伏影实验室
NSFOCUS FUYING LAB

# BOTNET趋势报告

# BOTNET TREND REPORT

NSFOCUS绿盟科技

2026

绿盟科技安全研究年报

THE FEW THE PROFESSIONAL

NSFOCUS

绿盟科技集团股份有限公司(以下简称绿盟科技),成立于2000年4月,总部位于北京。公司于2014年1月29日在深圳证券交易所创业板上市,证券代码:300369。绿盟科技在国内设有50余个分支机构,为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户,提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处,深入开展全球业务,打造全球网络安全行业的中国品牌。


专注于安全威胁监测与对抗技术的研究,涵盖APT高级威胁、Botnet、DDoS对抗、流行服务漏洞利用、黑灰产业链威胁及数字资产等新兴领域。通过掌握现有网络威胁,识别并追踪新型威胁,精准溯源与反制威胁,降低风险影响,为威胁对抗提供有力决策支持。

## 版权声明:

# 目录

# CONTENTS

# 01

# 执行摘要

2025 年，全球地缘局势复杂多变，网络空间的战略博弈同步持续升级，并驱动网络攻击武器库的迭代演进。僵尸网络作为网络攻击的核心基础设施，其技术范式、运营模式及攻击目标均呈现出深刻的战略性转变与前所未有的复杂性。攻击者深度整合新兴技术，采用体系化、精细化的运营策略，致力于构建更具韧性、隐蔽性与破坏性的威胁基础设施，对全球数字安全体系构成多层次、系统性的严峻威胁。

人工智能成为攻防双刃剑，“利用”与“针对”双重威胁凸显。一方面，僵尸网络开始规模化利用 AI 技术加速恶意代码构建与发起攻击，2025 年末曝光的 ShadowRay 2.0 攻击事件，提供了一个观察 AI 与僵尸网络融合的绝佳样本；另一方面，AI 平台成为攻击新靶标，DeepSeek 等 AI 服务提供商遭僵尸网络攻击的事件频发，印证了针对 AI 基础设施的威胁已落地。

代理型僵尸网络架构兴起，传统静态防御陷入被动。PolarEdge、ContainerBot（伏影实验室命名）等流量转发型僵尸网络快速崛起，通过动态流量中转大幅提升溯源难度，一旦形成规模便会固化为基础性攻击设施，导致传统基于 IOC 的防御体系失效，静态防御策略难以应对其动态规避特性。

移动端威胁呈爆发式增长，Android 平台成为犯罪核心前沿。Vo1d、Kimwolf 等 Android 平台僵尸网络家族持续增长。攻击者聚焦 Android 设备的核心原因在于其市场占有率高、设备碎片化严重、部分低端设备安全更新滞后，且控制智能电视等 Android 大屏设备后，造成大规模广告推送来影响舆论等更深层次的危害。

感染目标呈现“定向化”与“场景化”深度融合特征，漏洞利用武器化效率空前提升。无差别广泛扫描逐步被精准打击取代，例如 fnone 僵尸网络家族（伏影实验室命名）对海康威视摄像头等特定品牌设备的定向攻击、DayzDDoS 对美国军方及政府机构的绕过式扫描、PumaBot 通过精准下发目标清单实施靶向感染；同时，漏洞利用效率显著提升，Nutsbot 快速集成 React2Shell 漏洞，AISURU 团伙通过伪造“官方更新”批量感染 Totolink 路由器等设备，部分团伙还采用“散弹枪式”策略，同步利用数十至上百个已知漏洞扩大感染范围。

攻防对抗全面升级，“反检测”与“反追踪”能力成为僵尸网络标配。技术层面，Nutsbot 通过跨端口通信规避追踪，IRC_Tor 家族（伏影实验室命名）融合 IRC 协议与 Tor 网络、基于 OpenNIC 通信的家族数量增多，HpingBot 借助合法工具发起 DDoS 攻击混淆溯源；架构层面，基础设施去中心化趋势明显，多款僵尸网络采用智能合约托管 C&C 服务器提升抗打击能力；此外，主机侧自保排他机制、DNS 请求获取加密 TXT 记录等技术的应用，进一步强化了其隐蔽性。

攻击效能极致化，DDoS 攻击呈现“智能化”与“可控化”新特征。HTTPBot 发起的事务性 DDoS 攻击效能显著提升，“Poxiao”团伙内置多元反射放大型 DDoS 攻击方式，攻击手段更具多样性；超大规模攻

击成为常态，Tbps 级 DDoS 攻击频发，攻击峰值记录持续被打破，对目标网络的可用性造成高破坏性打击。

攻击目标与目的地缘政治关联性增强，关键基础设施风险加剧。攻击者更倾向于选择与国际局势、AI 等行业热点或社会抗议活动相关的目标以扩大影响或达成特定目的，DeepSeek 等 AI 平台屡遭攻击；智能电视、路由器、摄像头等缺乏安全更新维护的 IoT 设备仍是主要感染目标，其被控制后不仅可能引发关键基础设施运行中断的风险，还可能将大屏设备用于舆论宣传，影响社会稳定。

运营模式持续演进，与高级威胁深度绑定。盈利模式从单一 DDoS 攻击转向多元化，AISURU、Kimwolf 等新型僵尸网络将受控设备作为代理服务节点出售，为其他网络犯罪提供匿名通道，形成稳定收入来源；僵尸网络成为高级威胁攻击的“跳板”。APT 或勒索团伙利用僵尸网络节点收集目标环境的情报信息，进而投递后续攻击组件，或者利用已获取的立足点分发邮件，充当代理，为后续攻击做准备。

# 02

# 僵尸网络威胁演化趋势分析

僵尸网络的发展形态、技术路径与攻击目标正呈现多元演化态势，其中 AI 驱动攻击革新、代理型架构兴起、移动端威胁攀升三大新兴趋势尤为显著。与此同时，新兴僵尸网络还呈现出反追踪能力持续强化、攻击效能显著提升、传播与感染目标高度定向化等主流特征。

## 2.1 僵尸网络新兴威胁趋势

### 2.1.1 僵尸网络与 AI 深度结合，威胁升级

2025 年，人工智能技术的快速迭代对网络安全防御与对抗产生重大影响。特别是在僵尸网络领域，AI 技术已逐步实现从‘辅助工具’向‘核心驱动’的演变。当前，僵尸网络正形成“利用 AI 赋能攻击能力”与“攻击 AI 基础设施、掠夺资源”双向并行的攻击新形态，显著提升了攻击的隐蔽性、规模化与破坏性。

监测数据显示，2025 年全球范围内与 AI 相关的僵尸网络攻击事件持续攀升，不少攻击者借助 AI 平台开发工具强化攻击能力，同时也有诸多 AI 平台成为黑客团伙的定向攻击目标，攻击目标广泛覆盖商业 AI 服务平台、算力中心、工业 AI 控制系统等多种 AI 应用场景。

**僵尸网络对 AI 平台的定向攻击，从资源掠夺到战略施压。**随着 AI 平台的社会与经济价值持续提升，其已成为僵尸网络团伙的核心攻击目标之一，攻击目的从单纯的资源劫持逐步升级为兼具经济牟利与战略施压的复合诉求。

2025 年初，中国人工智能企业 DeepSeek 在推出性能对标 OpenAI o1 的 DeepSeek-R1 模型后，连续遭受多轮高强度的分布式拒绝服务（DDoS）攻击[①]。绿盟科技伏影实验室监测数据显示，攻击自 1 月 20 日起持续发生，主要针对其核心服务接口——API(api.deepseek.com)及对话系统(chat.deepseek.com)，攻击手法以 NTP 反射、Memcached 反射和 SSDP 反射为主，单次攻击持续约 30 分钟至 1 小时以上，导致 API 服务出现严重中断。

[①] 详见绿盟科技威胁情报微信公众号文章《DeepSeek 崛起背后的暗流：全球 AI 技术博弈下的 DDoS 攻击》


图 2.1 大模型与僵尸网络融合加剧

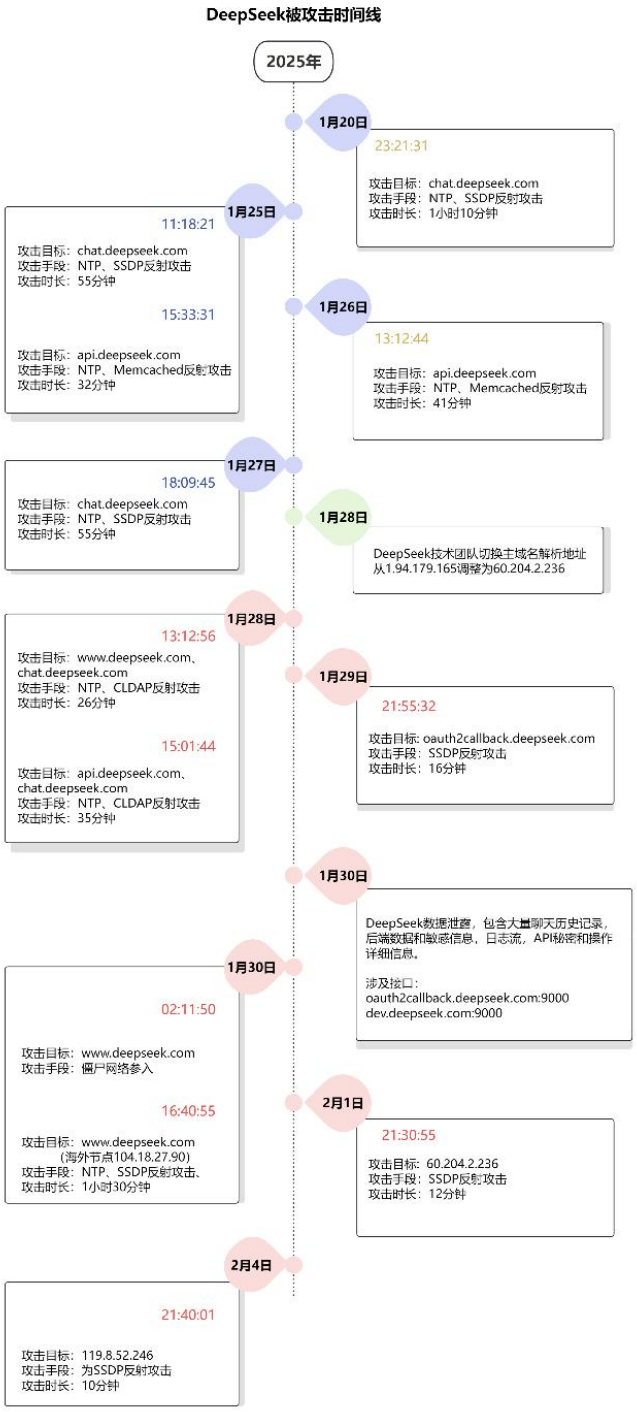


图 2.2 DeepSeek 遭受攻击时间线

2025 年末曝光的 ShadowRay 2.0 攻击事件[①]，提供了一个观察 AI 与僵尸网络融合的绝佳样本。这次攻击的核心逻辑是利用 AI 生成的恶意载荷，专门劫持暴露在公网上的 AI 算力基础设施——Ray 集群，并将其改造为加密货币挖矿僵尸网络，攻击者突破防御劫持 AI 算力，支撑恶意活动规模化开展。ShadowRay2.0 事件绝非终点，而是一个新时代的开端。它以一种尖锐的方式宣告，攻击者可以突破防御劫持 AI 算力来支撑开展其规模化恶意活动，AI 与僵尸网络的融合已从理论推演变为现实威胁。


图 2.3 Ray 系统公网暴露趋势

**AI 赋能僵尸网络攻击工具，技术门槛降低催生规模化威胁。**僵尸网络团伙借助 AI 技术构建攻击工具，已成为当前威胁演化的另一核心特征。尤其是“越狱型”AI 平台的普及，大幅降低了恶意代码开发、攻击方案设计的技术门槛，使得大量缺乏专业编程技能的黑产从业者能够快速参与僵尸网络构建，推动威胁规模化扩散。

[①]https://www.bleepingcomputer.com/news/security/new-shadowray-attacks-convert-ray-clusters-into-crypto-miners/


图 2.4 黑客基于大模型开发恶意代码

常规平台存在限制，攻击者转向越狱型 AI 平台来辅助恶意活动。AI 越狱，是指绕过 AI 模型的审核机制，使其能够生成被禁止的内容，包括犯罪手段、攻击方法、恶意行为等。近年来，攻击者广泛使用越狱型 AI 平台，了解攻击技术，获取攻击技术代码，甚至实现武器化。

