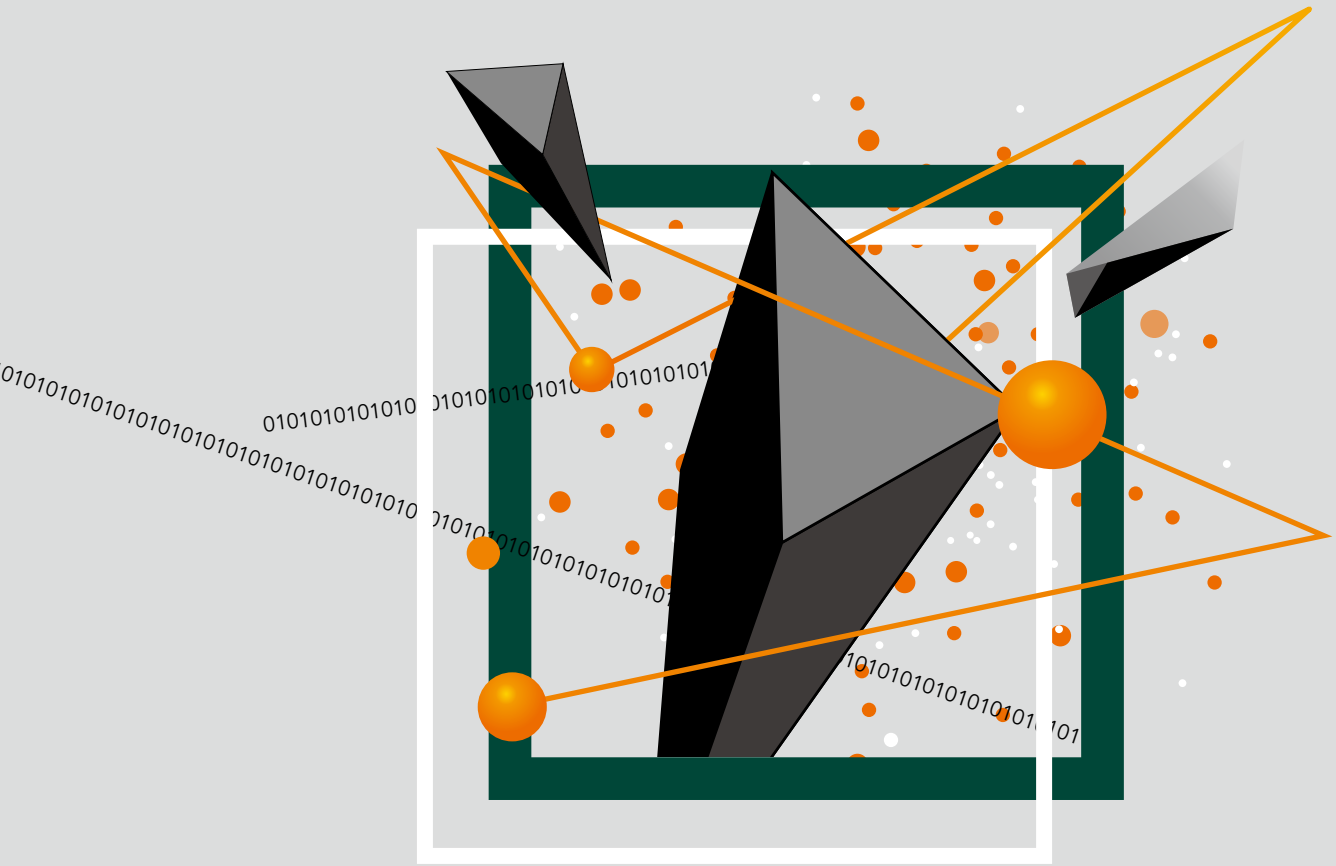


NSFOCUS

2017 Botnet 趋势报告

绿盟科技官方微信

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于2000年4月，总部位于北京。在国内外设有30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。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易。

股票简称：绿盟科技　股票代码：300369

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

目录

绿盟威胁情报中心（NSFOCUS Threat Intelligence, 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。

Botnet 一直以来都是互联网环境中不可忽视的危害。作为一种常见的恶意程序，它具有较强的隐蔽性，兼具蠕虫、木马的特征。Botnet 程序能够通过漏洞或者其他脆弱性获取目标主机的控制权，可以窃取目标主机中的信息或者操纵目标进行网络攻击。Botnet 对受控主机乃至整个网络环境都有极大的危害。

一般来说，黑客在初始阶段会通过欺骗或者漏洞利用的方式进入受害主机，这时“寄生”在受害主机中的往往只是一个简单的加载程序。然后加载程序通过访问远程主机，下载必要的程序代码，完成核心功能的安装。此时，黑客拥有了对目标主机的控制权，接下来，黑客可以盗取目标主机中的敏感信息、加密重要的文件进行勒索，或者通过控制主机 (C&C) 发送相关指令控制主机发起攻击行为。黑客利用 Botnet 进行的攻击通常包括：扫描探测、垃圾邮件、拒绝服务攻击（DDoS）等。

绿盟科技威胁情报中心（NTI）对 Botnet 有持续的跟踪，我们从 Botnet 的活跃度、规模变化和新的技术趋势方面给出了自己的观察。另外，作为近期在国内监测到的最活跃的 Botnet——“鬼影”，我们对该家族样本进行了持续的跟踪，并对“鬼影”家族的历史和近期态势进行了详细的梳理。在近期 Botnet 的态势中，我们观察到：

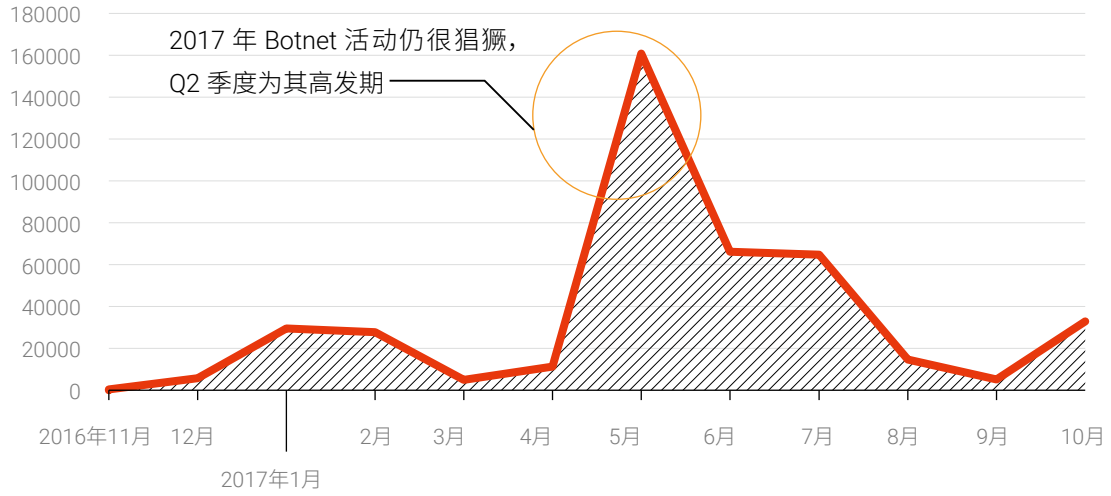
1. 近期 Botnet 的活动十分猖獗
2. Botnet 的规模在持续扩大
3. 由于物联网的迅速发展，Botnet 的战场局势正在发生明显的变化

1. 总体趋势

Botnet 活动十分猖獗

据绿盟威胁情报中心（NTI）监测的数据显示，2017 年 Botnet 活动仍然十分猖獗，尤其 Q2 季度更是 Botnet 活动的高发期。根据我们监控的 Botnet 的 C&C 攻击指令数据进行统计，Botnet 活动最高峰时期，平均每天共发出 5187 次指令，单个 C&C 每天最高能发起 114 次指令。

