# IOT 僵尸网络严重威胁网络基础设施安全

*北美 DNS 服务商遭 Mirai 木马 DDoS 攻击的分析思考*

**安天实验室**


**报告初稿完成时间：2016 年 10 月 23 日 00 时 47 分**

**首次发布时间：2016 年 10 月 24 日 9 时 30 分**

**本版本更新时间：2016 年 10 月 24 日 9 时 30 分**

# 目 录

# 1 概述

安天安全研究与应急处理中心（Antiy CERT）在北京时间 10 月 22 日下午启动高等级分析流程，针对美国东海岸 DNS 服务商 Dyn 遭遇 DDoS 攻击事件进行了跟进分析。安天分析团队认为，此事件有一定的政治因素背景，涉及到 IoT（Internet of Things，物联网）设备安全等多种因素，在表象的 DDoS 攻击和 DNS 安全之外，依然有很多值得关注和研究的问题。

事件相关背景如下：美国当地时间 2016 年 10 月 21 日，为美国众多公司提供域名解析网络服务的 Dyn 公司遭 DDoS 攻击。Dyn 公司在当天早上确认，其位于美国东海岸的 DNS 基础设施所遭受的 DDoS 攻击来自全球范围，严重影响其 DNS 服务客户业务，甚至导致客户网站无法访问。该攻击事件一直持续到当地时间 13 点 45 分左右。该公司在官网表示将追查此事，并将发布事件的分析报告。


**图 1-1Dyn 官方确认[1]**


**图 1-2 官网事件状态更新情况[2]**

本次Dyn遭到攻击影响到的厂商服务包括：Twitter、Etsy、Github、Soundcloud、Spotify、Heroku、PagerDuty、Shopify、Intercom，据称 PayPal、BBC、华尔街日报、Xbox 官网、CNN、HBO Now、星巴克、纽约时报、The Verge、金融时报等的网站访问也受到了影响。Dyn 公司称此次 DDoS 攻击事件涉及 IP 数量达到千万量级，其中很大部分来自物联网和智能设备，并认为攻击来自名为“Mirai”的恶意代码。

黑客组织 NewWorldHackers 和 Anonymous 宣称对此事件负责，此事件被认为是用以抗议正在厄瓜多尔驻英国大使馆避难的维基解密创始人阿桑奇遭遇断网的事件。

***名词解释：DNS 服务器，是进行域名和与之相对应的 IP 地址转换的服务器。DNS 中保存了一张域名和与之相对应的 IP 地址的表，以解析消息的域名。根据解析结果进行目标站点访问。若 DNS 服务器遭受 DDoS 攻击，则无法正常解析域名，故用户无法访问对应目标站点。***

## 2 安天对智能设备僵尸网络的捕获分析情况

目前，依托 IoT 设备的僵尸网络的规模不断增长，典型的 IoTDDoS 僵尸网络家族包括 2013 年出现的 CCTV 系列、肉鸡 MM 系列[3]（ChiekenMM，数字系列 10771、10991、25000、36000）、BillGates、Mayday、PNScan、gafgyt 等众多基于 Linux 的跨平台 DDoS 僵尸网络家族，安天对这些木马的规范命名如下。

| 家族名称 | 变种数量 | 样本 HASH 数量 |
|---|---|---|
| Trojan[DDoS]/Linux.Mirai | 2 | 大于 100 |
| Trojan[DDoS]/Linux.Xarcen | 5 | 大于 1000 |
| Trojan[DDoS]/Linux.Znaich | 3 | 大于 500 |
| Trojan/Linux.PNScan | 2 | 大于 50 |
| Trojan[Backdoor]/Linux.Mayday | 11 | 大于 1000 |
| Trojan[DDoS]/Linux.DnsAmp | 5 | 大于 500 |
| Trojan[Backdoor]/Linux.Ganiw | 5 | 大于 3000 |
| Trojan[Backdoor]/Linux.Dofloo | 5 | 大于 2000 |
| Trojan[Backdoor]/Linux.Gafgyt | 28 | 大于 8000 |
| Trojan[Backdoor]/Linux.Tsunami | 71 | 大于 1000 |
| Worm/Linux.Moose | 1 | 大于 10 |
| Worm[Net]/Linux.Darlloz | 3 | 大于 10 |

