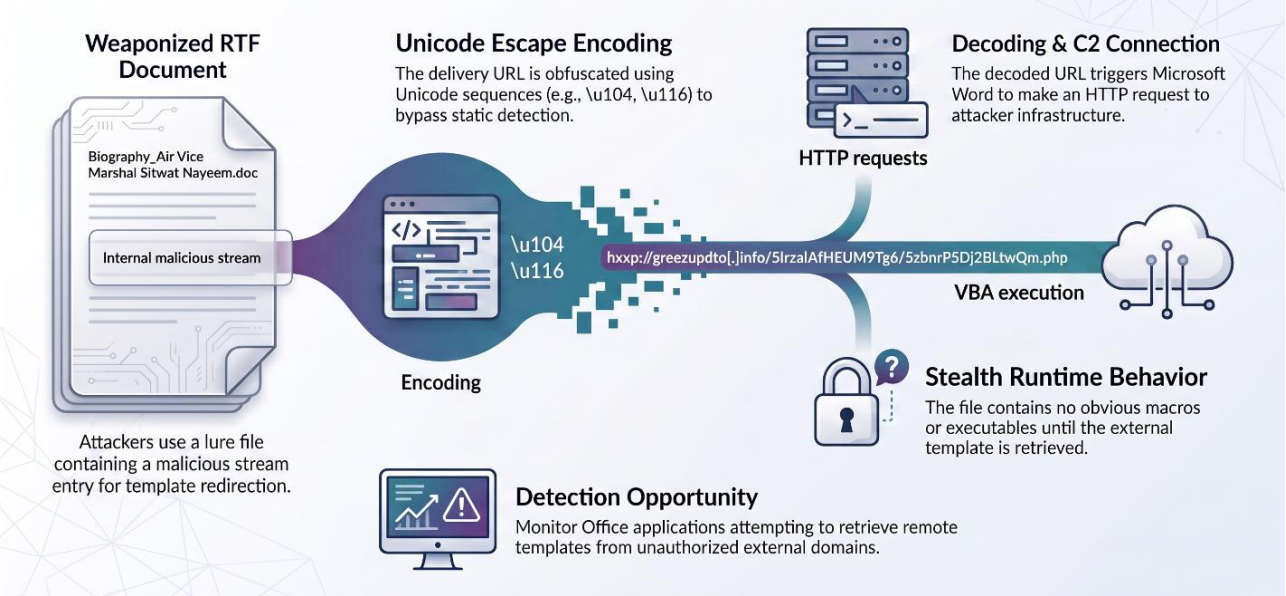

Figure: Remote Template Injection and Obfuscated External Template URL

Server-Side Geofencing and Victim Filtering

A particularly important feature of the campaign is selective payload delivery.

When researchers directly requested the malicious template URL, the server could return a clean Word template without executable content.

The infrastructure reportedly evaluates characteristics including:

- source IP/geolocation;
- request characteristics;
- Microsoft Word User-Agent behavior; and
- potentially whether the connection resembles automated analysis.

Consequently:

Intended victim: receives malicious template.

Researcher / sandbox / unsuitable request: receives benign template.

This provides an effective defense-evasion layer because automated URL scanners may incorrectly classify the infrastructure as benign.

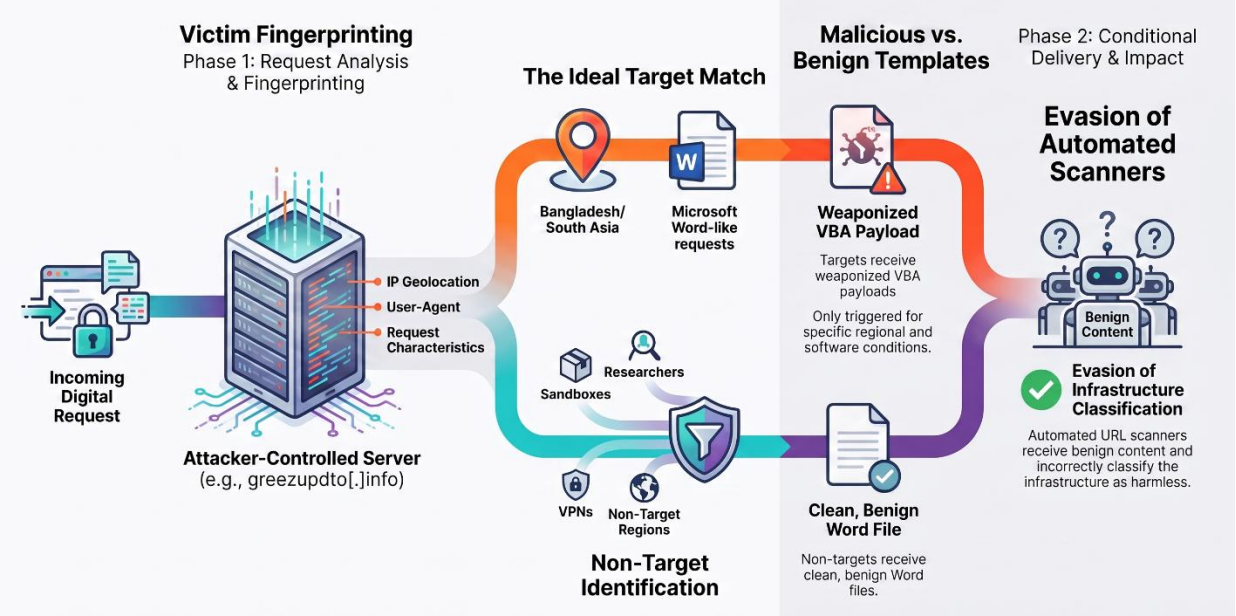

Figure: Server-Side Victim Filtering and Geofenced Payload Delivery

Malicious VBA Template

The malicious template contains three VBA procedures:

