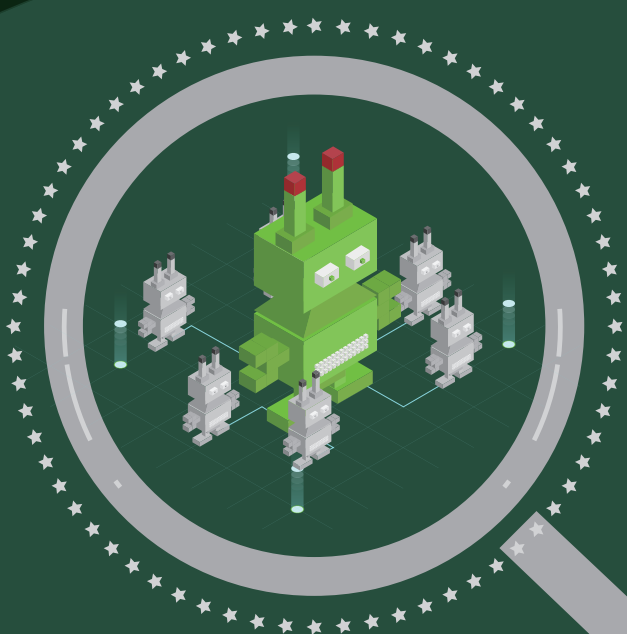
NSFOCUS

绿盟科技2022年度 BOTNET趋势报告



关于绿盟科技

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。

伏影实验室
NSFOCUSFUYING LAB

研究目标包括 Botnet、APT 高级威胁，DDoS 对抗，WEB 对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁及新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。

版权声明

NSFOCUS

CONTENTS

执行摘要

2022 年，各黑产组织争相逐利及世界政治经济格局的不稳定性，导致网络攻击活动持续激增。这些虚拟世界的冲突严重影响了网络安全，并对现实世界构成威胁。以 DDoS 为主的僵尸网络攻击所引发的安全事件屡见不鲜，并且开始向更多关键基础设施蔓延。无论是黑产组织之间的攻伐，俄罗斯和乌克兰的网络战争，还是国内的健康宝攻击事件，都有僵尸网络的参与。

伏影实验室研究发现，僵尸网络的运营策略和方式与之前相比出现较大变化。

僵尸网络团伙加大挖矿资源投入。受数字加密货币价格波动的影响，部分僵尸网络攻击团伙通过加大僵尸网络控制范围扩展攻击业务，以维持其收益的稳定性。尽管收益下降，但挖矿之利仍然是许多挖矿组织的主要收入来源，不断下跌的行情会令这些组织加大投入。“KekSec 效应”凸显，各僵尸网络团伙加大自我宣传力度。僵尸网络攻击团伙频繁地利用社交媒体进行宣传，吸引了更多“客户”购买或租赁僵尸网络。这种方式既可以提升团伙的知名度，吸引更多的资源，支撑后续发展，也可以通过聚集效应隐藏其真实身份信息，实现“KekSec 效应”。

隐匿性较强的社交媒体如 Telegram 已成为僵尸网络团伙活动的主要平台。由于该类社交媒体隐匿性强，在达成交易的情况下更有利于隐藏攻击者的真实身份信息。越来越多的攻击团伙通过此种途径进行僵尸网络相关的交易活动。 租赁服务仍是 DDoS 攻击团伙主要盈利模式。僵尸网络团伙的主要获利手段包括售卖木马、出租肉鸡、接单和 DDoS 勒索等。越来越多的僵尸网络团伙通过租售其所持有攻击资源获利。通过按月办卡，或提供带有相应接口工具的方式进行交易，可在一定程度上实现攻击资源与攻击者真实身份信息隐匿，为溯源分析带来了一定挑战。

伏影实验室认为，除运营策略和方式的变化外，僵尸网络运营者在木马的开发迭代、隐匿行踪、混淆等方面进一步对僵尸网络进行升级迭代。

在开发迭代方面，Go 语言是一种具有出色跨平台能力和交叉编译支持的编程语言，其在僵尸网络构建编程中出色的性能表现深受攻击者喜爱。它的打包机制使文件和函数数量巨大，对杀毒引擎的检测能力带来挑战，这种情况为僵尸网络家族的增长提供了便利条件。

在隐匿行踪方面，新型僵尸网络家族更加倾向于采用 CDN，ICMP 等隧道技术通信，这种趋势与其它类型的木马类似。攻击者在通信隐匿性方面的努力一直没有松懈过。强隐匿性是隧道通信的一大特点，其可在网络中建立一条安全的隧道，使得数据可以安全传输，难以破解。攻击者的攻击行为在隧道的帮助下更加隐蔽，能更好地避开安全系统的检测，从而达到保护信息安全的目的。在混淆迷惑方面，攻击者在构建新的僵尸网络家族时会使用已知家族的部分代码。由于这类僵尸网络主要攻击 IoT 设备，其能否被杀毒软件检测并不重要。通过使用已知家族代码，可对杀毒软件引擎进行欺骗，使杀毒软件误以为其为已知恶意程序，降低受害者方对其的重视程度与其被人工分析的概率。在应对 0day 等重量级武器测试时，攻击者也可以利用这种方式有效地隐藏自己，与构建 0 检测的全新家族相比，这种方法更不容易引人注意。

01

2022 年僵尸网络威胁全景

1.1 C&C 变化与黑产需求正相关

2022 年，伏影实验室威胁监控平台 BotHunter 监测数据显示，Mirai、Gafgyt 等热门家族的 C&C 主要活跃时段在一个月左右；少数 C&C 可以活跃两个月；只有数量极少的 C&C 具有两个月以上活跃度。特别地，虽然相比 Mirai、Gafgyt 等主流 IoT 家族，xorddos 的 cnc 总数较少，但其 cnc 中活跃时间超过 3 个月的却更多，具有更长的活跃周期。Mirai、Gafgyt 和 Gh0st 家族的代码均已开源，其使用者众多，而 XorDDoS 作为闭源家族，其 C&C 受小范围群体控制，是产生上述差异性的重要原因。

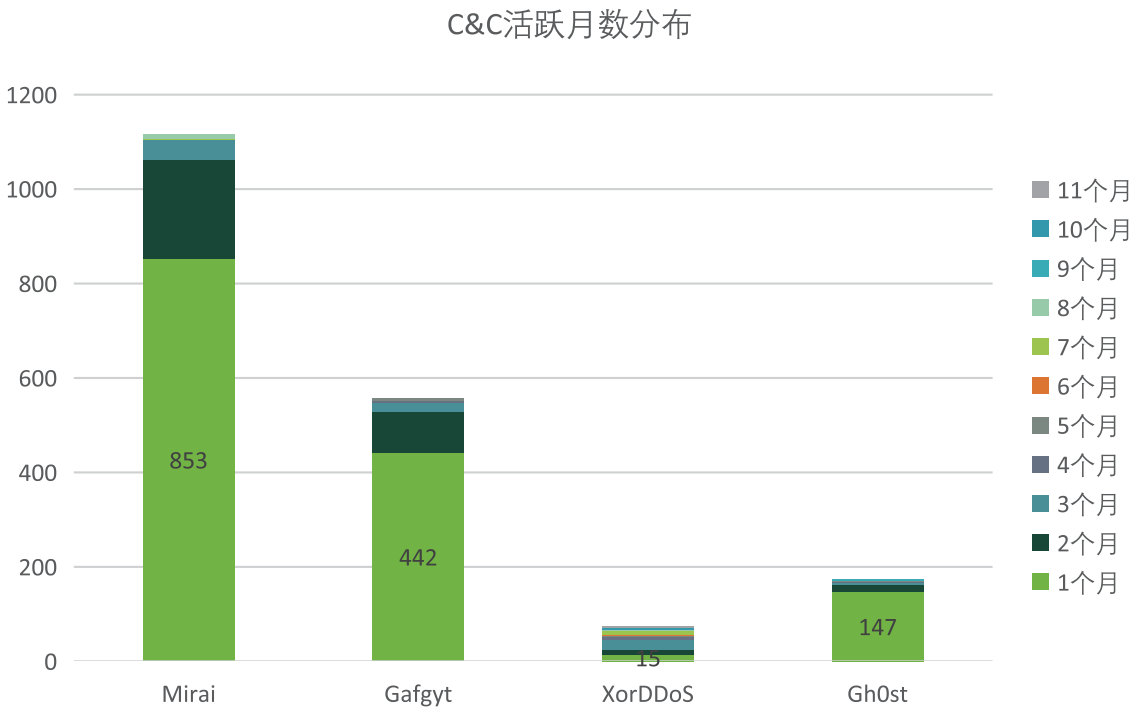


图 1.1 部分热门僵尸网络家族 C&C 月度变化图

Mirai、Gafgyt 等热门僵尸网络家族 C&C 数量的上升期集中在 4~7 月，并在 6~7 月左右达到峰值，之后开始下降；9-11 月期间，C&C 数量变化相对平缓，无显著波动。其中，Mirai 作为当今热门的头号僵尸网络之一，其月度 C&C 数量最多，每月 C&C 高达 130 个。这些变化与黑产需求存在一定关系。

