



## RootKiter

Learning and beating botnet...

<http://rootkiter.com>

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



• Nov 3, 2022 • 9 min read

Import 2022-11-30 11:16

## P2P 僵尸网络：回顾·现状·持续监测

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



· Nov 2, 2022 · 16 min read

Botnet

## Threat Alert: Log4j Vulnerability Has Been adopted by two Linux Botnets

The Log4j vulnerability that came to light at the end of the year can undoubtedly be considered a major event in the security community. Honeypot and botnet are our bread and butter, and we have been concerned about which botnets would be exploiting this since the vulnerability was made public.



· Dec 11, 2021 · 4 min read

Log4j

## 威胁快讯：Log4j漏洞已经被用来组建botnet，针对Linux设备

年末曝光的Log4j漏洞无疑可以算是今年的安全界大事了。作为专注于蜜罐和botnet检测跟踪的团队，我们自该漏洞被公开后就一直关注它会被哪些botnet利用。今早我们等来了首批答案，我们的Anglerfish和Apacket蜜罐先后捕获到2波利用Log4j漏洞组建botnet的攻击，快速的样本分析表明它们分别用于组建 Muhstik 和Mirai botnet，针对的都是Linux设备。样本分析 MIRAI 这一波传播的为miria新变种，相比最初代码，它做了如下变动：1. 移除了 table\_init/table\_lock\_val/table\_unlock\_val 等mirai特有的配置管理函数。2. attack\_init 函数也被抛弃，ddos攻击函数会被指令处理函数直接调用。同时，其C2域名选用了一个 uy 顶级域的域名，这在国内也是很少见的。Muhstik Muhstik 这个网络最早被披露于 2018 年，系一个借鉴了Mirai代码的Tsunami变种。在本次捕获的样本中，我们注意到新Muhstik变种增加了一个后门模块lsm，



· Dec 11, 2021 · 5 min read

Import 2022-11-30 11:16

## DNS data mining case study - skidmap

As the foundation and core protocol of the Internet, the DNS protocol carries data that, to a certain extent, reflects a good deal of the user behaviors, thus security analysis of DNS data can cover a decent amount of the malicious activities.

In the early days, typical scenarios for early



· Nov 30, 2020 · 9 min read

DNSMon

## DNSMon: 用DNS数据进行威胁发现

----发现skidmap的未知后门 更新记录 \* [2020-12-07] 在本文发布之后不久，我们注意到该后门的访问模式有了一定的调整。并在最近DNSMon发现攻击者已经启用了新的域名IOC。具体来说有如下变化： 1. 将rctl子域名变更为 r1 2. 新启用了mylittlewhitebirds[.]com, howoldareyou9999[.]com (比原先的howoldareyou999[.]com多了一个字符'9')，franceeiffeltowerss[.]com(比原先的franceeiffeltowers[.]com多了一个字符's')三个域名作为后面的备用域名。具体如下： r1.googleblockchaintechnology[.]com  
r1.howoldareyou9999[.]com r1-443.howoldareyou9999[.]com r1-443.franceeiffeltowerss[.]com



· Nov 25, 2020 · 19 min read

fbot

## The new developments Of the FBot

Update 2019.12.04: Recently we have received quite a few requests of comment about this blog. We feel it necessary to list following facts here: 1. Kenneth Crurrin Schuchman, with nicknames "Nexus" or "Nexus-Zeta", a 21 years old young man, has pleaded guilty on 2019.



· Feb 20, 2019 · 6 min read

DDoS

## FBot 新进展

【更新：2019年12月4日】近期我们多次收到针对本blog的询问。我们决定将一些事实补充列出如下： —— Kenneth Crurrin Schuchman，绰号 Nexus-Zeta，一名21岁的年轻人，已于2019年9月3日向美国阿拉斯加区域法庭认罪。Schuchman的认罪书表明，Schuchman及其同谋者通过感染大批设备，创建了一系列僵尸网络，包括 Satori, Okiru, Masuta, Tsunami, Fbot，并利用这些僵尸网络的DDoS破坏力牟利； —本 Blog 中涉及到的脆弱性并非发生在 Hisilicon。通过后续分析以及安全社区交流，我们确认该脆弱性发生在华为海思的供应链下游厂商。为了保护最终客户的利益，我们决定不公开脆弱性细节、攻击者使用的载荷或者具体厂商名字； —— 华为 PSIRT 对我们披露的安全事件，作出了负责任的响应； 读者在继续阅读本blog时，应当明确 blog 和样本中出现的 Hisilicon 字样，源自 Schuchman 及其同谋者的错误判断。实际上整个 IoT 产业链条庞杂，其体量远超攻击者或者任何单一从业人员能够理解的范围。只有产业界



