

Mirai

A collection of 23 posts

DDoS

Some details of the DDoS attacks targeting Ukraine and Russia in recent days

At 360Netlab, we continuously track botnets on a global scale through our BotMon system. In particular, for DDoS-related botnets, we further tap into their C2 communications to enable us really see the details of the attacks. Equipped with this visibility, when attack happens, we can have a clear picture of



· Feb 25, 2022 · 11 min read

Log4j

已有10个家族的恶意样本利用Log4j2漏洞传播

背景介绍 2021年12月11号8点整，我们率先捕获到Muhstik僵尸网络样本通过Log4j2 RCE漏洞传播，并首发披露Mirai和Muhstik僵尸网络在野利用详情[1]。2天来，我们陆续又捕获到其它家族的样本，目前，这个家族列表已经超过10个，这里从漏洞、payload、攻击IP 和样本分析等几个维度介绍我们的捕获情况。Apache

Log4j2 漏洞攻击分布 360网络安全研究院大网蜜罐系统监测到Apache Log4j2 RCE漏洞 (CVE-2021-44228) 扫描及攻击，源IP地址地理位置分布如下：国家/地区 攻击源IP数量 Germany 271 The Netherlands 143 China 134 United States 123 United Kingdom 29 Canada 27 Singapore 23 India 22 Japan 15 Russia 12 通过对扫描端口分析发现，



· Dec 13, 2021 · 18 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lmd，



· Dec 11, 2021 · 5 min read

nday

Mirai_ptea Botnet is Exploiting Undisclosed KGUARD DVR Vulnerability

Overview On 2021-06-22 we detected a sample of a mirai variant that we named mirai_ptea propagating through a new vulnerability targeting KGUARD DVR. Coincidentally, a day later, on June 23, we received an inquiry from the security community asking if we had seen a new DDoS botnet, cross-referencing some



· Jul 1, 2021 · 11 min read

nday

Mirai_ptea Botnet利用KGUARD DVR未公开漏洞报告

2021-06-22我们检测到一个我们命名为mirai_ptea的mirai变种样本通过未知漏洞传播。经过分析，该漏洞为KGUARD DVR未公开的漏洞。从我们的分析看该漏洞存在于2016年的固件版本中。我们能找到的2017年之后的固件厂家均已经修复该漏洞



· Jul 1, 2021 · 12 min read

GPON

GPON 漏洞的在野利用（三）——Mettle、Hajime、Mirai、Omni、Imgay、TheMoon

本文由 Hui Wang、LIU Ya、RootKiter、yegenshen 共同撰写。[更新 2018-05-21 17: 30] 这场GPON的聚会看起来永远不会结束了，现在 TheMoon 僵尸网络家族也开始加入了。文中增加了相关的描述。特别值得说明的，TheMoon僵尸网络所使用的攻击漏洞此前并没有披露过，看起来像是个 0day，我们选择不公开攻击载荷的详细内容。另外我们选择了两个版本的 GPON 家用路由器，TheMoon使用的攻击载荷均能成功运行。我们在之前的系列文章一和二里提及，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。这些各路僵尸网络一拥而上，争抢地盘，为 IoT 僵尸网络研究者们提供了一个绝佳的近距离观察机会。在我们的观察中，一个有趣的地方是各僵尸网络的漏洞利用代码均只能影响一小部分（



· May 18, 2018 · 11 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

IoT Botnet

安全威胁预警：Mirai变种Satori正在端口 37215 和 52869 上类似蠕虫式传播

作者：360网络安全研究院 [更新记录] - 2017-12-05 18:56:40 UTC，在我们的博客发出2个小时后，我们观察到C2服务器开始向bot发送停止扫描的指令，与此同时我们看到大网上这两个端口的流量开始下降。- 文中提到的C2地址 95.211.123.69:7654，实际是 95.211.123.69:7645 的笔误。在我们之前的blog中，我们提及有大

约10万个来自阿根廷的独立扫描IP正在扫描端口2323和23，并且确定这是一个新的mirai变种。在过去的几天中，扫描行为变得愈发严重，更多的国家出现在我们的ScanMon平台上。仔细分析后我们看到了更多的部分，意识到之前2323/23端口上的扫描还只是巨大拼图的一小部分。就在我们继续深入分析的时候，我们的注意到一个新的情况出现，值得引起安全社区立即注意。下面是对这个情况非常简短和粗糙的说明。大约从今天中午(2017-12-05 11:57 AM)开始，我们注意到Satori (一个mirai变种) 的新版本正在端口37215和52869上非常快速的传播。这个新变种有两个地方与以往mirai有显



· Dec 5, 2017 · 6 min read

IoT Botnet

Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869

Author: 360 netlab [Update History] - At 2017-12-05 18:56:40 UTC, 2 hours after our blog goes live, we observed the C2 sending kill scan command to the bots, and that explains why the scan activities on the two ports started to drop on a global scale. - The