其中在本次事件中被广泛关注的 Mirai 的主要感染对象是物联网设备，包括：路由器、网络摄像头、DVR 设备。DDoS 网络犯罪组织早在 2013 年开始就将抓取僵尸主机的目标由 Windows 转向 Linux，并从 x86 架构的 Linux 服务器设备扩展到以嵌入式 Linux 操作系统为主的 IoT 设备。

*Mirai 日语的意思是“未来”，研究人员将新变种命名为“Hajime”，日语的意思是“起点”。*

安天捕获并分析了大量关于智能设备、路由器的恶意样本，并配合主管部门对部分设备进行了现场取证。这些设备主要是 MIPS、ARM 等架构，因存在默认密码、弱密码、严重漏洞未及时修复等因素，导致被攻击者植入木马。由于物联网设备的大规模批量生产、批量部署，在很多应用场景中，集成商、运维人员能力不足，导致设备中有很大比例使用默认密码、漏洞得不到及时修复。包括 Mirai 等针对物联网设备 DDoS 入侵主要通过 telnet 端口进行流行密码档的暴力破解，或默认密码登陆，如果通过 Telnet 登陆成功，就尝试利用 busybox 等嵌入式必备的工具进行 wget 下载 DDoS 功能的 bot，修改可执行属性，运行控制物联网设备。由于 CPU 指令架构的不同，在判断了系统架构后一些僵尸网络可以选择 MIPS、arm、x86 等架构的样本进行下载。运行后接收相关攻击指令进行攻击。

从一个 Mirai 的样本里面可以看到如下的弱密码：

| root | admin | user | login | guest | support | oracle | netman | operator | Administrator |
|---|---|---|---|---|---|---|---|---|---|

| cisco | telnet | device | tech | netgear | toor | oracle | netgear1 | changeme | vizxv |
|---|---|---|---|---|---|---|---|---|---|
| 7ujMko0vizxv | juantech | realtek | xmhdipc | hi3518 | Zte521 | zlxx | supervisor | smcadmin | system |
| dreambox | meinsm | ubnt | klv123 | anko | xc3511 | 1234 | maxided | 12345 | 123456 |
| default | pass | vagrant | klv1234 | jvbzd | 7ujMko0admin | ikwb | password | | |

安天在此前跟进 IoT 僵尸网络跟踪分析过程中，发现如下包括 DVR、网络摄像头、智能路由器的品牌中有部分型号存在单一默认密码问题。


**图 2-1 部分型号存在默认密码的设备品牌**

Mirai Botnet 的相关源代码于 2016 年 9 月 30 日被一名 ID 为『Anna-senpai』的用户发布在 hackerforums 论坛。该用户声称，代码出于『让用户增加对安全工业的重视程度』的目的而发布。在代码被公布后，相关技术立刻被运用到其他的恶意软件项目中。在 2016 年 10 月 4 日，这份代码被上传到 github 上并很快被 fork 逾千次。[6]

