关于新型僵尸网络 FlyLegit 大范围传播的风险提示

本报告由国家互联网应急中心（CNCERT）与绿盟科技集团股份有限公司共同发布。

一、概述

近期，CNCERT 与绿盟科技集团股份有限公司联合监测发现，新型僵尸网络家族 FlyLegit 持续针对 Linux 服务器及 IoT 设备开展传播，远程控制相关设备发起 DDoS 攻击。该家族自 2025 年末进入监测视野后持续更迭版本，已对相关设备构成较大安全威胁。

FlyLegit 名称源自攻击者建立的 Telegram 群组 t.me/flylegit。攻击者通过 Telegram 群组进行宣传推广，吸引潜在客户或使用者。与主要用于 DDoS 攻击的传统僵尸网络相比，FlyLegit 除支持多种 DDoS 攻击外，还具备程序自更新、正向 Shell 和反向 Shell 等功能，可将受感染设备作为后续攻击的立足点，并根据需要投递其他恶意组件。

截至目前，已累计捕获 68 个下马地址、900 个用于下载不同架构木马的 URL 链接，覆盖 X86、x64、arm、mips、mipsel、sh4、ppc 等 7 种架构，对应 40 个 C2 节点，攻击者月均更换约 5 个 C2 节点。2026 年 9 月 3 日至 8 日期间，该僵尸网络在我国境内已确认的活跃“肉鸡”规模约 2015 台，境内日上线肉鸡数量最高达 427 台。

二、僵尸网络分析

（一）传播方式与基础设施

1.传播与投递

FlyLegit 僵尸网络主要通过 Telnet 弱口令扫描及漏洞利用（如 Realtek CVE-2018-10561 等）两类手段进行传播。落地木马文件统一以 iran 加架构标识命名，如 iran.x86_64；下载脚本多命名为 cat.sh。

下载脚本内置 x86_64、mips、arm 等多架构适配逻辑，通过 wget 或 curl 自动下载对应架构的木马至受害主机。木马执行时需附加运行参数，曾使用的参数包括 telnet、catloader、""、$@、"$@"及 Default（无参运行），这些参数后期被用于构建上线包。