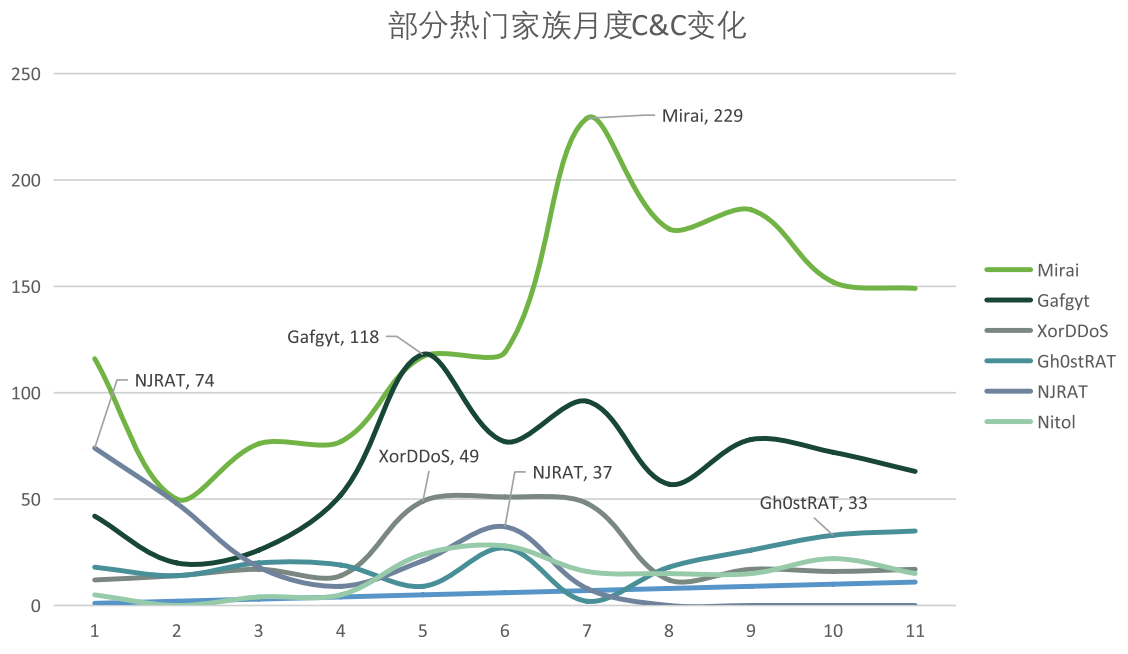


图 1.2　部分热门家族月度 C&C 变化

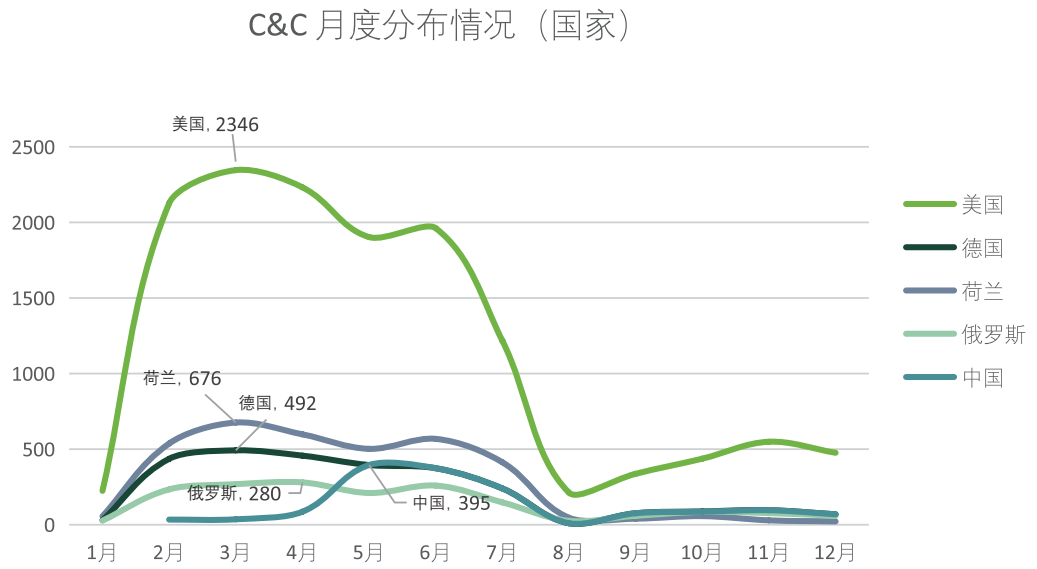


图 1.3　各国 C&C 月度分布

伏影实验室监控的热门家族 C&C 总数超 2000 个，分布在近 55 个国家，其中大部分位于美国，中国、荷兰、德国则紧随其后。从时间点上看，各国的 C&C 均在 5 月份前后达到峰值。这些 C&C 分属在超过 2000 个云服务商 / 运营商中，其中 Digital Ocean、微软云，FranTech，OVH 和 ColorCrossing 成为最受攻击者青睐的云服务商，黑产团伙选择非实名化的云服务提供商更有利于规避法律法规风险。

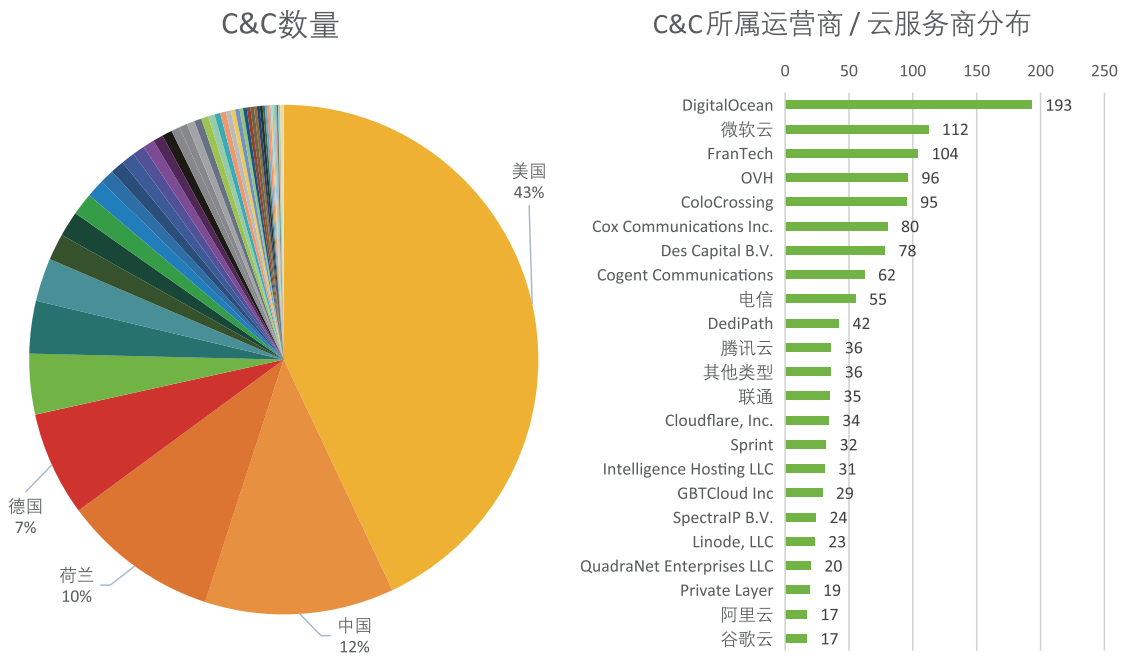


图 1.4　C&C 分布情况

1.2　DDoS 攻击的主要发起者仍为传统类家族

2022 年，伏影实验室威胁监控平台 BotHunter 共监测到 20 个有明显 DDoS 攻击活动的家族，相较于去年新增了 4 个。有 5 个家族较为活跃，分别是 Mirai，XorDDoS，Dofloo，Gafgyt 以及 Nitol。其中，Mirai 家族的攻击指令和攻击事件数在今年的 DDoS 攻击活动中占比最大。此外，Bothunter 在今年监控到了 XorDDoS 家族异常活跃，下发了大量的攻击指令，分析后发现 XorDDoS 家族会集中对目标进行攻击，具有极高的协同性和一致性，我们分析认为，该家族由单一控制者运营。

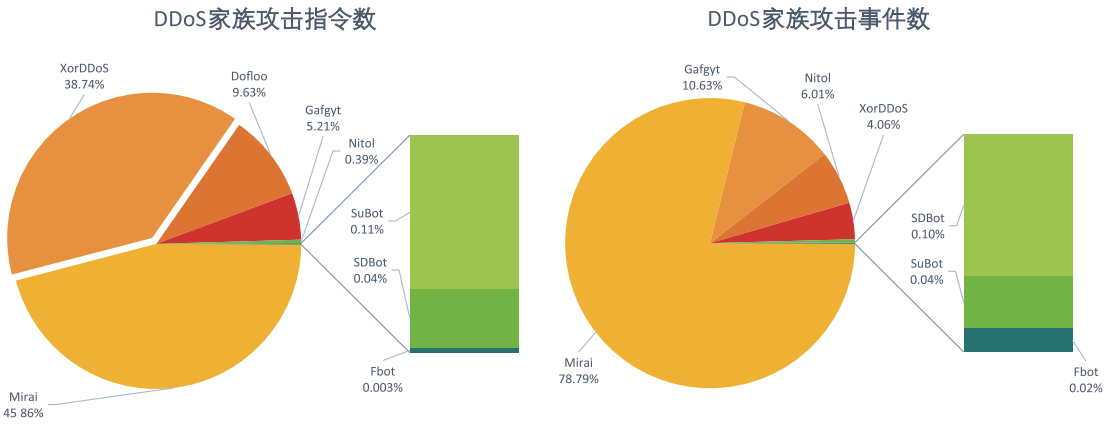


图 1.5　各 DDoS 家族攻击指令和攻击事件占比图

BotHunter 监测到逾五十万条 DDoS 攻击指令数以及超过五万起攻击事件。不同家族的攻击指令数和攻击事件数均呈现一定的波动趋势。XorDDoS 和 Mirai 的攻击指令在 6~8 月迎来一波高峰。例如某国内 IP - 103.91.*.*，仅在 6 月底至 7 月初几日内就持续受到超过 3700 条 DDoS 指令的攻击，经查该 IP 曾作为游戏私服使用，而私服恰为 DDoS 肆虐的一类重点目标。

