360Netlab

https://netlab.360.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

公有云威胁情报

公有云网络安全威胁情报（202204）

概述 本文聚焦于云上重点资产的扫描攻击、云服务器总体攻击情况分析、热门漏洞及恶意程序的攻击威胁。 * 360高级威胁狩猎蜜罐系统发现全球9.2万个云服务器IP进行网络扫描、漏洞攻击、传播恶意软件等行为。其中包括国内39家单位所属的云服务资产IP，这些单位涉及政府、医疗、建筑、军工等多个行业。 * 2022年4月，WSO2多个产品和Apache Struts2爆出高危漏洞，两个漏洞技术细节已经公开，并且我们发现两个漏洞都已有在野利用和利用漏洞传播恶意软件的行为。 * 本月共记录来源于云服务器的扫描和攻击会话3.7亿次，其中漏洞攻击会话2400万次，传播恶意软件会话77.2万次。 云上重点资产扫描攻击 四月份，我们共监测到全国39个公有云重点资产存在异常扫描及攻击行为。 随着云服务的普及，云安全问题也随之越发突出。攻击者常常入侵云服务器，并利用被入侵机器继续发动攻击。4月份我们发现了国内39个云服务器重点IP具有异常扫描攻击行为，由此我们认为该重点IP可能被入侵。从行业分布看，事业单位和政府机关的云上资产安全风险问题较大，此外，金融业和央企也面临较为严重的安全威胁。

· May 11, 2022 · 12 min read

公有云威胁情报

公有云网络安全威胁情报（202203）

概述 本文聚焦于云上重点资产的扫描攻击、云服务器总体攻击情况分析、热门漏洞及恶意程序的攻击威胁。 * 360高级威胁狩猎蜜罐系统发现全球12万个云服务器IP，进行网络扫描、漏洞攻击、传播恶意软件等行为。其中包括国内156家单位的服务器IP，涉及大型央企、政府机关等行业。 * Spring厂商连续公开3个关键漏洞，CVE-2022-22947、CVE-2022-22963、CVE-2022-22965，本文将对前两个漏洞进行细节分析，第三个漏洞细节点此查看。 * 本月共记录威胁攻击8亿次有余（其中包括漏洞攻击7.4亿余次、传播恶意软件超5500万次），新增IoC累计68万余个，其中针对IoT设备的漏洞攻击呈上升趋势。 云上重点资产扫描攻击 三月份，我们共监测到全国156个公有云重点资产存在异常扫描及攻击行为。 随着业务不断上云，发生在公有云平台上的网络安全事件和威胁数量居高不下，国内重点行业包括但不限于我国的科研机构、大型企业、政府及事业单位成为攻击者的重点攻击对象，合计攻击源156个。 根据所属云服务商来源，我们发现我国重点IP的云服务商以阿里云使用为主，其次为腾讯

· Apr 19, 2022 · 11 min read

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

Botnet

我们近期看到的针对乌克兰和俄罗斯的DDoS攻击细节

在360Netlab（netlab.360.com），我们持续的通过我们的 BotMon 系统跟踪全球范围内的僵尸网络。特别的，对于DDoS 相关的僵尸网络，我们会进一步跟踪其内部指令，从而得以了解攻击的细节，包括攻击者是谁、受害者是谁、在什么时间、具体使用什么攻击方式。 最近俄乌局势紧张，双方的多个政府、军队和金融机构都遭到了DDoS攻击，我们也不断接收到安全社区的询问，咨询对于最近乌克兰和俄罗斯相关网站 (.ua .ru下属域名）遭受DDoS攻击的具体情况，因此我们特意整理相关数据供安全社区参考。 针对乌克兰的DDoS攻击 下图是我们看到的针对域名以.gov.ua结尾的政府网站的攻击趋势。 可以看到攻击最早始于2月12号，攻击数量和强度都在持续变大，在2月16日达到顶峰，攻击类型则混合了NTP放大、UDP/STD/OVH flood等多种类型 下图是我们看到的针对另一个以.ua结尾的网站“online.oschadbank.ua”的DDoS攻击。 可以看到攻击开始自2月15日，持续了3天。值得注意的是攻击这个网站的C2 mirai_5.182.2

· Feb 25, 2022 · 12 min read

honeypot

Ten families of malicious samples are spreading using the Log4j2 vulnerability Now

Background On December 11, 2021, at 8:00 pm, we published a blog disclosing Mirai and Muhstik botnet samples propagating through Log4j2 RCE vulnerability[1]。 Over the past 2 days, we have captured samples from other families, and now the list of families has exceeded 10. It looks like the

· Dec 13, 2021 · 17 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

Import 2022-11-30 11:16

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

Most of the following article was completed around early 2020, at that time the vendor was trying different ways to recover the massive amount of infected devices, we shared our findings with the vendor, as well as to CNCERT, and decided to not publish the blog while the vendor'

· Oct 29, 2021 · 15 min read

Botnet

一个藏在我们身边的巨型僵尸网络 Pink

本文完成于2020年春节前后，为维护广大最终消费者的利益，一直处于保密期无法发表。近日 CNCERT 公开披露了相关事件，令本文有了公开契机。在保密期的这段时间里，Pink 也出现一些新的小变动，笔者筛选了其中一部分放到“新动向”章节，供其他同仁共同追踪研究。 概述 2019年11月21日，安全社区的信任伙伴给我们提供了一个全新的僵尸网络样本，相关样本中包含大量以 pink 为首的函数名，所以我们称之为 PinkBot。 Pinkbot 是我们六年以来观测到最大的僵尸网络，其攻击目标主要是 mips 光猫设备，在360Netlab的独立测量中，总感染量超过160万，其中 96% 位于中国。 PinkBot 具有很强的技术能力： 1. PinkBot 架构设计具备很好的健壮性，它能够通过多种方式（通过第三方服务分发配置信息/通过 P2P 方式分发配置信息/通过 CNC 分发配置信息）自发寻址控制端，并对控制端通信有完备的校验，确保僵尸节点不会因某一个环节的阻杀而丢失或被接管；甚至对光猫固件做了多处改动后，还能确保光猫能够正常使用；

· Oct 26, 2021 · 23 min read