- `Document_Open`
- `xmsttxruylzhq`
- `xyz`

`Document_Open` provides automatic execution when the malicious document is opened. The principal malicious routine contains separate shellcode arrays for 32-bit and 64-bit Microsoft Office processes and selects the appropriate payload based on architecture. The macro uses Windows APIs including:

- `ZwAllocateVirtualMemory`: allocates memory suitable for shellcode
- `RtlMoveMemory`: transfers the decoded payload into the allocated region
- `Internal_EnumUILanguages`: is abused as a **callback-based execution primitive**, transferring execution to attacker-controlled shellcode without relying on a conventional VBA process-creation sequence.

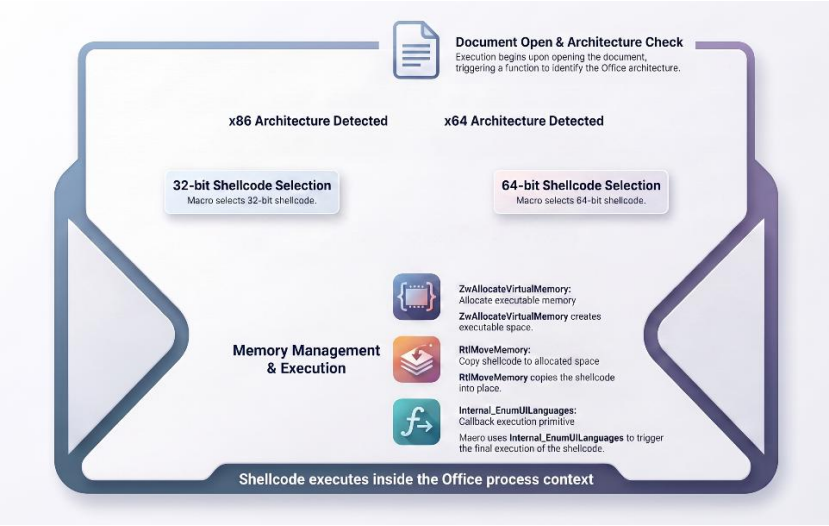

Figure: Architecture-Aware VBA Shellcode Injection and Callback-Based Execution

Shellcode Decoding

The initial shellcode is encoded rather than stored as immediately readable instructions.

The observed decoding routine performs:

Bitwise NOT; followed by **XOR 0x65.** This is effectively equivalent to **XOR with 0x9A.**

The decoding loop processes approximately **666 bytes** of encoded shellcode.

The shellcode also obtains its own execution address using an FPU-based **GetEIP** technique involving instructions such as `fldpi` and `fnstenv`. This provides position-independent execution while avoiding more obvious call/pop GetEIP sequences.