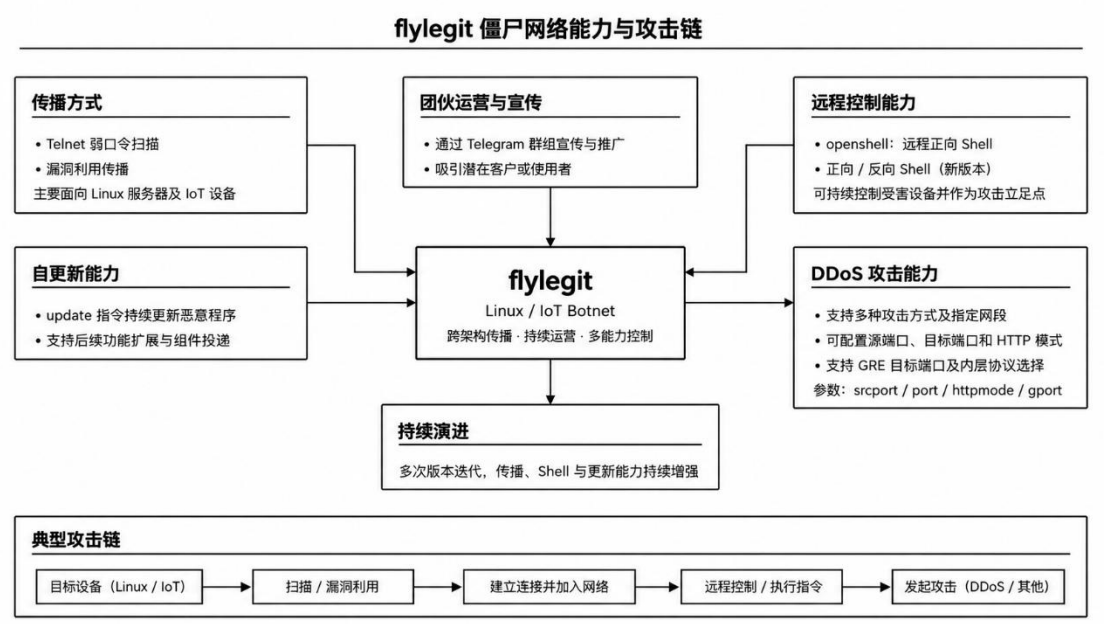


图 1 FlyLegit 僵尸网络能力与攻击链

2.传播节点

自 2025 年 12 月底以来，累计捕获 68 个下马地址、900 个用于下载不同架构木马的 URL 链接。攻击者约每隔一周

更换一次下马地址，传播文件多采用 iran 加架构标识的统一命名方式。现有监测数据反映，攻击者仍在持续维护和扩充该僵尸网络。



图 2 FlyLegit 每月新增下马地址

3.C2 分布

2025 年 12 月底至今，累计捕获 FlyLegit 僵尸网络 40 个 C2 节点。这些节点分布于德国、荷兰、法国等近 10 个国家，其中德国和荷兰占比分别为 43%和 28%。攻击者 C2 更换较为频繁，月均更换约 5 个节点；更换后倾向于复用原有端口，7080、8060、7777 等端口被多次使用。运营基础设施大量选用欧洲中小型主机服务商。

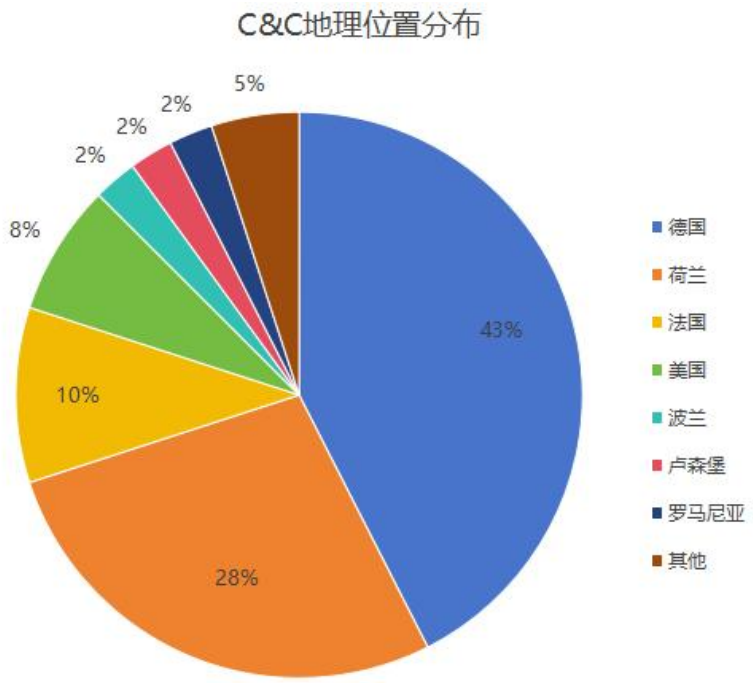


图 3 FlyLegit C2 地理位置分布

（二）样本技战术特点

1.版本更迭

不同时期，FlyLegit 所能处理的控制指令有所不同。初始版本支持 6 种 DDoS 攻击方式；2026 年 1 月至 6 月期间，部分版本缩减了控制指令和攻击方式；2026 年 7 月起，样本重新增加多种 DDoS 攻击指令，并加入 Telnet 扫描和 Realtek 相关漏洞扫描功能。除 ping 指令外，控制指令演变情况如下：