图 1 近期 C&C 指令数量的变化趋势 [1]（单位：次）



从 Botnet 活跃情况来看，Botnet 的活跃程度和一些重大事件是有关联的。3 月、9 月召开国家会议的期间，各地加强网络监控，Botnet 的活跃程度明显受到抑制。5 月左右，受到利用“永恒之蓝”漏洞的 WannaCry 勒索软件的影响，Botnet 的活跃程度也出现高峰。Botnet 的活动有很强的利益动机，当网络出现明显脆弱性的时候，Botnet 活跃度会呈现明显的上升态势，反之，治理力度强的时候，Botnet 为了规避风险，活跃度会相对较弱。

对这些指令进行统计分析，发现大部分是是 DDoS 攻击相关的指令，Botnet 活动以 DDoS 攻击为主要形式。Botnet 攻击的目标主要集中在游戏、娱乐行业，尤其是一些新兴业务，其中包括：福利游戏、bt 游戏、房卡游戏和直播视频等等。这类业务市场大、利润高，容易滋生黑色或者灰色产业，对手间通过网络攻击恶意竞争是一个普遍现象，成为 Botnet 理想的获利市场。

1 指令是指 C&C 向 Botnet 发送的控制信号，通过相关指令控制 Botnet 对目标发起攻击，指令发送的频率可以反映 Botnet 的活跃程度

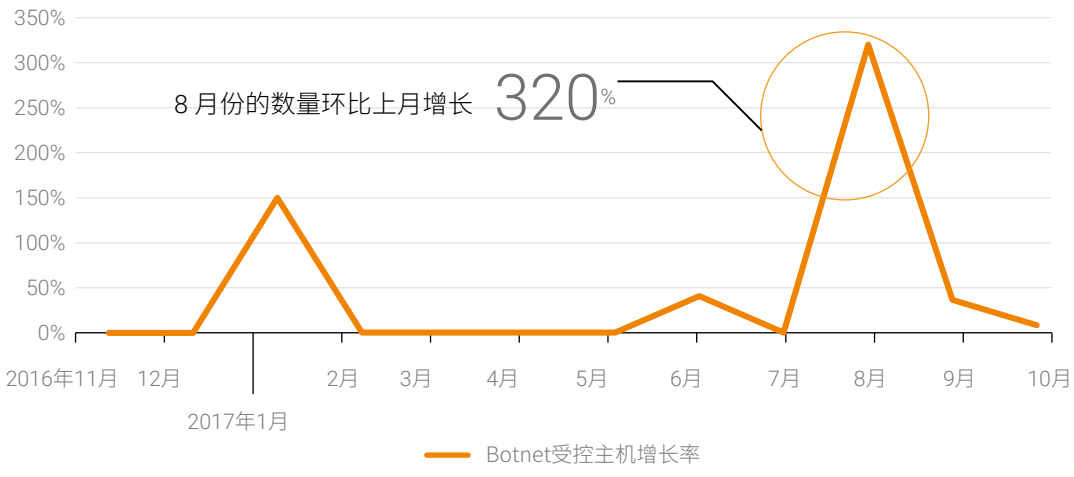
Botnet 规模持续扩大

主机数量

2017 年 Botnet 的数量和规模在不断扩大。其中，C&C 的数量持续不断增长，进入 8 月份后增速明显，10 月份环比增长达到 1.67%。另一方面，全球受控主机的数量间歇性增长，8 月份的数量环比上月增长高达 3 倍（增长 320%）。