安天 CERT 对 10 月 4 日上传到 github 上的 Mirai 源码进行了相应分析，梳理了其代码结构：

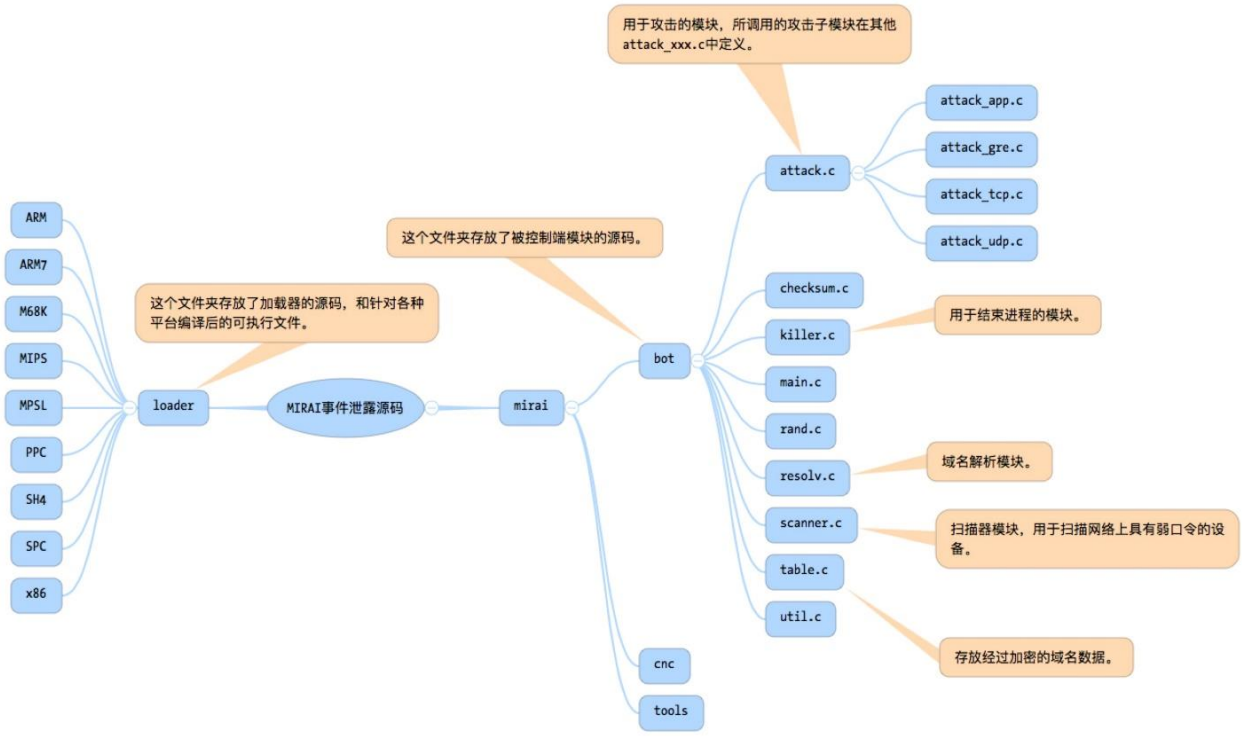


**图 2-2Mirai 源码目录结构分析**

泄露出的 Mirai 事件相关源码主要包括两部分：

（1） loader：加载器，其中存放了针对各个平台编译后的可执行文件，用于加载 Mirai 的实际攻击程序。

（2） Mirai：用于实施攻击的程序，分为 bot（被控制端，使用 C 语言编写）和 cnc（控制端，使用 Go 语言编写）两部分。

被控制端具有以下模块：

| 模块文件名 | 模块作用 |
| --- | --- |
| attack.c | 用于攻击的模块，所调用的攻击子模块在其他 attack_xxx.c 中定义。 |
| checksum.c | 用于计算校验码的模块。 |
| killer.c | 用于结束进程的模块。 |
| main.c | 主模块。用于调用其他子模块。 |
| rand.c | 用于生成随机数的模块。 |
| resolv.c | 用于解析域名的模块。 |

| | |
|---|---|
| scanner.c | 用于扫描的模块，可以扫描网络上可被攻击（如使用弱口令）的设备。 |
| table.c | 用于存放经过加密的域名数据的模块。 |
| util.c | 用于提供一些实用工具的模块。 |

