Import 2022-11-30 11:16

P2P 僵尸网络：回顾·现状·持续监测

360Netlab, RootKiter, LIU Ya

Nov 2, 2022 • 16 min read

缘起

P2P结构的网络比传统的C/S结构具有更好的可扩展性和健壮性，这些优点很早就为botnet的作者所认识到并被用到他们的僵尸网络中。从时间上看，2007年出现的Storm可以算是这方面的鼻祖，那时botnet这种网络威胁刚为大众所知。Storm之后，陆续又有Karen、ZeroAccess、GameOver、Hijime、mozi等20来种P2P botnet先后出现，它们在技术上各有特点，共同点就是规模大、防御难度大，想让它们彻底消失比较困难，比如Mozi在作者已经明确放弃甚至被抓几年之后还在活跃，可谓“百足之虫死而不僵”。

早期的P2P botnet主要针对Windows机器，比如Storm、ZeroAccess以及GameOver感染的都是Windows操作系统。2016年Mirai出现之后，网络上那些大量存在而又缺乏防御的Linux IoT设备开始成为许多botnet的目标，Hijime、mozi、pink等针对Linux设备的P2P botnet陆续出现。

由于P2P网络“无中心”的特点，使用传统的手段来评估其规模有点困难。为了解决这个问题，安全研究人员另辟蹊径，发明了P2P爬虫技术，通过它来跟踪某个P2P botnet，获取节点IP以及下载链接和配置等信息，用于规模评估和定点清除。

360 Netlab致力于及时发现和跟踪大网上活跃的botnet，对P2P僵尸网络当然不会放过，比如我们19年首先公开分析了mozi僵尸网络。为了更好的“看见”威胁，我们基于自身的积累以及业内已有的分析结果构建了一个针对P2P Botnet的工业级别跟踪系统，目标是覆盖所有活跃的P2P botnet，目前基于“历史规模较大”和“近期出现”这两个维度优先跟踪了Pink、Mozi、Hajime、FritzFrog和Panchan这5个仍在活跃的家族，本文基于这个系统产生的跟踪数据简单分析下这5个家族的现状。

PS: 除本文提到的 5 个家族外，也欢迎读者把其他感兴趣的活跃家族留在下方评论区，我们可以酌情优先安排盯梢。

跟踪策略概述

本小节会简单介绍一下跟踪系统中使用的主要跟踪策略，以方面读者理解文中所用数据的产生过程，增强数据的可解释性。

跟踪目标

该跟踪系统以记录节点IP为主要目标，通过模拟通讯协议的方法伪造一个节点，并使其加入对应的P2P网络，参与数据报文交换。每成功完成一次报文交换，便记录下对方的IP，最终实现对目标P2P网络所有节点的记录。

策略展开

PS：由于各P2P家族的协议设计各不相同，所以以下策略并不能全部利用在各个家族上，只能根据实际情况选择其中至少一个策略作为对应家族的跟踪策略。

主动探测：该策略从工作原理上看，有些类似于公网扫描器。它首先向目标节点投喂探测报文，然后对收到的回复报文进行解析，当返回的报文格式符合家族特征时，则将对端认定为对等节点。在实际操作中，我们会先划定一个探测范围，再对这个范围内的节点进行探测（其中探测范围可能由一个可疑网段组成，也可能是从其他策略中产生的可疑节点组成）。

最近通讯：常见 P2P 家族，会在每个节点内存中维护一个近期通讯过的“最近通讯列表”。在部分家族中，其他节点还可通过特定指令获取到这个列表，作为自身启动时的种子列表，从而快速加入 P2P 网络。我们可以通过遍历这个“最近通讯列表”，发现更多的对等节点。

节点心跳：当一个节点维护了“最近通讯列表”后，这个节点一般都会定期向列表中的节点发送心跳报文，声明自身在线情况。基于此，我们可以将“伪造节点”加入对

方的活跃列表中，以便于随时获取相应节点的活跃情况。一些情况下，还会通过发送心跳报文的方式保证自己不被踢出列表。

守株待兔：以Hajime 和Mozi 为例，这两个家族会利用“分布式哈希表技术”来实现其P2P网络结构。该技术在设计时为了加速数据查找速度，加入了一个信息到节点距离的规则，并将待存储信息优先保存在距离较近的那些节点上。基于此规则，我们在获知待获取信息后，可以伪造出一个距离该信息最近的节点等待其他节点的到来，当其他节点尝试从伪造节点获取对应家族的信息时，我们就可以直接将对方IP作为跟踪结果记录下来。

数据含义

跟踪家族选择依据

要想准确估计 P2PBotnet 的整体情况，选择哪些家族很重要，理想状态下肯定是把所有家族都放到一起进行比较，才客观公正，但每增加一个家族都会提高系统整体的完成难度，这是无法一蹴而就的。所以，我们考虑从以下两个维度来筛选合适的家族进行跟踪，以保证最终结果的相对客观。