图 2 近期 C&C 主机数量增长率的变化趋势

图 3 近期 Botnet 受控主机数量变化趋势



地理分布

绿盟威胁情报中心（NTI）跟踪的 C&C 服务器，大多位于中国的东南沿海和美国西海岸地区，Botnet 受控主机集中分布在中、美、俄三国境内。

图 4 C&C 主机全球分布热力图

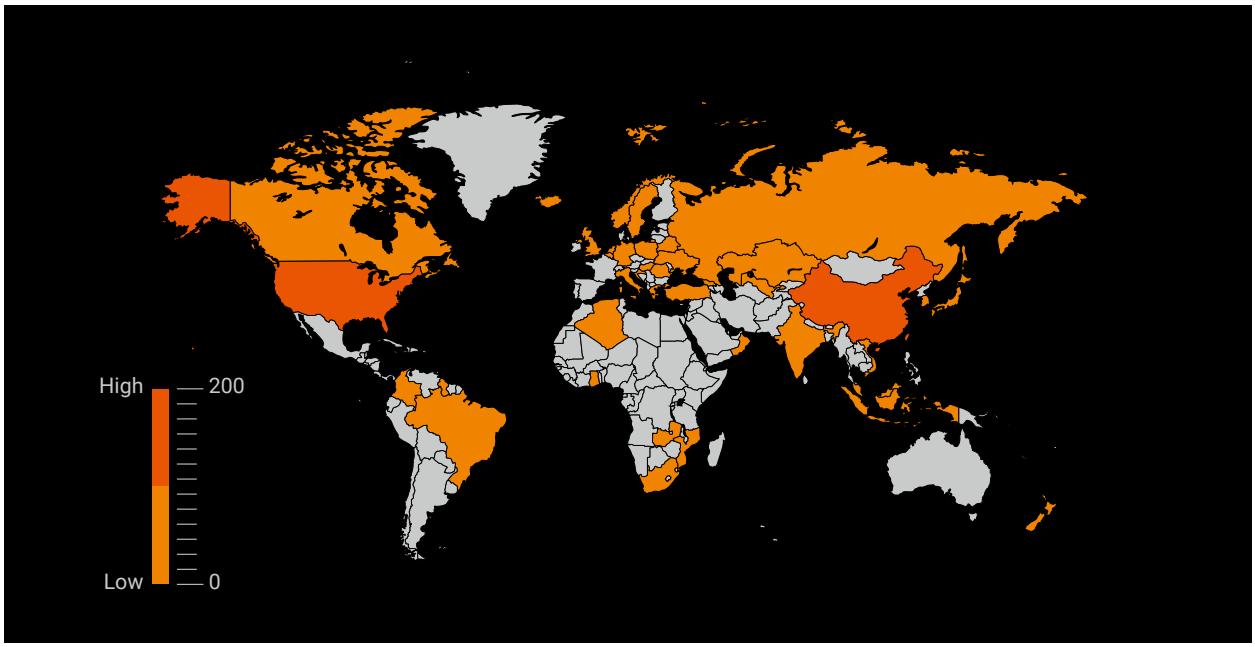
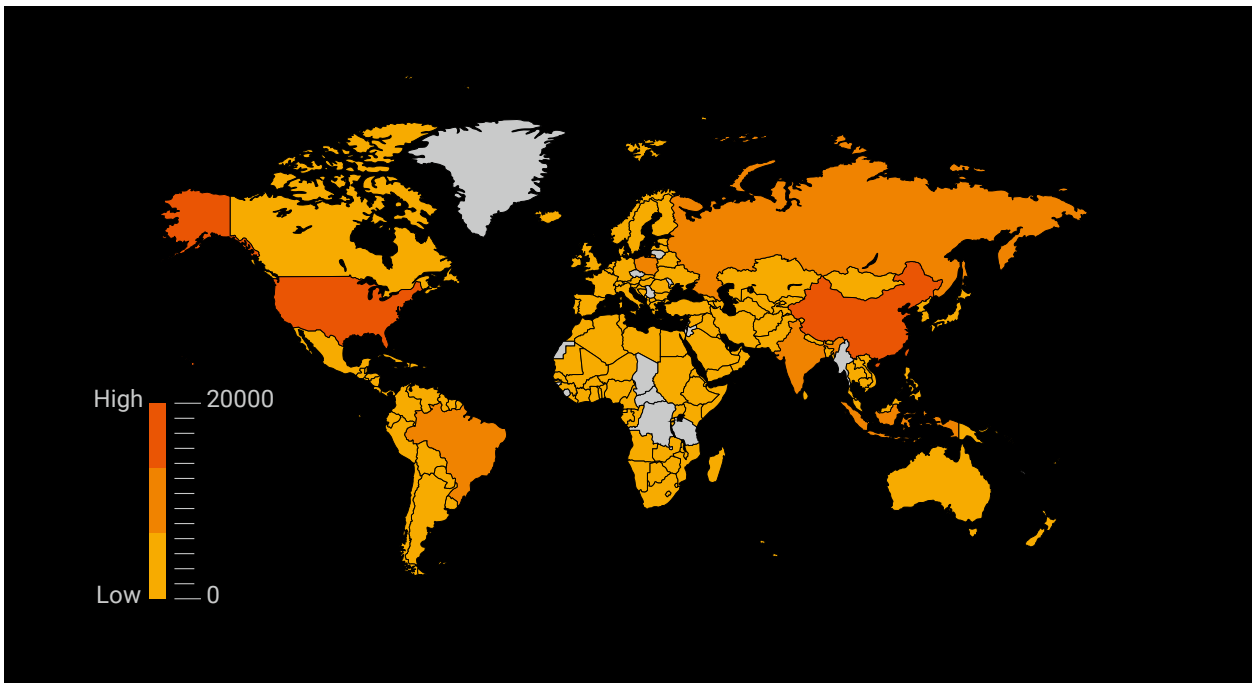
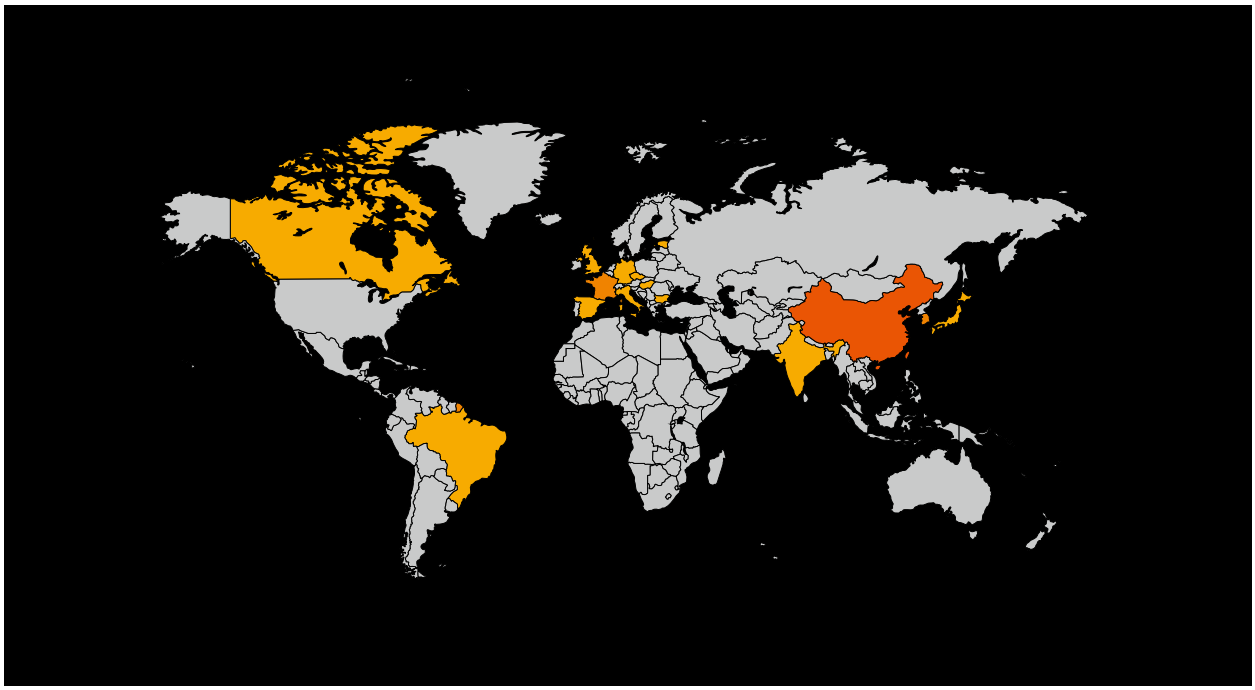


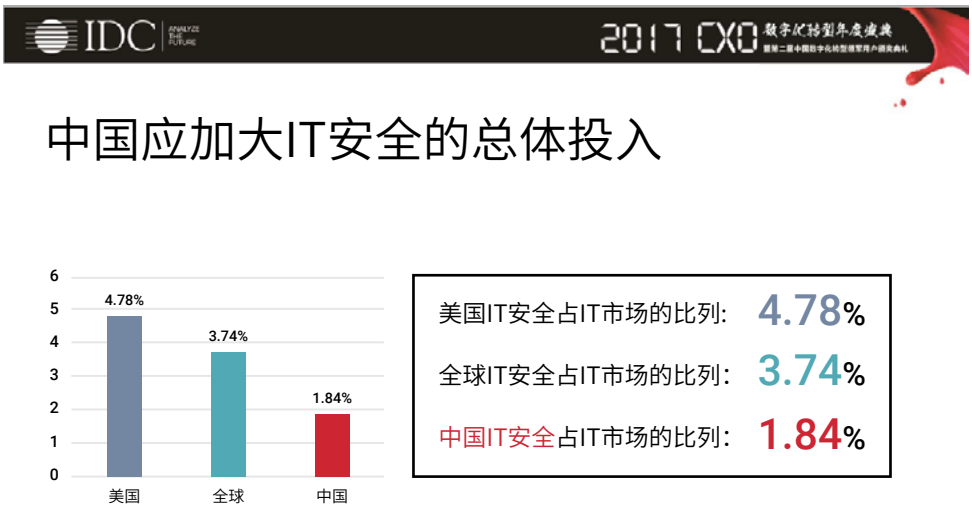
图 5 Botnet 受控主机全球分布热力图



当黑客初步获取主机权限后，主机会通过加载程序从远程的服务器下载恶意代码，完成 Botnet 相关功能的安装。这类存储服务器，存储了 Botnet 所需的各类功能模块，也是 Botnet 的重要基础设施。根据绿盟威胁情报中心（NTI）的监测，这类服务器在中国、法国、韩国、德国、加拿大等几个国家数量相对较多。



从地域分布上来看，中国 Botnet 的数量规模仍然是全球的重灾区之一。从 IDC 在 11 月份公布的统计数据可以看到，中国在 IT 安全投入上比例仍然低于全球平均水平，在安全上投入的不足也是造成 Botnet 泛滥的主要原因之一。[2]