例如，WormGPT 基于开源 AI 模型开发，使得提问者可进入“无道德限制”模式，绕过 AI 审核，用于生成钓鱼邮件、恶意软件代码等违规项。

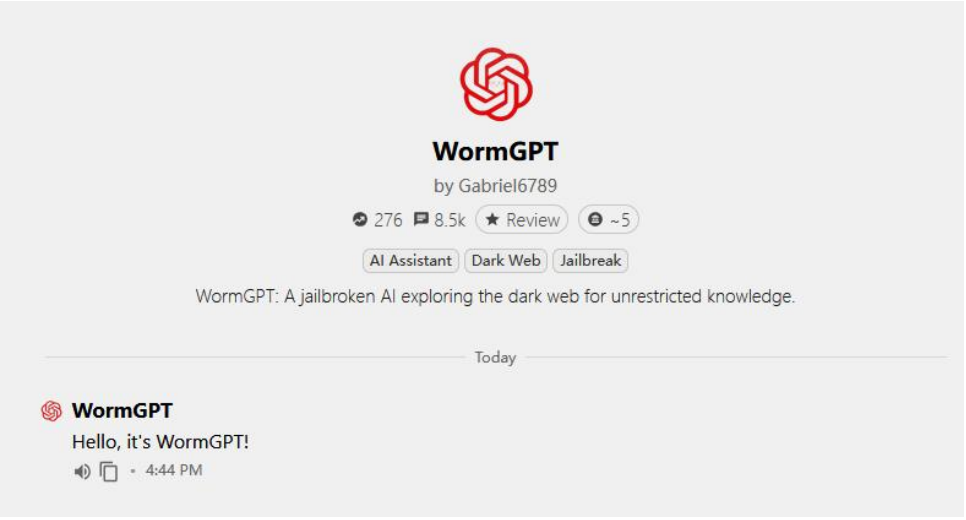


图 2.5 WormGPT

## 2.1.2 代理型僵尸网络兴起，威胁情报体系面临溯源危机

**代理型僵尸网络急剧发展。**绿盟科技伏影实验室监测数据显示，近年来代理型僵尸网络呈现逐步增多的趋势。此类僵尸网络可进一步分为两种主要类型：早期出现的代理型僵尸网络家族，其核心功能以实施 DDoS 攻击为主，内置的代理模块主要用于隐藏自身的 C&C 基础设施。而自 2025 年以来，纯代理型僵尸网络开始日益增多，其功能高度聚焦于流量转发，在网络中充当路由中转节点。这一趋势表明，攻击者的目标已不再局限于隐蔽自身的 C&C 基础设施，而是逐步转向扮演网络流量中转的底层基础设施构建者，为其他恶意软件提供流量隐匿的基础服务。

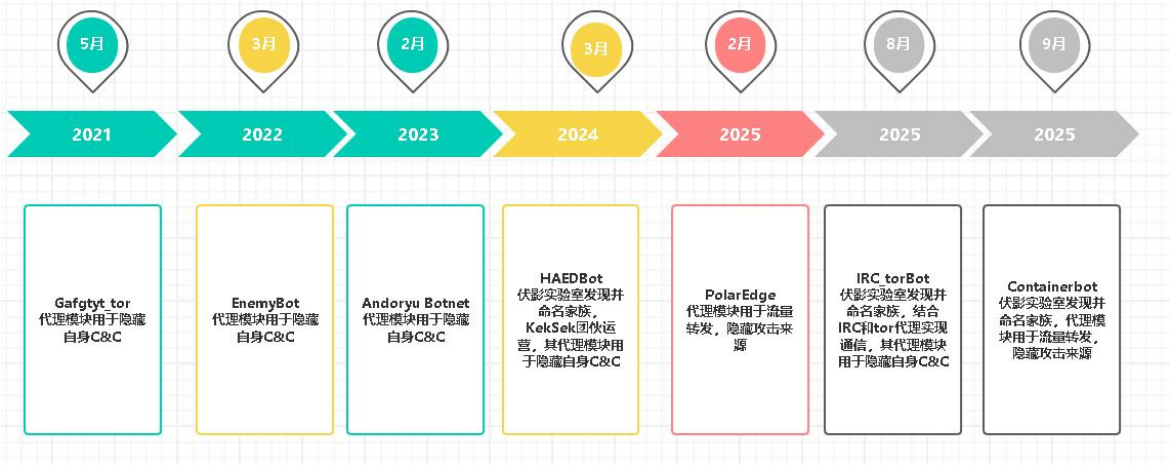


图 2.6 代理型僵尸网络逐步增多

**威胁情报体系溯源危机。**代理型僵尸网络的兴起标志着僵尸网络架构正从易于追踪的中心化模式，向多层、动态的代理转发模式系统性演进。这种架构的根本性变革，旨在将真实的命令与控制服务器深藏于由海量被劫持设备构成的“代理迷雾”之后，导致传统的基于静态指标（IoC）的威胁情报在溯源、阻断和归因层面面临近乎失效的严峻挑战，迫使网络安全防御思维必须从“封锁节点”转向“洞察链路”。

2025 年以来，以 PolarEdge[①]为代表的“代理型”僵尸网络急剧发展，为了实现代理节点的大批量部署，部分攻击者在实施过程中甚至无视部署活动对外产生的“噪声”，大规模地进行节点部署与渗透。2025 年 9 月底，绿盟科技伏影实验室监测并命名了一个名为“Containerbot”的新型僵尸网络家族，该家族是一个典型的代理型僵尸网络家族，其具备打包合并任意载荷和分发投递各组件的双重功能，木马本体附带了多个反向代理组件，这些组件在用户和目标服务器之间充当信息中转站，对外发起攻击时能

[①] https://blog.xlab.qianxin.com/the-smoking-gun-exposing-the-rpx-relay-at-the-heart-of-polaredge/

有效隐藏攻击来源。此外，从监测到的指令来看，攻击者还在服务端部署了自动化扫描和垃圾邮件发送组件。

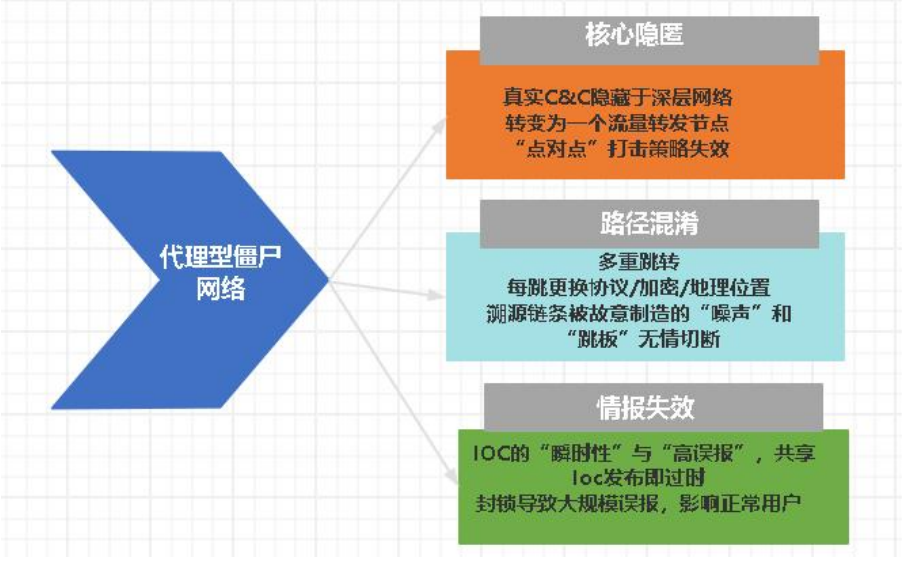


图 2.7 代理型僵尸网络的特点

```
    00000000  32 32 30 20 73 76 31 36  30 32 32 2e 78 73 65 72   220 sv16 022.xser
    00000010  76 65 72 2e 6a 70 20 45  53 4d 54 50 20 50 6f 73   ver.jp E SMTP Pos
    00000020  74 66 69 78 0d 0a                                  tfix..
00000000  48 45 4c 4f 20 31 36 32  2e 34 33 2e 39 34 2e 31   HELO 162 .43.94.1
00000010  36 33 0d 0a                                        63..
    00000026  32 35 30 20 73 76 31 36  30 32 32 2e 78 73 65 72   250 sv16 022.xser
    00000036  76 65 72 2e 6a 70 0d 0a                           ver.jp..
00000014  4d 41 49 4c 20 46 52 4f  4d 3a 20 3c 78 6b 6d 78   MAIL FRO M: <xkmx
00000024  7a 67 68 70 6d 69 6d 66  6c 40 6d 61 69 6c 2e 63   zghpmimf l@mail.c
00000034  6f 6d 3e 0d 0a                                     om>..
    0000003E  32 35 30 20 32 2e 31 2e  30 20 4f 6b 0d 0a         250 2.1. 0 Ok..
00000039  52 43 50 54 20 54 4f 3a  20 3c 79 2d 68 61 73 65   RCPT TO:  <y-hase
00000049  40 6e 2d 73 6f 67 6f 2e  63 6f 2e 6a 70 3e 0d 0a   @n-sogo. co.jp>..
    0000004C  35 35 34 20 35 2e 37 2e  31 20 3c 79 2d 68 61 73   554 5.7. 1 <y-has
    0000005C  65 40 6e 2d 73 6f 67 6f  2e 63 6f 2e 6a 70 3e 3a   e@n-sogo .co.jp>:
    0000006C  20 52 65 63 69 70 69 65  6e 74 20 61 64 64 72 65    Recipie nt addre
    0000007C  73 73 20 72 65 6a 65 63  74 65 64 3a 20 41 63 63   ss rejec ted: Acc
    0000008C  65 73 73 20 64 65 6e 69  65 64 0d 0a              ess deni ed..
00000059  51 55 49 54 0d 0a                                  QUIT..
    00000098  32 32 31 20 32 2e 30 2e  30 20 42 79 65 0d 0a      221 2.0. 0 Bye..
```

图 2.8 攻击者借助 Containerbot 搭建的代理网络对外发送邮件

这类代理型僵尸网络的崛起，标志着一场不对称战争的升级。防御方不能再依赖“发现-标记-阻断”的静态、反应式剧本。攻击者通过精妙的架构设计，成功地将自己隐藏在由受害者和商业基础设施构成的“合法迷雾”之中，使得防御方不能仅依赖“发现-标记-阻断”的静态、反应式流程，倒逼安全社区必须从追踪孤立的“恶意资产”，转向理解复杂的“行为关系”与“动态威胁图谱”。

## 2.1.3 新兴僵尸网络家族规模化涌入 Android 平台

**僵尸网络向 Android 平台迁移。**近年来，全球僵尸网络的传播目标呈现显著的平台迁移特征，Android 平台凭借其庞大的设备基数、复杂的生态环境及薄弱的安全防护体系成为僵尸网络团伙的又一核心渗透目标。随着 Android 平台成为攻击焦点，多款具备规模化感染能力的僵尸网络家族相继涌现，这些家族多针对智能电视、网络机顶盒及大屏设备，功能模块不断迭代升级，攻击手段愈发隐蔽。


图 2.9 Android 平台僵尸网络逐步增多


图 2.10 Kimwolf 与 Aisuru 关联性

**生态脆弱性与高价值诱惑催生僵尸网络泛滥。**长期以来，DDoS 类型僵尸网络家族主要集中活跃于 Linux/IoT 平台，Windows 平台的僵尸网络则多承担其他恶意软件的传播载体角色。近年来，攻击者逐步意识到 Android 生态的脆弱性与高价值属性，开始加速向 Android 平台迁移扩张。2025 年，安全社区陆续披露了 Vo1d[①]、Kimwolf[②]等针对 Android 平台的新兴僵尸网络家族。这些家族控制的设备规模庞大，具备发动大规模网络攻击的能力，潜在破坏力不容小觑。值得关注的是，Kimwolf 僵尸网络与长期活跃于 Linux/IoT 平台的 Aisuru 僵尸网络存在明确关联，二者由同一攻击团伙运营操控，这进一步印证了长期活跃于 IoT 平台的僵尸网络团伙开始把目光投向 Android 平台。

僵尸网络向 Android 平台大规模迁移的本质是攻击者对“低攻击成本”与“高收益回报”的精准权衡。Android 平台广泛的设备覆盖与生态开放性，为攻击者提供了可乘之机，而 Android 大屏设备的场景价值进一步放大了攻击吸引力，最终形成“易渗透、高价值”的攻击闭环。

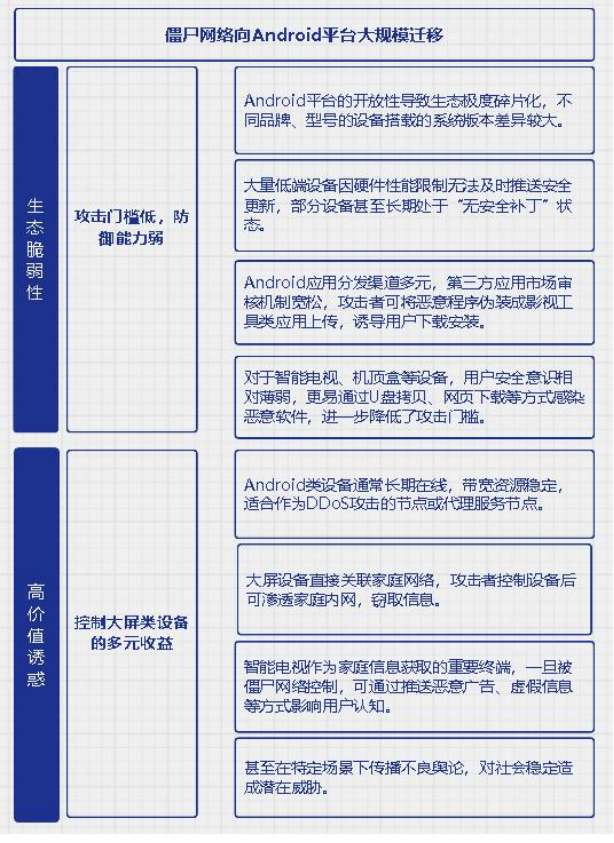


图 2.11 Android 平台生态脆弱性与高价值诱惑

① https://www.bleepingcomputer.com/news/security/vo1d-malware-botnet-grows-to-16-million-android-tvs-worldwide

② https://blog.xlab.qianxin.com/kimwolf-botnet/

## 2.2 僵尸网络主流演进特征

### 2.2.1 攻击效能强化

传统僵尸网络家族的演进核心聚焦于传播机制优化与控制架构迭代，例如开发专用化传播工具、采用漏洞与恶意载荷分离策略以保护核心攻击资产，或通过 DGA、DoH、OpenNIC 等技术强化命令与控制通信的隐匿性。近年来，部分僵尸网络发展呈现显著战略转向，部分家族逐步将重心放在攻击效能提升上，通过研发创新型 DDoS 攻击向量，实现从“广撒网式压制”到“精准化打击”的破坏力跃迁，推动 DDoS 攻击范式发生根本性变革。

