关于 Dysphoria 僵尸网络大范围传播的风险提示

本报告由国家互联网应急中心（CNCERT）与奇安信网神信息技术(北京)股份有限公司共同发布。

一、概述

近期，CNCERT 监测到一个新型僵尸网络正在互联网上大范围传播，该僵尸网络自 2026 年 3 月下旬起开始活跃。该家族被命名为 Dysphoria，它在短短几个月内经历了频繁的变种更新与技术迭代，展现出极强的生命力。其演进路径不仅横跨了 jackskid、fbot 变种，更在近期引入了基于区块链 ENS/SNS 域名的 C2 隐蔽解析机制，甚至开始将受害者主机转化为 C2 中继/代理节点。现将其主要情况分析披露如下。

二、僵尸网络分析

（一）Dysphoria 家族演进过程

Dysphoria 家族的迭代速度极快，其关键节点如下：

3 月 25 日（初见端倪）：捕获到 jackskid 变种，该变种通过 ENS 域名 m3rnbvs5d.eth 关联到 tg 频道信息，输出特异性字符串 android has no compatible libc library。

4 月 1 日（变种更替）：捕获 fbot 变种，成功运行后输出 hail china mainland\x00。

4 月 29 日至 4 月 30 日（算法升级）：该家族引入全新的 RC4 字符串加密算法与 C2 获取机制，开始大量复用 jackskid 的设计思维，并启用 ENS 域名 ukranianhorseriding.eth。

5 月初（引入多链）：该家族首次引入 Solana 系统的 SNS 域名 24carnforth2merseyside.sol，利用 TXT 记录下发资产。

6 月 10 日（域名更新）：该家族启用全新 ENS 域名 burrberry.eth。

6 月 25 日（功能分化）：捕获独立的功能变种，该样本不再具备 DDoS 攻击功能，而是纯粹作为中继/代理节点运作，开启了该家族的“中继化”进程。

6 月 27 日至 28 日（完全体形成）：该家族引入 UPnP 自动化端口映射增强内网穿透能力；同时构建了“DDoS 样本 + 动态 C2 中继节点列表”的混合型 C2 链路。

（二）核心样本技术分析

1.定制版 RC4 解密

Dysphoria 最新的 fbot 变种在字符串保护上应用了定制版 RC4 解密算法，该算法在一定程度上借鉴了 jackskid 的代码，分为三个阶段：

KSA 1 阶段：标准 RC4 初始化。

KSA 2 阶段：引入 LCG (线性同余发生器)算法，连续打乱 S 盒 5 次。

PRGA 阶段：在流生成过程中引入 LFSR (线性反馈移位寄存器)步进，并进行复杂的位移互换。

2.区块链域名 C2 隐蔽解析机制

Dysphoria 同时支持 ENS (以太坊域名服务)和 SNS (Solana 域名服务)。它会查询这些域名的 TXT 或特定自定义记录。不同域名对应的 Key 映射关系如下：

表 1 不同域名与对应查询 Key 的映射关系

域名类型	目标域名	对应查询 Key	作用
ENS	burrberry.eth	node	获取中继分发节点 IP
ENS	ukranianhorseriding.eth	network	基础网络基础设施
SNS	24carnforth2merseyside.sol	deserialized	基础网络基础设施

提取到记录后，文本中包含由“|”分割的虚假 IPv6 地址（例如 2001:db8:12e7:13d7::1）。样本通过逐个字节字符串对比的方式，过滤并提取出其中的 4 字节关键数据，再通过自定义置换函数 F 还原出真实的 IPv4 地址 (144.31.38.215)。

```
def ror8(x, r):
    return ((x >> r) | (x << (8-r))) & 0xFF

def F(x, i, key=0x80408454):
    x = ((x >> 4) | (x << 4)) & 0xFF
    x = ror8(x, i+1)
    k = (key >> (24 - 8*i)) & 0xFF
    return ((x ^ k) + k) & 0xFF

def decode_ip(ip_bytes):
    k = 0x80408454
    return ".".join(str(F(ip_bytes[i], i, k)) for i in range(4))

# 提取关键4字节示例（对应 12e7:13d7）
ip_bytes = bytearray.fromhex("12e713d7")
print(f"解密出的 IP: {decode_ip(ip_bytes)}")
```