基于规模: 在选择家族时，最优先考虑的指标就是要规模够大，或者说曾经历史上的规模够大，这样才能保证我们的评估结果有说服力，所以“Hajime”/“Mozi”/“pink”毫无疑问的中选了。

近期披露： 其次的选择就是新出现，并已经活跃一段时间，以避免后来者居上的情况发生，基于此，我们选择了本年新披露的 “panchan” 和 “frizefrog”作为跟踪目标。

受控端IP的含义

视宿主设备类型而定，受控端IP的含义会存在一些挑战，并不能直接反应受感染设备的真实数量。

受控宿主为常年在线服务器：这类服务器为了能够稳定的提供服务，其公网IP一般不会变化。此时受控端的公网IP和设备数量间有稳定的对应关系。

受控端宿主为IoT设备：这类设备一般出现在居民网段内。居民上网时，一方面会出现多户居民共用同一公网出口的情况（NAT网络），另一方面还会有拨号上网按时计费的情况，使居民的IP地址频繁变动。这会导致公网IP与设备间的映射关系出现较大的不确定性。多设备共用一个公网IP(NAT场景)，在一个时间窗口内设备多次切换不同的IP（拨号上网场景）。

各家族日活趋于稳定

作为对比，如果我们把 8月以来每个周一的日活数作为抽样，来绘制中长期跟踪图，如下所示：

从量级上，我们能首先得出，5个家族在日活规模上的大小关系：

Pink > Hajime > Mozi >> FritzFrog <> Panchan

其次，还可以看出，在三个月以来，各家族的日活数据变化并不大（关于 Pink 在8月份的波动情况见下文的讨论，这里暂时忽略）。面对这样的现象，我们大致讨论出了以下几点原因，供大家参考：

1. P2P 类型的僵尸网络，天然难以清理。集中式的僵尸网络只要打掉主控端，受控端很容易失去活性逐步被其他网络蚕食。而P2P类型则不存在严格的主控端，每个节点都是自发的扩展和传播，想要完全在网络上清理干净很难。
2. IoT类型的设备不会频繁更换和升级。这些僵尸网络的宿主大部分以 IoT 设备为主，不更换意味着长期处在“染毒”的状态，设备系统不升级，意味着长期处在“易感染”的状态。综合下来，这些僵尸网络的节点数量就会处在一个相对稳定的状态下。
3. 长期闷声，更新也不频繁。对于僵尸网络来说，每次“增加”或“减少”传播策略，一般都会引起僵尸网络节点数量的波动。而上述5中僵尸网络在近期并没有看到更新。所以节点数量会维持在一个相对稳定的状态。

4. 它们造成的恶劣影响，还不足以使安全社区产生强烈的清理愿望。另一方面，它们很长一段时间都没有更新，也没有机会在大众视野中亮相，这也会降低安全社区处置的欲望。

按家族分别统计

Pink

Pink 家族曾在中国境内感染了超过百万级的设备，其非实效性指令通过 P2P 传递，实效性强的指令通过集中控制的方式发布。是一个设计巧妙的 P2P 僵尸网络家族。更多相关信息可参考我们曾经发布过的报告：

《Pink, a botnet that competed with the vendor to control the massive infected devices》

地理分布

如图所示，Pink的影响范围是以国内IoT设备为主，下面是其在国内的分布情况：

日活波动

值得特别提到的是，该家族7月份以来的日活数据有较大的波动，首先在7月12日开始的一个星期内下降了一个数量级，日活达到2万左右级别，随后在8月20日之后的一段时间瞬间归零10天左右，9月份又回到2万级别日活。日活波动情况可参看下图：

为了分析波动原因，我们分别选取 7月12日/7月26日/9月1日 的日活数据分别绘制地理分布图，发现，大部分省份的日活数量发生显著的降低。如下三图所示：

基于以上内容，我们推测，在7月份，各省份进行了较为统一的处置工作，使受感染设备的数量出现大幅下降。而在8月末的波动中，则更可能是类似于防火墙短期规则产生的效果，阻断了跟踪器同PINK节点的通讯。

Hajime

Hajime 的出现时间与 MIRAI 同年，前后差不到几个月，其提示信息中一直声称是由“白帽子”运营的。Hajime 的各组件功能也以自传播为主要目标。其组件间的通讯及管理，大量使用了非对称加解密算法的特性，是一个极为经典的 P2P 僵尸网络家族。更多详细资料可参考我们曾经发布过的报告：

《Is Hajime botnet dead?》

地理分布

伊朗居首

作为IT从业者，提到伊朗，能想到的只有“伊核协议”或者“头巾”，似乎很难把它和“电子化”扯上关系。即使是多次在IoT设备感染列表的前列中看到来自伊朗的IP，也总觉得伊朗不会有那么多的智能设备，大概是数据失真了。