时期	版本	常规控制指令	DDoS 指令	扫描指令
2025.12-2026.01	V1	kill,stop, update	tcp flood, syn flood, http flood,udp flood, udpplain flood,icmp flood	无
2026.01-2026.04	V2	kill, stop	syn flood,udpplain flood	无
2026.05-2026.06	V3	kill, stop	syn flood, udpplain flood	无

时期	版本	常规控制指令	DDoS 指令	扫描指令
2026.07-2026.08	V4	kill,stop, update	tcp flood, syn flood, http flood,udp flood, udpplain flood,icmp flood, gre flood	selfrep telnet,selfrep realtek

2.驻留与对抗

FlyLegit 通过/etc/init.d、/etc/rc.local 等方式实现持久化，确保系统重启后自动恢复；同时清除竞争对手进程，以独占受控主机资源。早期部分版本采用 ChaCha20 算法对 C2 通信内容进行加密，最新版本已改为明文通信。

3.通信机制与命令控制体系

FlyLegit 命令控制体系主要包含上线认证、心跳应答和指令下发三个环节。上线包格式为<架构名称> <group 名称>，其中 group 字段用于区分不同活动批次，默认值为 default；如果启动脚本传入参数，木马会将该参数写入 group 字段。

该家族通过 ping-pong 命令实现心跳响应：攻击者下发 ping 指令，木马回复 pong 并携带主机架构信息。C2 指令采用字符串形式和 key=value 格式，支持配置攻击报文大小、源 IP 地址及端口等参数。部分版本的 C2 指令通过 ChaCha20 加密传输，木马内置初始密钥，下发数据开头包含解密所需的 nonce 参数。

4.核心攻击能力

FlyLegit 的核心攻击能力包括程序自更新、DDoS 攻击及 Shell 命令执行。!update 指令用于木马自更新：木马连接内置的硬编码 IP 和端口，发送 HTTP GET 请求下载新版木马，

优先保存至/tmp/目录；若该目录不可写，则依次尝试/var/、/dev/shm/及当前目录，下载完成后设置执行权限。

攻击者可通过指令控制木马在指定时间段内向目标发送攻击载荷，已发现的 DDoS 攻击指令如下：

指令	攻击手段	说明
tcp	TCP Flood	向目标发起多个三次握手连接。 载荷为随机数据。
syn	SYN Flood	采用原始套接字自构建 SYN 包。 支持针对目标网段进行攻击。 载荷为指定数据、随机数据或指定+随机数据填充。
udpplain	UDP Flood	支持针对目标网段进行攻击。载荷为指定数据、随机数据或指定+随机数据填充。
udp	UDP Flood	随机载荷，其余同 udpplain。
http	HTTP Flood	向目标发起多个三次握手连接。支持 GET、POST、HEAD。除 HTTP 头部外，仅 POST 模式携带少量数据部分，GET、HEAD 均不携带额外数据。
icmp	ICMP Flood	类型为 ICMP_ECHO。支持针对目标网段进行攻击。载荷为随机数据。
gre	GRE Flood	独立配置结构，支持 gre_proto/gport。 支持 TCP 或 UDP。支持针对目标网段进行攻击。

该家族还支持正向 Shell 和反向 Shell，可获取被控主机远程 Shell 访问权限并执行命令：

指令	说明
!openshell	正向 Shell，在被控主机监听指定端口，以口令作为准入凭据，攻击者可远程执行 Shell 命令
!shellcmd	反向 Shell，执行攻击者下发的 Shell 命令

三、僵尸网络感染规模

通过监测分析发现，2026 年 9 月 3 日至 8 日期间，FlyLegit 僵尸网络在我国境内已确认的活跃“肉鸡”规模约 2015 台，境内日上线肉鸡数量最高为 427 台。