在此基础上，我们统计了各活跃 DDoS 家族在针对单个目标时下发攻击指令的最大持续时间（下发指令间隔不超过 10 分钟，则算持续），其中 Mirai 的最长持续攻击时间达到近 6 天；其次是 XorDDoS，最长连续攻击时间近 1 天。

表 1.1　DDoS 家族针对单个目标的最长连续攻击时间

DDoS 家族	针对单个目标时下发攻击指令的最大持续时间
Mirai	8518 min
XorDDoS	1410 min
Gafgyt	890 min
Dofloo	721 min

攻击类型上，SYN_Flood (44.23%) 和 UDP_Flood（29.87%）占比最多。相比与去年，CC 攻击占比明显下降。

攻击目标上，上述活跃 DDoS 家族针对的攻击目标数量逾 61200 个，主要分布在美国、中国、德国和英国等国。

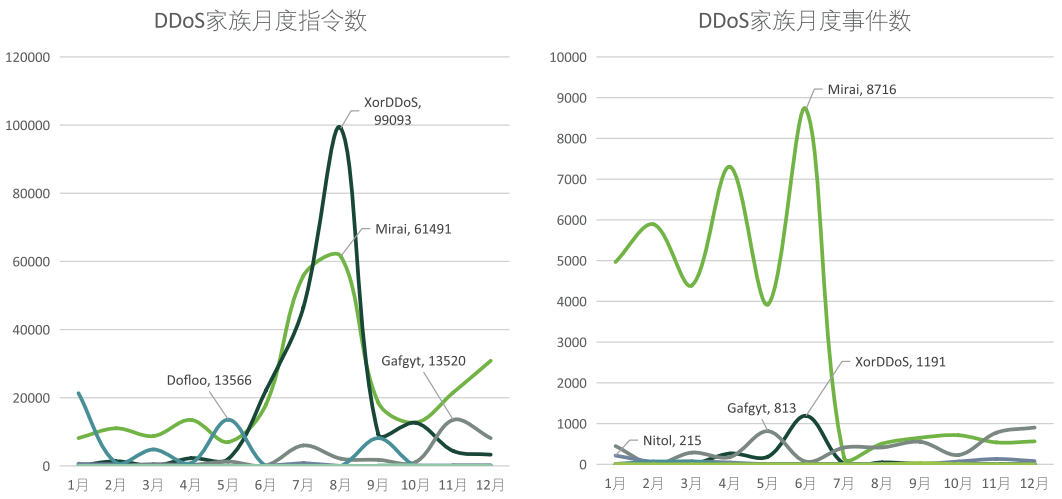


图 1.6　DDoS 家族攻击指令及攻击事件月度变化图

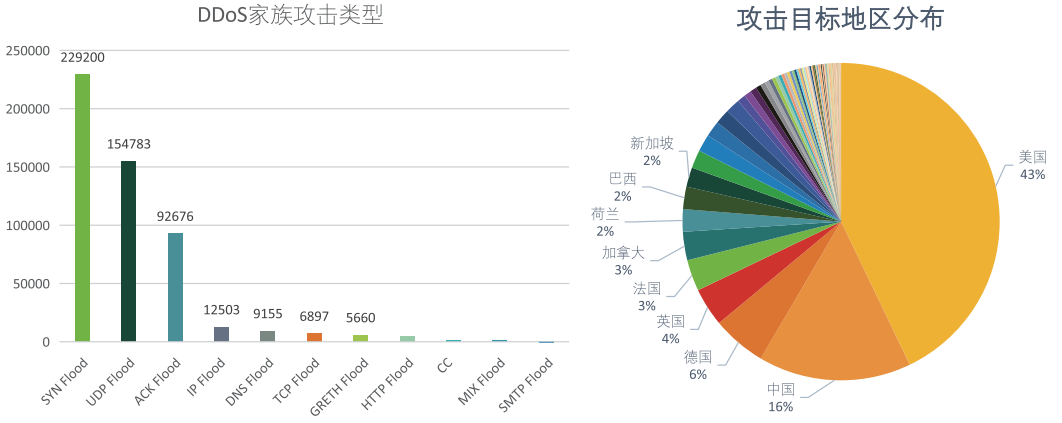


图 1.7　攻击目标分布

美国，中国，德国在内的大多数国家所受到的 DDoS 攻击事件多由 Mirai 和 Gafgyt 发起。而在本年度攻击指令数激增的 XoRDDoS 攻击目标主要集中在国内的北京，广州，深圳等经济较为发达城市。

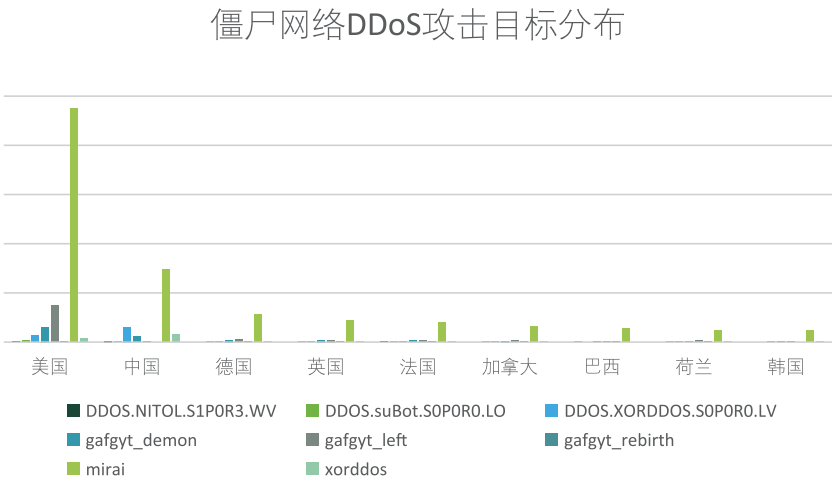


图 1.8　僵尸网络 DDoS 攻击目标分布

1.3　感染设备分布情况与政策执行息息相关

按照家族统计，XorDDos 和 Mirai 及其变种所控制的机器数量最多，分别占比达 49% 和 37%，活动频繁的 Dofloo 和 Gafgyt 及其变种，以及基于 Gafgyt 和 Mirai 源码混合修改而来的 HybridMQ 等家族所控制机器数占比在 2% 上下。

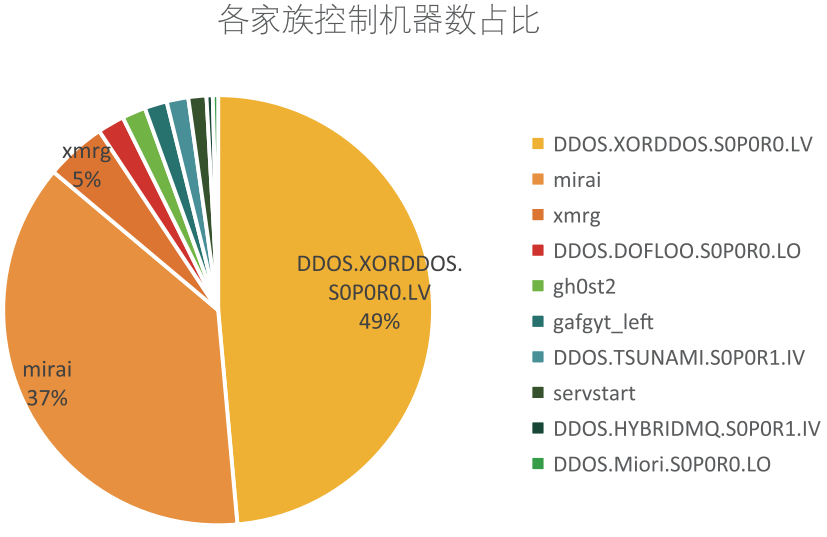


图 1.9　各家族控制设备数

根据Mirai，Gafgyt 在内的 61 个活跃度较高的僵尸网络家族所控机器数量的月度统计结果，各家族所控制的受感染机器总数在 7 月份达到顶峰，之后得益于相关执法部门的有效治理，受感染机器数量呈下降态势，其中，单个家族情况与总体相符。

图 1.10　各家族受感染设备数按月度统计

1.4　传播节点分布区域性集中

根据监测数据，国内传播节点数最多，占比达 48%，其次为美国，俄罗斯和巴西，分别占比 6%、5% 和 4%。传播节点数的分布一方面取决于整体网络安全环境，取决于是否及时修补网络环境中存在的大量漏洞，另一方面也与服务提供商的监管力度存在着关联。