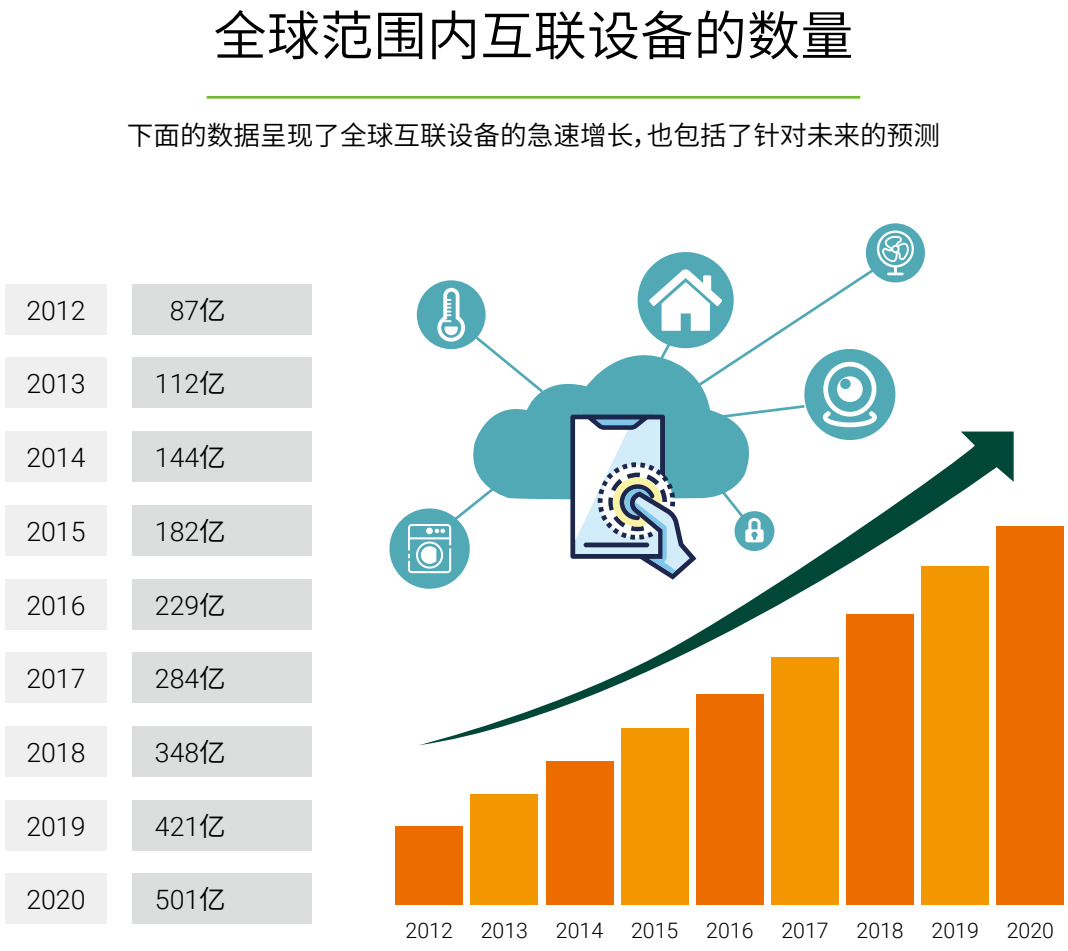


2 http://blog.nsfocus.net/idc-2017-james-wang-ppt/

正在变化的战场局势

在攻击者和防守者的博弈中，双方处于非常不对等的地位，攻击者只需要单点击破、层层突围，而防守者需要面面俱到，双方在这场博弈中付出的成本有着巨大的差异。随着新的移动、智能设备、物联网设备接入互联网，网络环境变得非常复杂，博弈双方不对等的情势变得更加严重。

图 6 MicKinsey 对全球联网设备增长趋势的预测 [3]



3 http://www.freebuf.com/articles/terminal/128148.html

新型的联网设备（包括物联网、移动智能设备等）本身具有一些特点，例如物联网设备数量多、安全措施普遍偏弱、设备种类繁多、更新快、且存在大量低成本的设备。物联网的这些特殊性，对传统比较单一的高成本防护方式提出了新的挑战。MicKinsey 预计到 2020 年全球联网设备数量会突破 500 亿[4]，对博弈的战场带来了挑战。

物联网设备特性	攻击者的优势	防守者的挑战
规模大	收益高、效果明显	成本高、效果不易度量
安全措施薄弱	攻击容易、门槛低	漏洞多、不易排查
设备种类多	多路玩家参与	技术技能线长
大量低成本设备	策划攻击的性价比高	安全投入的性价比低

在新的互联网业务环境中，许多新兴的厂商加入到这场持久的博弈中，它们关注新产品的功能的同时，可能缺乏必要的安全意识和防护能力。为了积极应对这样的变化，一方面安全厂商应该投入物联网领域的安全研究，培养市场的安全意识，另一方面，监管部门可以制定产品在网络安全上的有关标准，在市场中建立发现威胁、修复漏洞的有效机制，在这场博弈中发挥积极的作用。

4 http://www.freebuf.com/articles/terminal/128148.html

2. 僵尸网络的工作机制与技术趋势

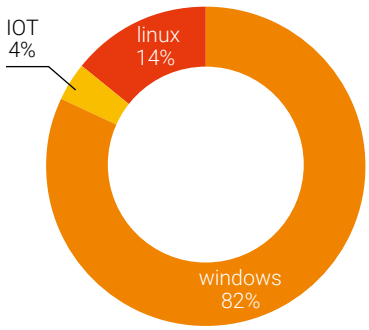
Botnet 技术发展符合这样一些趋势：

- **规模更大。**规模更大的 Botnet 具有更强的攻击能力，例如 DDoS 攻击的流量。而脆弱性高、数量多的 IoT 设备及移动智能设备成为非常理想的攻击目标。
- **隐蔽性更好。**对于 Botnet 来说，隐蔽性是其持续追求的目标。好的隐蔽性对顺利入侵和延长 Bots 的存活是必要的。一方面，Botnet 程序需要躲避 Bots 设备本身的安全防御措施的检测， Botnet 发动攻击时也需要规避检测，另一方面，对于攻击者来说，需要隐藏自己真实的身份。
- **传播快速。**正如所有的攻防场景一样，攻击者和防御者之间进行着一场速度的博弈。对于攻击者来说，能否目标获得防御能力前，尽可能多的扩大攻击战果是决定 Botnet 规模的关键因素。很多 Botnet 具有自传播的特性，能够尽可能多、尽可能快地扩大自身规模
- **控制方便。**对于大规模的 Botnet 来说，需要一个好的网络拓扑来保证 Botnet 的组织能力。由中心化多层级的 C&C 服务器控制的 Botnet 已经是一个较为成熟可靠的模式，目前一些新的模式，例如基于 P2P 协议去中心化的 Botnet 还在探索阶段，虽然隐蔽性和网络鲁棒性都有很大的潜力，但是鉴于控制难度大，技术复杂，使用者还比较少

跨平台的传播能力

正如在总体趋势中提到的，物联网和智能、移动设备构成的 Botnet 开始对 Botnet 战场的形势产生新的影响。我们持续跟踪的 Botnet 中，至少存在 4% 的样本攻击目标为物联网设备。虽然 Botnet 形式还是以 Windows 平台的设备为主，但是近年来，随着 IoT 设备、智能设备、移动设备的入网，我们认为针对 IoT 或其他智能、移动设备的恶意样本会越来越多

图 7 Botnet 运行平台的分布情况



对于 PC 用户，通过邮件、“水坑”站点或者在软件安装包中捆绑恶意代码都是很有效的入侵手段，而对于物联网设备来说，其在线时间长、用户普遍疏于升级和配置、数量规模大，黑客通过简单扫描就可以捕获大量存在漏洞的设备。今年 10 月绿盟科技情报中心发现并命名的机顶盒蠕虫，Rowdy，就是利用了机顶盒存在的脆弱性在国内互联网上大规模传播[5]。

5 http://blog.nsfocus.net/iot-set-top-box-malware-rowdy-network-analysis-report/

另外，我们注意到也出现了一些 Botnet 家族攻击的目标是 Android 平台的设备，典型的家族包括：Dendroid、FlexiSpy、GMbot 等， Botnet 是一个全平台存在的互联网威胁

