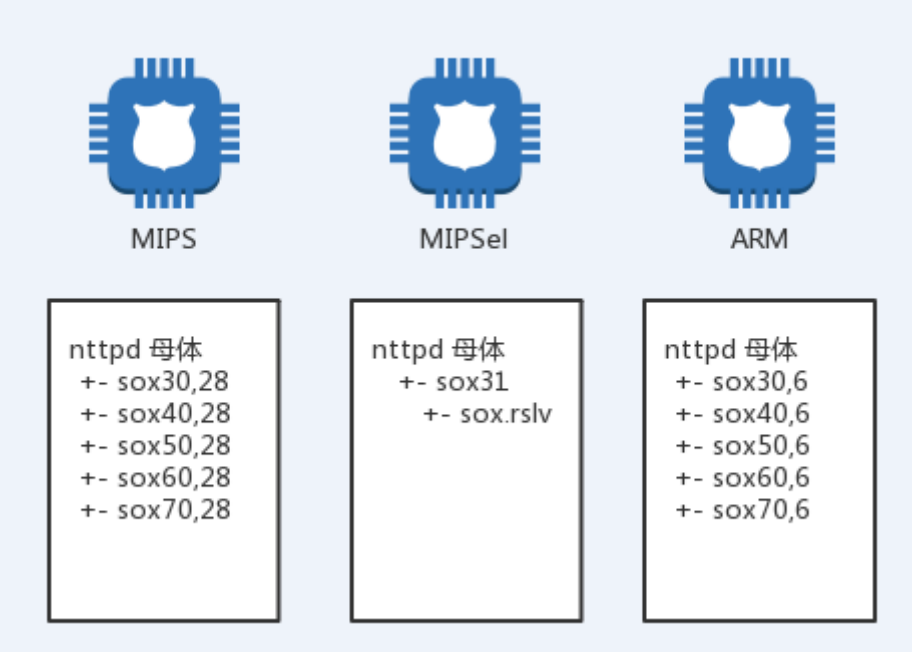
《TheMoon 僵尸网络》

##概要

TheMoon 僵尸网络属于 IoT 僵尸网络的一种，在公开信息中最早可追溯至 2015 年初。稳步发展至今，版本号也从 nttpd,14 更新到了 nttpd,21，它一直没有引起太多人的关注，可以说其比 Hajime 更神秘。在最新版中，TheMoon 已经发展为一个庞大的僵尸家族，其共存样本量（ELF 样本）已经超过 15 个（除此之外我们还收集到 3 个各不同的 shell 脚本）。其家族谱系（非功能模块未展示）如下图所示:



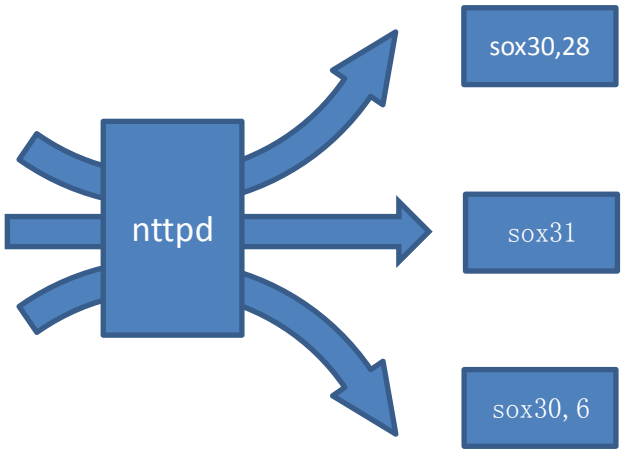
图中所有 sox 样本同时共存，可从“nttpd 母体”中传递并启动。

整体框架

从样本的逆向结果看，TheMoon 可同时具有 2 种工作模式，分别为主控模式和 P2P 模式，但其 P2P 模式现阶段还不够健全，虽有相关代码片段但仍处于未使用状态，所有指令仍然通过主控模式直接传递。
现阶段 TheMoon 的功能型 ELF 文件可大体分为两类，“母体 nttpd”及“sox 模块”。