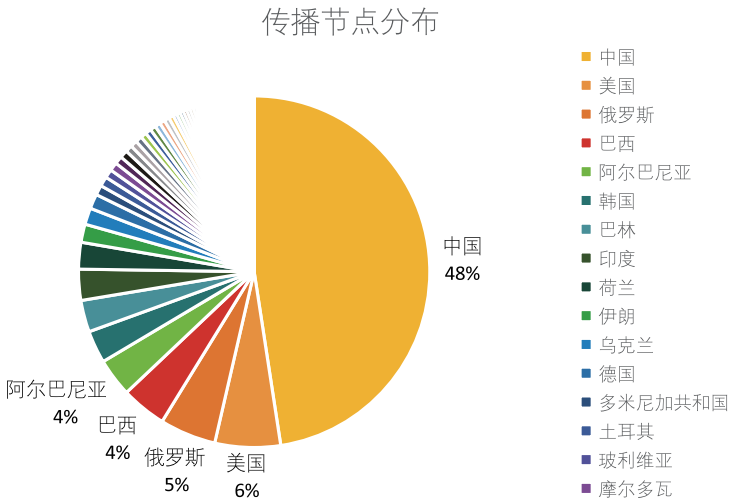


图 1.11　传播节点区域分布

1.5 弱口令、漏洞利用仍是 IoT 类僵尸网络主要入侵方式

本年度及以往观察数据显示，僵尸网络的入侵方式多种多样。实际过程中，攻击者基于目标平台环境及攻击目的的不同，使用了不同的入侵方式，包括但不限于以下手段：

- 弱口令：IoT 设备用户很少修改初始用户名和口令，导致弱口令成为重大风险。
- 设备及软件漏洞：IoT 设备由于功能需要，往往包含网络连接、应用服务等多种技术，而 IoT 厂商众多，技术水平和设备质量参差不齐，导致 IoT 设备也存在不同程度的安全风险甚至安全漏洞。

本年度观察数据显示，IoT 平台僵尸网络仍然以弱口令暴破、漏洞利用为主要入侵传播方式。此外，僵尸网络木马程序还借助已经成型的僵尸网络，利用已有的僵尸主机，使用同样方式进行入侵，从而达到快速发展壮大的目的。而 Windows 平台僵尸网络木马程序则经常通过网络钓鱼电子邮件进入系统，也会通过带毒激活工具进行传播，常被用来推广病毒和流氓软件。

1.6 新型漏洞利用的热度进一步增强

本年度， IoT 环境仍是各类漏洞利用的重灾区。

绿盟科技伏影实验室物联网威胁情报平台统计发现，本年度 IoT 僵尸网络漏洞利用整体分布情况与往年相似，各家族木马携带和利用最多的漏洞分别是：

CVE-2017-17215（华为 HG532 家庭网关设备上的命令注入漏洞）

CVE-2014-8361（Realtek rtl81xx 系列网卡远程代码执行漏洞）

CVE-2018-10561（GPON 光纤路由器漏洞）

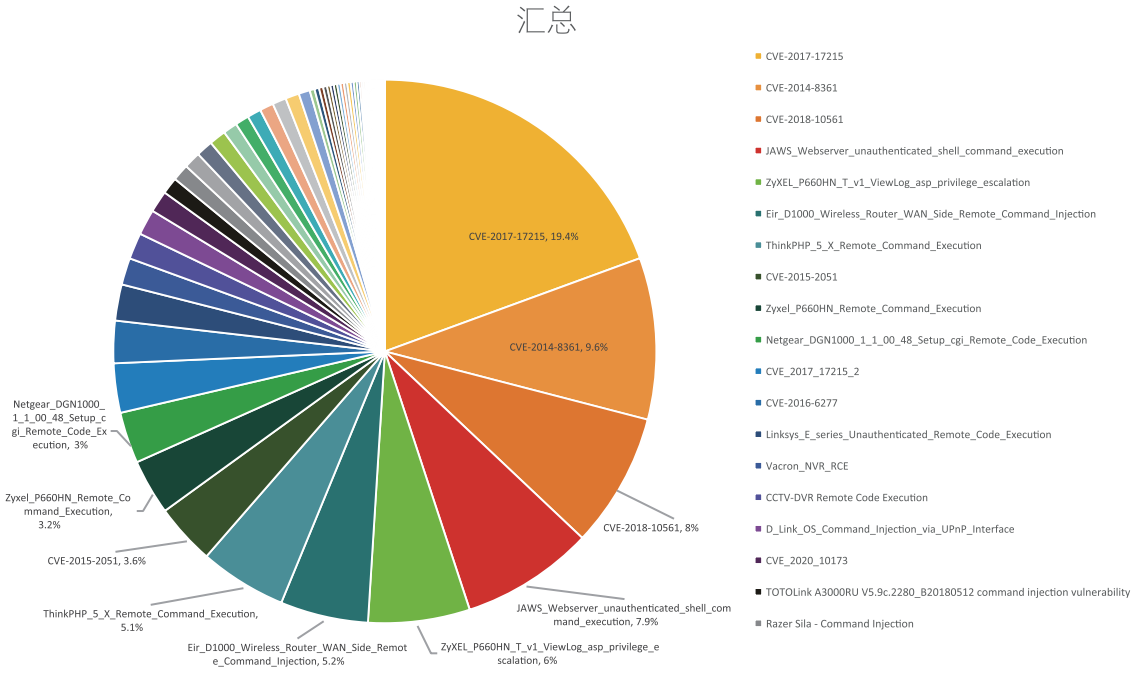


图 1.12　2022 年 IoT 漏洞统计

IoT 平台木马所携漏洞杀伤力强，年代跨度较大，这主要源于 IoT 设备在更新和维护方面的延迟性。此外，由于 IoT 木马运营门槛较低且竞争激烈，导致其运营者竞相争抢失陷主机节点，迫使漏洞利用转化周期越来越短。本年度被大量使用的新增漏洞如下表：

表 1.2　2022 年 BOTNET 新增漏洞表

漏洞	受影响服务或设备
CVE-2022-22947	Spring Cloud Gateway 3.1.0,3.0.0-3.0.6
CVE-2022-22954	VMware Workspace ONE Access 和 Identity Manager
CVE-2022-1388	F5 BIG-IP 多个版本
Adobe ColdFusion 11 - LDAP Java Object Deserialization Remote Code Execution	Adobe ColdFusion 11
Dbltek GoIP - Local File Inclusion	Dbltek GoIP
Razer Sila - Command Injection	Razer Sila
Scriptcase 9.7 - Remote Code Execution	Scriptcase 9.7
TOTOLink A3000RU V5.9c.2280_B20180512 command injection vulnerability	TOTOLink A3000RU
WordPress Plugin cab-fare-calculator 1.0.3 - Local File Inclusion	WordPress Plugin cab-fare-calculator 1.0.3
WordPress Plugin video-synchro-pdf 1.7.4 - Local File Inclusion	WordPress Plugin video-synchro-pdf 1.7.4

02

新型僵尸网络团伙

本年度，绿盟科技伏影实验室依托全球威胁狩猎系统发现了六个新型僵尸网络攻击团伙，包括：“L33T”，“Frosted”，“落叶飞花”，“第一楼”，“维塔斯”以及“Tigger”DDoS 攻击团伙。

表 2.1　2022 年新型僵尸网络团伙发现情况

团伙名称	发现时间	典型特征
“落叶飞花”僵尸网络攻击团伙	2022 年 1 月	多次使用“luoyefeihua.site”作为其服务器基础设施
“L33T”僵尸网络攻击团伙	2022 年 9 月	习惯于入侵时留下签名信息“daddyL33T's back”
“Frosted”僵尸网络攻击团伙	2022 年 9 月	习惯于在样本中留下“You Can Find Me At FrostedFlakes666 on Google”的组织信息
“第一楼”DDoS 攻击团伙	2022 年 10 月	又称“红豆”DDoS 攻击团伙，长期通过 Telegram 租售所持有资源。
“维塔斯”僵尸网络攻击团伙	2022 年 11 月	长期活动于 Telegram，声称拥有 30-50k 肉鸡
“Tigger”DDoS 攻击团伙	2022 年 11 月	习惯于在 DDoS 攻击活动中留下“Tigger DDoS Group”信息