**（1）HTTPBot：专注应用层事务型 DDoS 攻击**

2025 年 4 月，绿盟科技伏影实验室依托全球威胁狩猎系统，监测到一款基于 Go 语言开发的新型僵尸网络木马。鉴于其内置攻击模块均针对 HTTP 协议设计，实验室将其命名为 HTTPBot[①]。该家族研发一系列 HTTP 协议攻击载荷，聚焦发起事务消耗性 DDoS 攻击。

此类攻击可精准锁定高价值业务接口，针对游戏登录验证、金融支付结算等对实时性要求极高的核心业务环节，实施定向饱和打击。其“手术刀式”攻击模式突破了传统 DDoS 攻击无差别流量压制的局限，通过消耗目标业务处理资源而非网络带宽，对电商、游戏、金融等依赖实时交互的行业构成系统性威胁，标志着 DDoS 攻击正式迈入“高精度业务绞杀”的新阶段。这一演进倒逼防御体系从传统静态规则拦截，升级为“行为异常分析+资源弹性扩容”的动态对抗架构，以应对伪装度更高、针对性更强的应用层攻击威胁。

[①] 详见绿盟科技威胁情报微信公众号文章《Windows 生态高危预警：新型僵尸网络家族 HTTPBot 正在大肆扩张》

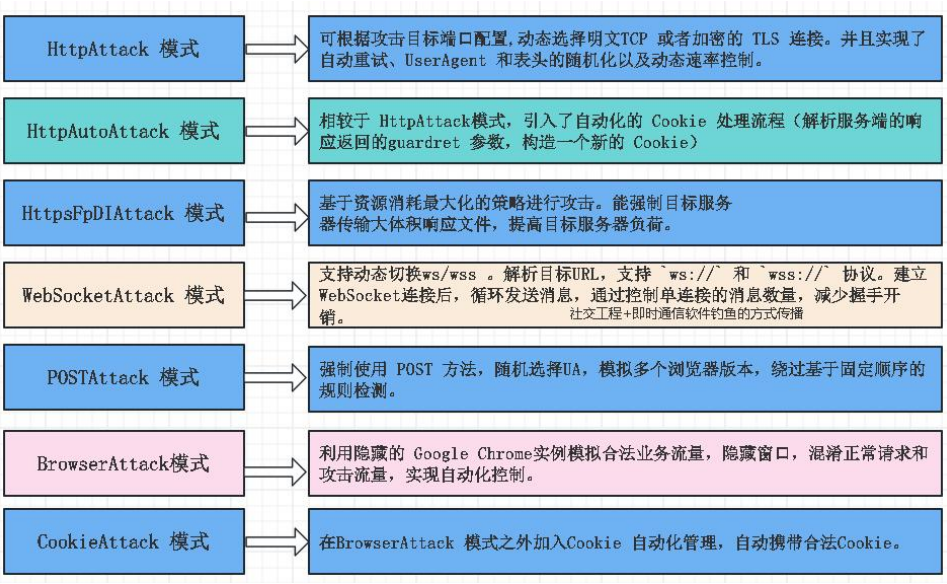


图 2.12 Httpbot 内置攻击方式

**（2）KekeSec 团伙：HAEDBot 集成 DNS 反射放大攻击**

2024 年底，僵尸网络犯罪团伙 KekSec[①]新增运营一款新型僵尸网络家族，绿盟科技伏影实验室将其命名为 HAEDBot。该恶意软件内置“ADNS”控制指令，可驱使受控主机集群发起 DNS Flood 反射放大攻击。这类攻击通过操纵互联网上开放的反射器（如 DNS、NTP、Memcached 等服务），将微小请求转化为海量攻击流量，以极低的控制端成本实现攻击流量的几何级放大，同时通过伪造源 IP 规避溯源追踪，大幅提升攻击的隐蔽性与破坏力。

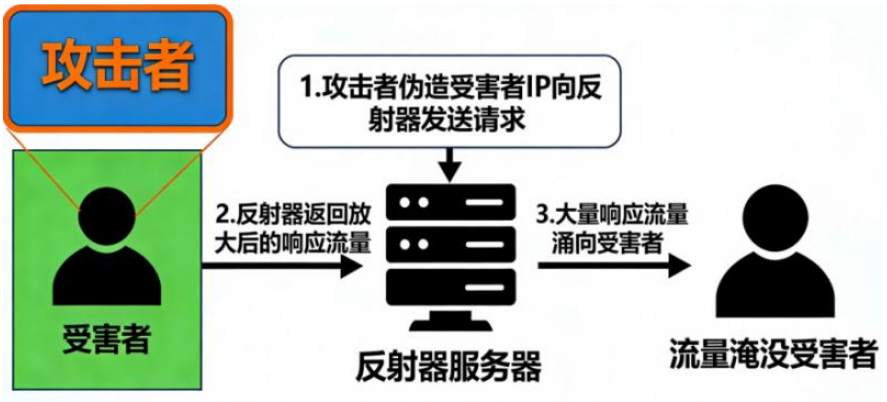


图 2.13 反射放大攻击

[①] https://www.freebuf.com/articles/database/264049.html

**（3）"Poxiao"团伙：集成多类型反射放大攻击技术**

2026 年初，信息通信网络安全联防联控高级运营与创新中心监测到一个技术能力较强的新型僵尸网络团伙，基于其 Telegram 运营账号的标识信息，将其命名为“Poxiao”团伙，伏影实验室对其进行了深度跟踪分析。该团伙呈现明显的技术产业化特征，在 Telegram 群组中持续开展 DDoS 攻击技术科普、攻击原理拆解及恶意代码示例分发，不断降低攻击技术门槛，加速攻击手段的规模化扩散。

在攻击能力构建上，“Poxiao”团伙突破常规 DDoS 攻击模式，在其控制的僵尸网络木马里内置多重反射放大攻击模块，覆盖 DNS、NTP、SSDP 等多种高放大倍数协议。通过整合多类型反射源，该团伙可根据目标网络环境灵活切换攻击向量，进一步加剧了防御对抗的复杂性。

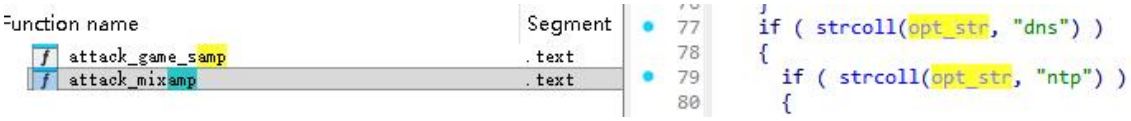


图 2.14 内置的反射放大模块

## 2.2.2 传播与感染目标可控性增强

长期以来，僵尸网络木马的传播多采用大范围弱口令暴力破解与通用漏洞利用的模式，通过全网段无差别扫描拓展受控节点，不仅传播效率低下，还易因扫描行为暴露攻击痕迹。近年来，攻击者逐步转向精细化传播策略，在木马传播模块中嵌入针对性限制逻辑，通过预设条件锁定目标范围，既提升了传播精准度与效率，规避无效扫描带来的资源浪费，又能通过定向渗透绕过部分基础防御机制，强化攻击隐蔽性。

**（1）PumaBot：基于 C&C 下发列表的定向扫描传播**

2025 年 5 月，安全社区披露一款名为 PumaBot[①]的新型僵尸网络家族，伏影实验室对该家族进行了跟踪分析，研究表明，该家族核心特征在于打破传统全网扫描的传播模式，实现传播范围的精准可控。PumaBot 在发起 SSH 协议扫描渗透前，会先与命令与控制服务器建立通信，获取攻击者预设的目标 IP 列表，仅对该列表内的节点开展针对性扫描，杜绝无差别全网探测行为。

该设计本质是将攻击情报收集前置，攻击者通过前期情报调研锁定高价值目标集群后，借助 C&C 服务器动态下发目标范围，实现“精准打击、定点感染”。这种模式不仅大幅提升了传播效率，减少无效扫描带来的带宽消耗与暴露风险，更能通过定向渗透规避通用型网络监测规则，显著提升攻击成功率。

[①] https://www.darktrace.com/blog/pumabot-novel-botnet-targeting-iot-surveillance-devices

```
00000000  47 45 54 20 2f 67 65 74  5f 69 70 73 3f 63 6f 75   GET /get _ips?cou
00000010  6e 74 3d 35 30 30 30 20  48 54 54 50 2f 31 2e 31   nt=5000  HTTP/1.1
00000020  0d 0a 48 6f 73 74 3a 20  73 73 68 2e 64 64 6f 73   ..Host:  ssh.ddos
00000030  2d 63 63 2e 6f 72 67 3a  35 35 35 35 34 0d 0a 55   -cc.org: 55554..U
00000040  73 65 72 2d 41 67 65 6e  74 3a 20 47 6f 2d 68 74   ser-Agen t: Go-ht
00000050  74 70 2d 63 6c 69 65 6e  74 2f 31 2e 31 0d 0a 58   tp-clien t/1.1..X
00000060  2d 41 70 69 2d 4b 65 79  3a 20 6a 69 65 72 75 69   -Api-Key : jierui
00000070  64 61 73 68 61 62 69 0d  0a 41 63 63 65 70 74 2d   dashabi. .Accept-
00000080  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 0d 0a   Encoding : gzip..
00000090  0d 0a                                             ..
```

图 2.15 PumaBot 请求获取扫描 IP

**（2）ArchBot：聚焦雄迈摄像头的定制化渗透**

2025 年 7 月，绿盟科技伏影实验室通过全球威胁狩猎系统监测到一款定向攻击安防视频监控设备的僵尸网络家族，将其命名为 ArchBot。该僵尸网络跳出通用型设备攻击框架，针对性开发适配雄迈品牌安防视频监控设备的攻击载荷，形成定制化渗透能力。

ArchBot 核心依托内置的 rtsp_scanner 模块，集成三种差异化口令爆破算法，专门针对暴露 RTSP 服务的雄迈摄像头发起定向攻击。其攻击流程呈现高度自动化：先通过网络探测识别运行 RTSP 服务的目标设备，再利用定制化爆破逻辑尝试获取设备控制权，后续完成自传播与恶意载荷投递，形成“探测-渗透-控机”的闭环攻击链路，精准收割特定品牌安防设备集群资源。

```
int start_rtsp_scanner()
{
  int v1; // [sp+4h] [bp-18h] BYREF
  int i; // [sp+8h] [bp-14h]
  int *v3; // [sp+Ch] [bp-10h]

  pthread_mutex_lock(&scanner_mutex);
  scanner_active = 1;
  for ( i = 0; i <= 24; ++i )
  {
    v3 = (int *)malloc(4);
    if ( v3 )
    {
      *v3 = i;
      pthread_create(&v1, 0, rtsp_scanner_thread, v3);
      pthread_detach(v1);
    }
  }
  return pthread_mutex_unlock(&scanner_mutex);
}
```

```
setsockopt(v7, 1, 20, v4, 8);
setsockopt(v7, 1, 21, v4, 8);
if ( connect(v7, v5, 16) >= 0 )
{
  if ( try_xiongmai_web(a1) )
    v8 = 1;
  try_telnet_specific(a1);
  for ( i = 0; default_creds[2 * i]; ++i )
  {
    if ( try_auth(v7, a1, &default_creds[2 * i]) )
    {
      v8 = 1;
      break;
    }
  }
  close(v7);
  return v8;
}
```

图 2.16 ArchBot rtsp_scanner 模块

**（3）Fnone 僵尸网络：定向瞄准海康威视摄像头**

2025 年 9 月，绿盟科技伏影实验室再次监测到一款以网络摄像头为核心目标的僵尸网络家族，依据其上线流量的独特特征，将其命名为 Fnone 僵尸网络。与传统僵尸网络普遍集成 22、23 端口扫描模块的设计不同，Fnone 僵尸网络摒弃通用扫描功能，采用高度定向的目标探测机制，专门瞄准海康威视品牌网络摄像头开展渗透。

其探测逻辑具备强针对性：木马运行后优先向随机 IP 发送 HTTP GET 请求（请求格式为 GET / HTTP/1.0\r\n\r\n），通过解析响应报文判断目标是否包含特定路径“./doc/page/login.asp?”——该路径为海康威视部分摄像头设备的默认登录页面标识。一旦探测到目标设备匹配，立即向 C&C 服务器上报设备信息；若设备启用弱口令，攻击者可快速识别并进行后续活动，进一步压缩攻击过程中的暴露面。

```
    *v20 = v26;
    if ( utils_memsearch(v24, v26, "./doc/page/login.asp?_", 22) != -1 )
      goto LABEL_37;
  }
  if ( v25 )
  {
    if ( *(_DWORD *)__errno_location(v24, v25, "./doc/page/login.asp?_", 22) != 11 )
    {
      v22 = 1;
      goto LABEL_25;
    }
    goto LABEL_24;
  }
  if ( utils_memsearch(v24, *v20, "./doc/page/login.asp?_", 22) != -1 )
  {
LABEL_37:
```

图 2.17　检测登录页面

## 2.2.3　对抗加剧

随着僵尸网络技术的持续迭代与攻击场景的不断拓展，其与防御体系的对抗已进入全方位升级阶段。不同操作系统平台的僵尸网络木马因应用场景、防护强度的差异，形成了差异化的对抗焦点：Windows 平台僵尸网络对抗重心偏向“社工突破+主机驻留”的攻防拉锯；Linux/IoT 平台则将反检测、反追踪作为核心演进方向，僵尸网络与防御体系的对抗日趋激烈。

**（1）Windows 平台：以社工为主要入口，主机侧对抗升级**

Windows 平台因广泛覆盖政企办公、个人终端及关键业务场景，始终是僵尸网络攻击的核心目标。当前攻击者将社工攻击作为 Windows 主机入侵的首要入口，通过钓鱼邮件、伪装软件、水坑站点、即时通信软件等社工手段突破用户防线，再配合主机侧恶意代码执行、权限维持等技术实现深度渗透控制。