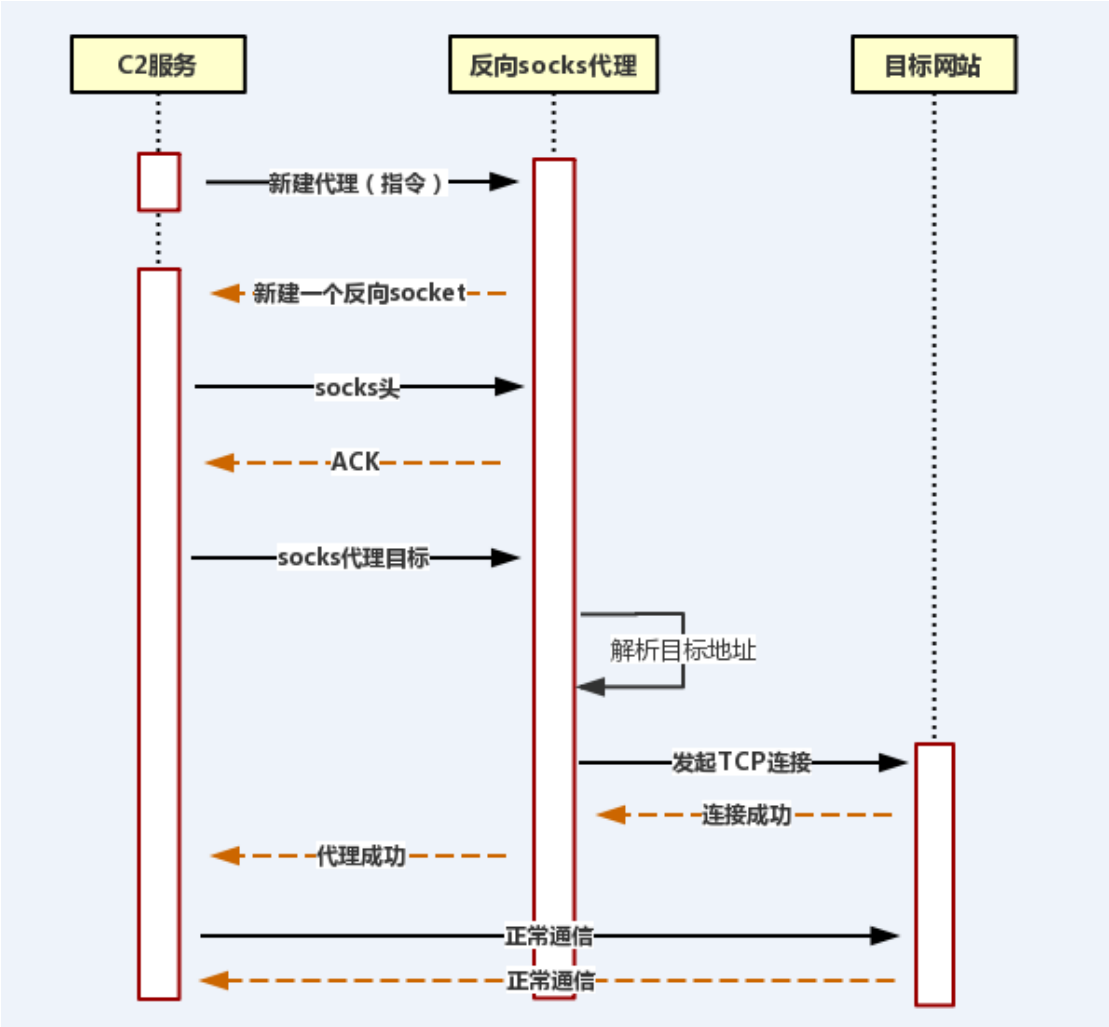
母体 Nttpd

其中“感染母体 nttpd”是样本传播阶段种植到 IoT 设备中的基础文件，它负责维护了一个模块分发网络，通过这个网络，攻击者可随时向僵尸网络投入新的执行模块，以便随时增加对新功能的支持。



Sox 模块

该模块可通过 nttpd 母体被分发至受感染设备。其最核心的功能便是提供一个 socks 代理服务。攻击者可以随时使用这个代理服务访问其他网络资源。在早期版本中，该模块被设计为一个正向的无认证机制的 socks 代理，其监听端口视 IP 地址内容而定，在《![解密“智魁”攻击行动](https://security.alibaba.com/blog/blog.htm?spm=0.0.0.0.mO6T6P&id=26)》中有对该现象较为详细的阐述，这里不再赘述。而在其近期的实现版本中，这个 socks 服务变成了一个反向提供的代理服务。新的实现方式，提高了他人窃取代理服务使用权的难度，相对的也降低了网络提供服务的效率及灵活性。该实现的时序图如下图所示：