· Feb 20, 2019 · 8 min read

HNS

## HNS Botnet Recent Activities

Author: Rootkiter, yegenshen HNS is an IoT botnet (Hide and Seek) originally discovered by BitDefender in January this year. In that report, the researchers pointed out that HNS used CVE-2016-10401, and other vulnerabilities to propagate malicious code and stole user information. The HNS communicates through the P2P mechanism, which is

 · Jul 6, 2018 · 3 min read

Botnet

## HNS Botnet 最近活动更新

作者: Rootkiter, yegenshen HNS 僵尸网络 (Hide and Seek) 是最初由 BitDefender 于今年 1月 报告 的一个 IoT 僵尸网络。在那份报告中研究人员指出, HNS 会利用CVE-2016-10401、其他漏洞以及Telnet弱口令投入恶意代码, 有执行任意指令和盗取用户信息的恶意行为, 传播方式类似蠕虫, 感染规模在1月23日至1月24期间快速增长到超过32k。并且, HNS内部通过P2P 机制通信, 这是我们所知继 hajime之后第二个利用P2P通信的IoT 僵尸网络。P2P类的僵尸网络很难被根除, HNS 僵尸网络也是如此。在过去的几个月中 HNS 僵尸网络一直在持续更新, 我们看到其更新活动包括: \* 增加了对 AVTECH全部设备 (网络摄像头、网络录像设备)、CISCO Linksys路由器、JAWS/1.0 Web服务器、Apache CouchDB、OrientDB的漏洞利用; 加上原始报告中提到的2 种, 目前HNS已经支持7种漏洞利用方式; \* 内置的P2P节点地址增加到了171 条;

 · Jul 6, 2018 · 5 min read

Botnet

## 威胁快讯：一次僵尸挖矿威胁分析

友商发布了一个威胁分析 报告, 我们阐述一下从我们的角度看到的情况。核心样本 `hxxp://120.55.54.65/a7` 核心样本是个 Linux Shell 文件, 后续动作均由该样本完成, 包括: \* 挖矿获利 \* 确保资源 \* 逃避检测 \* 横向扩展  
挖矿获利 具体的挖矿动作是由下面一组样本完成的: \* `hxxps://www.aybc.so/ubuntu.tar.gz` \*  
`hxxps://www.aybc.so/debian.tar.gz` \* `hxxps://www.aybc.so/cent.tar.gz` 样本中的挖矿配置如下: \* 矿池地址: `xmr-asia1.nanopool.org:14433` \* 钱包地址:

 · Jun 26, 2018 · 2 min read

Satori

## Botnets never Die, Satori REFUSES to Fade Away

Two days ago, on 2018-06-14, we noticed that an updated Satori botnet began to perform network wide

scan looking for uc-httdp 1.0.0 devices. Most likely for the vulnerability of XiongMai uc-httdp 1.0.0 (CVE-2018-10088). The scanning activities led to a surge in scanning traffic on ports 80

 · Jun 15, 2018 · 5 min read

Satori

## 僵尸永远不死，Satori也拒绝凋零

两天前，2018-06-14，我们注意到 Satori 的作者开始扫描收集 uc-httdp 1.0.0 设备的IP地址列表。这或许是为了针对4月公开的脆弱性 XiongMai uc-httdp 1.0.0 (CVE-2018-10088) 在做准备。这些扫描活动导致了近期在 80 和 8000 端口上的扫描流量大涨。3小时前，就在我们撰写本篇文章的同时，Satori 作者又发布了一个更新版本。这个更新是个蠕虫，针对 D-Link DSL-2750B 设备，对应的漏洞利用在5月25日刚刚公开。僵尸永远不死 Satori 是 Mirai 僵尸网络的一个变种，我们首次注意到该僵尸网络是 2017-11-22。一周之后，2017-12-05，Satori在12小时内感染了超过26万家用路由器设备，成为臭名昭著的僵尸网络。从那以后我们不再使用“一个mirai僵尸网络变种”称呼它，而是给予了它一个独立的名字 Satori。