图 1 还原混淆地址示例

动态 C2 的完整获取流程为：

第一步，DDoS 样本首先解析 burrberry.eth 的 node 记录，解密出一组中继分发节点的 IP（例如 144.31.38.215 等）。

第二步，DDoS 样本随后向这些分发节点发起 HTTP GET 请求：http://<node_ip>:9000/nodes?key=meowmeowmeow。

第三步，该接口返回的 IP 列表被 DDoS 样本作为真正的 C2 交互地址。然而在实际追溯中发现，这些返回的真实 C2 地址全部是由其他被感染的肉鸡所转换的中继节点。

3.网络协议与指令结构

在 fbot 的基础上，Dysphoria 重新定制了其底层通信协议，上线包与心跳包均为固定 78 字节，结构如下：

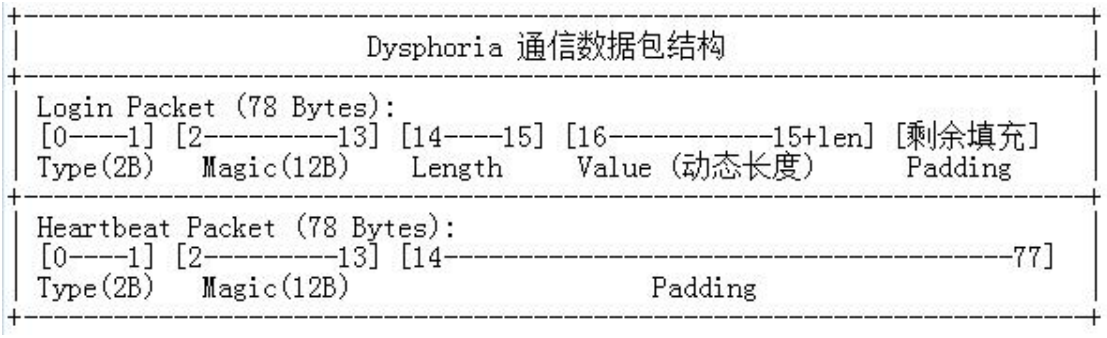

图 2 上线包与心跳包结构

Login Magic: 00 80 00 5a 00 57 00 c8 00 f0 00 1e (MsgType: 02 00)

Heartbeat Magic: 22 ba 15 24 1a 6f 04 d4 1f 9c 0d 06 (MsgType: 00 00)