样本细节

注册包标记值

同其他常见僵尸网络不同，TheMoon 注册包中含有两个标记值，只有当这两个标记值均设置正确后，才是一个合法的注册包。有趣的是，这两个标记值在不同功能或 CPU 平台下表现不同。具体差别情况如下表所示:

样本名	所属 CPU 结构	标记值 1	标记值 2
nttpd,21-mips-be	MIPS	0xb7	0x6D61641C
sox30,28-mips-be		0xc7	0x6D61642C
sox40,28-mips-be			
sox50,28-mips-be			
sox60,28-mips-be			
sox70,28-mips-be			
nttpd,21-mips-le	MIPSel	0x8f	0x6D6163F4
sox,31		0x9F	0x6D616404

nttpd,21-arm-le	ARM	0x84	0x6D6163E9
sox30,6-arm-le		0xD2	0x6D616437
sox40,6-arm-le			
sox50,6-arm-le			
sox60,6-arm-le			
sox70,6-arm-le			

文件的压缩传输

从 nttpd,19 版起，TheMoon 的 ELF 文件开始逐步更换到使用压缩形式传输。
虽然传输的文件仍然是 ELF 可执行文件，但样本的实际内容却以压缩形式保存在了文件的 data 段中。所以样本在运行后，会先将 data 段的压缩内容还原到当前目录的一个隐藏文件中，随后再执行新生成的文件。这种方式的好处有两点：

1. 可以用更少的字节数传递 ELF 文件，提高网络利用率；
2. 给逆向分析人员带来了一定的困扰；

该样本使用的压缩算法是一个公开的压缩算法，可以 rfc1950、rfc1951 中找到具体的设计细节，相信有了这个提示，可以降低给逆向分析人员带来的困扰。

PS：这一块的的内容是方丈帮忙确认的，并完善了代码实现。

关于 MIPSel

仔细阅读以上图文会发现，TheMoon 的大部分样本都集中在 ARM 和 MIPS 体系中，且两个平台的样本具有一一对应关系，而 MIPSel 则仅包含两个样本（其实是 3 个，sox,31 样本会孵化一个名为 sox.rslv 的文件）。这个细节令笔者也困惑了相当一段时间，一直以为是自己的跟踪系统出了问题，但经一系列排查后，排除了这种可能性。最后一个有趣的推测浮出了水面，那就是：**攻击者试图用 MIPSel 体系的样本为其他样本打掩护！**这是一个比较有意思的推测，理由如下：

1. MIPSel 被全面曝光，该体系危险系数增加。
2. 未曝光就代表没被发现，由于大家没提 ARM 和 MIPS，这就表明这两个平台现在很安全。
3. 既然 MIPSel 已经被曝光，那我就推迟更新，这样安全人员的注意力将集中在这个平台，可以在一定程度下为其他平台打掩护。

我准备在这一小节详细阐述下理由。

从 TheMoon 曝光说起

在互联网上能搜到关于 TheMoon 的重要报告有两篇，分别为《![解密“智魁”攻击行动](https://security.alibaba.com/blog/blog.htm?spm=0.0.0.0.mO6T6P&id=26)》和《![TheMoon](https://blog.fortinet.com/2016/10/20/themoon-a-p2p-botnet-targeting-home-routers)》而这两篇报告无论在截图还是分析内容上均以 Mipsel 版本的样本为主，这导致 Mipsel 系列的样本被全方位曝光，任何没有接触到样本的人均可以通过这些报告了解到 Mipsel 样本的部分细节。这一定会让作者多少有些警觉起来。

未曝光就代表没被发现

Fortinet 在《TheMoon》这篇报告的一张截图中，直接公布了 TheMoon 的 5 个 C2 地址，但如果是细心的读者，会发现该图公布的地址其实有 6 个，只不过这个地址未被直接标出。这个未标出的 IP 地址是 185.53.8.22，其对应的 hex 码为 0xB9350816，如下图所示：

```
HardcodedPeers: .word 0xB9350816          # DATA XREF: func_r
                                          # func_RegisterToHa
                                          # func_OP01handler:
                                          # .got:0041A198↓o
                .word 0xB9381EBD          # 185.56.30.189
                .word 0xD94FB6D4          # 217.79.182.212
                .word 0x55728714          # 85.114.135.20
                .word 0x5FD58FDC          # 95.213.143.220
                .word 0x2E94129A          # 46.148.18.154
                .byte    0
```