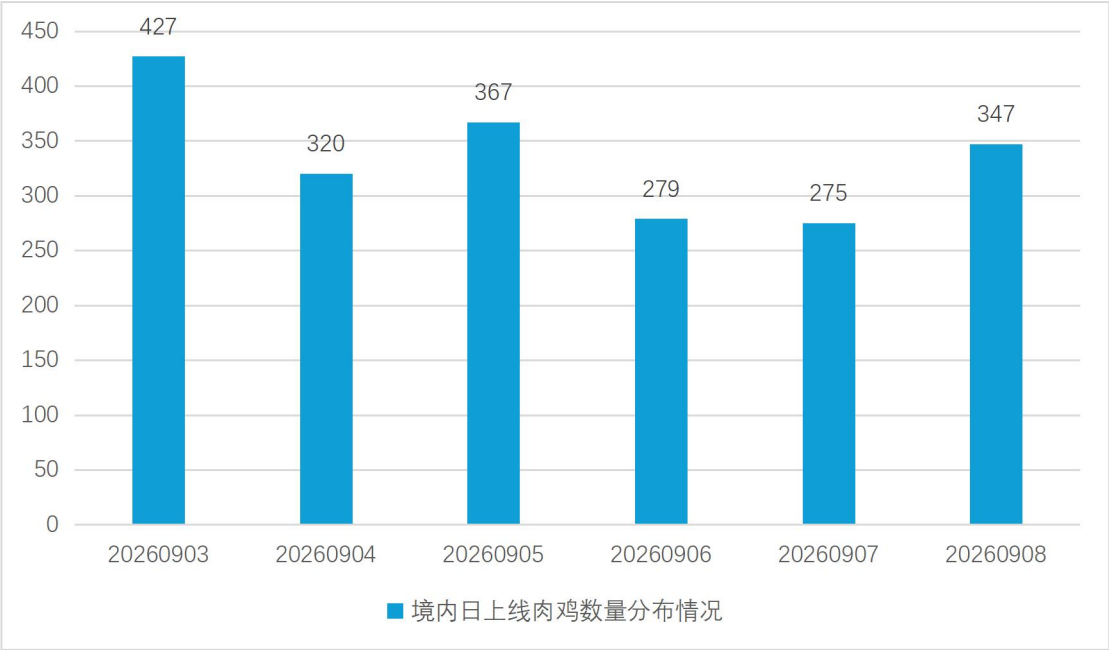


图 4 境内日上线肉鸡数量分布情况

四、防范建议

请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：

（1）关闭不必要的 Telnet、SSH 及设备远程管理接口，禁止将管理端口直接暴露在公网；

（2）修改设备默认口令，使用强口令，并避免多台设备共用同一密码；

（3）排查并修复报告涉及的漏洞，及时升级设备固件和 Linux 系统组件；

（4）在网络侧监测异常扫描、下马请求、C2 连接和异常 DDoS 流量；

（5）发现感染后立即隔离设备，保留必要日志和样本，核查入侵入口，完成漏洞修复和凭据更换后再恢复业务；

（6）对无法安装终端防护软件的 IoT 设备，通过访问控制、网络分区和出口限制降低风险。

五、相关 IOC

（一）C2

C2	C2	C2	C2
165.22.247.105:2220	176.65.139.35:7080	85.11.167.182:5855	83.168.110.191:1336
38.60.216.39:13322	94.249.228.212:6767	176.65.139.67:17692	192.109.200.199:23
174.138.43.79:6060	45.156.87.176:7080	134.199.219.57:6060	140.233.190.82:6221
176.65.139.18:7000	130.12.180.85:7080	34.107.120.7:1150	45.153.34.77:6000
64.89.161.81:6667	31.56.120.29:7080	130.12.180.80:7080	87.121.84.11:7080
45.153.34.195:7080	36.255.97.23:7777	167.86.99.169:8060	31.77.227.119:8060
165.22.69.214:3131	94.154.43.88:8060	195.201.123.9:8060	103.83.87.122:8060
176.65.139.51:7080	94.26.106.236:777	176.65.139.121:7080	82.25.63.213:7080
31.56.209.72:621	176.65.139.196:621	176.65.139.161:25596	176.65.139.7:1337
176.65.139.45:6060	176.65.139.36:5555	82.26.74.181:7080	176.65.139.61:5090