正如在前文提到的，Botnet 持续不断的追求规模的扩张，通过俘获大量设备提升自身攻击的能力，IoT 设备具有的脆弱性使其成为理想的切入点。但是贪婪的黑客们野心并未停止，我们观察到有的 Botnet 已经具备了跨平台的能力，他们在兼具自传播的特点时，同时能够根据设备类型，植入对应平台的程序来获取控制权限，进一步提升了自己的传播能力。下面是几个典型的具有跨平台传播能力的 Botnet：

物联网设备特性	攻击者的优势
Rowdy	linux(x86/x86_64、arm、arm4、arm7、mips、mpsl 等)
Mirai	windows，linux（ARM,EABI4,MIPS, MIPS-I,PowerPC or cisco 4500,Renesas SH,SPARC,Intel 80386）
Gafgyt.bax	linux(x86/x86_64、ARM、Mips、PowerPC、SuperH 以及 Motorola 68000）
darkshell 族	Windows、linux(x86)
jRAT（远控）	依赖 java 环境实现跨平台，windows linux macos freebsd 等

从 Botnet 采用的程序语言上，也可以发现跨平台的趋势。C 语言和脚本语言具有良好的跨平台能力，无论在 arm 架构的嵌入式系统中，在 linux、Windows 系统中都有良好的适应能力。在此基础上构建的 Botnet 程序，可以具备跨平台传播运行的能力。

Botnet 家族	编写语言
Rowdy	C++
Gyddos	C++
LuaBot	Lua
Aldi_bot	Delphi
yi2.0	易语言

另外，脚本语言的编写相对比较容易，可以更加快速高效地实现一个新的 Botnet 程序。较低的门槛、快速的收益吸引着更多的黑客加入进来，使得网络中 Botnet 的威胁形势更加严峻。

隐蔽性与控制复杂性的平衡

Botnet 采用的通信协议常常是与其本身的网络架构设计紧密关联的。正如前文提到，Botnet 时刻需要保护自己的隐蔽性，避免防御者探知自身的存在。为此，Botnet 的设计者需要在控制复杂性和隐蔽性之间找到一个合理的平衡。

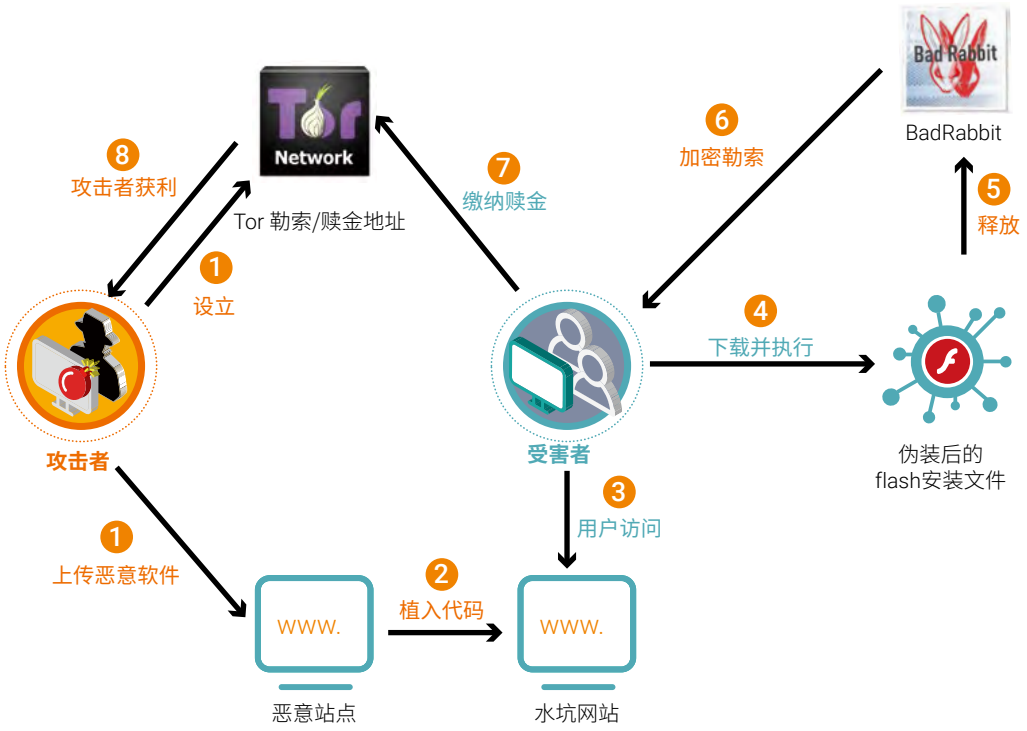
代表家族	主要协议
AldiBot、Vertexnet、LokiBot	HTTP
TrickBot	HTTPS
Zeroaccess、Hajime	p2p
Zeus	IRC、Tor
GyDDoS、Rowdy	TCP

Botnet 主要的网络拓扑还是 C&C 服务器控制 Bots 的模式，Bots 和 C&C 服务器之间需要经常通信，通信的内容包括客户端升级、发起攻击、回传本地信息等。主机间的通信大多数是基于 TCP 构建的自定义协议，这些流量混杂在正常业务流量中，具有一定的隐蔽性。也有部分 Botnet 实现了较为复杂的通信方式，例如使用 IRC、P2P、Tor 协议作为主机间的通信方式。但是这些网络架构控制复杂性相对较高，尚未成为主流。

更有效的传播方式

传统的传播方式，一般会通过诱导用户触发恶意程序的方式实现感染，例如发送带有恶意附件的邮件、诱骗用户点击恶意链接、网页挂马、在正常程序中捆绑恶意代码。这些触发方式效依赖于用户的行为，因此 Botnet 在隐蔽性上，除了与设备、程序中的防御机制对抗，还需要实现对用户有效的欺骗。

今年几个流行的 Botnet 家族，在传播过程中，通过伪装成正常的升级、安装流程，实现了更加有效的欺骗，几个 Botnet 的规模也因此迅速扩大。例如 BadRabbit，伪装为 flashplayer 正常的安装，在“水坑”站点提示用户安装 flashplayer 插件，在获取用户同意后，下载并执行恶意文件，实现感染，具有很强的欺骗性。[6]



另外通过扫描探测的方式也能实现高效的传播，黑客利用弱口令、软件漏洞实现有效入侵。例如，今年 ShadowBroker 公布的“永恒之蓝”漏洞被 WannaCry 集成利用，实现了大规模的传播。需要再次提到的还是物联网、移动智能设备带来的“红利”，这些设备长期在线、普遍缺乏维护及安全防护措施，通过此类方式可以获取到大量 Bots。

6 http://blog.nsfocus.net/badrabbittechnical-analysis-protection-scheme/

僵尸网络的常见用途

- **DDoS**

  Botnet 利用其规模效应最最直接的应用之一就是 DDoS。Botnet 规模动辄上千上万台主机，加之廉价的带宽资源、主机长时在线等等呢改革中因素使得僵尸网络发动的 DDoS 攻击越来越常见。在我们监控中 Mirai、鬼影等僵尸网络活动是非常频繁的，甚至将自己的能力包装成服务，提供 DDoS 攻击，这样一来普通人也可以利用僵尸网络进行攻击，是的僵尸网络的危害进一步深化。

- **垃圾邮件**

  垃圾邮件也是 Botnet 非常常用的场景之一。垃圾邮件的危害近年来颇受关注，除了发送大量的广告、诈骗信息，垃圾邮件还参与了恶意软件的投递，包括社工诈骗，例如著名的垃圾邮件僵尸网络 Necurs。