此外，我们还对包括“KekSec”和“8022“僵尸网络团伙在内的多个已知的僵尸网络攻击团伙进行了深入分析和长期监测。研究发现：

（1）2022 年，“KekSec 效应”显著增强，越来越多的僵尸网络攻击团伙利用社交媒体进行宣传；

（2）隐匿性比较强的社交媒体如 Telegram 已经成为僵尸网络团伙活动的主要平台；

（3）僵尸网络团伙主要通过四种手段获利：售卖木马、出租肉鸡、接单和 DDOS 勒索。在本年度，我们观察到越来越多的僵尸网络团伙通过出租自己拥有的资源来获利。

我们在后续章节中选择了六个具有代表性的僵尸网络攻击团伙，向读者详细展示新型僵尸网络攻击团伙在 2022 年的攻击活动情况。

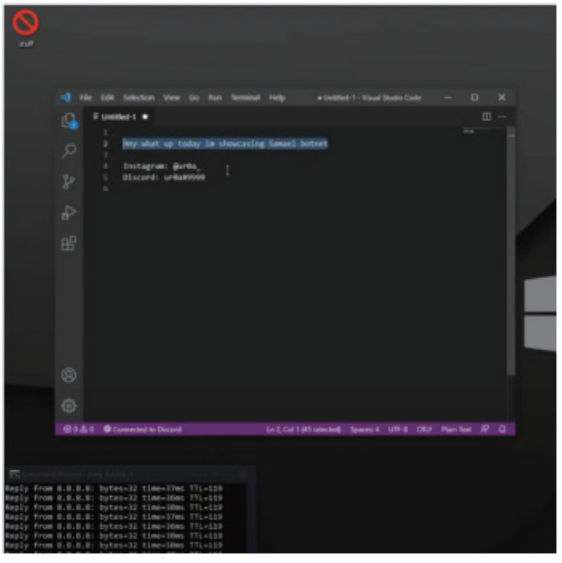
2.1　KekSec

2022 年，KekSec 团伙[1] 的攻击活动愈发频繁，其运营的 EnemyBot，Gafgyt_Tor 及 Necro 不但经历了多次版本更迭，而且出现相同代码片段在多个家族中被复用的情况，例如在 Necro、EnemyBot 及 Gafgyt_Tor 中都存在着 lolfme 代码的影子。此外，KekSec 运营的 lolfme 僵尸网络家族一改既往风格，开始尝试隐藏自身，不再如以往张扬，也更具备了实战

[1]　详见绿盟科技微信公众号文章《剑指物联网安全，揭秘首个物联网攻击组织 -FreakOut of KekSec》

意义，这或与该组织阶段目标的转变有关。经历过去一年的发展，KekSec 已走过宣传时期，开始步入获利阶段。

表 2.2 “KekSec”团伙资产信息

团伙代号	“KekSec”
团伙特征	KekSec 黑客组织成立于 2016 年，是一个非常活跃的黑客组织。该组织主要通过 DDoS 攻击和勒索活动获利，素来高调，常常在入侵设备后留下组织信息以表明身份。今年，该团伙的活动尤为频繁。
涉及家族	lolfme ur0aBot Necro EnemyBot
C&C 基础设施	45.*.*.229 45.*.*83 162.*.*..213 193.*.*.224 156.*.*.244 35.*.*.250
社交信息	KekSec YouTube： 用户名：itz UR0A 

近年来，僵尸网络犯罪团伙逐渐加大社交媒体宣传力度，从“幕后”走向“台前”，并在 2022 年愈发频繁。一方面，这种方式有助于扩大知名度，吸引更多资源，支撑后续发展。另一方面，随着宣传的聚集效应，真实身份信息也能有效隐匿，达成“KekSec 效应”。在宣传的同时，僵尸网络运营者也在不断提升自身实力，长期运营并更新版本，在一定程度上攻击者更舍得投入资源，这值得引起我们的警惕。

2.2 L33T

2022 年 10 月底，绿盟科技伏影实验室联合 CNCERT 物联网威胁研究团队共同披露了“L33T”僵尸网络犯罪团伙[2]。该团伙命名来源于溯源过程中发现的字符串——攻击者在入侵时留下签名信息“daddyL33T's back”，该签名在 2017 年被证实由一个 13 岁少年黑客拥有。“L33T”团伙控制着 Mirai_L33T,Gafgyt_L33T 以及 BOAT_L33T 在内的多个僵尸网络家族，这些家族大部分修改自开源代码，存在泛 Mirai-Gafgyt 的特点，不易与已知家族区分开来。

表 2.3 “L33T”团伙资产信息

团伙代号	“L33T”
团伙特征	散布多种包含“daddyL33T”信息的僵尸网络木马
涉及家族	Gagfyt_L33T Mirai_L33T BOAT_L33T
C&C 基础设施	Gagfyt_L33T： *.*.49 37.*.*.187 31.*.*.162 *.*.2 *.*.217 *.*.233 BOAT_L33T： 45.*.*.114 46.*.*.102 Mirai_L33T： 103.*.*.233
社交信息	YouTube: https://www.YouTube.com/channel/UC870HD8GBg57p6Qn9Vw5AhQ

该团伙从 2021 年 9 月份就开始大规模布局，其基础设施在荷兰，美国，越南等地均有分布，攻击范围涵盖了中国，德国，英国在内 78 个国家和地区，攻击目标包含了游戏，私服，教育网站等行业。在该团伙的操纵下，国内的广东，香港，四川，台湾等地均受到了影响。

其中，L33T 运营的 Mirai_L33T 僵尸网络更是在 2022 年 7 月 29 日至 8 月 22 期间下发了近 5000 条 DDoS 攻击指令，涉及攻击目标 3000 多个，其单日下发指令数最高达到 1000 条以上 , 其活跃度和布局显示该团伙进入黑产行业的野心不小。

[2] 详见绿盟科技微信公众号文章《新型僵尸网络犯罪团伙系列之：“L33T”团伙》

2.3 Frosted

2022 年 10 月初，绿盟科技伏影实验室依托全球威胁狩猎系统发现了一个 DDoS IoT 僵尸网络犯罪团伙，将其命名为“Frosted”[3]，经溯源分析，该团伙于 2017 年开始活跃，至少已有 6 年以上的僵尸网络运营及售卖经历。自 2018 年 10 月份以来，该团伙开始在 Twitter，YouTube 等社交平台宣传及兜售其开发的僵尸网络木马，类型多样。2022 年 10 月份以来该团伙愈发活跃，并公开叫嚣“You Can Find Me At FrostedFlakes666 on Google”，挑衅意味十足。

表 2.4 “Frosted”团伙资产信息

团伙代号	“Frosted”
团伙特征	攻击样本中存在签名“FrostedFlakes666”，运营多个社交账号兜售僵尸网络木马
涉及家族	TerryPanel Botnet（内部标记：Gafgyt_Fro） Darkness Botnet （内部标记：Gafgyt_Fro） Mirai_Fro
C&C 基础设施	5.*.*.118 美国 俄勒冈州 本德 178.*.*.41 德国 萨克森自由州 法尔肯施泰因
社交信息	Twitter: https[:]//twitter.com/frostedflakes29 YouTube: https[:]//www.youtube.com/channel/UC8pJ3-gedaif5tnz7a6x4AQ Discord: https:/t.co/ Nem2R7iMh Telegram:https://t.me/addstickers/FrostyBot

该团伙的攻击资源大都位于国外，国内只有少数受到感染的机器。河北是受影响的严重地区，近一半的失陷主机位于该区域。此外，辽宁、山东和天津等地也受到了影响。大多数失陷主机属于小型企业或黑灰产。运营期间，该团伙发起了针对游戏、私服、代理服务等相关行业的 DDoS 攻击，主要攻击目标为保加利亚和美国等地区。

2.4 落叶飞花

绿盟科技伏影实验室于 2022 年 1 月份首次发现了一个控制着十余类僵尸网络家族，拥有较高自研能力的僵尸网络团伙。鉴于该团伙多次使用“luoyefeihua.site”作为其服务器基础设施，伏影实验室将其命名为“落叶飞花”。该团伙攻击目标以国内为主，欧美地区也有波及，国内受害者中江苏为重灾区，其次是山东，北京，香港等地。

[3] 详见绿盟科技微信公众号文章《新型僵尸网络犯罪团伙系列之二：Frosted》

表 2.5 “落叶飞花”团伙资产信息

<table>
<tr><td>团伙代号</td><td>“落叶飞花”</td></tr>
<tr><td>团伙特征</td><td>多次使用“luoyefeihua.site”作为控制服务器，所运营恶意软件含有中文字符，通过各种社交媒介售卖僵尸网络木马。</td></tr>
<tr><td>涉及家族</td><td>Mediocre（kaiji）
DnsAmp
ServStart
XorDDoS
LanDDoS
BlackMoon</td></tr>
<tr><td>C&C 基础设施</td><td>luoyefeihua.site
linuxddos.net
193.*.*.152
103.*.*.32
103.*.*.155
150.*.*.165</td></tr>
<tr><td>社交信息</td><td>
<table>
<tr><th>账号类型</th><th>账号用户名</th></tr>
<tr><td>腾讯QQ_1</td><td>315**537</td></tr>
<tr><td>腾讯QQ_2</td><td>171**50790</td></tr>
<tr><td>腾讯QQ_3</td><td>732**7693</td></tr>
<tr><td>腾讯QQ_4</td><td>22****7906</td></tr>
<tr><td>腾讯QQ_5</td><td>22**887906</td></tr>
<tr><td>腾讯QQ_1关联手机号</td><td>1831****733</td></tr>
<tr><td>腾讯QQ_2关联手机号</td><td>1501****420</td></tr>
</table>
</td></tr>
</table>