类似的“开源”行为提供了极坏的示范性，会进一步降低其他攻击者危害 IoT 设备的成本。鉴于此，本文不对代码进行解读。

## 3 安天对 IoT 僵尸网络的监测情况

安天的态势感知与监控预警系统可以对僵尸网络的样本传输、上线控制、攻击指令进行持续监控。除了 Mirai 相关事件外，我们也可以看到 IoT 僵尸网络对其他目标的攻击事件。

| 攻击起始开始时间 | 样本家族（原厂命名） | 攻击目标 | 攻击类型 |
|---|---|---|---|
| 2016-10-22 9:36:48 | Mayday 家族 | 203.195.*.*:15000 广州腾讯 | tcp flood |
| 2016-10-20 8:12:57 | DDoS 家族 | www.52***.com X X 阁 | |
| 2016-10-20 1:36:20 | DDoS 家族 | www.ssh***.com/user.php 深圳X X X X X X 公司 | |
| 2016-10-918:52:35 | Billgates 家族 | 121.199.*.* 杭州X X 云 | |
| 2016-9-5 10:57:00 | Billgates 家族 | 59.151.*.* 北京X X 通 | |

**表：典型的 IoT 僵尸网络攻击事件**

2014 年之前使用 Linux 系统的 IoT 设备被植入恶意代码主要通过扫描弱密码。但在破壳漏洞(CVE-2014-6271)[5]出现后，互联网上也出现了大量利用该漏洞进行扫描植入恶意代码事件。根据当时安天蜜罐系统捕获的情况来看，破壳漏洞出现后，针对 Linux 主机入侵的事件呈现全面上升趋势。安天发现的首例通过破壳漏洞实际感染的事件是在 2014 年 9 月份[6]。而后安天 CERT 陆续发了多篇 IoT 设备上的恶意代码分析报告如:《利用路由器传播的 DYREZA 家族变种分析》[7]、《黑客用 HFS 搭建服务器来传播恶意代码》[8]，另有一篇《Trojan[DDOS]/Linux. Znaich 分析报告》当时并未公开，因此作为本报告附件。而其他少数具备获取主机权限的漏洞也发现被攻击者利用。

## 4 分析小组的一点思考

安天分析小组认为，IoT 僵尸网络的快速蔓延来自如下因素的组合：

1、 随着小到智能家居、大到智慧城市的物联网蓬勃发展，在线 IoT 设备数量大幅增加；

2、 随着作为主流桌面操作系统的 Windows 的内存安全（如 DEP、ASLR、SEHOP）等方面的能力不断强化，依托远程开放端口击穿 Windows 变得日趋困难，但对于普遍没有经过严格的安全设计的 IoT 设备的远程注入的成功率则高的多。

3、 IoT 设备自身多数未嵌入安全机制，同时其又多半不在传统的 IT 网络之内，等于游离于安全感知能力之外，一旦遇到问题有的也不能有效响应。

4、 IoT 设备往往更多 24 小时在线，其是比桌面 Windows 更“稳定”的攻击源。

两年前，安天论述了“威胁将随‘互联网+’向纵深领域扩散与泛化”的观点[8]，并使用泛化（Malware/Other）一词来说明安全威胁向智能设备等新领域的演进，而正如我们所担心的那样，安全威胁在智能汽车、智能家居、智能穿戴，大到智慧城市中已经无所不在。


图 4-1 网络安全威胁泛化与分布图（引自安天 2015 年网络威胁年报[8]）

因此，这次针对 Dyn 的 DNS 服务的大规模 DDoS 事件中，安天更重视其中暴露的 IoT 安全问题。尽管 DNS 的确被很多人认为是互联网的阿喀琉斯之踵。但我们同样不要忘记，互联网是依托 IP 地址联通的，而域名是为便于人记忆而产生的。对于北美大型行业用户来说，其更多广泛采用 VPN 和 IP 地址链接，其基本系统运转并不依赖 DNS 的解析。因此，如此大流量的 DDoS，尽管给网民访问网站带来一定阶段性的不便，但其并不足以冲击北美社会运行和互联网的根基。从这个意义上看，这个事件的热度，更多来自媒体对公众感觉的放大，而其实际影响则相对有限。而更危险的行为是有针对性的、有放大效应的针对重要节点的威胁行动，特别是能够产生实体空间后果的威胁。