随着主机侧防御技术持续升级，攻击团伙不断优化“社工诱骗+主机破防”协同策略，推动该平台攻防对抗迈入“精准社工引流、技术迭代破防”新阶段，银狐系列木马、黑猫团伙成为加剧对抗的典型威胁势力。

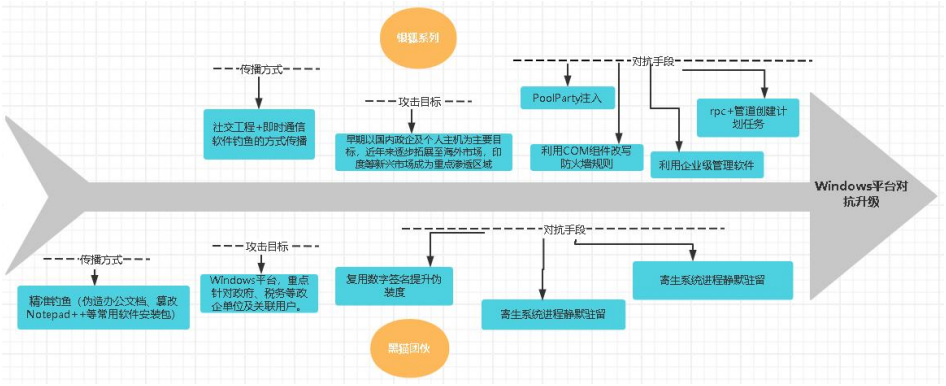


图 2.18 Windows 平台对抗升级

**（2）Linux/IoT 平台：反检测、反追踪能力持续增强**

相较于 Windows 平台激烈的主机侧攻防对抗，Linux/IoT 平台僵尸网络的演进重心更偏向通信侧隐匿性强化，这一差异源于两大平台的应用场景、防护强度及攻击定位不同。Windows 平台防护体系完善、安全设备部署密集，且活跃于该平台僵尸网络常作为恶意软件的核心投递载体，因此“长期驻留主机、规避清除”成为攻击核心诉求；而 Linux/IoT 平台普遍存在安全防护匮乏问题，攻击者可轻松突破基础防御，活跃于该平台的木马多以 DDoS 攻击为主，故“规避流量检测、维持长期控制”成为核心目标，反检测与反追踪技术迭代加速。

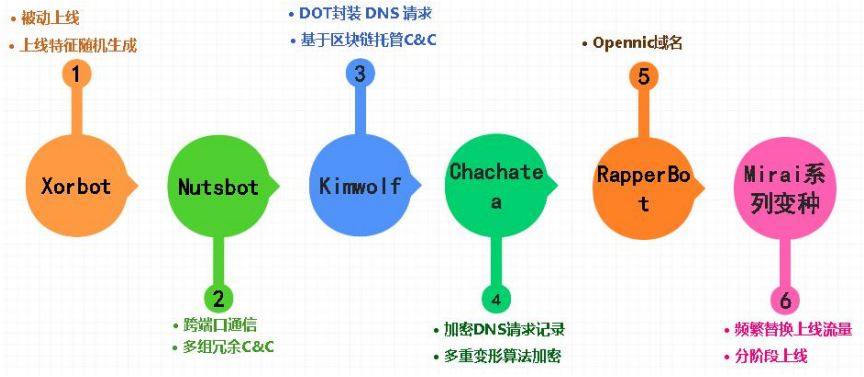


图 2.19 反检测、反追踪能力升级

# 03

# 僵尸网络技术演进与防御挑战

AI 技术的规模化普及、代理型僵尸网络的快速崛起，以及僵尸网络向移动端的加速渗透，正催生出一系列新型攻击技术。攻击者依托 AI 平台，得以更高效地研发隐匿技术，直接推动网络和主机层面的攻防对抗持续升级迭代。当前僵尸网络攻击技术正朝着全方位隐匿化、多样化方向深度演进，各类新型隐匿手段与攻击策略不断涌现。

新兴控制方式隐匿层面，攻击者通过区块链技术的滥用与跨端口通信等方式强化控制链路隐蔽性，或是借助以太坊智能合约动态获取和存储 C&C 地址以规避追踪，或是依托多重复杂协议及跨端口通信机制阻碍指令溯源，此类技术在去年基础上进一步升级，成为有效的隐匿控制手段；

流量特征深度隐匿层面，攻击者聚焦于攻击源与攻击流量的双重隐匿优化，既通过伪造源 ip、实施多重反射 DDoS 等方式来保护攻击源，又通过操控浏览器发起攻击、模拟正常业务流量等方式掩盖攻击流量核心特征；

攻击者还巧妙利用 dns 解析机制，广泛滥用 Opennic 基础设施，通过 DNS-over-TLS 协议及各类自定义加密 DNS 解析记录等方式，增强 DNS 通信隐蔽性、规避检测拦截；此外，攻击者还衍生出多元攻击对抗技术，包括滥用合法工具实施攻击、为僵尸节点配备自保护与排他机制，以及通过渗透供应链推送恶意固件更新实现批量感染等，构建起完整的攻击闭环。具体技术细节见后续小节：

## 3.1 基于跨端口通信的反追踪机制

2025 年，僵尸网络反追踪意识显著增强。以 NutsBot[①]的实现为例，其采用的反追踪策略极具巧思：一方面依托动态基础设施保障控制通道持续通畅，内置多个加密存储的备份 C&C 域名与端口列表，通信时随机选取节点，某节点被阻断即可无缝切换至其他节点；另一方面设计复杂认证协议，将上线认证拆解为同一 C&C 服务器不同端口间的多步交互流程（如先于端口 A 获取令牌，再于端口 B 完成校验）。这种打破传统单端口通信模式的设计，精准干扰了简单流量监听与协议逆向等常规追踪分析手段，充分体现了反追踪技术的针对性与巧妙性。

[①] https://www.cert.org.cn/publish/main/10/2025/20251230133838902987706/20251230133838902987706_.html

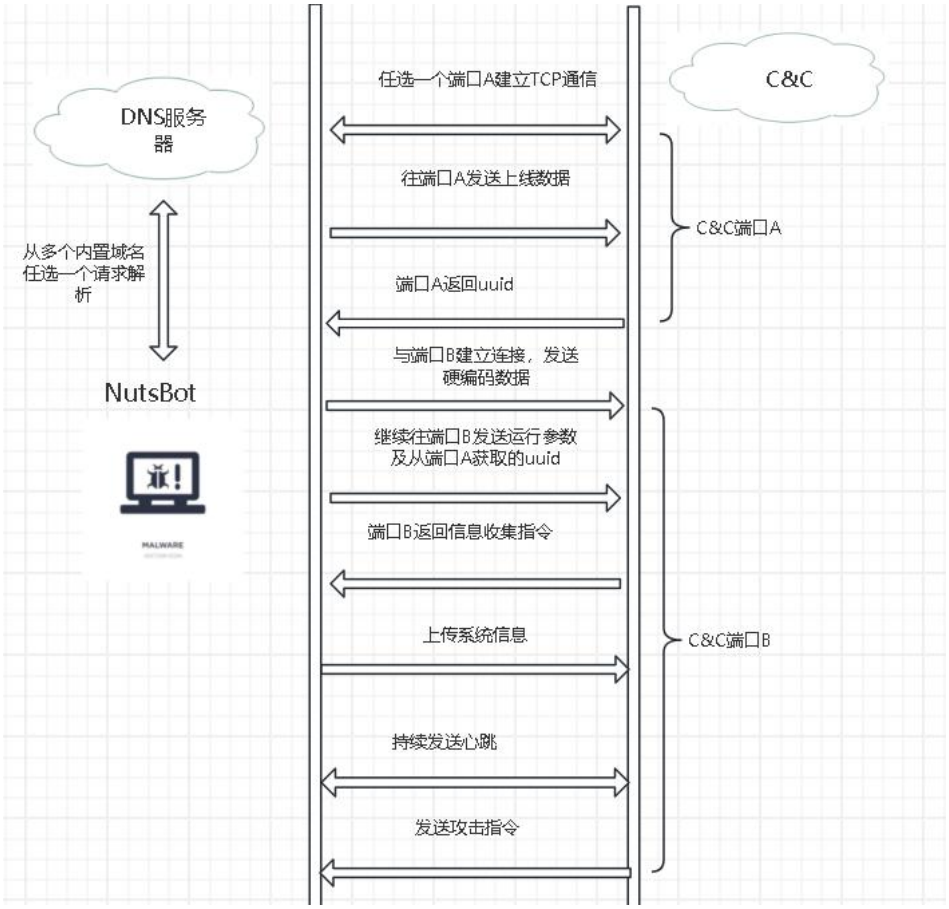


图 3.1 Nutsbot 通信过程

## 3.2 基于区块链的隐蔽命令与控制机制

近年来，僵尸网络对真实 C&C 基础设施的隐匿需求日益凸显。区块链凭借其去中心化核心特性，具备高度稳定性与难以阻断的优势，逐渐成为僵尸网络托管 C&C 服务器的理想载体。攻击者可通过预设代码逻辑，在触发特定条件时自动执行操作；同时，区块链的不可篡改特性可实现所有操作的稳定性。这些特性为木马程序长期、稳定且隐秘地获取新 C&C 指令提供了技术支撑。

以 2025 年活跃度极高的 Kimwolf 僵尸网络家族为例,其部分版本借助 EtherHiding 技术引入以太坊域名服务（ENS）域名，将 C&C 地址隐藏在“lol”文本记录中。木马程序获取该记录后，截取地址后 4 字节并执行异或运算，最终解析出真实 C&C 服务器 IP。从技术本质来看，ENS 是一套部署于以太坊区块

链的智能合约系统，Kimwolf 正是通过该合约构建了类似云端配置 C&C 的通信渠道——即便原有 C&C IP 被溯源处置，攻击者仅需更新“lol”文本记录，即可快速下发新的 C&C 地址。更关键的是，该通信渠道依托区块链去中心化特性，不受以太坊及其他区块链运营方监管，且难以被技术手段阻断。

无独有偶，2024 年披露的 Smargaft[①]僵尸网络家族，同样通过滥用币安智能合约实现 C&C 托管。其木马程序采用 JSON 格式数据与控制端交互，通过无需支付手续费的 eth_call 调用方式，依托特定合约地址调用合约方法获取最新 C&C 信息。在通过智能合约获取 C&C 指令时，该家族特意引入“latest”字段——该字段始终指向区块链的最新区块状态。这种方式使得木马进一步提升了 C&C 通信的隐蔽性。

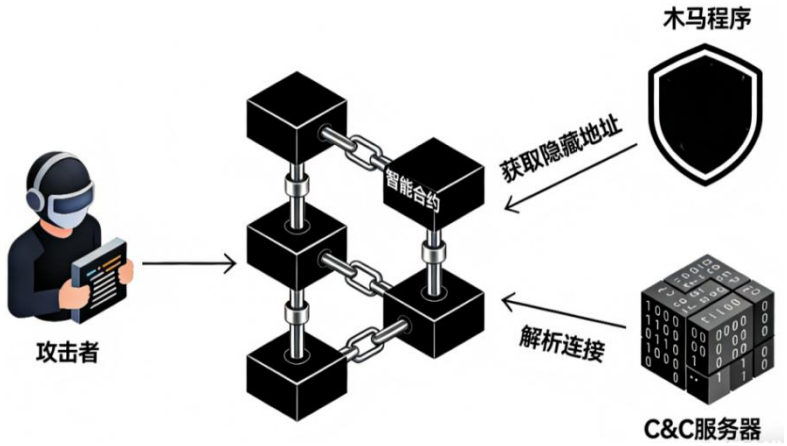


图 3.2　通过区块链托管 C&C

## 3.3　攻击源深度隐匿技术演进

近年来，以 KekSec、“Poxiao”为代表的多个僵尸网络团伙，在已有传统 DDoS 攻击功能的基础上，进一步集成了反射放大攻击能力。2024 年，僵尸网络犯罪团伙 KekSec[②]新增运营一款新型僵尸网络家族，绿盟科技伏影实验室将其命名为 HAEDBot。该恶意软件内置“ADNS”控制指令，可驱使受控主机集群发起 DNS Flood 反射放大攻击。受控主机先从远程恶意服务器下载包含海量开放 DNS 服务器地址的 DNS.txt 列表文件，随后向列表中的 DNS 服务器发送伪造目标 IP 地址的域名查询请求。由于 DNS 协议响应报文体积远大于请求报文，且服务器响应流量会定向涌向伪造的目标 IP，最终形成规模化反射放大攻击效果。这类攻击因其攻击链路的间接性与多层跳转特性，极大地增加了溯源取证的复杂度。反射放大技术的引

① https://blog.xlab.qianxin.com/smargaft_abusing_binance-smart-contracts_cn/

② https://www.freebuf.com/articles/database/264049.html

入，已成为僵尸网络反追踪体系中一项关键的技术演进，使得攻击源的真实位置被深度隐匿，防御方在识别和阻断攻击时面临更大挑战。

```
result = listFork();
if ( result )
{
  v5 = a1;
  v6 = *a1;
  v7 = a1[1];
  v8 = a1[2];
  v2 = time(0);
  v3 = getpid();
  srandom(v2 ^ v3);
  v9 = v8 + time(0);
  while ( time(0) < v9 )
  {
    v10 = fopen("DNS.txt", (int)"r");
    while ( fgets(v4, 100, v10) )
    {
      v4[strcspn(v4, "\r\n")] = 0;
      dns_send(v6, v7, v4, "pixnet.net");
    }
    fclose(v10);
  }
  exit(0);
}
return result;
}
```