 · Jun 15, 2018 · 8 min read

Satori

## GPON Exploit in the Wild (II) - Satori Botnet

This article was co-authored by Rootkiter, Yegenshen, and Hui Wang. In our previous article, we mentioned since this GPON Vulnerability (CVE-2018-10561, CVE-2018-10562 ) announced, there have been at least five botnets family mettle, muhstik, mirai, hajime, satori actively exploit the vulnerability to build their zombie army in just 10 days. We

 · May 17, 2018 · 7 min read

Mirai

## GPON 漏洞的在野利用（二）——Satori 僵尸网络

本篇文章由 Rootkiter, yegenshen, Hui Wang 共同撰写。我们在之前的 文章 里提及，在本次GPON漏洞 (CVE-2018-10561, CVE-2018-10562) 公布以来，10天内已经有至少5个僵尸网络家族在积极利用该漏洞构建其僵尸军团，包括 mettle、muhstik、mirai、hajime、satori等等。在上一篇文章里，我们详细介绍了

muhstik 僵尸网络的情况。在那篇文章发布的前后，通过与安全社区共同的努力，我们累积关闭了muhstik僵尸网络在 OVH 上的12 个IP地址，以及在微软网络上的 1 个IP地址。详细的IP地址列表，见附件 IoC部分。【更新：值得一提的是，当前绝大部分这些僵尸网络的漏洞利用部分效果是有问题的。根据我们的估计，只有大约2%的特定版本GPON家用路由器受到这些僵尸网络的影响，绝大部分位于墨西哥。这时由于这些僵尸网络使用PoC的方式造成的。】 其他的僵尸网络包括： \* Satori: satori是臭名昭著的mirai僵尸网络变种，该恶意代码团伙在2018-05-10 05:51:

 · May 16, 2018 · 9 min read

Hajime

## 8291端口告警事件简报

结论 本次8291扫描事件由更新后的Hajime僵尸网络引起，在新版本中，有两个新的特性： 1. 利用对8291端口的扫描来确定存在'Chimay Red' Stack Clash Remote Code Execution漏洞MikroTik设备。 2. 利用上述漏洞...

 · Mar 28, 2018 · 3 min read

Hajime

## Quick summary about the Port 8291 scan

Summary This 8291 scan event is caused by a Hajime botnet variant. Compared to the old Hajime, this one adds two new features: 1. Check port 8291 to determine if the target is a MikroTik device 2. Use...



· Mar 28, 2018 · 2 min read

Android

## ADB.Miner: More Information

This blog is a joint effort of 360 Beaconlab, 360 CERT, 360 MobileSafe, 360Netlab and 360 Threat Intelligence Center. Overview About 48 hours ago, we reported an Android worm ADB.miner in our previous blog. This malware can replicate itself over Android devices by utilizing the opened ADB debugging interface.



· Feb 6, 2018 · 4 min read

Android

## ADB.Miner 安卓蠕虫的更多信息

本篇技术分析，由360手机卫士，360威胁情报中心，360烽火实验室，360-CERT，360网络安全研究院联合发布。综述 大约48小时之前，我们发布文章 报告了ADB.Miner，一种新型的安卓蠕虫。该蠕虫可以借助安卓设备上已经打开的adb 调试接口传播，且初期传播的增速很快，约每12小时翻一番。在过去的48小时内，我

们对 ADB.Miner 做更进一步的分析，目前的结论如下，供安全社区参考：1. 当前感染量已经稳定：日活感染量在增长到7千(2018-02-05 15:00 GMT+8)后不再快速增长。这个数字已经保持稳定了超过 20 小时，可以认为蠕虫已经经过了爆发期，进入稳定期。2. 确认电视盒子被感染：确认被感染的都是安卓设备。进一步分析能够确认部分设备是电视盒子，其他设备不能认定是何种设备，也不能确认是安卓手机 3. 对样本的分析，排除了样本从远程开启 adb 调试接口的可能。



· Feb 6, 2018 · 6 min read

Botnet

## TheMoon :一个僵尸网络的老皇历和新变种

TheMoon 是一个恶意代码家族的代号。早在2014年2月，该恶意代码家族就引起了安全研究人员的普遍关注。在当时，TheMoon是一个针对 Linksys 路由器的、有类似蠕虫式传播行为的僵尸网络。由于其感染传播能力较强，安全社区里的讨论较多。2014~2017年期间，又陆续有各安全厂商对TheMoon恶意代码家族做了分析。报告反应了当时 TheMoon 家族的演化情况。从2017年开始，我们也对 TheMoon 家族做了持续跟踪，并注意到以下的新发现： \* 感染阶段：TheMoon 集成了最近的一组漏洞利用代码，提高其感染能力； \* 运营阶段：TheMoon 的代理网络，由正向代理改为反向代理，避免被安全研究人员探测度量； \* 样本特征：TheMoon 开始使用压缩外壳，提高安全研究人员分析的难度 下文仅仅是我们对 TheMoon 恶意代码家族监控结果的概括描述，详细的技术分析文档可见 TheMoon-botnet.pdf 2017年以前的 TheMoon 2014-02-13，这是我们能查到的 TheMoon 相关最早记录。当时，SANS