图片来源《TheMoon-A P2P botnet targeting Home Routers》

这本来只是个无伤大雅的小问题，然而在随后的更新中却出现了一个有趣的现象，这个被间接曝光的 IP 在所有版本的 nttpd 中均有出现/使用，并一直持续到最新的 nttpd,21 版本中。比如在 nttpd,21-mips-be-t2-z 中的截图如下：

```
.data:0041A2FF                  .byte    0
.data:0041A300                  .globl net_twn_tab
.data:0041A300 net_twn_tab:     .word 0x5BD79E76          # DATA XREF: sub_4036C
.data:0041A300                                            # sub_4036C4+2A4↑o ...
.data:0041A304                  .word 0xB9350816
.data:0041A308                  .word 0x95CAD3E3
.data:0041A30C                  .word 0xD06E4222
.data:0041A310                  .word 0xADD0DB2A
.data:0041A314                  .word 0
```

PS: 样本 MD5: 53494b8867654d06ea1b5aec0ed981c1 该样本是压缩样本，分析需先解压还原

PPS: 那我为什么在这个图中不标记注释呢，因为这样的话作者就不知道我已经曝光 C2 地址了 ☺

从这个现象，不难得出一个推测，TheMoon 的作者并不懂程序逆向，你没指出来，我就认为你没看到，这是一个真实版的“掩耳盗铃”。

MIPSel 已经不安全了

在曝光后（《TheMoon》中曝光的样本为 nttpd,17-mips-el 版本），作者有了一个重要发现：MIPSel 版本被曝光了，有人盯上它了，好在其他平台报告里没提，这真是太棒了。于是乎，又一次掩耳盗铃上演了，作者虽然在每次更新中都带着 MIPSel 更新，但这个系列的样本内容一直无太大修改，主要的修改都集中在了 MIPS 和 ARM 版中。下面以对样本压缩这个特性的支持情况为例来看作者的更新情况。

	nttpd,18	nttpd,19	nttpd,20	nttpd,21
ARM	-	-	✓	✓
MIPS	-	✓	✓	✓
MIPSEL	-	-	-	-

上表可以看出，对压缩支持上 MIPSel 已经慢了若干拍（红对号为支持压缩）。

另一方面，sox,31-mips-el 这个样本本身也一直在原地踏步，该样本是我在 2018-01-07 获取到的最新版本，其 MD5 为 7138d91df4b03a014a9317d5cc1bf1ba。该样本运行后会先释放一个名为 sox.rslv 的文件，这是一个负责做 dns 解析的文件，同时，sox,31 这个样本会监听一个端口并用于 socks。这是一个正向的 socks 服务，而这个工作模式和《解密“智魁”攻击行动》中提到的一模一样。也就是说这种工作模式已经持续了 2 年多没变了，对比下另两个 CPU 体系下的 sox 样本现已支脉庞杂，每个架构下都有从 sox30 到 sox70 五种样本，代理模式也从正向 socks 代理切换为反向 socks 代理。

推迟更新

以上种种现象，并不能说明作者停止了对这个系列的更新，起码版本号还一直在推进中。那么我们只能认为作者在有意推迟对 MIPSel 平台的更新。从对压缩的支持情况，我们不难发现，MIPSel 一直没有支持，逆向分析人员仍然可以参考已有报告分析该样本，并得到一些初步结论，当尝试深入跟踪时会发现该系统下没有收到有价值的指令，而这一套工作下来，几天的时间就过去了，基本也没有心思再去分析另两个平台的压缩算法和样本细节了，从我们接受的 sox 指令来看，指令源主要源于 arm 平台，mips 平台同步了 5 个 sox 模块，mipsel 则仅同步到一个 sox 模块且 sox 模块也没有后续指令，关于跟踪到的具体内容，我将在后面章节详细阐述。