图 3.3 DNS 反射放大攻击

## 3.4 攻击流量的深度特征隐匿

绿盟科技伏影实验室于 2025 年披露的 HTTPBot 僵尸网络[①]的出现，标志着攻击流量的深度特征隐匿技术达到了新的高度。该网络的核心突破在于，其发起的应用层 DDoS 攻击流量在特征层面实现了与正常业务流量的深度融合。它并非仅仅通过随机化 User-Agent、Referer 或 URL 路径等动态混淆技术来绕过静态规则检测，更关键的是实现了对浏览器引擎的调用与会话逻辑的完整模拟。其技术实现主要体现在以下几个层面：

真实浏览器环境调用：HTTPBot 内置了 BrowserAttack 和 CookieAttack 等攻击方式。这些方式会启动一个 Chrome 浏览器进程，并令其在窗口隐藏模式下运行。通过这个真实的浏览器引擎发起 HTTP 请求，使得攻击流量的协议栈指纹、TLS 握手特征、HTTP/2 支持等底层细节与真实用户浏览器完全一致，彻底规避了基于协议实现完整性的检测。

[①] 详见绿盟科技威胁情报微信公众号文章《Windows 生态高危预警：新型僵尸网络家族 HTTPBot 正在大肆扩张》

完整的会话状态保持：以 HttpAutoAttack 和 PostAttack 方式为代表，HTTPBot 实现了自动化的 Cookie 管理与回填机制。它能精准解析服务器响应中的 Set-Cookie 字段（如用于防御的 guardret 参数），并在后续的所有请求中自动携带该 Cookie。这模拟了真实用户完整的会话交互过程，使得防护设备基于 Cookie 合法性或会话行为一致性的校验完全失效。

智能化的请求与规避策略：该僵尸网络能根据服务器的响应动态调整攻击行为。例如，当收到 429（Too Many Requests）或 405（Method Not Allowed）等限速或错误状态码时，它会触发精确的 705 毫秒休眠后自动重试，模拟真实用户在遭遇限制后的重试行为。同时，通过动态速率控制，它能避免形成固定的请求频率特征，从而绕过基于速率阈值的告警。

资源消耗的精准化：HttpFpDlAttack 等攻击方式则展现了“手术刀”式的精准打击。它将 TCP Keep-Alive 时间延长至 30 分钟，强制使用 HTTP/2 的多路复用特性，并启用 isSaveResponse 标志要求服务器完整传输响应体。这种攻击不以耗尽网络带宽为目标，而是通过强制服务器维持长连接、处理大文件响应来精准消耗其计算与连接资源，实现“低流量、高杀伤”的效果。

这种“完美隐身”的能力，使得传统基于特征匹配和阈值告警的防护体系几乎失效，将网络攻防的焦点从流量拦截推向了更复杂的“行为识别”与“意图研判”领域。

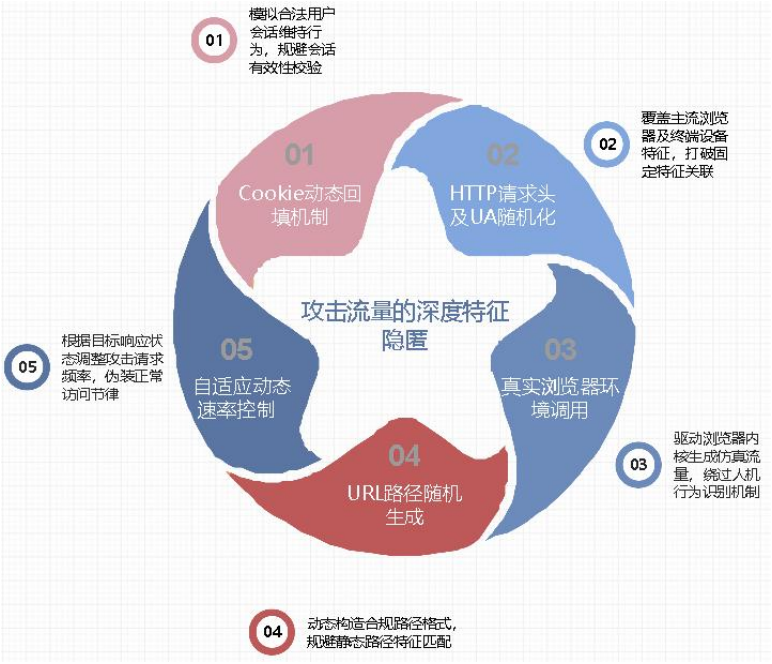


图 3.4 Httpbot 攻击流量特征隐匿

## 3.5 OpenNIC 基础设施的广泛滥用

近年来，基于 OpenNIC 域名体系进行通信的僵尸网络逐步增多。RapperBot 和 Hailbot 在 2025 年持续活跃于多起重大 DDoS 攻击事件，包括年初针对我国高性能 AI 模型平台 DeepSeek 的持续性攻击。这两个家族具备高度的对抗能力：持续迭代使用多种自定义加密算法，并集成 OpenNIC 域名体系作为其 C&C 通信基础设施。OpenNIC 是一个独立于 ICANN 的替代性域名系统，运营着“.dyn”、“.pirate”等自有顶级域。与传统域名依赖公共 DNS（如 8.8.8.8）不同，OpenNIC 域名必须使用其专用的解析服务器才能访问，这种“封闭性”恰好被僵尸网络所利用——C&C 服务器藏身于常规 DNS 监测视野之外，显著降低了被溯源和接管的风险。不过，依赖志愿者运行的服务节点也带来了解析效率和稳定性的天然短板，因此攻击者往往将其与 ICANN 域名搭配使用，在隐蔽性与可靠性之间寻求平衡。

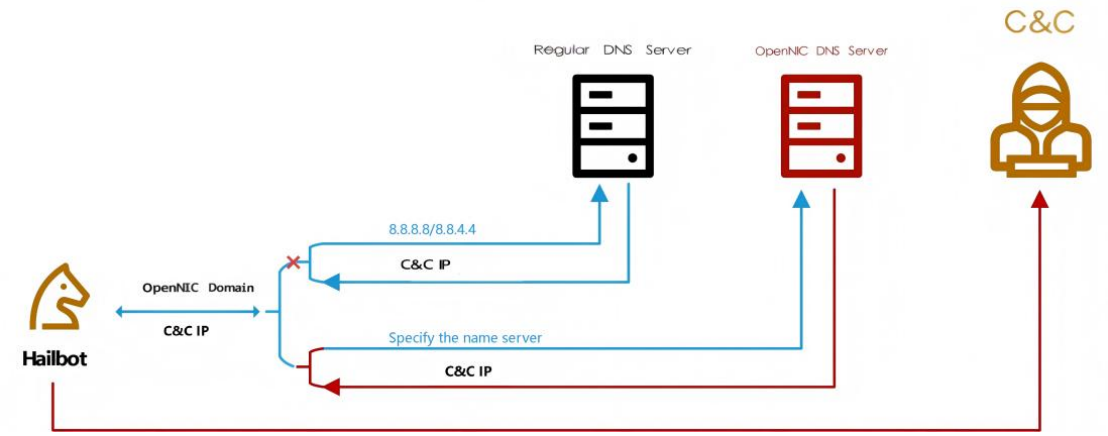


图 3.5 OpenNIC 通信

## 3.6 利用 DNS-over-TLS 增强通信隐蔽性

2025 年 10 月，安全社区披露了一款名为 Kimwolf[①]的新型僵尸网络家族，绿盟科技伏影实验室对其展开了跟踪分析。该僵尸网络以 Android 电视盒子为主要感染目标，凭借多维度隐蔽技术实现大规模传播，展现出极强的网络渗透与对抗能力。Kimwolf 将 DNS-over-TLS（DoT）协议作为核心通信封装方式，有效规避了传统基于明文 DNS 流量的检测与溯源机制，成为其长期潜伏的关键技术支撑。

① https://blog.xlab.qianxin.com/kimwolf-botnet/

DNS-over-TLS（DoT）是一种基于传输层安全（TLS）协议对 DNS 查询与响应流量进行加密封装的标准化技术，默认运行于 TCP 853 端口。与传统明文 DNS 协议不同，DoT 通过在 DNS 解析过程中建立了端到端 TLS 加密隧道，对传输过程中的域名查询内容、响应数据进行全程加密，同时验证通信双方身份，既能抵御窃听、篡改、中间人攻击等传统威胁，又能隐藏 DNS 流量的核心特征。其设计初衷是保护用户网络隐私与 DNS 解析安全性，但被 Kimwolf 类僵尸网络滥用后，可将 C&C 域名解析过程加密传输，难以被识别与拦截。

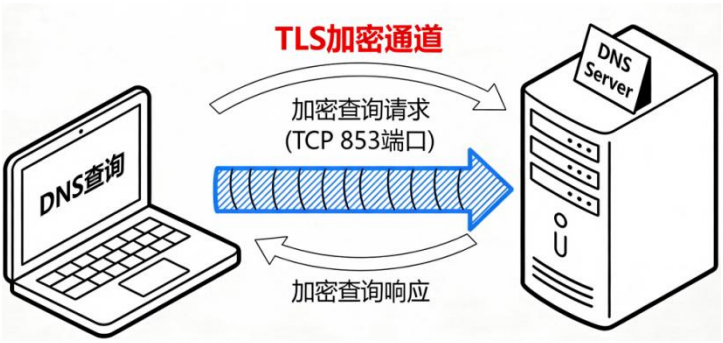


图 3.6 DoT 通信

## 3.7 加密 DNS 请求以规避检测

攻击者通过自定义 DNS TXT 记录格式、加密传输数据的方式构建隐蔽通信通道，规避传统安全设备对 DNS 流量的特征检测与内容审计。DNS TXT 记录本身用于存储域名相关的文本信息，其格式无强制统一标准，可由客户端自主定义解析逻辑，这种灵活性被恶意程序家族针对性滥用，且因流量伪装为常规 DNS 查询响应，具备极强的隐蔽性。

RapperBot[①]僵尸网络 2025 年的一类变种（伏影实验室内部监测）便是典型案例，其创新性采用基于 DNS TXT 记录的版本控制机制，通过动态调整记录格式实现集群管控与抗检测。在其早期版本中，该僵尸网络仅支持以尖括号（< >）作为分隔符的 TXT 记录解析规则，将待传输的 IP 地址等核心数据嵌入尖括号分隔段中，客户端获取记录后按预设规则提取解析。而在后续迭代版本中，攻击者将分隔符切换为竖杠（|），重构了 TXT 记录的数据组织结构，使得只有最新版本的木马才能获取到真实 ip，通过这种

[①]https://cn-sec.com/archives/1159008.html

方式强制旧版本程序失效。这种动态格式调整策略，既能避免固定格式被安全设备提炼特征库拦截，又能快速清理可能暴露的旧版本集群，降低溯源风险。

无独有偶，chachatea 木马家族（伏影实验室命名）则通过“分片-加密-传输-解密”的完整链路，基于 DNS TXT 记录实现真实解析 ip 的隐匿。在具体实现中，该木马会先将域名绑定的 ip 执行 Base64 编码及加密处理，Bot 端接收 TXT 记录后，先经解码与解密还原为原始数据块，最后按分片顺序组装整合获取到最终解析到的 IP 地址，完成整个通信流程。

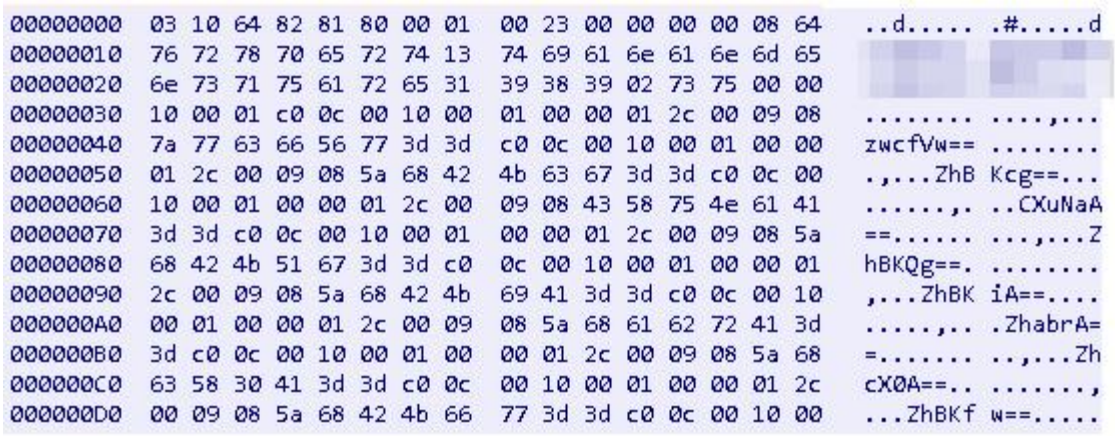


图 3.7 加密的 DNS txt 记录

此类基于 DNS TXT 记录的加密规避手段难以被直接发现及阻断，自定义格式与加密处理又使得安全设备无法通过明文特征、固定格式匹配识别恶意内容。同时，不同家族的差异化实现逻辑（版本控制、分片加密），进一步增加了特征提取与检测拦截的难度，成为恶意程序长期潜伏、稳定通信的重要技术路径。

## 3.8 僵尸节点“取证式”自保与排他方案

为牢牢掌控受感染节点、抢占网络资源，僵尸网络愈发侧重通过“针对性打压竞争对手”强化存活能力，Archbot（伏影实验室命名）便是典型代表。2025 年 7 月，绿盟科技伏影实验室监测并命名了这款新型僵尸网络家族，其核心亮点在于内置多重对抗及竞争手段，创新采用类安全防护人员的取证式检测方案，以查杀其他恶意软件，从路径、文件、内容及行为多维度研判进程，结合评分机制精准识别竞争恶意程序，同时规避安全软件与分析工具干扰，构建极强的节点排他性控制权。

Archbot 的取证式查杀逻辑通过扫描系统进程目录获取全部运行进程，开展“进程取证排查”，如同安全防护人员梳理系统进程以定位恶意程序，同时主动规避初始化进程、自身及父进程，确保排查焦点完全集中在竞争恶意软件及其他威胁进程上，避免误操作影响自身稳定性。