- **加密货币**

  Botnet 分布式的特征被其所有者物尽其用，今年来以比特币为代表的加密货币市场看好，这里面自然少不了黑客的参与。一方面，与传统行业一样，数字货币行业也会遭受各样的攻击，另一方面我们观察到，出现了针对加密货币矿机的攻击行为，我们猜测，黑客这样做，很可能是一种与加密货币业务特征密切相关的竞争行为，如果矿机因为攻击算力受到影响，那么与其同时挖矿的其他矿机收益概率就会大幅提升。另外，黑客也利用 Botnet 集群的算力参与到了挖矿的行列中。

绿盟科技在物联网僵尸网络方面的追踪

前文我们说到，物联网的兴起对僵尸网络态势有着重要的影响，绿盟科技威胁情报中心对物联网僵尸进行了关注。下面列举了近年来热度最高、影响广泛的物联网僵尸网络。

Mirai

这是 2016 年出现的一个非常重要的物联网僵尸网络。Mirai 事件回顾如下[7]：

1. 2016 年 8 月 31 日，逆向分析人员在 malwaremustdie 博客上公布 mirai 僵尸程序详细逆向分析报告，此举公布的 C&C 惹怒黑客 Anna-senpai。
2. 2016 年 9 月 20 日，著名的安全新闻工作者 Brian Krebs 的网站 KrebsOnSecurity.com 受到大规模的 DDoS 攻击，其攻击峰值达到 665Gbps，Brian Krebs 推测此次攻击由 Mirai 僵尸发动。
3. 2016 年 9 月 20 日，Mirai 针对法国网站主机 OVH 的攻击突破 DDoS 攻击记录，其攻击量达到 1.1Tpbs，最大达到 1.5Tpbs
4. 2016 年 9 月 30 日，Anna-senpai 在 hackforums 论坛公布 Mirai 源码 , 并且嘲笑之前逆向分析人员的错误分析。
5. 2016 年 10 月 21 日，美国域名服务商 Dyn 遭受大规模 DDoS 攻击，其中重要的攻击源确认来自于 Mirai 僵尸。

Mirail 仍然在互联网中活跃，2017 年 12 月，Mirai 的新变种 Satori 于 12 月 5 日已经激活超过 28 万个不同

7 引用自：http://www.freebuf.com/articles/terminal/117927.html

的 IP。2018 年 1 月，研究人员 unixfreaxjp 发现首款专门感染 ARC CPU 的 Linux 恶意软件，并将这款新型 Linux ELF 恶意软件命名为“Mirai Okiru”。当时几乎所有反病毒产品均未检测出这款恶意软件。

Rowdy

2017 年 8 月，绿盟科技 DDoS 态势感知平台监控到某客户的网络带宽流量存在异常情况，经分析确认是 DDoS 攻击事件。攻击类型多样，包括 TCP Flood、HTTP Flood、DNS Flood 等。通过对攻击源 IP 进行溯源，发现攻击来自有线电视的终端设备 – 机顶盒，然后提取了相关样本，进一步分析其攻击行为特征。经过评估发现，Rowdy 在短短数月时间已经形成了规模不小的 Bot 僵尸网络，感染的设备涉及国内 5 家厂商。国内的机顶盒使用量有多大？据国家统计局 2 月份发布的《中华人民共和国 2016 年国民经济和社会发展统计公报》显示，该设备实际用户到达 2.23 亿户，同时据奥维云网《2017 年中 OTT 运营大数据蓝皮书》显示，该设备实际用户达到 2.4 亿台。如此庞大的网络，一旦被 Rowdy 快速渗透，带来的后果不堪设想。

DarkCat

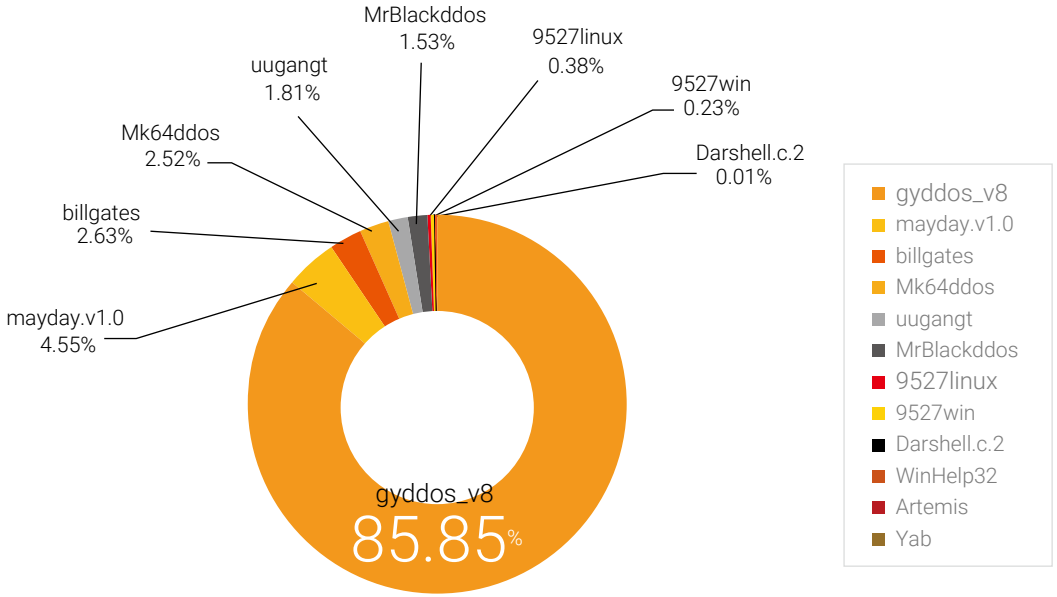
家用机顶盒、光纤猫，路由器等终端网络设备大多采用 MIPS 架构的嵌入式 Linux 系统。其管理方式除 web 外，通常还支持 Telnet、SSH 等远程管理协议，此外大多设备还支持通过内置的 BusyBox 执行常见的 shell 命令，如：ps、netstat、ls、cat 等，而其中很多设备管理密码为出厂默认或者弱口令。2017 年年底，绿盟科技应急响应团队陆续接到多个运营商客户的安全事件反馈，大量用户终端的光猫设备存在流量异常。通过抓包分析，发现感染蠕虫。该病毒程序命名由 cat+5 位随机字符组成，如：catburhk，由此我们将此蠕虫命名为 DarkCat。

3. 最活跃的 Botnet: 鬼影

“鬼影”是一个在中国非常活跃的僵尸网络，是基于 Windows 平台发展的一个影响广泛的僵尸网络。在近期 Botnet 活动监测中，我们看到“鬼影”的活动十分频繁，这个家族出现时间早、变种多，具有相当成熟的商业运作。对此，我们认为需要特别关注和治理。

活跃度极高

在对国内最常见的几个家族样本的监控中，我们发现，从指令频率和数量上统计，“鬼影”家族是近期活动最频繁的家族。在对 C&C 通信指令的监控中，gyddos-v8[8] 一个家族的 C&C 主机所发出的指令数量占比就超过了 85.85%，高居榜首。