DDoS 攻击指令采用了多流嵌套结构，具体结构如下：

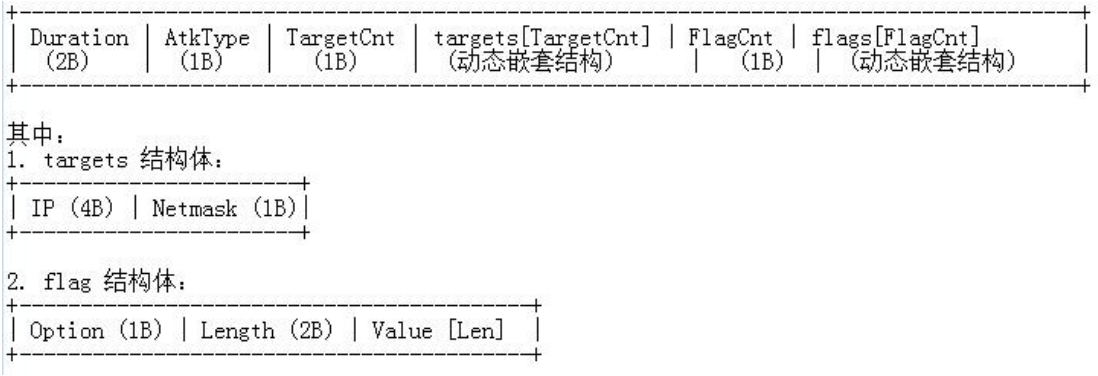

图 3 DDoS 攻击指令结构

（三）“中继/代理样本”机制分析

6 月下旬出现的全新独立变种功能十分纯粹，它剥离了所有的 DDoS 攻击模块，仅负责将被感染的肉鸡彻底转变为黑产集团的隐蔽网络中继站。

1.自动化 UPnP 内网穿透

由于大部分物联网设备或个人 PC 处于 NAT 后方，外部无法直接连接。该中继样本启动后，会在局域网内广播寻

找支持 UPnP (通用即插即用)的网关设备，随后强制调用 WAN 连接服务，在路由器上瞬间流式映射 155 个端口。

2.双向非阻塞高效中继 (Epoll)

肉鸡在本机成功监听上述 155 个端口。一旦有外部流量（如来自攻击者或 DDoS 样本的前端请求）接入肉鸡的某个端口 bot:P，该中继样本会立即向真正的远程 c2:P（相同端口）发起出站连接，然后在底层利用 Linux 高性能的 epoll 异步非阻塞 I/O 驱动，将两端连接进行绑定，实施双向非阻塞数据透明中继。

3.中继状态上报

中继节点每隔 4 秒以上，会向心跳收集域名 login.trees4sale.net:9000 发送一次 JSON 格式的健康状态报告，汇报自身的可用性，具体结构如下：

```
{
"status":"ONLINE",
"connections":42,
"bandwidth_mbps":12.5
}
```

（四）传播方式

Dysphoria 样本主要通过 Telnet/SSH 弱口令爆破以及已知 IoT 设备远程代码执行（RCE）漏洞进行传播，攻击目标涵盖路由器、网关、摄像头、及其他嵌入式 Linux 设备。已监测到其利用的部分漏洞包括：

CVE-2013-3307

CVE-2016-20016

CNVD-2017-38447

CNVD-2018-01041

CNVD-2020-35174

CNVD-2020-70958

CNVD-2020-08128

CNVD-2021-79445

CVE-2022-35733

CNVD-2025-12011

CVE-2025-34152

CNVD-2025-29924

CVE-2025-9528

其中既包含长期被僵尸网络广泛利用的经典 IoT 漏洞（如 CNVD-2017-38447、CNVD-2020-08128 等），也包含近年来披露的新漏洞，表明 Dysphoria 仍在持续维护和更新其传播能力，以提高对不同品牌和型号 IoT 设备的覆盖能力。与此同时，Telnet/SSH 弱口令攻击仍然是其最主要、最稳定的感染方式，与漏洞利用共同构成了其主要传播渠道。

三、僵尸网络感染规模

通过监测分析发现，2026 年 7 月 14 日至 20 日期间，Dysphoria 僵尸网络在我国境内已确认的活跃“肉鸡”规模达 4401 台，境内日上线肉鸡数量最高达 1801 台，肉鸡 C2 日访

问量最高达 74 万次。因其使用被控肉鸡作为 C2 中继，可以观测到其境外肉鸡规模更大，日上线境外肉鸡数最高达 23.9 万台。境内日上线肉鸡数量情况如下图所示：