近期有机会在“俄乌战场”上看到“伊朗无人机”发挥的效果，可以说是挺超出预期的。现在笔者开始想，如果排除数据失真，就意味着伊朗在一些地方是超出多数人想象的，虽然看到的这些东西还远谈不上先进，但是他们能大量的制造无人机，提纯核原料，网络上还有着大量的智能设备，这些侧面都表明他们在“工业化”和“电子化”上是有积累的，背后肯定有大量受过高等教育的工程师。他们有着和中西方完全不同的文字和文化，正在另一个世界里猥琐发育呢。

Hajime 中的CPU分布情况

Hajime是基于文件传递构建的P2P网络，每个Hajime在运行期间，会尝试寻找最新版本的 .i.xxx 和 atk.xxx 文件(比如：atk.arm7/.i.arm7)，这就给了我们评估“Hajime网络”中 CPU 分布情况的一个机会。当 Hajime 节点向我方询问哪些节点包含相应文件时，会得到一次 DHT.search 计数。当 Hajime 节点向我方请求下载相应文件

时，会得到一次 uTP.Request 计数。两种文件，两种计数，汇总后就可以得到如下四张饼图分布情况：

基于以上饼图，我们可以确定，在 Hajime 网络中，MIPS 的宿主最多，远超其他类型宿主之和，而MIPSEL 的宿主节点最少。

如果考虑到 Hajime 曾集成过大量的漏洞用于传播，这个数据甚至可以在一定程度反应各类型CPU在智能设备中的分布情况。

Mozi

Mozi 起初是一个以 DDoS攻击 为获益目标的P2P家族，后来还增加了挖矿获益的部分。其网络拓扑是以 DHT 协议为基础，构建起来的。更多的信息可以参考我们发布过的报告。

《Mozi, Another Botnet Using DHT》

《The Mostly Dead Mozi and Its' Lingering Bots》

地理分布

从排名上看，第一严重是中国，第二严重是印度。前两年中印边境闹磨擦的时候，正赶上大量 Mozi 的节点从印度扫描国内设备，还闹的大家有些紧张。后来嘛，抓到人了，就又不那么紧张了。

FritzFrog

FritzFrog 是一个以挖矿为获益目标的 P2P 家族，其依托于 SSH服务构建起 P2P网络。由 akamai 最先披露。更多详细资料可参考下面的报告（有趣的是，它的收益钱包地址和 Mozi 有关）：

《FritzFrog: P2P Botnet Hops Back on the Scene》

地理分布

FritzFrog中的账户口令

由于 FritzFrog 的P2P机制是基于SSH实现的，所以爬取回来的数据中存在宿主机器口令组合，我们可以看一下口令组合的分布情况，统计一下哪些口令贡献了最多的宿主机

组合排名第一的是一个 `1` 开头的密码，有看客能把它补全不?

Panchan

Panchan 是一个 Go 语言开发的 P2P 僵尸网络，以挖矿为获益手段，利用 SSH 弱口令为传播途径。其代码中包含大量 日文片假名，这表明 Panchan 的开发者可以熟练使用日文。另一个有趣的点在于：它在监听端口上，利用协议复用的思路实现了一个交互控制台，允许管理员从网络上对节点进行一些简单的查询和管理工作。更多详细信息可参考如下报告：

《Panchan's Mining Rig: New Golang Peer-to-Peer Botnet Says "Hi!"》

地理分布

panchan 的日活长期稳定在两位数，相比其他几个动辄5位数日活的家族来说，感染规模并不算大。

别被美国的红色吓到，其实只有14个日活。

结论

本文利用跟踪数据，综合评估了各 P2P 型僵尸网络的规模和活跃情况，并从不同的跟踪数据中看到了一些网络安全以外的现象。

解决方案

基于Netlab多年研究工作孵化的360全系列DNS安全产品均已支持文中远控服务器的拦截和检测，同时内置多种算法可有效发现和拦截各种未知威胁，建议企业客户接入360 DNS安全SaaS平台或部署本地360DNS安全产品，及时防范此类新型威胁，避免企业资产失陷。联系人: wangkun-bd@360.cn

联系我们

感兴趣的读者，可以在 twitter 或者通过邮件**netlab[at]360.cn**联系我们。

— 360 Netlab Blog - Network Security Research Lab at 360 —

Import 2022-11-30 11:16

Import 2022-11-30 11:16

P2P Botnets: Review - Status - Continuous Monitoring

Origins P2P networks are more scalable and robust than traditional C/S structures, and these advantages were recognized by the botnet authors early on and used in their botnets. In terms of time, Storm, which appeared in 2007, can be considered the progenitor of this area, when botnet threats were

Botnet

Fodcha Is Coming Back, Raising A Wave of Ransom DDoS

Background On April 13, 2022, 360Netlab first disclosed the Fodcha botnet. After our article was published, Fodcha suffered a crackdown from the relevant authorities, and its authors quickly responded by leaving "Netlab pls leave me alone I surrender" in an updated sample.No surprise, Fodcha's authors

DDoS

See all 249 posts →

Nov 3, 2022 • 9 min read

Oct 31, 2022 • 16 min read