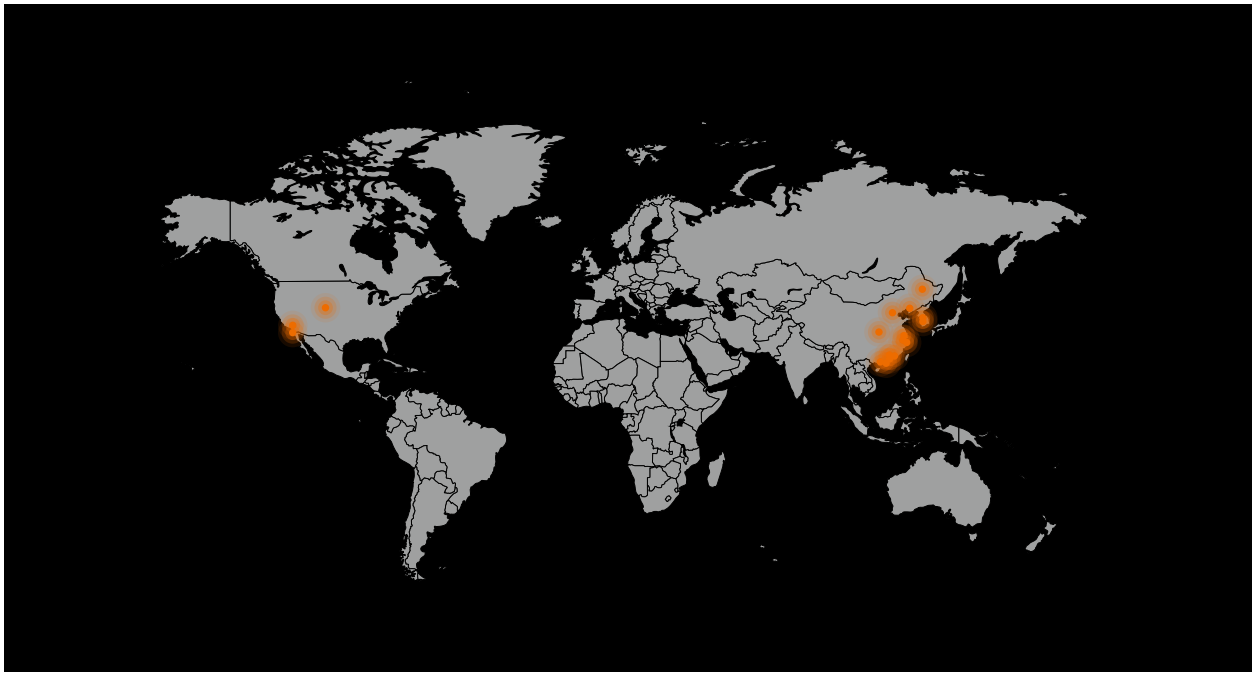


活动最频繁的时候，一天能够检测到 31264 次攻击行为。

8 “鬼影”样本在我们监测中，共有 10 个不同的变种，分别命名为 gyddos-v1,gyddos-v2…gyddos-v9,gyddos-X1

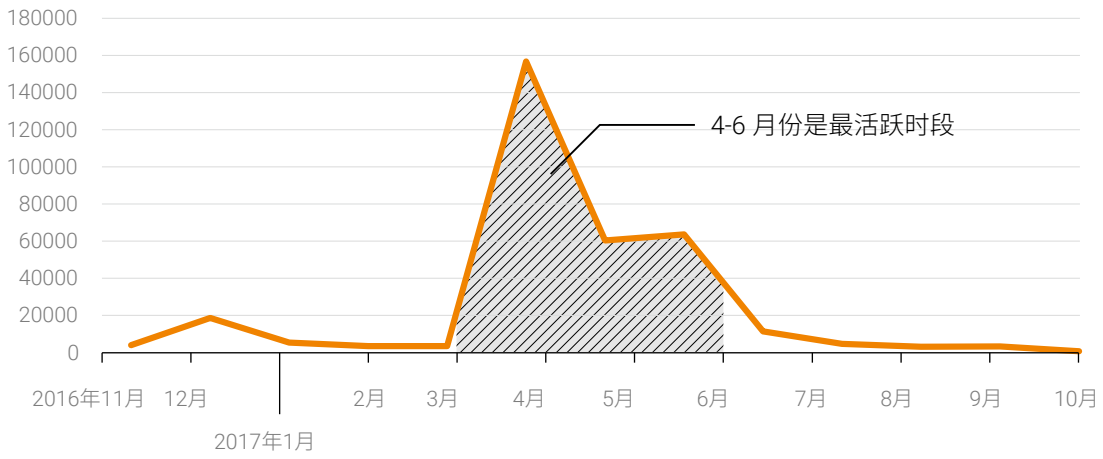
在我们的监测中，这个家族的 C&C 主机主要集中在中美韩三国，其中中国又以东南沿海为主要分布地区。

图 8 gyddos-v8 的 C&C 服务器地理分布



下图是今年对 gyddos-v8 指令通信的监测情况，在 4-6 月份是其活动的最活跃的时段

图 9 gyddos-v8 C&C 服务器指令数量的变化趋势



出现时间早

该家族最早在 2012 年 9 月被微软发现，命名为 Nitol，从生成的恶意文件名称推测[9]，Nitol 应该就是由“鬼影”工作室开发的 gyddos 家族的早期版本。2012 年 9 月，微软公司发现，在一些供应商销售的计算机中，预装了恶意软件，其中包括 Nitol，它们的 C&C 服务器地址多数位于域名 3322.org。微软公司在随后获得美国弗吉尼亚州东区地区法院批准，获取了 3322.org 域名的相关权限，切断了与该域名的所有通信，有效缓解了包括 Nitol 在内多个 Botnet 家族的网络活动。[10]

变种很多

“鬼影”目前至少存在 10 个不同的版本，每个版本与之前一个版本相比都增加了新的功能，DDoS 攻击技术也不断升级迭代。目前“鬼影”已经成为一个可发动大流量攻击、可大规模传播、支持不同模式商业运作的成熟软件。

- **gyddos v1-v4**

  完成基本的指令功能和普通攻击方式（TCP_Flood、UDP_Flood）

- **gyddos v5**

  添加 upx 选项，可压缩被控端体积

  添加 CC 攻击模块（参照 ImDDoS 源码）

  添加 lpk.dll 劫持功能，使得任意 exe 文件都可成为复活媒介

  添加内网 IPC$ 传播功能（暴力猜解密码）

  添加 DNS_Flood 模块

  上线包增加网卡信息内容

- **gyddos V6**

  添加 DownloadFile_Flood 模块

  解决同一台肉鸡重复上线的 BUG（使用互斥体）

  lpk 感染模块免杀处理

- **gyddos V7**

  添加远控模块（cmdshell、文件传输、批量重启 / 关机等）

  添加用户自定义包结构的 TCP_Flood/UDP_Flood 功能

- **gyddos V8**

9 http://www.freebuf.com/articles/network/147591.html

10 https://blogs.technet.microsoft.com/microsoft_blog/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain/