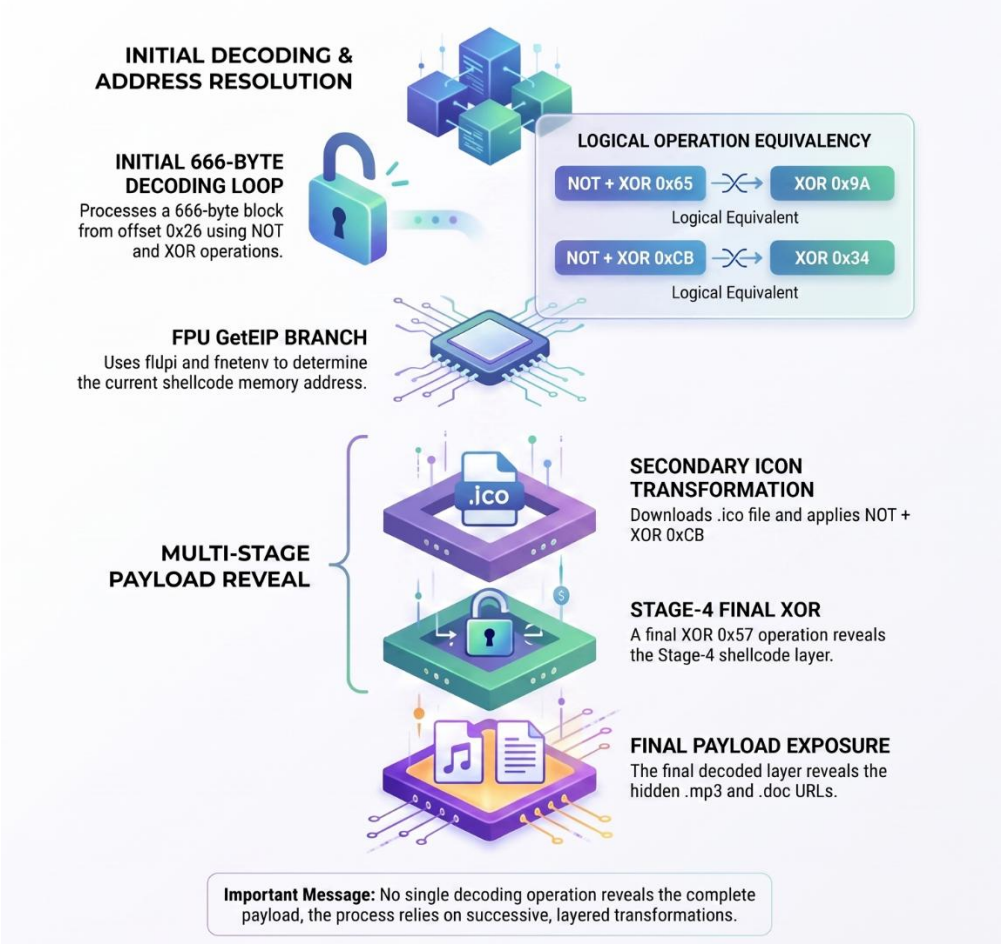

Figure: XOR-Based Shellcode Decoding and Position-Independent Execution

Shellcode Downloader

The decoded shellcode dynamically resolves required Windows APIs rather than storing readable API names. It walks the **Process Environment Block (PEB)** to identify loaded modules and parses module export tables.

Function resolution uses **ROR7-based API hashing**, allowing Windows APIs to be located without embedding their plaintext names. This significantly reduces useful strings available to static scanners.

Anti-Hooking and Analysis Evasion

Before invoking resolved functions, the shellcode checks initial function bytes for indicators commonly associated with inline hooks or debugging:

- `0xE8` – CALL
- `0xE9` – JMP
- `0xCC` – INT3
- `0xEB` – short JMP

Where suspected hooks are identified, execution logic attempts to adjust the target to avoid the modified instructions. This behavior is intended to reduce visibility to security software using user-mode API hooking and complicate debugging and malware analysis.

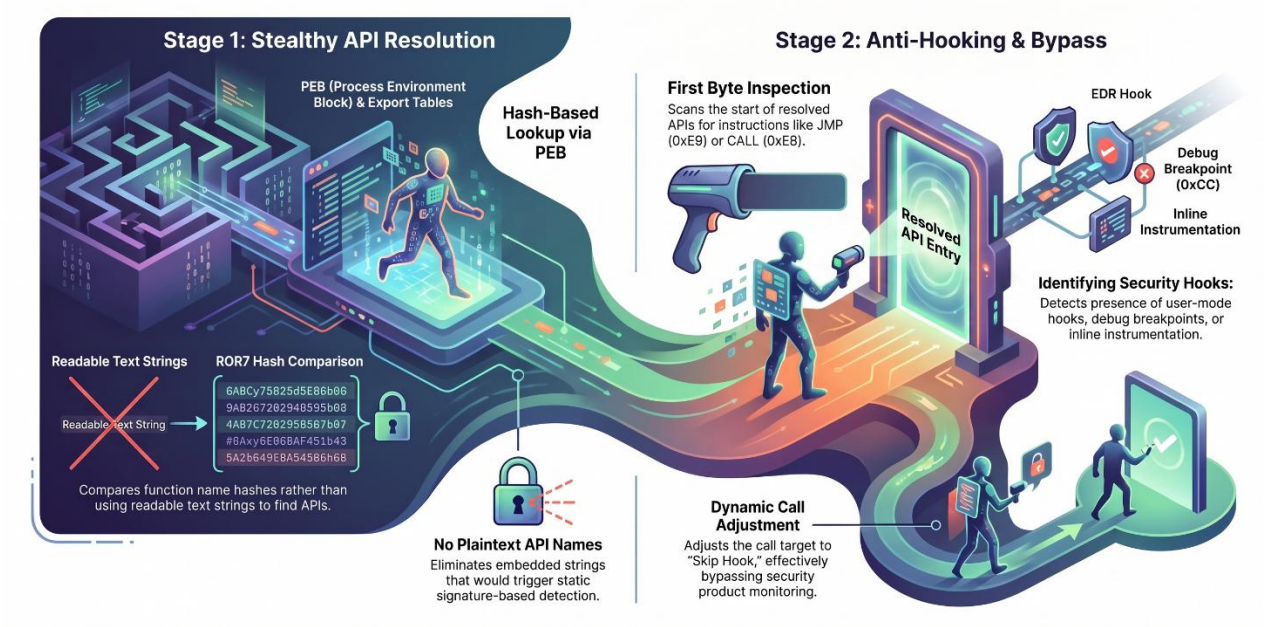

Figure: Runtime API Resolution and Anti-Hooking Mechanism

Multi-Layer Payload Retrieval

The shellcode retrieves subsequent payloads from the same attacker-controlled infrastructure while masquerading malicious content as ordinary files.

Observed extensions include: `.ico, .mp3, .doc`

One shellcode stage was delivered as an apparent icon file.

The retrieved data undergoes another decoding operation: **NOT + XOR 0xCB** which is functionally equivalent to: **XOR 0x34**

A subsequent stage applies another: **XOR 0x57**

The decoded shellcode then reveals additional download URLs. The `.mp3` path delivers the next malicious payload, whereas the `.doc` path is associated with decoy content.

This layered approach means that decoding one stage does not immediately expose the entire attack chain.