监测数据显示，该团伙于 2018 年开始活跃起来，主要通过 QQ，论坛等社交媒介出售 DDoS 攻击工具的方式获利，同时运营着多个平台的恶意软件家族，早期以窃密软件为主，后转向 DDoS 攻击。该团伙所运营的家族中 ,XorDDoS 传播量最广，而 Nitol 和 Dofloo 下发攻击指令最为频繁；此外，该团伙也尝试构建原创型僵尸网络木马，其中以 Go 语言编写的 Mediocre Botnet 体现了该团伙的原创能力；该团伙运营的僵尸网络的 C&C 命名具有相似的风格，经常使用汉语拼音或含义明确的命名，识别度很高。例如“luoyefeihua.site”（汉语名“落叶飞花”）和“linuxddos.net”（意为“针对 Linux 平台的 DDoS 攻击”），这种命名方式使得这个团伙的活动更易于辨认。

2.5 8220

“8220”团伙[4]最早出现于 2017 年，攻击 Linux 平台和 Windows 平台，主要目的为构建僵尸网络进行挖矿。伏影实验室对其进行跟踪分析并持续监控，根据现有数据，该团伙一直保持活跃，善于“利用已知漏洞”和暴力破解等方式部署其恶意程序，从出现至今攻击愈演愈烈。直至 2022 年 6 月，“8220”控制的主机从 21 年的 2,000 台到达了现在 30,000 余台。

2022 年，“8220”团伙更新了挖矿程序，该程序是基于开源挖矿程序“XMRig”开发的“PwnRig”的新版本，其矿池地址指向包含巴西联邦政府域名的虚假子域，创建虚假的矿池请求，以掩盖真实的资金流向。

除挖矿之外，该团伙还散布具有远程控制、DDoS 攻击等功能的 Tsunami 木马，显示其破坏活动从单一挖矿扩展到 DDoS 攻击，需引起足够重视。

表 2.6 “8220”团伙信息

团伙代号	8220
团伙特征	8220”团伙出现于 2017 年，根据现有数据，该团伙一直保持活跃，且善于利用已知漏洞和暴力破解等方式部署其恶意程序，其攻击同时面向 Linux 平台和 Windows 平台，主要活动以构建僵尸网络，进行虚拟货币挖矿为主。
武器库	Tsunami PwnRig
C&C 基础设施	104.*.*.25 51.*.*.23 104.*.*.132

8220 团伙增加 DDoS 活动或与挖矿收益下降有关。2022 年数字加密货币价格暴跌，作为对策，该组织通过加大僵尸网络控制范围及扩展攻击业务，来保持与之前相同的收益。尽管收益下降，但挖矿之利仍然是许多挖矿组织的主要收入来源，不断下跌的行情会令这些组织加大投入。

[4] https://www.antiy.cn/research/notice&report/research_report/20220428.html

2.6 Jester

Jester 团伙[5] 出现于 2021 年 7 月 20 日。该团伙在网络上公开售卖 Jester Stealer 木马。21 年 10 月份，该团伙将 Jester Stealer 功能植入新的僵尸网络木马 Lilith 中，开始出售 Lilith BotNet 木马。21 年 11 月份，该团伙开始销售 Trinity 挖矿木马。

表 2.7 “Jester”团伙信息

团伙代号	Jester
团伙特征	Jester 团伙出现于 2021 年 7 月 12 日。该团伙依靠出售商业木马获利，所售类型多为窃密、远程控制及挖矿木马。
武器库	Trinity Jester Stealer Lilith
C&C 基础设施	45.*.*.45

从该组织的行为来看，其编写售卖的木马程序在市场竞争下不断改进，从最开始的盗窃木马发展为整合了窃密，挖矿和劫持钱包等功能的复合型木马，以满足当前黑产市场偏向于综合性多角度的获利需求。

Jester 团伙 21 年 7 月首次售卖，到同年 10 月就完成新的木马，这种给更新速度体现了该组织具有完善的分工及对该木马的重视。

[5] https://www.antiy.cn/research/notice&report/research_report/20220510.html
https://www.antiy.cn/research/notice&report/research_report/20220902.html

03

IoT 新型僵尸网络家族

本年度，绿盟科技伏影实验室依托全球威胁狩猎系统发现了 14 个新型僵尸网络家族。相比于其他家族滥用 Mirai/Gafgyt 源码，这些家族采用了全新的代码架构和通信逻辑，具有较高的创新性。以往情况，大量攻击者滥用开源代码导致各类已知家族的变种频繁出现，且相似度甚高。例如，Mirai 类变种多由源代码修改而来，只做了一些简单的修改，如修改上线包、添加新的攻击方式、添加团伙标记字符串等。但今年监测发现到一些改动较大的变种，虽然来自已知家族，但在结构或功能上都存在明显不同之处。本年度发现的新家族以及一些区分度较高的新变种如下。

表 3.1　2022 年僵尸网络家族发现情况

捕获时间	捕获到的新家族	捕获到的部分新变种
3 月份	（1）Botnatest（攻击方式以 attack_method_* 的方式命名）	（1）MEDIOCRE（又称 Yeskit，Go 语言开发）
	（2）senderbot（攻击方式以“send_*”的方式命名）	（2）NEKONEBOT（因样本中多次出现 Neko 字符串而得名）
		（3）lolfme_killer（使用多个传播漏洞，存在与 lolfme 相同的加密算法）
4 月份	（3）hackerBot（通信数据含“hi hacker welcome”）	（4）lolfme_DB2（lolfme 结构重构版本，原有特征字符基本全删）
5 月份	（4）yeskit（含汉语信息，Go 语言编写）	（5）Necro_tor（Necro 首次采用 tor 通信的新版本）
		（6）bigbots（自称 bigbots，部分代码源自 lolfme）
	（5）Pandora（以“Pandora”文件名传播）	
	（6）EnemyBot（自称“EnemyBot”）	
6 月份	（7）boat（故意粘贴已知家族源码，防止被重点关注，后续有多个变种）	（7）Fbot_SV（修改 Fbot 上线包及攻击方式，此后捕获多个该类型变种）
	（8）boota（故意粘贴已知家族源码防止被重点关注）	（8）Mirai_miori（修改自 mirai，安全社区称之为“Miori”）
	（9）RapperBot（样本中含黑人 rapper 信息）	
	（10）Tbot（安全社区称其为 RobinBot，至今有 3 个版本）	
7 月份	（11）XorBot（仅支持 UDPFlood 的测试版 bot，采用简单的 XOR 加密）	（9）BotaX（完全重构了的 Bota 家族）
8 月份		（10）Gafgyt_suBot（对 Gafgyt 做了较大修改，攻击活动频繁）
		（11）GoBrut 新变种（3.32 版本）
9 月份	（12）GoBotV1（存在签名“GoBotV1”，Go 语言编写，传播名“Bins_Bot_hicore”）	（12）Fbot_abot（基于 Fbot 修改，上线信息包含“abot”字符）
10 月份	（13）Go_SHELLBOT（Go 语言编写，攻击方式命名多采用 Main_Shell_* 方式命名）	（13）hbot（自称 hbot，存在部分 lolfme 代码） （14）Znaich（修改上线逻辑，添加新功能） （15）STOLENBOTS（自称是 STOLENBOTS，复用 Gafgyt 通信逻辑）
	（14）ToggleDDoS（函数命名多次出现“Toggle”）	
11 月份		（16）Gafgyt_conbot，采用 Gafgyt 通信逻辑，其他部分自行设计的新变种
		（17）Mirai_tor（采用 Tor 通信的一类修改自 Mirai 的变种）
		（18）lolfme_fbot（融合 lolfme 部分代码和 Fbot 架构的新变种）

此外，结合安全社区提供的线索，本年度我们对新出现的 Fodcha 家族及活跃度较高的 Fbot 家族在内多个僵尸网络家族同样进行了深入分析和长期监测，研究结果显示如下：

（1）僵尸网络的高速扩张对关键基础设施的威胁愈发严重，不管是北京健康宝攻击事件，还是俄乌网络战中的 DDoS 攻击活动，都值得引起我们的深思；

（2）攻击者越来越喜欢使用 Go 语言来构建新的僵尸网络木马。绿盟科技伏影实验室于本年度检测到的多个新型僵尸网络家族均是采用 Go 语言构建；

（3）本年度，我们观察到攻击者在构建新的僵尸网络家族时会使用已知家族的部分代码，与构建 0 检测的全新家族相比，这种方法更不容易引人注意；

（4）僵尸网络的成败与僵尸网络木马自身使用的技术点并不成正比，而是更多取决于运营水平，取决于是否能够应对变化多端的网络环境，保证僵尸网络长期稳定运行。

在后续章节中我们挑选了五个代表性的僵尸网络家族展开，向读者详细展现新型僵尸网络家族在 2022 年表现出来的特点以及攻击活动情况。

3.1 boat 系列

2022 年 6 月 15 日，伏影实验室僵尸网络追踪系统告警发现了两个新的僵尸网络变种，经过分析研判后，我们确认这两个新的家族分别为 Boota 和 BOAT[6]。在识别过程中，我们发现它们都包含 Mirai 和 Gafgyt 的基因片段，融合了开源僵尸网络 DDoS 攻击源代码，但又都具有全新的代码结构和通信协议。这两个家族由同一批攻击者制作，功能基本相似，主要功能包括：信息搜集、DDoS 攻击、弱口令扫描以及自删除等。

其中，BOAT 家族自今年 6 月份以来不断升级，相较于最初版本已经“脱胎换骨”。我们在分析早期版本的 BOAT 时就发现其存在不合理之处，如在上线交互过程中，C&C 会下发弱口令对。最新版本的发现则证实了这一点，该家族对整体设计进行了修正，将弱口令对直接用于扫描模块，比原版更加合理。