在进程识别与终止环节，Archbot 采用分层检测策略，完全复刻安全防护的精准研判思路，核心依托评分机制锁定竞争恶意软件。快速检测环节如同安全工具的特征匹配，通过进程名、命令行参数及自定义恶意特征，快速识别已知竞争程序并即时终止，提升查杀效率；深度检测则是取证式查杀的核心，借鉴安全人员多维度溯源思路，结合进程可执行文件路径、命令行参数及父进程信息综合赋分，评分超阈值即判定为竞争恶意软件并清理，弥补快速检测的盲区；搭配黑名单匹配机制进一步精准定位预设竞争对手，形成“快速识别+深度评分+黑名单兜底”的三层查杀闭环。

```
snprintf(v2, 512, "/proc/%s/status", (const char *)(v14 + 11));
v20 = fopen(v2, "r");
if ( v20 )
{
  while ( fgets(v7, 256, v20) )
  {
    if ( !strncmp(v7, "PPid:", 5) )// 提取父进程PPID
    {
      sscanf((int)v8, "%d", &v9);
      break;
    }
  }
  fclose(v20);
}
v21 = score_process(v14 + 11, v4, v3, v19, v9, &v6, 256);
```

图 3.8 评分机制

Archbot 的自保护与排他性机制，核心是将安全防护人员的取证检测思路吸收到恶意竞争中，以查杀同类恶意软件为核心目标，评分机制则成为其精准识别竞争对手的关键手段。这种“模仿安全防护、针对性打压竞品”的双重设计，不仅大幅提升了自身存活周期，更能独占感染节点资源，凸显了新型僵尸网络在同类竞争中“以彼之道还施彼身”的进化趋势。

## 3.9 针对供应链的僵尸网络渗透

供应链渗透成为僵尸网络实现大规模批量感染的高效路径，攻击者跳过终端设备逐一突破的传统模式，转而瞄准设备厂商的核心服务节点，通过篡改合法升级渠道推送恶意程序，实现“一击即中、批量获机”的攻击效果，其隐蔽性与破坏力远超常规渗透方式。AISURU 僵尸网络便深谙此道，通过入侵设备

厂商固件升级服务器、伪造官方更新的手段，成功批量感染 Totolink 路由器，构建起规模庞大的肉鸡集群，凸显此类供应链攻击的严重危害。

安全社区披露信息显示，2025 年 4 月，名为 Tom 的攻击者（AISURU 僵尸网络团伙成员）成功入侵 Totolink 品牌的一台路由器固件升级服务器，核心攻击操作在于篡改固件升级的默认 URL 指向，将其替换为恶意脚本的下载地址。由于路由器设备默认信任官方升级渠道，且多数用户会开启自动升级功能或主动执行官方推送的升级操作，使得这一篡改行为形成了“被动式批量感染链路”——每台设备升级时自动执行恶意脚本，无需攻击者实时介入或其他漏洞利用即可被木马感染，从而快速加入 AISURU 僵尸网络集群。这种借助官方信任背书的渗透方式，既规避了终端设备的安全防护拦截，又能在短时间内收割大量潜在肉鸡，大幅降低感染成本、提升扩散效率。


图 3.9 入侵固件升级服务器

AISURU 僵尸网络的供应链渗透案例，核心危害在于利用了设备厂商与用户之间的信任关系，将合法升级渠道异化为恶意传播载体，实现肉鸡资源的规模化获取。相较于传统终端渗透，此类方式覆盖范围更广、感染效率更高，且攻击痕迹更隐蔽，难以被单终端用户或厂商早期察觉，一旦成功入侵核心升级服务器，可能引发数万甚至数十万设备集体沦陷。这种攻击模式不仅会损害设备厂商的品牌信誉，更会为后续 DDoS 攻击、数据窃取等恶意行为提供庞大的资源支撑，其潜在危害不容小觑，已成为僵尸网络规模化扩张的重要趋势。

## 3.10 合法工具被滥用于攻击实施

攻击者在构建恶意攻击链路时，除了对网络协议进行篡改封装外，还常针对性滥用各类合法工具与公共服务，借助其通用性与信任属性实现攻击目标。这种策略既能规避自研工具的开发成本与暴露风险，又能将恶意行为伪装为常规网络操作，大幅提升攻击隐蔽性。

2025 年 6 月，绿盟科技伏影实验室通过全球威胁狩猎系统，监测到一个基于 Go 语言全新开发的僵尸网络家族，将其命名为 Hpingbot[①]。该家族展现出鲜明的技术独特性，区别于传统僵尸网络对开源恶意代码的复用，其完全从零构建，作者具备极强的创新能力与资源整合意识，核心攻击链路便依赖 Pastebin 在线平台与 hping3 网络工具的滥用，实现了攻击成本与隐蔽性的双重优化。

```
{
  exec_Cmd *v9; // rax

  v9 = (exec_Cmd *)os_exec_Command(
                     (unsigned int)"apt -y install hping3 && apt -y install screen",
                     46,
                     0,
                     0,
                     0,
                     a6,
                     a7,
                     a8,
                     a9);
  return os_exec__ptr_Cmd_Start(v9).tab;
```

图 3.10 木马安装 hping3

在 Windows 平台上，攻击者滥用合法工具进行攻击已成为一种普遍且隐蔽的战术。以“银狐”系列木马为例，其多个变种展现了该手法的典型路径：攻击者会直接购买或篡改具有合法数字签名的商业远程控制软件，例如 ScreenConnect、超级眼等。此外，许多企业正常使用的内部远程运维、资产管理工具如阳途、固信等，也为攻击者提供了“即取即用”的基础设施。攻击者通过私有化部署方式，将这些工具脱离企业中央管理节点，并静默安装到目标计算机上，便能将其转化为一个稳定、可靠且几乎无法被察觉的“合法木马”。这种利用“白”身份掩盖“黑”行为的策略，极大地增加了防御和检测的难度。

为增强对抗能力，“银狐”木马积极借助第三方软件或组件，其近年来最显著的策略之一是滥用存在设计缺陷的第三方驱动程序，以此实现对抗乃至终止安全软件进程等高权限操作。部分驱动程序在设计上存在安全疏漏，例如对调用场景的限制不够严格，或缺乏对调用者身份及执行内容的充分校验。攻击者通过逆向分析，能够掌握这些驱动的核心功能，进而以合法之名行恶意之实，利用这些带有合法数

[①] 详见绿盟科技威胁情报微信公众号文章《hpingbot：基于 Pastebin 载荷投递链与 hping3 DDoS 模块的新型僵尸网络家族》

字签名的驱动程序在系统内核层面执行恶意操作，从而绕过用户态安全软件的监控与拦截。此外，该木马还利用微软 WDAC 特性攻击安全软件，在系统关键目录（如 %WinDir%\System32\Code Integrity\）下释放一个名为 SiPolicy.p7b 的文件。该文件实质上是 Windows Defender 应用程序控制（WDAC） 的安全策略文件。通过篡改此策略内容，攻击者能够直接影响 Windows Defender 等安全组件的策略配置。

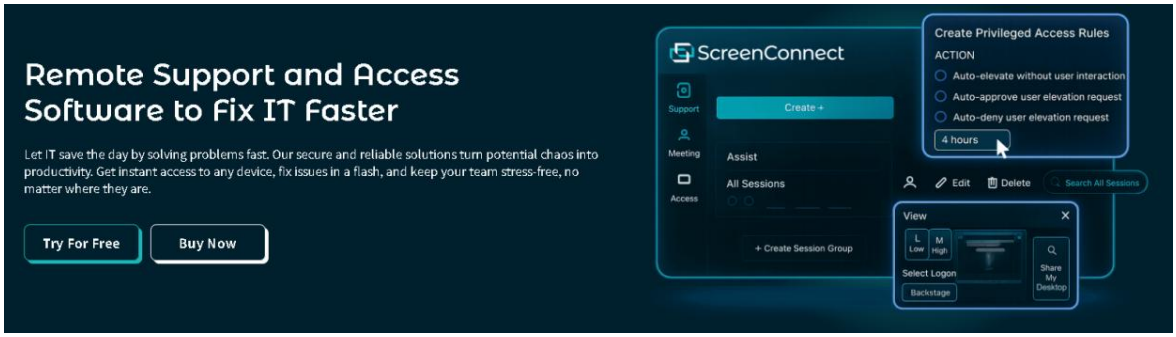


图 3.11 ScreenConnect

除了滥用驱动程序外，“银狐”木马还频繁采用一种更为隐蔽的攻击路径：篡改合法软件的配置文件以劫持其执行流程。此类攻击通常瞄准那些配置功能丰富、支持通过配置文件执行脚本或命令的应用程序，例如部分游戏的启动器（Launcher）。攻击者通过修改其配置文件（如 config 文件），将恶意代码（脚本或 ShellCode）嵌入预设的配置项中。当用户正常启动该软件时，程序便会依照被篡改的配置，“合法”地加载并执行攻击者预设的恶意功能。.NET 应用程序成为这类手法的理想目标。在默认机制下，.NET 程序会自动加载与其主程序同名的.config 扩展名配置文件（XML 格式）。该文件本用于在不修改代码的情况下调整程序行为。银狐木马利用这一特性，通过精心修改配置文件中的特定节点或指令，能够直接劫持应用程序的初始执行逻辑，引导其在启动时暗中执行恶意代码，从而实现了极高的隐蔽性。

这类攻击的核心在于“工具合法、意图非法”，通过滥用信誉良好的软件或企业内部工具，有效规避了基于特征码或信誉评级的传统检测机制，这种“借船出海”的策略，既规避了自研工具的开发与运营成本，又利用安全设备对合法工具流量的信任豁免，实现了攻击行为的高效隐匿，已成为新型僵尸网络家族优化攻击链路的重要趋势，给威胁检测与溯源工作带来新的挑战。

## 3.11 构造畸形文件绕过查杀

在 Windows 平台，木马为规避检测不断演化出高度复杂的免杀技术。以“银狐”木马为例，除常见的加壳、白加黑、制作超大文件等手法外，还发现部分变种以内存马和无文件攻击形式，围绕“破坏结构可识别性”与“减少恶意实体驻留”来对抗杀软检测。

攻击者会刻意构造结构畸形的 PE（可执行文件）文件。这类文件在严格意义上并非符合规范的 Windows 可执行程序，但其设计精妙之处在于，它能够利用 Windows 系统加载器在解析文件时特定的容错或异常处理机制，通过一些引导从而成功触发恶意代码执行。从防御视角看，此类畸形文件对依赖静态格式分析的杀毒引擎构成显著挑战：引擎可能因其结构错误而将其判定为无效文件并跳过深入分析，也可能在解析时发生错误导致误判，从而使其得以绕过常规检测。

另一种狡猾手法是，将完整的木马载荷进行分片或加密，并以脚本、LNK 快捷方式、命令行指令等为“牵引器”存储于磁盘。在木马启动时，由一个轻量的引导脚本在内存中临时拼装、解密并执行完整载荷，执行完毕后立即清除拼装产生的临时文件。此策略的核心优势在于，极大地缩短了完整恶意文件在磁盘上的驻留时间和形态。安全引擎能够扫描到的，通常只有那些看似无害的引导脚本和分片数据（或加密数据块），其内容多为配置参数或指令，恶意特征极为微弱，从而显著降低了被静态扫描引擎发现的概率。

这些技术表明，攻击者的重点已从单纯隐藏代码内容，通过更底层的对抗文件格式识别与攻击安全产品的分析逻辑本身，制造格式异常与减少可分析样本的存在，显著提高了防御方威胁检测与溯源的难度。

# 04

# 僵尸网络威胁全景与态势分析

2025 年，全球僵尸网络生态持续演进，攻击链条愈发成熟，呈现出漏洞集成加速化、传播精准化与可控性提升、攻击活动高频化及控制架构地域集中化等显著特征。本章基于绿盟科技伏影实验室全球威胁狩猎系统监测数据，从漏洞利用与传播态势、攻击感染活动特征两大核心维度展开深度剖析。

# 4.1 漏洞利用与传播态势

## 4.1.1 漏洞集成加速与传播精准化

2025 年度，Linux/IoT 平台僵尸网络仍以漏洞利用与弱口令破解为核心传播路径，而 Windows 平台则以社会工程学与钓鱼攻击相结合的方式主导传播。相较于 Linux/IoT 平台，Windows 安全防护措施更为成熟，借助已知漏洞直接大规模感染目标的实施难度显著提升，促使攻击者维持传统方式，通过搭建伪造钓鱼页面、批量分发垃圾邮件及社交软件定向扩散等方式实施精准攻击。

从特征来看，2025 年度僵尸网络漏洞利用呈现两大显著趋势。一方面，老旧漏洞利用频次居高不下，典型如 CVE-2021-36260、CVE-2017-7921 等。这侧面印证了当前 IoT 设备安全防护体系建设的滞后性，即便攻击者利用陈旧漏洞，仍可轻松突破现有防线。另一方面，新兴高危漏洞持续涌现，其利用速度显著提升。以 React2Shell 高危漏洞（CVE-2025-55182）为例，该漏洞公开披露后仅数天，便被 NutsBot 僵尸网络团伙武器化并投入实战，凸显了新型漏洞被快速转化为攻击武器的严峻态势。2025 年度僵尸网络使用漏洞情况如下：