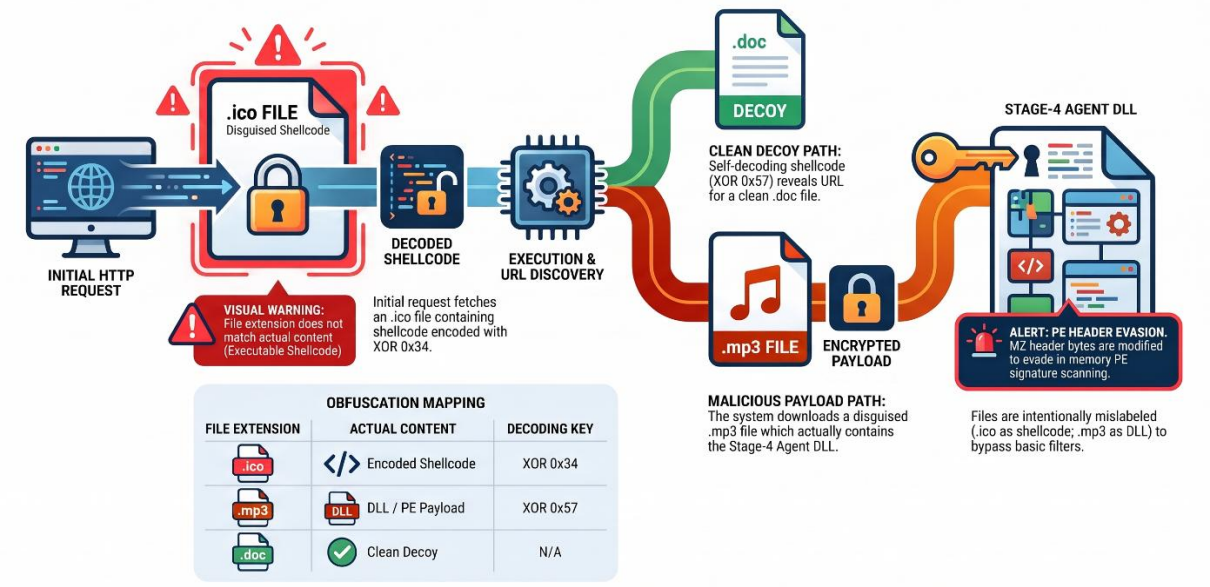

Figure: Multi-Layer Payload Staging Using .ico, .mp3, and .doc Masquerading

DLL Agent

The final stage of this portion of the infection chain is a DLL implant providing:

- persistence;
- system reconnaissance;
- encrypted C2;
- victim registration;
- conditional payload retrieval;
- modular follow-on capability; and
- artifact deletion.

The DLL exposes the entry point: `a4Strau` and is executed using: `rundll32.exe`

The observed Stage-4 sample has SHA-256:
`d2af373a6da05fb7a9d06b83ff82ecd12952c655551673f8bbd8dc6d21cecea8.`

Configuration Protection

Sensitive configuration strings inside the implant are encrypted using AES-128-CBC and decrypted at runtime. Recovered configuration identifies:

- `reggyupdated[.]info` as C2;
- `rundll32.exe` as an execution component;

- campaign identifier `MFG`;
- `mopd=` and `malp=` HTTP POST parameters;
- staging directories and module names;
- scheduled-task metadata; and
- `%PDF` as a response marker.

The use of runtime configuration decryption prevents many C2-related strings from being immediately visible during static inspection.

Persistence

The implant creates a Windows Scheduled Task through the Task Scheduler API.

The task observed by researchers was designed to resemble legitimate OneDrive telemetry:

```
OneDrive Reporting Task-S-1-5-21-...
```

The corresponding action executes a DLL through:

```
rundll32.exe %TEMP%\BinSat\dn110mploc.dll,a4Strau
```

The malware copies itself into: (before registering persistence)

```
%TEMP%\BinSat\
```

Using **OneDrive-related naming and an apparently legitimate SID-style suffix** increases the likelihood that the task will be overlooked during routine administrative review.