[6] http://blog.nsfocus.net/boat-booat-0day/

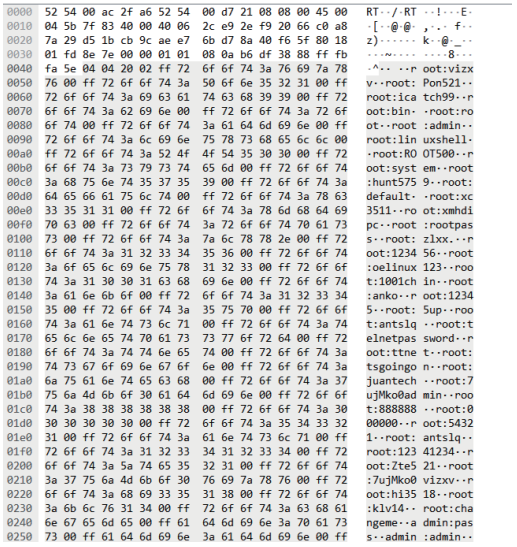


图 3.1　BOAT 家族家族下发的弱口令

我们认为，攻击者在构建新的僵尸网络家族时会使用已知家族的部分代码。这不仅仅是为了图便利代码复用，而且可以通过此种方式欺骗杀毒引擎，降低被单独拎出进行人工分析的概率。由于这类僵尸网络主要攻击缺乏终端安全软件的 IoT 设备，所以它们能否被杀软检测并不重要。在进行 0day 等重量级武器测试时，攻击者也可以利用这种方式有效地隐藏自己，与构建 0 检测的全新家族相比，这种方法更不容易引人注意。

3.2　YesKit 系列

2022 年 5 月中旬，绿盟科技伏影实验室全球威胁狩猎系统监测到一种新型僵尸网络木马利用 F5 BIG-IP 漏洞（CVE-2022-1388）大范围传播。在经过人工分析和研判之后，将该僵尸网络命名为“Yeskit”[7]。其攻击 payload 如下：

```
POST /mgmt/[illegible]/bash HTTP/1.1
Host: [illegible]:443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2866.71 Safari/537.36
Content-Length: 51
Authorization: Basic [illegible]
Connection: close
Content-Type: application/json X-F5-Auth-Token: a
Accept-Encoding: gzip, deflate
Connection: close
{
   "[illegible]d": "run",
   "[illegible]Args": "-c id"
}
```

图 3.2　Yeskit 攻击 payload

[7]　http://blog.nsfocus.net/yeskit-f5-big-ip/

Yeskit 僵尸网络采用 Golang1.18 编写，虽然它源自 MEDIOCRE（kaiji）僵尸网络，但它们二者又完全不同，是一个新型的僵尸网络家族。该僵尸网络于 2022 年 4 月份开始活跃，从首次发现至今已经历了三次版本更新。它的主要功能是 DDoS 攻击，同时也具有反连 shell、执行脚本等能力。研究发现，Yeskit 背后的运营者管理着一个由多个僵尸网络家族组成的网络，包括 Mirai 和 Xorddos。

2022 年 3 月初，伏影实验室披露了新版本的 MEDIOCRE Botnet 僵尸网络的最新攻击活动。后续，我们发现该僵尸网络的运营者显然加快了版本更新的进度，并且在后期捕获的样本中已经开始刻意隐藏在我们分析文章中提及的特征信息。Yeskit 同样源自 MEDIOCRE Botnet，但在代码结构、功能和编码习惯上都有所改变，关键代码几乎全部重新构建。

近年来，攻击者越来越喜欢使用 Go 语言来编写木马。Go 语言因出色的跨平台能力和对交叉编译的支持而颇受欢迎。它的打包机制使文件体积和函数数量巨大，对杀毒引擎的检测能力带来挑战。

3.3 RapperBot 系列

2022 年 6 月底，绿盟科技伏影实验室全球威胁狩猎系统告警发现了 1 个新的僵尸网络变种，经过人工分析和研判，确定了新的僵尸网络家族 Rapperbot[8]。Rapperbot 进行 DDoS 攻击，利用 SSH 暴破传播，因其控制台输出信息包含黑人 rapper 相关信息而得名。Rapperbot 代码源于 Mirai 架构，但进行了较大调整，呈现出全新的通信结构。

Rapperbot 僵尸网络近期一直在更新其版本，最新的样本增加了持久化功能，确保即使在设备重新启动或恶意软件删除后，攻击者仍然可以通过 SSH 访问被入侵的主机。最近一次大规模攻击活动发生在 2022 年 10 月，与 6 月份的攻击活动相比，存在一些相似之处，表明两次攻击可能由同一个攻击者完成，也有可能是代码被滥用。两次活动中表现出的特点如下：

（1）C&C 命令和相应的 ID 在两个活动中是相同的（不包括与 Telnet 相关的命令，因为这些命令不适用于 RapperBot）

（2）这两次活动中，暴力破解代码方面得到优化，比典型的物联网恶意软件更加结构化。

（3）RapperBot 还支持 Mirai 惯用的 TCP STOMP 攻击方式。在上述早期的活动中没有观察到这种攻击。

[8] 详见绿盟科技威胁情报微信公众号文章《预警 | 新僵尸网络家族正在利用 IoT 设备构建攻击网络》

3.4 Fbot 系列

Fbot 以 DDoS 攻击为主要功能，是基于 Mirai 源码修改而来，最早于 2018 年披露。根据全球威胁狩猎系统的监测数据，仅 2022 年，Fbot 就经历了四次重大版本变化，其中最显著的部分体现在控制协议格式的修改方面。这也使得对它的稳定监测变得相对困难，需要有较快的响应速度。

Fbot 以 DDoS 攻击为主要功能，拥有多种 DDoS 攻击方式，该家族对新漏洞的快速融合能力也暗示了背后攻击团队的专业性。最新版本的 Fbot 具备的 DDoS 攻击方式如下：

```
byte_51F740 = 10;
qword_51F748 = (__int64)attack_udp_vse;
byte_51F6B0 = 1;
qword_51F6B8 = (__int64)flood_udp_classic;
LOBYTE(conn_table) = 6;
qword_51F708 = (__int64)flood_tcp_gsyn;
byte_51F710 = 7;
qword_51F718 = (__int64)flood_tcp_gack;
byte_51F6E0 = 4;
qword_51F6E8 = (__int64)flood_udp_plain;
byte_51F6D0 = 3;
qword_51F6D8 = (__int64)flood_tcp_syn;
byte_51F6C0 = 2;
qword_51F6C8 = (__int64)flood_tcp_ack;
byte_51F6F0 = 5;
qword_51F6F8 = (__int64)flood_tcp_sack;
sigintr = 8;
qword_51F728 = (__int64)flood_tcp_stomp;
byte_51F730 = 9;
qword_51F738 = (__int64)flood_udp_bypass;
byte_51FCD0 = 99;
qword_51FCD8 = (__int64)flood_tcp_socket;
```

图 3.3 Fbot 攻击方式

2022 年，DDoS 攻击对关键基础设施的危害性日益突出，由 DDoS 攻击引发的安全事件也不在少数。不论是俄罗斯和乌克兰的网络战争，还是国内的健康宝攻击事件，都出现了 Fbot 的身影。Fbot 已经发展成为不容忽视的威胁源，其攻击目的也不再仅仅是为了获利。越来越多的攻击活动带有政治倾向，这值得我们密切关注。伏影实验室将持续监测 Fbot 及其背后的攻击者。

3.5 Fodcha 系列

2022 年 4 月份，安全社区首次披露了新型僵尸网络家族 Fodcha。经过绿盟科技伏影实验室的监测，该家族今年一直十分活跃，发起大量 DDoS 攻击。研究显示，Fodcha 是一个商业驱动的僵尸网络家族，并尝试实行攻击即勒索的商业模式。

Fodcha 命名的来源是由于该僵尸网络最初使用的 C&C 域名 folded.in，以及使用 chacha 算法来加密网络流量。Fodcha 主要通过 NDay 漏洞和 Telnet/SSH 弱口令传播，此外，运营者还会利用 Telnet 暴破工具进行 Telent 暴力破解。该家族从首次发现至今已经历过四次版本的更迭，版本间的区别主要体现在 Config 组织方式的不同，以及支持的 C&C 种类的不同，早期版本采用并列的 Config 组织方式，而最新版本采用结构化的 Config 组织方式。攻击目标涵盖了 mips、mpsl、arm、x86 等 CPU 架构。

Fodcha 作者具有较强的开发能力，严谨地设计了 Bot，注重 Bot 的安全性和通信协议的隐蔽性，体现如下：

（1）Fodcha 使用一种多重 Xor 的加密方式来保护其敏感资源；

（2）当成功和 C&C 建立连接后，Bot 与 C&C 必须经过 5 轮交互，才能真正和 C&C 建立通信；

（3）使用 OpenNIC / ICANN 双 C&C 的冗余结构。

近年来，僵尸网络的运营者不断在增强僵尸网络通信隐匿性方面进行尝试。无论是选择 Tor 进行通信，还是使用隧道通信，或是设计复杂的交互逻辑，都对溯源带来了新的挑战，在一定程度上攻击者愿意投入更多的资源。这值得引起我们的重视。