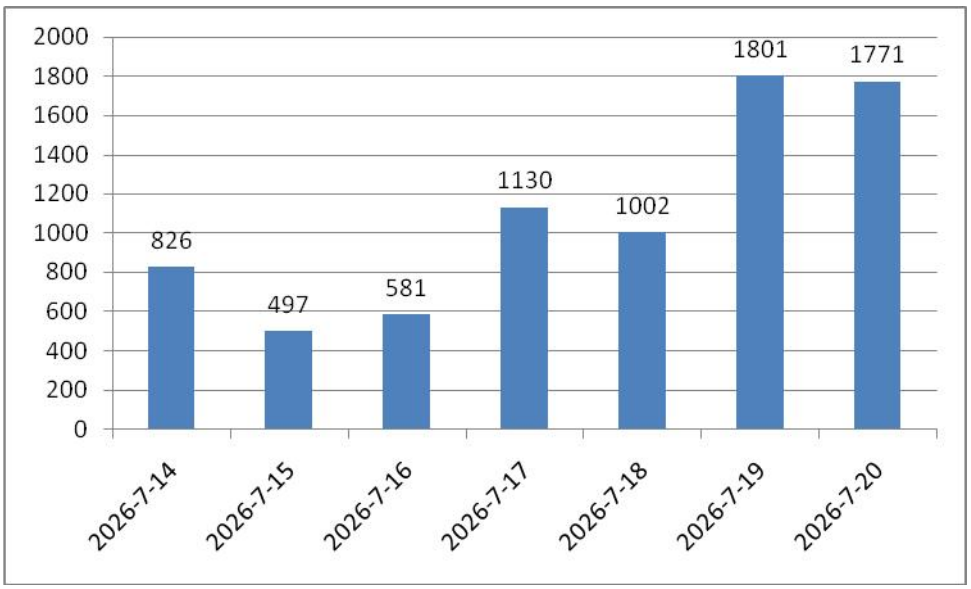

图 4 境内日上线肉鸡数量分布情况

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）梳理已有资产列表，及时修复相关系统漏洞，包括历史漏洞和最新曝光的漏洞。

（2）加强口令强度，避免使用弱口令，密码设置要符合安全要求，并定期更换。建议使用 16 位或更长的密码，包括大小写字母、数字和符号在内的组合，同时避免多个服务器使用相同口令。

（3）当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

五、相关 IOC

样本 HASH：

c1bedea261f325441fb9a75c50b11d0c8fb01ac6(早期变种)

a3b9575897c16cbf6afe3af1aa8b55171ea6edf9

8db6c78533c176f13b61405cdc3f8fad703325f1(Hailbot 回归)

9c1716d770ea69e8e1418d96d52222396ecb4362

73651c02b29f1c07e3177e86c967fc45e9f30f0f

955ff909972958098f0d4a06bcc4d6b9eea90449

25081bdec05f64eb4f313420c82d8de957e30026

dcea71b9ab9de8efca301de9e2f7bf11c7132364

df510f6f69a5c149c216c7b3accc4f460d8cf363

b0782a9d6eef2ce02f734a6e5e1d8e0f9a2b65be(纯中继代理样本)

e7e1694162639ed587625432a79cfaa49f560d11(UPnP 映射样本)

b7faa44ab0772047a8581bbfdd9c561e28fc66de(混合拓扑完全体)

e999d3d31c623ab5618b251c9b0e11f8ebcdde12

9311fb79fbfe1b180ed634315457212eb0fc885c

9ba9b4c24f1913a8644969a271f62b828e79f4c7

1b1ed06fdbe73446b1503c016be6c3bf5d8299e4

2f7f577d76df6db398a90e34b4d14907a25b1ff9

Download/C2 服务器(包含特异性 FTP Banner)：

217.60.195.160

76.164.203.171

92.42.100.131

78.153.155.152

Banner 特征：220 cool ftp server hosted on brian krebs' giant ass 4head

基础设施域名：

i.peer4you.net

o.peer4you.net

login.trees4sale.net

www.trees4sale.net

c2.saintpetersburgresident.ru

peer.saintpetersburgresident.ru

kieron.androiddebugbridge.su

dysphoria.androiddebugbridge.su

telaviv.androiddebugbridge.su

jerusalem.androiddebugbridge.su

node.androiddebugbridge.su

wow.androiddebugbridge.su

区块链域名：

m3rnbvs5d.eth (ENS)

burrberry.eth (ENS)

ukranianhorseriding.eth (ENS)

24carnforth2merseyside.sol (SNS)

控制域名：

boblazar.inhumanencounters.org

roswell.inhumanencounters.org

www.c1s.su

www.oppenheimer.su