· Dec 5, 2017 · 4 min read

IoT Botnet

安全威胁早期预警：新的mirai僵尸网络变种正在端口23和2323上积极传播

【2017-11-28 更新】 * 原文中提到的两个C2均已被安全社区sinkhole。 * 原文中的 admin/CentryL1nk 是 admin/CenturyL1nk 的笔误。大约60个小时以前，从2017-11-22 11:00开始，360网络安全研究院注意到在端口2323和23上的扫描流量有一个暴涨现象。其中主要扫描者，大约10万个扫描IP地址位于阿根廷，同时360网络安全研究院也注意到大约有5千个IP地址来自国内。分析以后，目前比较确定这是一个新的mirai变种。根因分析 在我们蜜罐中，最近有两个新的用户名密码被频繁使用到，分别是 admin/CentryL1nk 和 admin/QwestM0dem 。值得一提，admin/CentryL1nk 这对用户名密码是针对ZyXEL PK5001Z 调制解调器的，在一份上月底的利用 中被披露。上述两个用户名密码对，被滥用的初始时间在2017-11-22 11:00附近，在 2017-11-23 日间达到顶峰。这个时间曲线与我们在Scanmon上观察到2323/23端口的扫描曲线比较一致。另外



· Nov 24, 2017 · 5 min read

IoT Botnet

Early Warning: A New Mirai Variant is Spreading Quickly on Port 23 and 2323

[Updates on 2017-11-28] * Both C2s have been sink-holed now by security community. *

admin/CentryL1nk is a typo for admin/CenturyL1nk. About 60 hours ago, since 2017-11-22 11:00, we noticed big upticks on port 2323 and 23 scan traffic, with almost 100k unique scanner IP came from Argentina. After investigation,

 · Nov 24, 2017 · 4 min read

IoT Botnet

IoT_reaper: A Rappid Spreading New IoT Botnet

On 2017-09-13 at 01:02:13, we caught a new malicious sample targeting IoT devices. Starting from that time, this new IoT botnet family continued to update and began to harvest vulnerable iot devices in a rapid pace. The bot borrowed some code from the famous mirai botnet, but it

 · Oct 20, 2017 · 4 min read

IoT Botnet

IoT_reaper: 一个正在快速扩张的新 IoT 僵尸网络

从2017-09-13 01:02:13开始，我们捕获到一个新的针对iot设备的恶意样本出现，在随后的这个一个多月时间里，这个新的IoT僵尸网络家族不断持续更新，开始在互联网上快速大规模的组建僵尸网络军团。该僵尸网络脱胎于mirai，但是在诸多方面比mirai更进一步，特别是开始放弃弱口令猜测，完全转向利用IoT设备漏洞收割，成为IoT僵尸网络里的新兴玩家。我们将之命名为IoT_reaper。IoT_reaper规模较大且正在积极扩张，例如最近的数据昨日(10月19日)在我们观察到的多个C2中，其中一个C2上活跃IP地址去重后已经有10k个，此外还有更多的易感设备信息已经被提交到后台，由一个自动的loader持续植入恶意代码、扩大僵尸网络规模。所幸目前该僵尸网络还尚未发出植入恶意代码以外的其他攻击指令，这反映出该僵尸网络仍然处在早期扩张阶段。但是作者正在积极的修改代码，这值得我们警惕。我们公开IoT_reaper的相关信息，希望安全社区、设备供应商、政府能够采取共同行动，联合遏制该僵尸网络的扩张。源于mirai，高于mirai 该僵尸网络部分借用了m

 · Oct 20, 2017 · 6 min read

RSAC

Netlab's ScanMon at RSA Conference 2017

The RSA Conference 2017 will be held during Feb 13 - 17 at Moscone Center, San Francisco. This year in the conference, we will introduce our Network ScanMon system to global security community. Network scanning is a prevalent threat in the Internet. It can discover active hosts or services in

 · Feb 4, 2017 · 1 min read

RSA大会 '2017上的ScanMon

RSA大会 '2017 即将在2月13日至17日期间在美国旧金山Moscone中心举办。在今年的这次大会上，我们向全世界安全社区推出我们的 ScanMon 系统。网络扫描是互联网上一种流行的威胁，经常被攻击者用来发现网络空间里存活的主机或者服务，并随后可能被用来定位潜在的受害者。扫描行为通常发生在恶意攻击行为的早期，所以如果能及早发现扫描行为会对抵御对应的攻击有显著改善。360网络安全研究院的 ScanMon 系统提供全球范围内实时和历史扫描行为的监控和分析。ScanMon 通过分析大量多样的网络数据，包括但不限于网络流、蜜罐等等，来精确有效的检测扫描行为。对已检出的扫描事件，ScanMon 会展示扫描行为的关键信息和统计数据，例如扫描源IP、受害者端口、扫描数量、分布、扫描源之间的伴生关系，等等。基于这些信息，使用者可以第一时间感知网络扫描行为，并方便有效的识别对应的攻击者。例如，近期360网络安全研究院在针对 mirai 僵尸网络出现、发展、新变种的持续跟踪中，就大量借助了 ScanMon 的能力。您可以在这里观看在线视频（记得调到1080P），也可以试用我们的在