· Jan 30, 2018 · 8 min read

Botnet

## 偷盗的艺术: Satori 变种正在通过替换钱包地址盗取 ETH 数字代币

在我们2017年12月5日发布的关于Satori的文章中，我们提到Satori僵尸网络正在以前所未有的速度快速传播。自从我们的文章发布以后，安全社区、ISP、供应链厂商共同协作，Satori 的控制端服务器被 sinkhole、ISP 和供应链厂商采取了行动，Satori的蔓延趋势得到了暂时遏制，但是Satori的威胁依然存在。从 2018-01-08 10:42:06 GMT+8 开始，我们检测到 Satori 的后继变种正在端口37215和52869上重新建立整个僵尸网络。值得注意的是，新变种开始渗透互联网上现存其他Claymore Miner挖矿设备，通过攻击其3333 管理端口，替换钱包地址，并最终攫取受害挖矿设备的算力和对应的 ETH 代币。我们将这个变种命名为 Satori.Coin.Robber。这是我们第一次见到僵尸网络替换其他挖矿设备的钱包。这给对抗恶意代码带来了一个新问题：即使安全社区后续接管了 Satori.Coin.Robber 的上联控制服务器，那些已经被篡改了钱包地址的挖矿设备，仍将持续为其贡献算力和 ETH 代币。到



· Jan 17, 2018 · 10 min read

Botnet

## Art of Steal: Satori Variant is Robbing ETH BitCoin by Replacing

# Art or Steal: Satori Variant is Robbing ETH Bitcoin by Replacing Wallet Address

The security community was moving very fast to take actions and sinkhole the Satori botnet C2 after our December 5 blog. The spread of this new botnet has been temporarily halted, but the threat still remains. Starting from 2018-01-08 10:42:06 GMT+8, we noticed that one Satori's

 · Jan 17, 2018 · 5 min read

IoT Botnet

## Is Hajime botnet dead?

概述 我们于近期决定公开一部分Hajime相关的研究结果及数据，供社区成员查阅。本文的核心内容包含以下几点： \* Hajime跟踪主页上线。结合Hajime的通讯特点（DHT+uTP），我们实现了对Hajime各Bot节点的长期跟踪，同时还在主页绘制了日活及地域分布情况。 \* 通过逆向分析，我们代码级重现了密钥交换过程，在该工作的帮助下，可以随时获取到Hajime网络中的最新模块文件。 \* 跟踪过程中，我们发现一个包含x64配置项的 config 文件，该发现预示着，原作者有意将PC平台作为下一个感染目标（这里也存在原作者密钥泄露的可能性）。 Hajime背景与 MIRAI 的张扬不同，Hajime是一个低调神秘的Botnet，在诞生后的这一年中并没有给公众传递太多的恐慌。MIRAI在明，Hajime在暗，两者相得益彰。在MIRAI源码公开期间，已经有友商详细阐述过其工作机制。 Hajime的核心特点在于：它是一个P2P botnet，安全人员无法通过黑名单的方式直接堵死 Hajime 的指令传输渠道，达到遏制的目的。所以，其一旦广泛传播便极难彻底清除。

 · Sep 20, 2017 · 10 min read

IoT Botnet

## Is Hajime botnet dead?

Overview The mysterious Hajime botnet was first discovered by Rapiditynetworks in Oct 2016, and it was all over the news earlier this year, but it seems that nobody talks about it any more now, is this botnet gone? The answer is no, our team has been tracking this botnet for

 · Sep 20, 2017 · 6 min read

New Threat

## Http 81 Botnet: the Comparison against MIRAI and New Findings

Overview In our previous blog, we introduced a new IoT botnet spreading over http 81. We will name it in this blog the http81 IoT botnet, while some anti-virus software name it Persirai, and some other name it after MIRAI. In this blog, we will compare http81 against mirai at