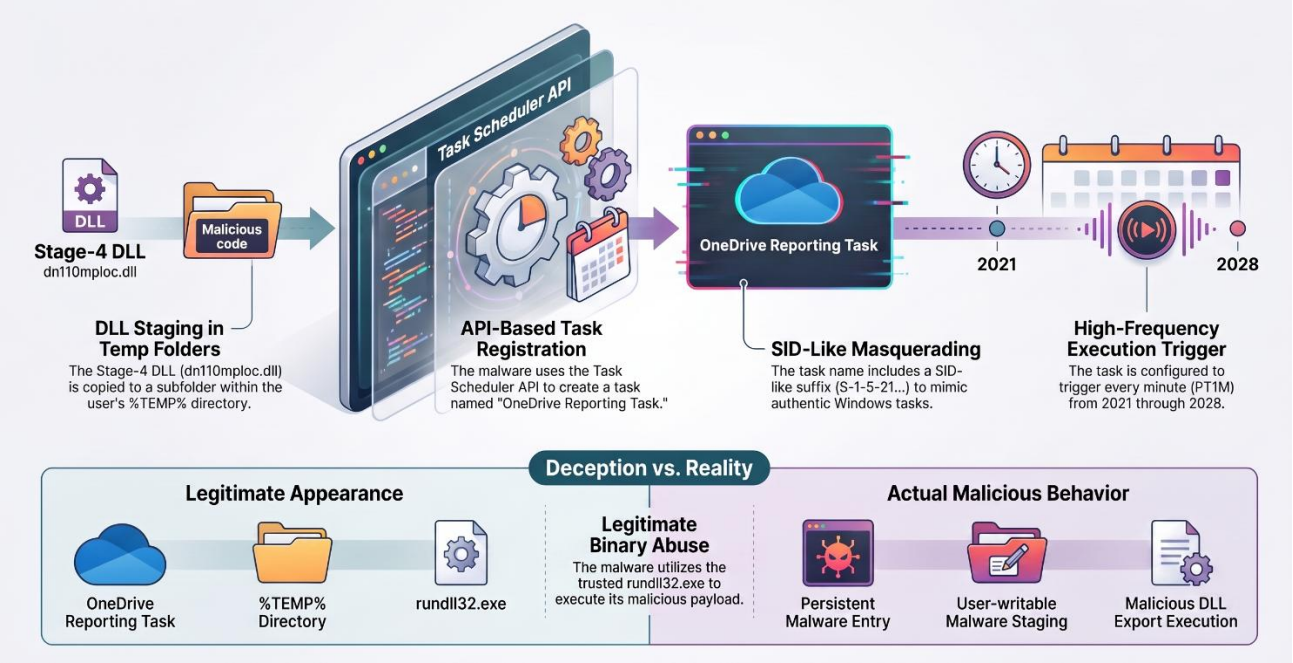

Figure: Scheduled-Task Persistence Masquerading as Microsoft OneDrive Telemetry

System Reconnaissance and Victim Profiling

Before requesting additional payloads, the malware generates a detailed profile of the infected endpoint.

Collected information includes:

- CPU information;
- operating-system version;
- username;
- computer/hostname;
- hardware identifier; and
- installed software.

The system profile is serialized, padded to an AES block boundary, encrypted using AES-CBC and then Base64 encoded.

The resulting information is transmitted using the HTTP POST parameter: `mopd=`

This architecture allows the operator to evaluate the strategic relevance and technical characteristics of a victim before committing additional tooling.

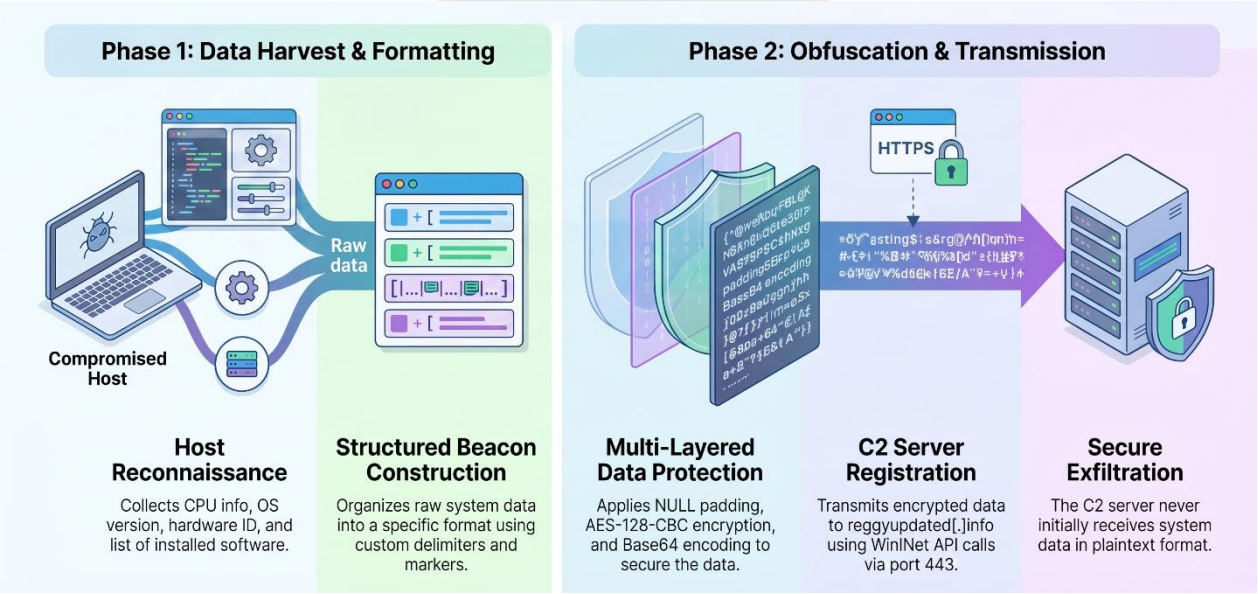

Figure: Victim Profiling and Encrypted System-Reconnaissance Beacon

Command-and-Control Protocol

The Stage-4 implant communicates using HTTPS over TCP port **443** through the Windows WinINet API.

Confirmed C2: `reggyupdated[.]info`

Observed registration path: `/ZxStpliGBsfdutMawer/sIOklbgrTYULKcsdGBZxsfetmw`

The protocol implements a two-stage victim-validation and payload-delivery process.

Phase 1 – Victim Registration

System information is encrypted and submitted using: `mopd=`

The server can return different responses.

A `finder` response causes the implant to remain in its polling loop.

A response containing: `MFG?<value>` indicates campaign matching and whether an additional payload is available.

Phase 2 – Payload Retrieval

When instructed to proceed, the implant sends another POST request using: `malp=` to a separate payload-delivery URI.

The request contains the encrypted victim profile together with the requested module information.