 · Feb 4, 2017 · 2 min read

Mirai

New Mirai DGA Seed 0x91 Brute Forced

Up till very recently, through the samples we had learned that the Mirai DGA seeds are all fixed to 0, as detailed in blog Now Mirai Has DGA Feature Built in, and were able to predict all corresponding DGA domains. Surprisingly, although we have not see any related samples, just

 · Dec 16, 2016 · 3 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 Few Observations of The New Mirai Variant on Port 7547

Much of the new mirai variant that scans port 7547 has been covered by various sources. In this blog, we will not repeat such known facts, and we are just going to list a few observations that we have seen so far. Mirai First Hit and Capability Assessment All the



· Nov 30, 2016 · 3 min read

Botnet

德国电信断网：mirai僵尸网络的新变种和旧主控

【更新】 1. 2016-11-29 18:40:00 初始版本 2. 2016-11-29 20:10:00 增加了对德国电信断网事件相关的描述
德国电信断网事件 2016-11-28 德国电信在2016年11月28日前后遭遇一次大范围的网络故障。在这次故障中，2千万固定网络用户中的大约90万个路由器发生故障（约4.5%），并由此导致大面积网络访问受限。很多媒体给出了网络受限的示意图，如下。德国电信进一步确认了问题是由于路由设备的维护界面被暴露在互联网上、并且互联网上正在发生针对性的攻击而导致。德国电信连夜与设备供应商生成了新的升级包，并且要求客户如果怀疑受到影响就断电重启路由器，之后利用自动/手动的升级过程来减轻问题显然，德国电信还采取了一系列的过滤措施来保证升级过程不受攻击影响。德国电信对该事件给出了较为详细的描述。

<https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862>
按照360网络安全研究院对这次事件



· Nov 29, 2016 · 15 min read

Mirai

关于 mirai 僵尸网络控制主机的数据分析

之前的文章中已经提及，我们的僵尸网络跟踪系统对mirai僵尸网络控制主机做了持续跟踪，并且在文章的结尾处，依据跟踪结果排除了僵尸网络操作者位于北京时区的可能。在这篇文章中，我们将进一步分析mirai僵尸网络的控制主机的行为和特征。之前文章链接如下：<http://blog.netlab.360.com/a-dyn-twitter-ddos-event->

report-and-mirai-botnet-review/ 目前为止，我们与安全社区合作共享了两位数域名上的超过50个mirai僵尸网络主控。但本文后面的分析仅针对360网络安全研究院独立发现的主控，即13个域名上的16个主控主机名，其中8个在持续对外发起攻击。在时间线上，我们可以看到各主控随时间变化的注册、在DNS中首次出现、持续保持IP地址变化、首次被监控到发起攻击等事件。地理分布方面，主控的IP地理分布主要在欧洲和美国，尤以欧洲为甚，亚洲很少，这从侧面增强了之前“mirai控制者不在北京时区”的判断。域名注册信息方面，绝大多数主控在域名注册时在TLD、注册局、注册邮箱方面设置了多重障碍阻滞安全社区的进一步分析

 · Oct 27, 2016 · 7 min read

Mirai

关于 dyn / twitter 受攻击情况的说明和 mirai 僵尸网络的回顾

【更新记录】 2016-10-23 初始版本 2016-10-27 获得了少量攻击现场数据，分析结果与之前观点吻合一致。北京时间2016年10月21日晚间，北美地区大量反馈若干重要的互联网网站无法正常访问。涉及到的网站包括twitter, paypal, github等等，由于这些网站与北美地区日常生活强烈相关，这次网络故障被北美主要媒体广泛报道，也引起了安全社区的强烈关注。我们与国外安全社区一起协同，对本次网络事件提供数据、加以分析并做了溯源跟踪。目前我们已经能够确定本次事件是一次DDoS网络攻击事件，攻击目标主要是Dynamic Network Services (dyn) 公司，twitter、paypal、github等网站作为dyn公司的客户，在本次攻击中不幸被波及。在攻击持续溯源的过程中，虽然目前Flashpoint公司已经确认最近广泛关注的mirai僵尸网络参与了本次网络攻击，但是我们倾向认为虽然mirai贡献了本次攻击的部分攻击流量，但并非所有的攻击流量都来自原始泄漏版本mirai。具体来源不明，可能是源自我们数据地缘性导致的分析误差，也可能是来自

 · Oct 23, 2016 · 14 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