（二）Hash

Hash	Hash
4de9763c9bdd12fb25f907bcef4144af	d02158d0fc4233f9654225a3bfc2ea95
0370683c629a40cc495915161cf3f975	b0b959b1d9c06322391d3b39843a9a07
89d3f3ce6f654953e2cee1101db8de0d	9f16e5596a7d2fa48d7be03a71fdb21b
76ad977cdbf28f1cf82bba1bdf67303c	1dff9725fb3889423d8249e1dadade57
931224bbb764aab452b2a1ae545b3a23	018caecd80077ec3d2a9453270a6a784
4cad9ad790f6d573986497c20ed5dfca	7bb1e14c29188186670478c2bd99fb9b
d284088eff26ebf3b192c01abd269fe0	c34b4e4a8958653bdd3b01870b97f87b
e362076dd212b2e211638bad035bd997	c0a9a8933607d59f5d5daee74403df05
17303c070fd6660cc0c5ff77aa9ec165	fe45e8d7f7afeae48e9edd2fbdae52c5
870497c8ff0c4ef447dc3989d767834c	67ab69aa3ff21a5deb7bbc5b266306d4
c831f502474dc988bc9b21eee10a3178	2c135e3d6ec2cbf9535b071f09b2576c
1a3461022e05789e226537e18fe3109b	1904a7168d08625d3321d0d0eef80e5a
44b9c9b80a57e83c336e6a5218fabcf2	a9cae0f2350f48350ace1528f3a5be84
70ace99ef8f3b9350063af10303bfd92	dca40f08cc93bc2fba8e3f5fec18593f
f2d5837da4ebe93a67ec5b0a8a8507c7	71075cdbcc330b42f0ae68be6ff44ea3

Hash	Hash
7a9248f3420d8b3d6b94ba346aea6254	0e54628ea332bec9a12705b76a729a0c
62a0e401fcc42c435e66fae9f71d6c10	5d5aeddab8cddb7536ce44dbfd23daef
2b1931ca78a0c1832deb0d154fbd17a1	fc453bc95d34da863f4c3d1cbec45df7
3ce8a714552d621ba5bb10edcb838078	cdeacf6fae101680001237b643b12063
a2913a2ccbe45c273287dd285c0e54e1	15c99f12454b0678ffd6bcdef1a1bb77
1d7f5fe93a49193020ab25f13ae6c170	a83ee62337e4218437d35daa84961324
0f729e7a9bd73eed5759f1a18358650c	e36870a89afdc8acb6730da78d831737
b8f998dbf01a5237de323d6cb6b8ea84	1ebf44143d7c2e71bb294fdcd862a1f4
4ba79ef0833c5b390f5a7b29f3bee399	cdffbebdcab69edbe8b42fd15544a1fb
b8ae867c8b82e47272e15b23e72df2ce	a17d6def8c4db71feb8492db1cb90f6b
f226e5066a68f1ff726206c5eafb611f	b228d31b6630a892200b4be0a4396c0f
644b654a6bb931d8be34de2d491ecf89	39cbaaf449babd4f6ea1e7525d29deea
bb474861b2e5c7a6eb1013b60b416740	45a160258e51e30c74ec313f452dbe89
a108a29b2fdc2918d7e8285c33860394	95353f04087412d8adf9c9c4f01a1fc3
6a27151a55536335f48a54789c3515ac	e6ac4beb231201daffbdcd76d8889ebc
3473a76c22c93ab8289360c5770059cf	903d78539ceb95324d6f0f5cdb9c71dc
ed06f2ac6907f89a09f8bc5d6988700c	0a553af07ee56bf11694dcb6246e504d
7f0e5f422dec2a152787e38f22851cd2	