The server may return content prefixed with: `%PDF`

The implant removes the wrapper before writing the actual payload, providing another layer of content masquerading intended to complicate network inspection.

Follow-On Module

Researchers successfully queried the active delivery endpoint and obtained a second-stage DoNot module identified internally as: `ejtest.dll`

SHA-256:

`1cf7b7bb094821cc6518c21958a8e4b597c232c1d9b87082c5e0861aececb7de`

The retrieved module maintains similar operational characteristics, including:

- WinINet HTTPS communications;
- AES-128-CBC encrypted beaconing;
- Base64 encoding;
- modular payload retrieval; and
- campaign-specific C2 URI structures.

The follow-on module communicates with: `exessupdate[.]info`

The fact that a valid payload could be retrieved from the infrastructure provides strong evidence that the campaign infrastructure was operational and configured to distribute additional modules.

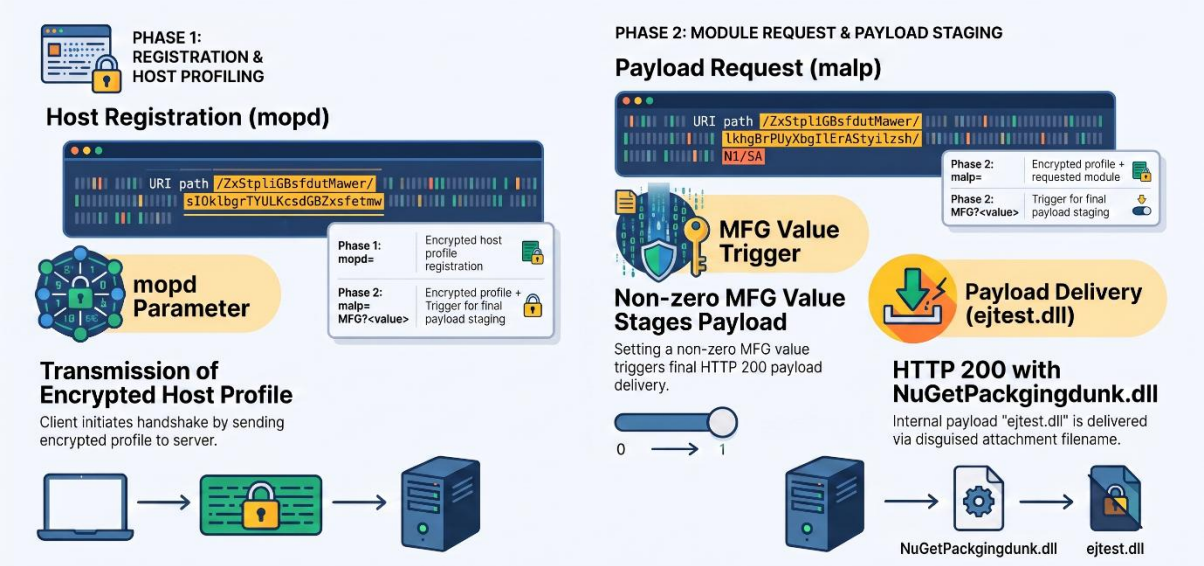

Figure: Two-Phase DoNot C2 Handshake and Conditional Payload Delivery

Self-Deletion and Artifact Removal

After persistence and registration, the malware attempts to delete its original file. The observed technique uses `cmd.exe`, a delayed `ping` operation and subsequent forced deletion.
This represents deliberate cleanup designed to reduce readily available forensic artifacts after successful installation.

Defenders should therefore not assume the absence of the original DLL means an endpoint was not compromised

Infrastructure Analysis

Three domains are directly associated with major stages of the campaign:

Domain	IP Address	Role
greezupdto[.]info	193[.]149[.]190[.]30	Template injection / shellcode staging
reggyupdated[.]info	45[.]61[.]136[.]27	Stage-4 DLL C2
exessupdate[.]info	139[.]180[.]186[.]155	Follow-on module C2

Infrastructure clustering identified numerous additional domains exhibiting similar naming and hosting characteristics, including deliberate misspellings and recurring themes involving “update”, “program”, “solution”, and `.info` domains.

Organizations should therefore not limit blocking and hunting exclusively to the three confirmed domains.