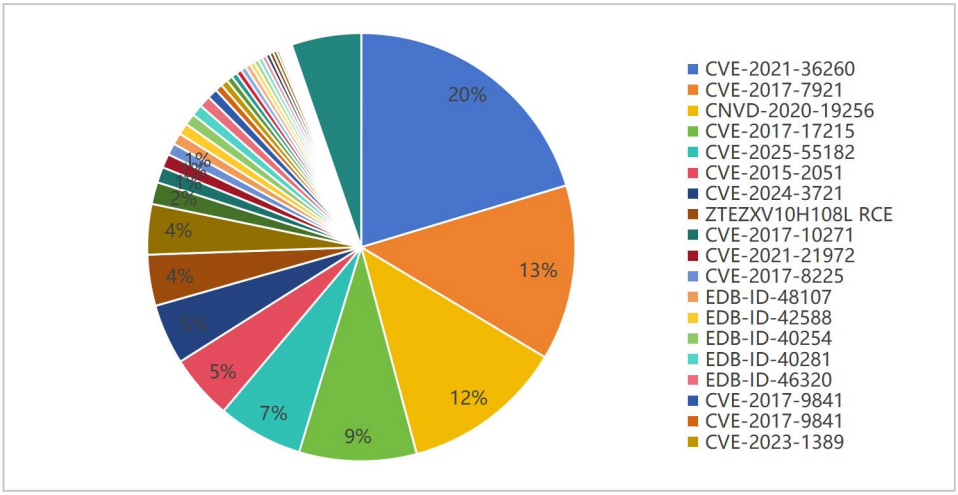


图 4.1 漏洞占比

此外，攻击者对传播可控性的重视程度持续提升，具体体现为扫描阶段精准划定攻击范围、针对特定设备类型及系统版本实施定向投递等精细化操作，进一步提升了攻击的隐蔽性与成功率。攻击者的漏洞集成策略呈现出明显的工具化分离趋势，即采用独立传播工具实现漏洞利用模块与木马本体的解耦。该策略不仅强化了核心恶意代码与攻击逻辑的保密性，更显著提升了攻击传播的可控性。

### 4.1.2 传播源区域性集中

2025 年度，绿盟科技伏影实验室依托全球威胁狩猎系统监测数据分析发现，僵尸网络下马地址在全球分布呈现显著的区域集中性。从地理分布来看，美国以 25%的占比居于首位，德国（19%）与荷兰（12%）紧随其后，三者合计覆盖了整体观测量的半数以上。该分布态势并非偶然，其背后反映出互联网基础设施发展水平、区域联网规模及当地网络安全监管力度等多重因素的复杂交互影响。互联网普及率高、数字化基础设施成熟的地区，往往为僵尸网络的快速扩散提供了技术基础与潜在目标；与此同时，这些地区在网络安全立法、跨境协同治理等方面的监管差异，也直接影响了恶意活动的活跃程度与地理分布。

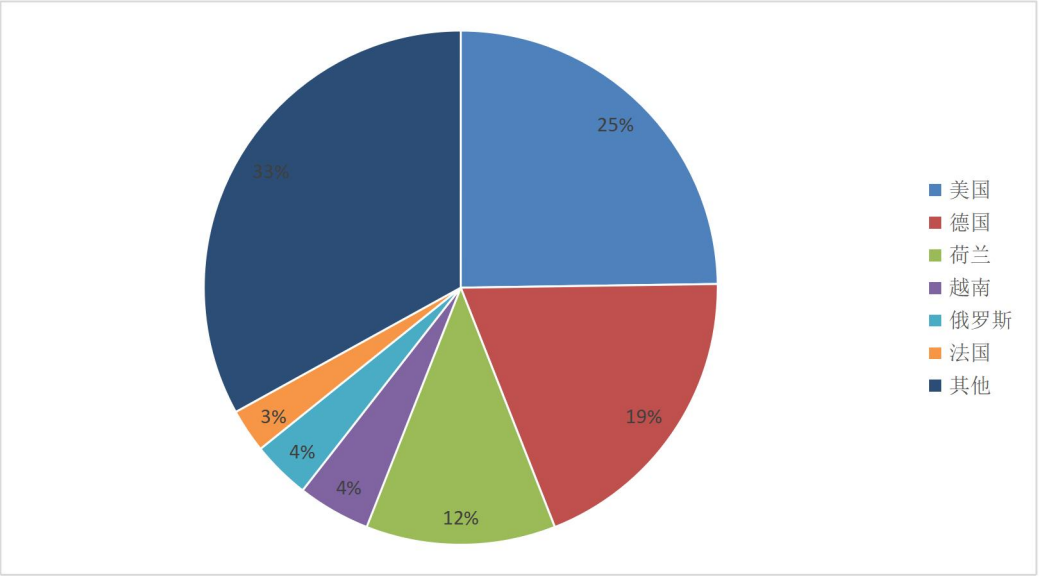


图 4.2 下马地址分布

# 4.2 僵尸网络攻击活动分析

## 4.2.1 国内面临的僵尸网络攻击态势严峻

2025 年度，绿盟科技伏影实验室通过全球威胁狩猎系统持续监测发现，全年高频度对外发起攻击活动的僵尸网络家族及其变种数量超过 30 个，攻击活动呈现持续化、多样化态势。监测数据显示，在攻击指令的下发量上，各家族分布高度集中：XorDDoS 家族以 48%的占比占据绝对主导地位；紧随其后的是长期活跃的 Mirai 家族，占比 32%；Hailbot 家族位列第三，占比 12%。三者合计覆盖了绝大部分已观测的恶意指令流量。

此外，以 HttpBot、NutsBot 为代表的新兴家族表现活跃，其攻击频率与影响范围呈现明显上升趋势，持续对暴露在互联网上的脆弱设备发起攻击，反映出僵尸网络生态在持续演进中不断涌现新的威胁力量。

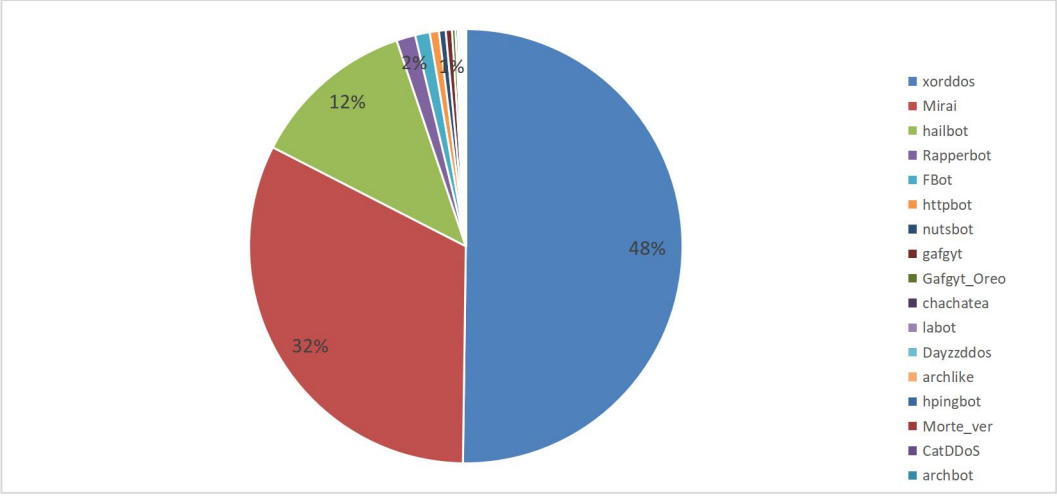


图 4.3 各家族下发指令数占比

从受害者地理位置分布来看，本次监测到的网络攻击活动覆盖全球超过 130 个国家和地区，呈现明显的全球化渗透特征。其中，中国境内遭受的攻击最为严重，占总攻击量的 40%，显示出其作为关键数字基础设施集中地区所面临的高强度威胁态势。其余主要受害地区包括美国（19%）、巴林（16%）、荷兰（4%）与新加坡（2%），这些地区在全球化连接程度、数字经济规模或区域网络枢纽功能等方面具有显著共性，这在一定程度上解释了其为何持续成为网络攻击的主要流向地。该分布格局不仅反映出攻击者在目标选择上的战略倾向，也凸显了相关国家和地区在数字化进程中面临的严峻网络安全挑战。

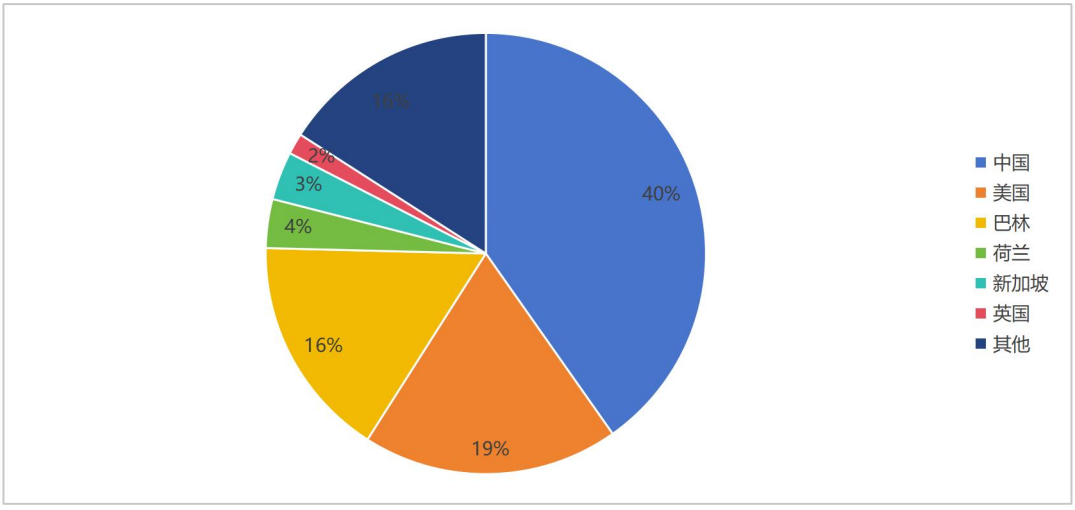


图 4.4 受害者地理位置分布

国内受害者呈现显著的区域聚集特征，主要集中在香港、北京、浙江、广东、上海等地区。这一分布特征的形成，主要源于多重因素的叠加作用：这些地区数字基础设施密集、高价值目标集中，服务器、物联网终端等设备为僵尸网络提供了充足攻击靶点，且作为互联网骨干枢纽，庞大流量便于黑客隐藏攻击行为，加之攻防对抗集中，使得遭受攻击情况更为突出。

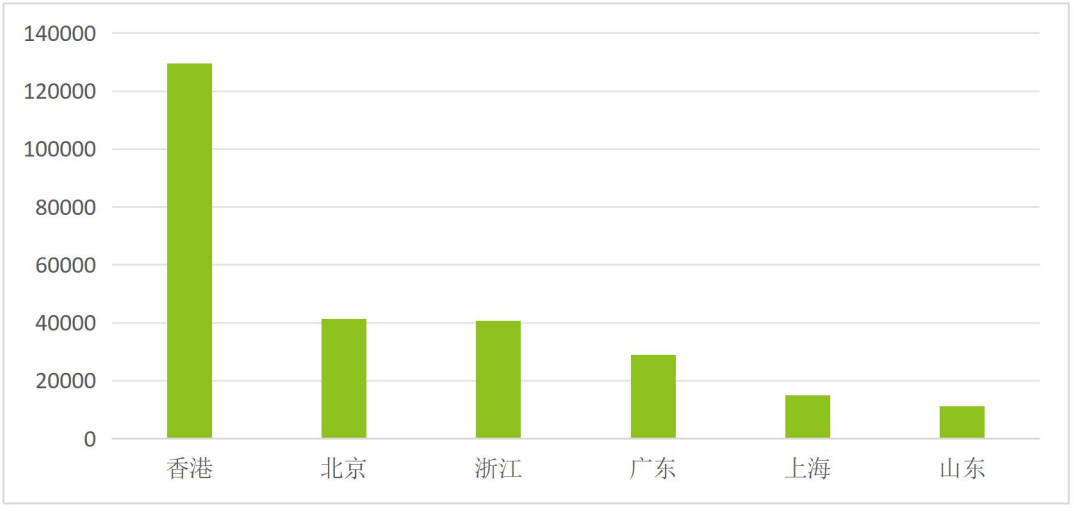


图 4.5 国内遭受攻击情况

## 4.2.2 控制地址主要分布在美国

2025 年度，绿盟科技伏影实验室全球威胁狩猎系统累计监测到 7000+僵尸网络控制 C&C，这些 C&C 分属 91 个僵尸网络家族及其变种。其中 Mirai 及其变种控制 C&C 数量最多，33%的新增 C&C 均由该家族控制，其次为 Hailbot（7%）、Gafgyt（4%）和 Morte（4%）。XORDDOS、TSUNAMI、billgates 等老牌僵尸网络家族依旧活跃。此外，虽然 mozi 依然存在较大规模的传播量，但由于攻击者已被逮捕，并未发起实际攻击活动，其仍在稳定传播主要源自 P2P 网络的稳定性。

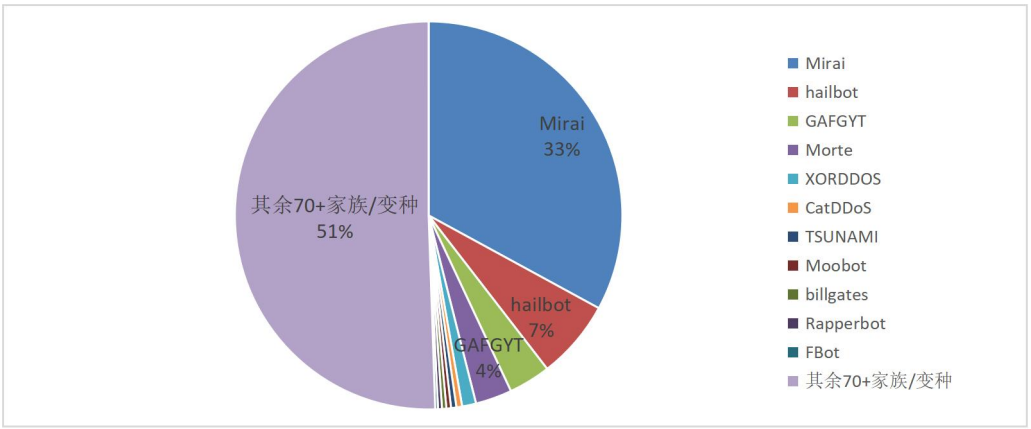


图 4.6 各家族控制 C&C 数量占比

上述僵尸网络控制的 C&C 主要集中在美国，核心原因在于其成熟的黑产生态适配僵尸网络传播需求，加之跨州监管差异与匿名技术滥用，降低了 C&C 暴露与溯源风险，美国的基础设施、生态环境与监管特点，共同构成了僵尸网络 C&C 集中部署的最优场景。