添加多任务轮询模块（可以使肉鸡进行脉冲式的攻击，或随时切换攻击方式）

优化 DNS_Flood 模块

- **gyddos V9**

  添加肉鸡租赁模块（将肉鸡暂借给其他用户）

  添加肉鸡统计模块（统计肉鸡数量、系统、地区分布等）

- **gyddos X1**

  添加 SSDP 放大攻击模块

  添加 NTP 反射攻击模块

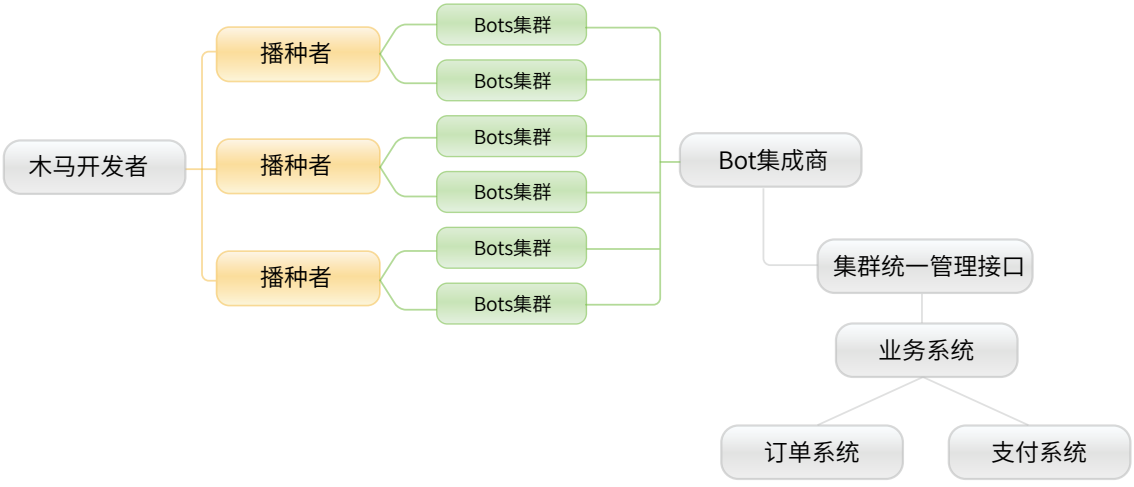
存活时间长

我们最早监测到该家族的活动是在 2013 年 11 月，其间陆续跟踪监测百余个 C&C 服务器，迄今为止，大部分 C&C 服务器以及控制的 Botnet 仍然存活，存活时间超过 4 年，生命力非常顽强。

在绿盟威胁情报中心（NTI）的监测中，时常能够观察到该家族发起的攻击，是一个在国内分布很广、影响很大的 Botnet 家族。

商业化的运作模式

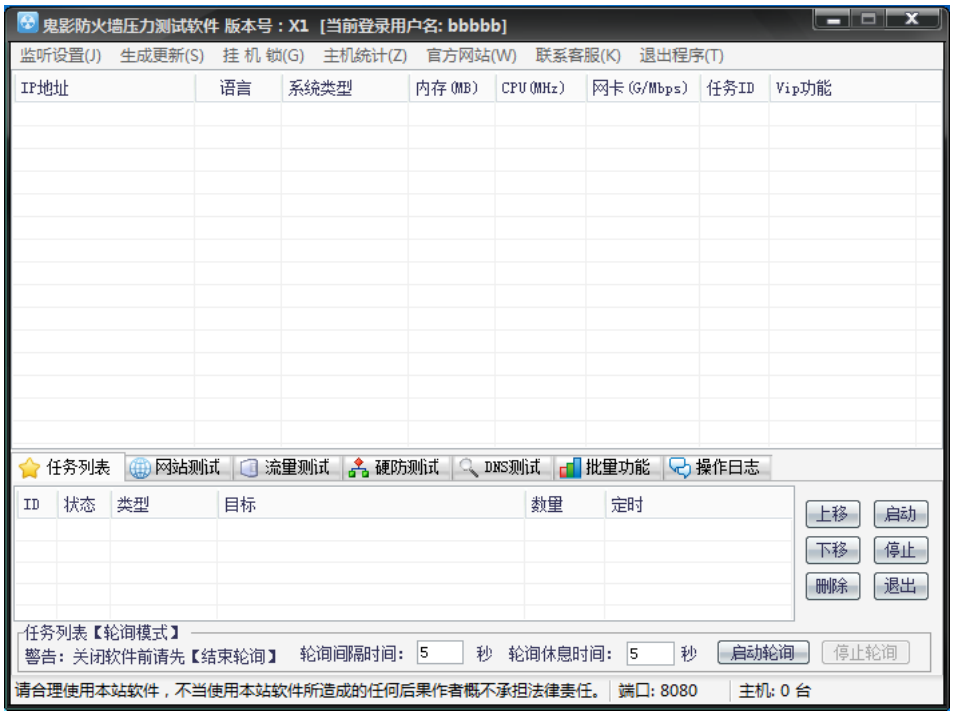
Botnet 已经是一个相当成熟 Botnet 感染手法有较为固定的流程和阶段，在黑产链条中不同的角色参与到各个环节的利益分配中。



很多时候，多个角色可能由同一个组织、个体兼任，但是通过黑产链条角色划分，让我们可以比较清楚的掌握 Botnet 地下市场的生态面貌。对木马开发者来说，主要通过售卖代码的方式获取利益，并不直接参与黑客攻击，很多开发者，名义上开发的是测试工具，实质却通过地下渠道贩卖获利。而真正的“脏活”从播种者开始，他们专门负责大规模地传播恶意程序，扩大感染规模，把获取到控制权的主机售卖给 Bots 集成商。Bots 集成商能够整合 Bots 资源，集中管理大规模的 Bots 集群，通过一个客户端程序或者 web 界面为用户提供便捷的攻击订制，

客户通过代币[11]，在支付系统上完成交易。另外，作为黑产价值链的出口，集成商也着力开展有关的市场活动来推广 Botnet 业务。

从“鬼影”的版本演变来看，持续优化和增加管理类的功能，使得集群的控制能力更为稳定可靠，为黑产商业化服务提供了技术条件。“鬼影”的 Bots 集成商，通过 QQ 群、论坛、微信群的方式推广 DDoS 业务，向购买者提供业务系统的客户端程序，用户登录获取的账号后，可以调动平台资源完成目标攻击。



从我们长期的观察中，期望实施 DDoS 打击的单位，多为色情、赌博、彩票、私服、变态游戏、福利游戏的的经营者。主要动机是为了打击行业内的竞争对手。从用户的角度，并不需要黑客技能就能够发动一次大流量的攻击，加之网络交易的隐蔽性，身份暴露的风险很低。成本低、风险小、效果明显，使得这一业务能够大规模推广开来。

11 代币是指游戏点卡、比特币等虚拟的货币形式，不同的代币与真实货币之间可以通过某种比率进行兑换。通过代币可以比较容易的进行非实名制交易，在一定程度上隐藏了交易人的身份。

4. 僵尸网络的攻击与防御

Botent 是一个传统的互联网威胁，但是在新的网络环境中它也展现出了新的威胁形势。伴随着互联网的发展，Botnet 的规模也在不断扩大、适应能力不断增强，给防护提出了更多的挑战。Botnet 活动可以作为评价互联网综合环境安全的一个指标，在对 Botnet 持续跟踪的过程中，我们发现目前国内互联网环境有很多复杂因素，给企业的管理、政府的治理增加了许多难度。在技术日新月异的时代，Botnet 飞速地进化，它们不断探测新设备、新软件应用中的脆弱性，整合新的攻击工具和技术扩大自身规模，Botnet 与互联网的发展相生相伴，顽强地寄生在不成熟的网络环境中。从 Botnet 的扩散情况，我们看到，互联网上大量的弱配置或者漏洞设备，是孕育大规模 Botnet 的温床，我们可以预期这样的情况在相当长的时间内会继续存在，甚至有所加剧。作为企业或者普通互联网用户来说，出于两个目的需要，应该加强自身的防护：一方面，做好设备、软件的配置，定期升级维护，采用必要的安全手段，例如安装杀软、采用成熟的安全解决方案等，从而有效防止成为 Botnet 利用的对象，从源头上削弱 Botnet 扩张的趋势；另一方面，应该关注 Botnet 态势，了解 Botnet 的实际威胁，针对性地进行相关的安全部署，在攻击中，才能有效地维持相关业务的正常运行。

绿盟科技威胁情报实验室（NTI）将持续关注 Botnet 变化态势，定期发布 Botnet 活动的相关安全情报，辅助企业进行安全防御，在持续变化的安全态势中，提供有价值的参考。

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