毫无疑问 DNS 体系是信息基础设施，但 IoT 僵尸网络绝不仅仅是这起攻击事件的道具。物联网就是物物相连的互联网，是未来信息社会重要基础支撑环节之一。物联网是在互联网基础上延伸和扩展的网络，物联网并不仅仅是网络，它还可以利用感知技术、信息传感等技术的嵌入式传感器、设备及系统构建成复杂的涉及实体社会空间的应用，这些应用所在的设备很多都是维系民生的重要节点的关键基础设施设备，甚至包括关键工控设施的基础传感器。被入侵的这些设备本身具有更多的资源纵深价值，这比使用这些设备参与 DDoS 攻击所带来的危险更为严重。其大面积的脆弱性存在，有着更为隐蔽、危害更大的社会安全风险和国家安全风险。只是这种风险，更不容易被感知到罢了。

把公众影响力作为衡量网络安全事件的主要度量衡，是大规模蠕虫爆发时代的惯性。但在安全威胁日趋变得更加定向而隐蔽的时候，如果我们只关注容易看见的威胁，就必然会放过更危险的敌人。克劳赛维茨说：“几乎所有的战局，间歇和平静的时间远远多于行动的时间。”对于安全工作者来说，还有什么比毫无先兆的平静更令人恐惧的呢？

加强 IoT 设备的安全防护，提高攻击入侵 IoT 设备的成本，以及加强 IoT 设备的安全威胁监测预警，是安天已经在进行的工作，就像我们在过去十年让安天 AVL SDK 引擎运行于数万台防火墙和数亿部手机中一样。

## 附录一：参考资料

[1] Dyn 官网事件更新

https://www.dynstatus.com/incidents/nlr4yrr162t8

[2] Dyn 官网事件公告

https://www.dynstatus.com/incidents/5r9mppc1kb77

[3] 安天实验室，DDoS 攻击组织肉鸡美眉分析

http://www.antiy.com/response/Chicken_Mutex_MM.html

[4] https://en.wikipedia.org/wiki/Mirai_(malware)

https://github.com/jgamblin/Mirai-Source-Code

https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

[5] 安天实验室，Bash 远程代码执行漏洞“破壳”（CVE-2014-6271）分析

http://www.antiy.com/response/CVE-2014-6271.html

[6] 安天实验室，“破壳”漏洞相关恶意代码样本分析报告

http://www.antiy.com/response/Analysis_Report_on_Sample_Set_of_Bash_Shellshock.html

[7] 安天实验室，利用路由器传播的 DYREZA 家族变种分析

http://www.antiy.com/response/dyreza.html

[8] 安天实验室，黑客用 HFS 搭建服务器来传播恶意代码

http://www.antiy.com/response/hfs.html

[9] 安天实验室，2015 年网络安全威胁的回顾与展望

http://www.antiy.com/response/2015_Antiy_Annual_Security_Report.html

## 附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为以安天实验室为总部，以企业安全公司、移动安全公司为两翼的集团化安全企业。安天始终坚持以安全保障用户价值为企业信仰，崇尚自主研发创新，在安全检测引擎、移动安全、网络协议分析还原、动态分析、终端防护、虚拟化安全等方面形成了全能力链布局。安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展工程师团队作业能力、缩短产品响应周期。结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了应对高级持续性威胁（APT）和面向大规模网络与关键基础设施的态势感知与监控预警解决方案。

全球超过三十家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近两亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、震网、破壳、沙虫、方程式等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）
http://www.antiy.net （英文）
安天企业安全公司更多信息请访问：http://www.antiy.cn
安天移动安全公司（AVL TEAM）更多信息请访问：http://www.avlsec.com