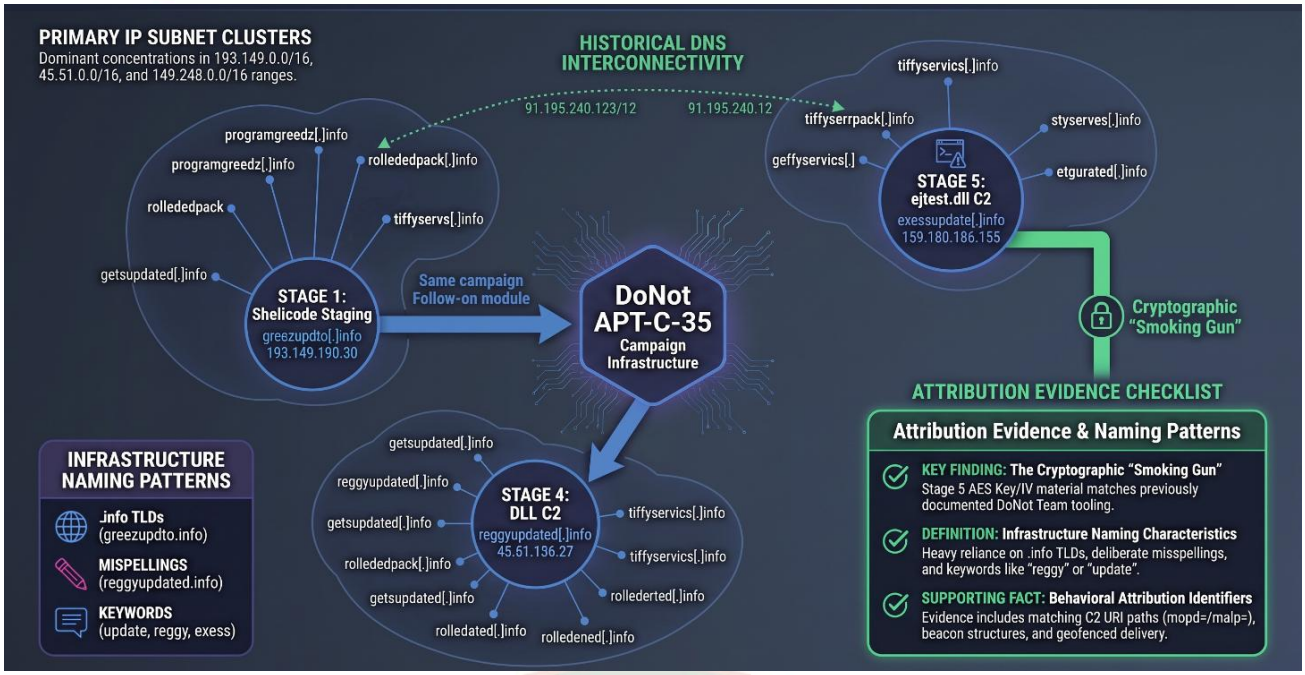

Figure: C2/domain relationship

Attribution Assessment

The source assesses the campaign with **high confidence** as DoNot Team/APT-C-35.

Technical evidence supporting this assessment includes:

1. C2 URI paths matching previously analyzed DoNot tooling.
2. `mopd=` and `malp=` protocol parameters.
3. Consistent system-reconnaissance beacon structures.
4. Remote-template injection matching documented DoNot tradecraft.
5. Callback-based VBA shellcode execution.
6. Multi-stage `.ico`/`.mp3` payload masquerading.
7. Infrastructure patterns consistent with prior operations.
8. Cryptographic overlap between the retrieved `ejtest.dll` and independently analyzed `DoNot` malware.

Most significantly, AES key and IV material recovered from the retrieved Stage-5 module reportedly matches independently documented `DoNot` malware **byte-for-byte**, providing strong cryptographic linkage.

MITRE ATT&CK Mapping

Tactic	Technique	ID	Observed Activity
Initial Access	Spearphishing Attachment	T1566.001	Weaponized biography-themed RTF
Execution	User Execution: Malicious File	T1204.002	Victim opens malicious document
Defense Evasion	Template Injection	T1221	Remote VBA template retrieval
Defense Evasion	Obfuscated Files or Information	T1027	Unicode URLs, XOR, encrypted strings
Defense Evasion	Deobfuscate/Decode Files	T1140	Runtime XOR/AES decoding
Defense Evasion	Process Injection	T1055	Shellcode execution within Office context
Defense Evasion	Masquerading	T1036.005	.ico, .mp3, OneDrive naming
Defense Evasion	File Deletion	T1070.004	Self-deletion after installation
Persistence	Scheduled Task	T1053.005	OneDrive-themed scheduled task
Discovery	System Information Discovery	T1082	CPU/OS/hostname collection
Discovery	Software Discovery	T1518	Installed software enumeration
C2	Web Protocols	T1071.001	HTTPS communications
C2	Ingress Tool Transfer	T1105	Additional DLL retrieval
C2	Encrypted Channel	T1573.001	AES-encrypted C2 data
Collection	Data from Local System	T1005	Host/system information collection

Indicators of Compromise (IoC)

File Hashes

Artifact	SHA-256
Biography lure	feab754463aeb5e97f429b4db8c882c3 db5a114434527fe3397ff95101d86521
Stage-4 Agent DLL	d2af373a6da05fb7a9d06b83ff82ecd1 2952c655551673f8bbd8dc6d21cecea8
Stage-5 ejtest.dll	1cf7b7bb094821cc6518c21958a8e4b5 97c232c1d9b87082c5e0861aececb7de
ICO-masqueraded shellcode	ad844edf7104d73d9dd45569ba8cebbf 0a248546c1be4f53b8387a1371ab8eda

Confirmed Network Infrastructure

Domain	IP
greezupdto[.]info	193[.]149[.]190[.]30
reggyupdated[.]info	45[.]61[.]136[.]27
exessupdate[.]info	139[.]180[.]186[.]155

Host Indicators

Indicator	Description
%TEMP%\BinSat\	Stage-4 staging/persistence directory
dn110mploc.dll	Persisted DLL filename
a4Strau	DLL exported execution function
OneDrive Reporting Task-S-1-5-21-*	Suspicious scheduled-task pattern
rundll32.exe ...dn110mploc.dll,a4Strau	Malware execution pattern
%TEMP%\Inititate\	Follow-on staging directory
TermdyunkSyubtyqdz.dll	Follow-on local filename
NuGetPackgingdunk.dll	Requested module name
mopd=	C2 registration parameter
malp=	Payload retrieval parameter
MFG	Campaign identifier