04

Windows 僵尸网络家族的攻防对抗

伏影实验室对 Windows 平台下的僵尸网络监控与分析始终保持着高度的重视，在本小结中，我们选取了 4 个 2022 年值得关注的僵尸网络家族向读者们呈现本年度执行与活跃的 Windows 僵尸网络是如何传播以及如何与防守方对抗的。

Orchard 家族是一个使用 DGA 技术生成域名的僵尸网络家族，给预测和防御造成很大困难。同时快速更新迭代，Orchard 的活跃程度与开发者的技术平都很高，具有很大威胁。

Sysrv-K 家族使用 Telegram bot 进行通信，增加 Sysre 的隐蔽性，加大了溯源的难度。一年中历经数十次维护更新，以适配不断变化的环境。其通过快速更新与灵活多样的攻击方式，不断扩大该僵尸网络。抑制其过快的发展速度是一项新的挑战。

Kraken 家族也是本年度非常得关注的 Windows 僵尸网络，该程序使用 Powershell 设置排除文件绕过 Windows Defender。并多次更新提高窃密能力。但却未使用窃取到的信息，猜测 Kraken 还会有更多动作。

还在测试中的 BlackMoon 僵尸网络家族也同样值得关注。该家族使用 Rovnix 僵尸网络进行传播。控制肉鸡 IP 超过 100 万，尽管尚未进行大规模 DDoS 活动，但 BlackMoon 背后组织维护的僵尸网络规模巨大，不排除后续会有新活动，伏影实验室将继续监控该僵尸网络动向。

4.1 Orchard

Orchard 于 2021 年 2 月首次出现，在安全社区发布报告讨论了该僵尸网络家族的同时，伏影实验室对该报告中涉及的僵尸网络进行了跟踪分析。Orchard 是一个使用 DGA 技术生成域名的僵尸网络家族，主要功能包含发送用户系统信息，下载并执行程序，感染 USB 设备，最新版本使用 Orchard 下载并运行挖矿程序，获取虚拟货币。Orchard 运行于 Windows 平台上，迄今为止，已控制超过 3,000 台主机，其大部分位于中国境内。DGA 算法广泛运用于僵尸网络木马程序中，通过使用同样的种子运行 DGA，生成大量域名，逐个访问这些域名，检测是否存在，如果该域名未注册，程序继续检测其他域名，如果该域名已注册，那么恶意软件将选择使用该域名联系 C&C 服务器。

Orchard 会使用多种形式的加载器释放 Orchard 木马，使用 Process Hollowing 技术将进程注入到 System32 或 SysWOW64 路径下的任意程序，运行后发送木马上线包，当 Bot 接收到 C&C 发来的挖矿指令后，执行下载的挖矿软件，并通过连接到 Bot 的 USB 设备进行横向传播。

至今 Orchard 已出现三个不同的版本，第三个版本中的 DGA 算法输入是一个地址为“1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa”的钱包的余额信息。可能为中本聪本人所持有，此钱包在十几年间，每天都有数量不一的比特币汇入，使用该钱包的余额信息作为 DGA 的输入，防守方难以预测并通过抢注域名的方式切断 C&C 与被控主机的联系，增大了防御的难度。Orchard 僵尸网络在一年时间内完成了三次更新，甚至更换不同的编程语言，使用难以预测的 DGA 输入，增大预测和防御的难度。可以见得程序开发者对此程序的用心程度与技术水平，也说明了 Orchard 的活跃程度，需要对该组织密切关注。

4.2 Sysrv-K

Sysrv 僵尸网络于 2020 年 12 月被阿里云首次发现，主要目标为挖矿，兼有横向移动及清除竞品等功能。该家族在 2021 年 3 月开始活跃，此后多次迭代，一年中历经数十次维护升级，涉及通信方式、入侵与横向传播利用手段，以适应不断变化的环境。

Sysrv 也是 golang 语言开发的恶意软件大军中的一员。Golang 因跨平台且编写便利，加上生成的可执行文件不易分析，所以越来越多被用来开发恶意软件。Sysrv 编写者借助这种便利对木马不断升级，使得 Sysrv 在保持较高活跃度的同时，也能够隐蔽通信，并维持较强的传播能力。

2022 年 5 月 13 日，微软声明发现 Sysrv 新变种 Sysrv-K。[9] 新变种可从互联网中扫描存在 Spring Framework 和 WordPress 插件漏洞的 Web 服务器并发起攻击，并可通过 Telegram bot 进行通信来增强流量的隐蔽性，能力更加全面。

4.3 Kraken

Kraken 僵尸网络 [10] 首次发现于 2021 年 10 月，一直面向 Windows 平台。伏影实验室对该僵尸网络进行了跟踪分析。该版家族包含下载并执行程序、获取屏幕截图，执行 Shell 命令等功能。虽然功能不多但保持更新。更新后的 Kraken 与 SmokeLoader 勾结，通过后者进行释放，并添加了窃取加密货币功能，同时将自身目录设置为 Windows Defender 白名单来进行绕过系统杀软。

[9] https://twitter.com/MsftSecIntel/status/1525158219206860801?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1525158219206860801%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https://securityaffairs.co/wordpress/131290/cyber-crime/microsoft-sysrv-botnet-new-exploits.html

[10] https://www.zerofox.com/blog/meet-kraken-a-new-golang-botnet-in-development/

在 2022 年 2 月 17 号的版本中，Kraken 又添加了对更多浏览器的支持以窃取其 Cookie。目前尚未观测到 Kraken 的运营者在销售其窃密信息，同时运营者依然在耗费精力频繁对该家族进行更新，表明其可能处于未获利阶段，可能会继续活跃。

4.4 BlackMoon

BlackMoon 僵尸网络家族专注于 Windows 平台，主要用于 DDoS 攻击。今年 1 月，监测显示 BlackMoon 僵尸网络控制 IP 已超过 100 万 [11]，每日上线肉鸡多达 21 万，如此规模对网络安全危害极大。

伏影实验室对 BlackMoon 进行了跟踪分析。该家族通过 Rovnix 僵尸网络进行传播，后者主要通过用户执行包含恶意载荷的激活工具来传播木马，涉及的激活工具包括：

（1） 暴风激活

（2） 小马激活

（3） KMS

BlackMoon 通常分为两个部分，一个是用于与 C&C 进行指令交互，另一个用于发动 DDoS 攻击。在目前的版本中 BlackMoon 仅保留 DDoS 攻击功能，且只保留一个目标对象，但一直没有发起攻击，故猜测该版本还在测试阶段。尽管尚未进行大规模 DDoS 活动，BlackMoon 背后组织维护的僵尸网络规模巨大，不排除后续会有新活动，伏影实验室将继续监控该僵尸网络动向。

[11] https://www.cert.org.cn/publish/main/10/2022/20220301130309305840180/20220301130309305840180_.html

05

未来展望——僵尸网络发展趋势预测

过去一年中，僵尸网络在运营和迭代升级上均有加强。各类僵尸网络木马及其变种不断出现。有的家族修改自开源代码，平平无奇，也有家族推陈出新，采用新架构。这些家族背后的僵尸网络团伙形形色色，有的尚未成熟，大肆宣扬，招摇过市，渴望获得更多知名度；有的则是悄无声息，闷声发财。基于这些现象，我们对僵尸网络有了新的思考：

运营方面，僵尸网络团伙“思变求新”，以加强传播效果，从而不断获利。宣传上，“KekSec 效应”会愈演愈烈；社交上，Telegram 等隐匿性强的社交媒介会成为僵尸网络团伙的聚集地；业务上，租赁服务仍是主流获利方式，而部分团伙为弥补原有业务下降带来的损失，将业务从单一攻击类型扩展到双重乃至多重类型。此外，世界局势的复杂变化导致更高级势力渗入，使得部分团伙不再是简单地从黑吃黑中获利，而是介入了地缘政治。这种业务拓展会使得“北京健康宝 DDoS 攻击事件”这类针对关键基础设施的恶意行为持续增多。

迭代升级方面，僵尸网络团伙不断更新木马功能，提升对抗，增强在文件隐匿性和通信隐匿性方面的投入，以追求僵尸网络持久稳定地运行。文件侧，除了常规规避检测的方式外，“混淆视听”成为新的思路，不但减少了木马制作者的工作量，还可以防止木马被安全研究人员重点关注。编程侧，使用 Golang、Rust 语言类型的僵尸网络木马将持续增多，在减少开发周期的同时也为检测提出更高要求；流量侧，隧道，DGA 等隐匿性更强的通信方式会被更多使用，复杂且更不易被监测的通信交互方式也会越来越多。

综上所述，尽管僵尸网络属于黑产，但因其取财于现实，所以仍受到世界政治经济格局的不稳定性的影响。攫取利益的源动力驱使僵尸网络在运营和技术上不断更新，导致攻击活动激增，使得网络安全的威胁态势会更加严峻。

关于绿盟科技

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 日起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 40 多个分支机构，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、新加坡设立海外子公司，深入开展全球业务，打造全球网络安全行业的中国品牌。

关于伏影实验室

研究目标包括 Botnet、APT 高级威胁，DDoS 对抗，WEB 对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁及新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。

NSFOCUS

THE EXPERT BEHIND GIANTS

巨人背后的专家

扫描绿盟科技官微二维码
可在手机端直接观看报告电子书