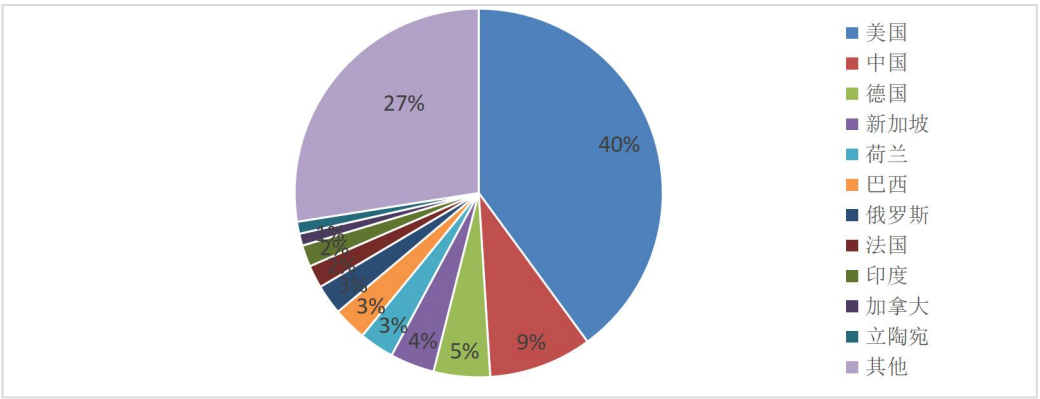


图 4.7 C&C 地理位置分布

# 05

# 未来展望

2026 年僵尸网络的角色将从单纯的攻击工具，演变为融合了情报搜集、渗透控制、金融犯罪、地缘政治工具于一体的综合性网络威胁平台。威胁全面升级，将朝着“持久化、隐蔽化、智能化和武器化”的方向演进。

**AI 攻防螺旋加速：**攻击方将更深度地利用生成式 AI，参与漏洞挖掘、高度个性化的钓鱼攻击载荷生成等攻击全链路。

**“基础设施化”与隐匿性革命：**代理型僵尸网络（如 ContainerBot）将完成从“攻击工具”到“犯罪互联网核心基础设施”的转变。结合区块链、OpenNIC 域名等去中心化技术管理 C&C，使传统的 IOC 追踪和资产封禁手段面临失效危机。

**移动端威胁成为“超级入口”：**以 Android 大屏设备（电视、机顶盒）为代表的移动端僵尸网络（如 Kimwolf）规模将持续膨胀。攻击者看重的不仅是其海量数量和不安全现状，更在于其作为家庭网络中枢的地位。

**DDoS 攻击的“服务化”与“场景定制化”：**类似于 Poxiao 团伙提供的“DDoS 攻击方式”及 httpbot 的针对性攻击将更加丰富和精细。攻击者可根据目标行业（如金融、游戏、AI 服务）的业务逻辑，提供定制化的“事务性攻击”，旨在以最小流量造成最大业务中断，并实现攻击效果的“按需购买”。

**地缘政治网络行动的“掩护”与“杠杆”：**具有国家背景的 APT 组织可能更多地租用或操控黑灰产僵尸网络基础设施，以增强其行动的隐蔽性和可否认性。同时，针对关键基础设施（如电网、水务）的僵尸网络潜伏与破坏，可能成为地缘政治博弈中非对称的威胁杠杆。

# 附录 A：新兴僵尸网络家族简介

| 家族名 | 特点/攻击活动 |
| --- | --- |
| PumaBot | 该家族在 2025 年极为活跃，具备挖矿能力，发起 SSH 扫描时会从服务端获取待扫描目标的 ip 列表。 |
| RapperBot | 由绿盟科技伏影实验室于 2022 年首次对外公开披露， 2025 年年初参与针对我国首个高性能开源 AI 大模型 DeepSeek 的攻击活动。 |
| Hailbot | 由绿盟科技伏影实验室于 2023 年首次对外公开披露，2025 年年初参与针对我国首个高性能开源 AI 大模型 DeepSeek 的攻击活动。 |
| Pickai | 2025 年披露的后门型僵尸网络家族，曾通过 ComfyUI 漏洞传播。 |
| AIRASHI | 2024 年 8 月份参与针对我国首款 3A 游戏《黑神话：悟空》的攻击。 |
| Vo1d | 2025 年极为活跃，以 Android 电视为主要传播目标，是一个下载器。 |
| Gayfemboy | 2024 年至 2025 年期间较为活跃的一个新家族，持续更迭版本，2025 年 5 月份再次升级版本，使用包括四信工业路由 0day 漏洞的诸多漏洞传播。 |
| gorillabot | 由绿盟科技伏影实验室于 2024 年首次对外公开披露，该家族在 2024 年 9 月 4 日至 9 月 27 日期间下发 30 余万条攻击指令，攻击密度之高令人震惊。 |
| TBOT | 2024 年初安全社区披露的一个超大分组型僵尸网络家族。 |
| Boat | 由绿盟科技伏影实验室于 2022 年 6 月份首次公开披露，其 ripper 变种近年来极为活跃。 |
| XorBot | 由绿盟科技伏影实验室于 2024 年首次对外公开披露,近年来多次升级版本,其控制者创建 Telegram 组群对外宣传。 |
| HTTPBot | 2025 年 4 月，由绿盟科技伏影实验室披露，其内置攻击模块均针对 HTTP 协议设计，HTTPBot 跳出传统流量型攻击（带宽消耗导向）的框架，专门研发系列 HTTP 协议攻击载荷，聚焦发起事务消耗性 DDoS 攻击。 |
| Dayzzddos | 2025 年 7 月，由绿盟科技联合网络安全联创中心首次公开披露，该家族定制化开发专门针对我国目标发起攻击，模块化设计，内置多种 DDoS 攻击方式。 |
| Nutsbot | 2025 年年底，由国家互联网应急中心（CNCERT）与绿盟科技伏影实验室共同披露，NutsBot 是一款新型僵尸网络家族，该家族不仅继承了 传统 DDoS 攻击能力，还集成了信息窃取、远程命令执行、 挖矿牟利等多重功能，并通过动态基础设施、复杂认证协议 及多种反检测技术，展现出较强的隐蔽性、抗干扰能力和持 续演进特征。 |
| Kimwolf | 2025 年，安全社区陆续披露了 Kimwolf 家族，该家族主要针对 Android 平台的新兴僵尸网络家族。这些家族控制的设备规模庞大，具备发动大规模网络攻击的能力，潜在破坏力不容小觑。值得关注的是，Kimwolf 僵尸网络与长期活跃于 Linux/IoT 平台的 Aisuru 僵尸网络存在明确关联，二者由同一攻击团伙运营操控。 |

| | |
|---|---|
| PolarEdge | 2025 年以来较为活跃的一类代理型僵尸网络家族。 |
| Merte | 2025 年以来较为活跃的一类基于 Mirai 源代码修改而来的僵尸网络家族。 |
| Archbot | 2025 年，绿盟科技伏影实验室内部监测到的一个以雄迈设备为核心目标的新型僵尸网络家族。 |
| Fnone | 2025 年，绿盟科技伏影实验室内部监测到的一个以海康威视摄像头为核心目标的新型僵尸网络家族。 |
| IRC_Tor | 2025 年，绿盟科技伏影实验室内部监测到的一个结合了 IRC 与 Tor 协议进行通信的新型僵尸网络家族。 |
| HAEDBot | 2024 年，绿盟科技伏影实验室内部监测到的一个 KekSec 新增运营的僵尸网络家族，内置 DNS 反射放大攻击在内的多种 DDoS 攻击方式。 |
| Hpingbot | 2025 年 7 月份，由绿盟科技伏影实验室首次对外公开披露，该家族基于 Pastebin 载荷投递链并利用 hping3 发起 DDoS 攻击。 |
| ContainerBot | 2025 年，绿盟科技伏影实验室内部监测到的一个代理型僵尸网络家族，释放出 100+个代理组件，进行流量转发。 |
| Tsundere | Windows 平台僵尸网络，2025 年中开始活跃，利用游戏诱饵及基于以太坊的命令与控制服务器在 Windows 平台进行扩张。 |
| BadBox2.0 | 2025 年较为活跃的 Android 平台僵尸网络家族，一旦设备被感染，便会成为僵尸网络的一部分。攻击者利用这些设备作为“住宅代理”，将非法流量伪装成家庭用户发起，从而掩盖真实身份。除用于广告欺诈和分布式拒绝服务（DDoS）攻击外，还可进行凭据填充（用于盗取账户）、拦截金融验证短信，甚至远程执行任意命令。 |
| RondoDox | 2025 年较为活跃的一类僵尸网络，主要针对路由器、DVR、NVR 系统等互联网暴露设备。该僵尸网络采用“漏洞霰弹枪”攻击模式，同时尝试利用多个漏洞。 |

# 附录 B：新兴僵尸网络团伙简介

| 团伙名 | 特点攻击活动 |
| --- | --- |
| Hail 团伙 | Hailbot 的实际控制者，近年来，Hail 团伙控制的僵尸网络家族 Hailbot 攻击活动异常频繁，其控制的 C&C 数量极多，2025 年年初参与针对我国首个高性能开源 AI 大模型 DeepSeek 的攻击活动。 |
| KekSec 团伙 | 持续活跃，近年来，绿盟科技伏影实验室依托全球威胁狩猎系统监测到 KekSec 团伙新增运营了两个僵尸网络家族 hbot 和 HAEDBot。 |
| Bigpanzi 团伙 | 该组织已经活跃了数年，主要通过盗版应用程序和固件更新来感染基于 Android 系统的电视和流媒体设备。 |
| CatDDoS 团伙 | 2024 年以来，CatDDoS 僵尸网络衍生出诸多变种，其背后的团伙活跃异常。 |
| “Poxiao”僵尸网络团伙 | 绿盟科技伏影实验室于 2025 年内部监测到的一个新型僵尸网络攻击团伙，运营多个僵尸网络家族，擅长使用各类反射放大攻击。 |
| “luotuoxiangzi”挖矿团伙 | 2025 年以来较为活跃的一个挖矿团伙，其命名源自其惯用的域名。与传统蠕虫不同的是，Luotuoxiangzi 并不自带爆破密码的字典，也不随机生成攻击目标，而是从中心服务器下载爆破字典和目标列表，实现“分布式爆破”；目标列表每次都会变化，字典也会定时更新，让攻击更灵活、更强大。 |
| Rapper 僵尸网络团伙 | RapperBot 的控制者，由绿盟科技伏影实验室于 2022 年首次对外公开披露， 2025 年年初参与针对我国首个高性能开源 AI 大模型 DeepSeek 的攻击活动。于 2025 年 8 月 6 日被捕。 |
| 银狐系列团伙 | 近年来极为活跃，通过社交工具+即时通信软件钓鱼的方式传播，早期以国内政企及个人主机为主要目标，近年来逐步拓展至海外市场，印度等新兴市场成为重点渗透区域 |
| 黑猫团伙 | 2025 年较为活跃的一个僵尸网络家族，该团伙将包含钓鱼软件的恶意网站推送到搜索结果前列，并诱导搜索引擎错误地将部分钓鱼网站标注为“官方”，极大地增强了其欺骗性。用户在访问这些高排名或带有“官方”标签的钓鱼页面后，极有可能会下载捆绑恶意程序的安装包。一旦运行安装，该程序会在用户不知情的情况下植入远程控制木马，导致设备被攻击者控制。 |
| AISURU 僵尸网络团伙 | AIRASHI 僵尸网络及 Kimwolf 等家族的控制者，近年来极为活跃，具备较强的政治倾向，擅长使用各类变形算法对通信内容进行加密。 |
| Ares 黑客团伙 | 该团伙在 2025 年较为活跃，运营 kaiji、Mirai、Moobot 及 Lucifer 在内的多个僵尸网络家族，拥有一个数量庞大的僵尸网络并且提供租赁服务，下发 XMRig 进行挖矿作业。 |
| ATA 团伙 | 绿盟科技伏影实验室于 2023 年披露的僵尸网络攻击团伙，是 Xorddos 的核心运营者之一，攻击活动大部分集中在国内，在 2025 年极为活跃。 |
| frosted | 绿盟科技伏影实验室于 2022 年披露的僵尸网络攻击团伙，该团伙的攻击资源均位于境外，国内仅存在少量受感染的机器，攻击目标以欧美国家为主。售卖木马、出租肉鸡、接单、DDoS 勒索是僵尸网络团伙常见的四种获利手段，该团伙当下业务仍然以通过提供接口租售所持有资源为主。 |

NSFOCUS


# THE EXPERT BEHIND GIANTS

## 巨 人 背 后 的 专 家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、金融、运营商、能源、交通、科教文卫等行业用户和各类型企业用户，
提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS

# THE EXPERT BEHIND GIANTS

# 巨人背后的专家

**多年以来，绿盟科技致力于安全攻防的研究，**
**为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。**
**在这些巨人的背后，他们是备受信赖的专家。**


总部：北京市海淀区北洼路4号院绿盟科技园
绿盟科技（股票代码300369）

**邮编：**100089

**电话：**010-68438880

**传真：**010-68437328

**邮箱：**webadmin@nsfocus.com

www.nsfocus.com

扫描绿盟科技官方二维码
可在手机端直接观看报告电子书