Related Infrastructure

programgreedz[.]info
getsupdated[.]info
reggysolution[.]info
golledsack[.]info

```
scriptlydev[.]com
hillisolutions[.]info
tiffyservics[.]info
makerolleds[.]info
shadoworkz[.]info
cosmicupto[.]info
solutionpelle[.]info
solutionlogz[.]info
altzserberin[.]info
hafybreaks[.]info
rollededpack[.]info
programseeget[.]info
```

These related domains were identified through infrastructure clustering and should therefore be treated as **hunting indicators rather than necessarily confirmed malicious activity on every occasion.**

Detection and Monitoring

Organizations should prioritize detection across email, Microsoft Office, endpoint, DNS, proxy and network telemetry.

Email / Office

Monitor for:

- unsolicited RTF/DOC files using military or government themes;
- Microsoft Word retrieving remote templates;
- Office applications establishing unexpected outbound Internet connections;
- documents requesting users to enable editing or active content.

Endpoint

Monitor for:

- suspicious memory allocation originating from Office;
- abnormal callback-based execution;
- `rundll32.exe` executing DLLs from `%TEMP%`;
- creation of `%TEMP%\BinSat\`;
- OneDrive-themed scheduled tasks not deployed through approved software;
- Office processes followed by DLL creation or unusual network activity.

Network

Monitor for:

- connections to identified C2 infrastructure;
- HTTPS POST traffic containing `mopd=` or `malp=`;
- downloads with `.ico` or `.mp3` extensions followed by memory execution or DLL creation;

- suspicious `.info` domains;
- recently registered or low-reputation domains with deliberate misspellings.

Threat Hunting

SOC teams should correlate: (Office document opened)

- external template request
- Office memory-execution behavior
- `.ico/.mp3` download
- `rundll32.exe`
- scheduled task creation
- HTTPS beaconing.

This sequence should be treated as a high-confidence compromise pattern.

Recommended Actions

BGD e-GOV CIRT strongly recommends that military, government, CII and organizations supporting Bangladesh's defence ecosystem immediately:

- Block the confirmed domains, IP addresses and file hashes at firewall, DNS, proxy, secure email gateway, EDR/XDR and SIEM layers.
- Search historical telemetry for the IOCs rather than limiting analysis to current connections.
- Hunt for the biography-themed RTF document and related spear-phishing attachments across email gateways, endpoints and file repositories.
- Block external remote-template retrieval from Microsoft Office wherever operational requirements permit.
- Disable or tightly control Office macros originating from Internet-sourced documents.
- Investigate Microsoft Word or other Office processes making unexplained Internet connections.
- Hunt for `rundll32.exe` loading DLLs from temporary or user-writable directories.
- Search endpoints for suspicious OneDrive-themed scheduled tasks.
- Monitor HTTPS POST requests containing `mopd=` or `malp=`.
- Treat systems communicating with confirmed campaign infrastructure as potentially compromised, isolate them and conduct full forensic investigation.
- Reset credentials used on confirmed compromised endpoints and investigate potential credential exposure.
- Ensure EDR, SIEM, DNS, proxy and email telemetry are retained for sufficient periods to support historical threat hunting.

Incident Response Guidance

If any IOC or associated behavior is identified: **Isolate the endpoint immediately.**

Preserve volatile evidence before remediation where forensic capability exists.

Collect:

- memory image;
- RTF/DOC attachment;
- Office process telemetry;
- scheduled-task configuration;
- `%TEMP%` contents;
- DNS logs;
- firewall/proxy logs;
- EDR process trees;
- email headers;
- browser/network artifacts;
- Windows Event Logs.

Determine whether the endpoint communicated with: `greezupdto[.]info`, `reggyupdated[.]info` or `exessupdate[.]info`.

Presence of Stage-4 persistence or C2 communication should be treated as evidence that execution progressed beyond initial document delivery.

Presence of `mopd=` traffic indicates host registration behavior, while subsequent `malp=` communication may indicate progression toward additional module retrieval.

Where follow-on payload execution is confirmed, organizations should broaden the investigation beyond the initially affected workstation because the final objectives and capabilities of every module delivered by the actor may not yet be known.

The observed DoNot (APT-C-35) campaign represents a **targeted cyber-espionage threat against Bangladesh's military and defence ecosystem** rather than an opportunistic malware campaign. The combination of military-specific social engineering, remote-template injection, geofenced payload delivery, architecture-aware shellcode, layered obfuscation, anti-analysis functionality, OneDrive-masqueraded persistence and AES-encrypted modular C2 demonstrates a deliberate effort to evade conventional security controls while maintaining long-term access to selected high-value targets.

Organizations within Bangladesh's government, military, defence, diplomatic and critical infrastructure sectors should immediately hunt for the identified indicators and behaviors, investigate suspicious Microsoft Office remote-template activity, and treat any confirmed communication with the campaign's C2 infrastructure as a potential security incident requiring comprehensive investigation.

References

- https://www.cyderes.com/howler-cell/tracking-donot-apt-c-35-bangladesh-military-intrusion
- https://ti.qianxin.com/blog/articles/analysis-of-the-attack-activity-of-the-apt-q-38-using-pdf-document-decoys-cn/