TheMoon 跟踪

指令时间选取(20180104 11:41 到 20180108:120:13) 之间。

Nttpd 指令接收情况

nttpd 构建的是一个文件同步网络，其指令主要用于下载新文件，指令统计情况如下所示。

	指令条数	样本同步情况	获取到的样本名
mips-be	45	8 个	10f57a21bc5e533fa8462374eb6b74d1__sox70_28 3e865bb785a280c864e742827ba15f18__sox40_28 5c3b756d613148b1fbc1c62e10b1c10e__sox30_28 60f8dd3c0184afd846f8b63c8e0628ac__sox60_28 e41794081e93231d6bcd8c95c5b44e8f__sox50_28 b2ac8ad1646cef7d648df76c18688c57__plk_1 9a9fecefceb47ee2247cae26b88472cf__reg_0 e75734a7d21c184dc542c0c1c5e4fbeb__soxP_0
mips-le	4	2 个	7138d91df4b03a014a9317d5cc1bf1ba__sox_31 8ea383b35f98eb007895b697bcf3741b__dns_1
arm-le	51	8 个	1fba1831c5590a3aaafe09b8d2281fbc__plk_1 293b1c731def4243537d68334da3a8a0__sox30_6 48acb7e812f22ee4f9aa49548c1a3d2c__sox60_6 8c7e68017929afe171de59a8d2dc884c__sox70_6 8e69b450e87e7bd89d521026744f3f78__sox50_6

			f485be9faa3eb147df1eb173e149c3d6__sox40_6 9a9fecefceb47ee2247cae26b88472cf__reg_0 e75734a7d21c184dc542c0c1c5e4fbeb__soxP_0

Sox 指令接收情况

共收到 sox 请求指令 1339 条（均为 arm 平台的指令，mips 和 mipsel 平台未收到 sox 请求指令），其中成功解析的代理指令 781 条，连接目标域名或地址 231 个，代理数据内容中大部分为明文 web 请求及 HTTPS 加密的数据。在明文请求中共过滤出 364 条 http 请求头数据，将请求头的 Refer 字段和 Host 字段继续过滤后可得到 30 条域名及 Ip 地址数据。分别如下:

109.206.180.190
192.133.137.143
1nqrf.redirectvoluum.com
247-video.net
cdn.datatables.net
c.gcnhu.com
crypto-wealth.bitsociety.co
http://1nqrf.redirectvoluum.com
http://247-video.net/
http://alivedirectory.com/
http://aroundhoustonweddings.com/
http://crypto-wealth.bitsociety.co
http://lucrosa.profit-opportunity.com
http://mmoframes.com
http://naic.org/
http://track.eovnx.com
http://trinibase.com/
i4track.net
lucrosa.profit-opportunity.com
mmoframes.com
ninjagod.com
search.clickmenia.com
served.tequilan.club
tangoads.vertoz.com
track.eovnx.com
track.freemmo2017.com
traffic.vespymedia.com
xml.hueads.com
xml.pdn-5.com
xml.vespymedia.com

在这些域名对应的 HTTP 请求中涵盖了色情，赌博，大忽悠等广告信息。下面简单贴几个访问 URL 以供娱乐消遣。

跨国版大忽悠	http://crypto-wealth.bitsociety.co/cws-updated.php
	http://lucrosa.profit-opportunity.com/
	http://alivedirectory.com/
	https://www.mycashnetwork.net/p/partial/acceleratedincomeprogram
色情	http://mmoframes.com
	tangoads.vertoz.com/cf?id=7255116551710110118&sid=bMiYQtLV&subid=1770&fid=2315
	ninjagod.com/?source=traffic&id=7708597&position=3&feed_id=1103571&bid=0.000233&signature=dd7ae1419255738ef2154f08ccb7e25a9f1609eaebe0489af6ba43beaba409ee&s2=28da1b3c8e0a4b00fc75a516f33c3329e99945f271c14587e1641815538bb29d&vip=207.148.64.32&ua=Mozilla%2F5.0%28Macintosh%3BIntelMacOSX10.11%3Brv%3A51.0%29Gecko%2F20100101Firefox%2F51.0&sip=108.59.8.71&ssid=837354&tracker=1232-1770
	http://aroundhoustonweddings.com
赌博	http://18clubsg.com/Default.aspx?utm_source=plugrush&utm_medium=S5093348

总结

TheMoon 僵尸网络与常见 DDOS 型僵尸网络不同，其当前的主要工作目标是建立一个 socks 代理资源池，在资源池中会看到一些灰黑色流量的访问。通过近几日的观察，网络大部分时间处于闲置状态，指令数量不多。从已有数据很难看出其套现及盈利模式。

这个网络在收益上似乎是个矛盾体，一方面网络已经持续了 3 年之久，且一直在更新维护，这是一个长期的投入；另一方面网络中数据量很少，即使有盈利也不会太多，很难判断作者这么多年是怎么坚持下来的。