

Botnet

A collection of 115 posts

Botnet

僵尸网络911 S5的数字遗产

概述 2024年5月29日，美国司法部发布通告，声称其执法活动摧毁了"史上最大的僵尸网络" 911 S5，查封了相关域名，并且逮捕了其管理员YunHe Wang。Wang及其同伙通过创建并分发包含恶意代码的免费VPN程序感染用户，并且在名为911 S5的住宅代理服务中出售对被感染设备构成的代理网络的访问权。按照360威胁情报中心的分析，911S5从2014年开始运营，到2022年7月关停，在2023年10月又摇身一变，化名CloudRouter继续其肮脏生意，终于在2024年5月被多国联合执法摧毁。911S5的僵尸网络运行时间长、涉及多个国家的19M个IP地址、行为高调，虽然经过执法行动后大势已去，但是其数字遗产仍然对网络空间构成了现实且显著的威胁，下文是我们对威胁分析的结果。“空手套白狼”的911 S5 911S5出售的代理服务背后是数千万被感染的设备。受害者主动或被动下载捆绑了恶意代码的软件、免费VPN程序等。在程序启动后，恶意代码将会创建持久化服务作为后门，为911S5客户提供代理服务。在2023年以前，911S5使用的免费VPN包括ProxyGate、Mas



• Jun 14, 2024 • 7 min read

Botnet

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

Overview On Oct 21, 2022, 360Netlab's honeypot system captured a suspicious ELF file ee07a74d12c0bb3594965b51d0e45b6f, which propagated via F5 vulnerability with zero VT detection, our system observes that it communicates with IP 45.9.150.144 using SSL with forged Kaspersky

certificates, this caught our attention. After further lookup,



· Jan 10, 2023 · 13 min read

Botnet

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

概述 2022年10月21日，360Netlab的蜜罐系统捕获了一个通过F5漏洞传播，VT 0检测的可疑ELF文件 ee07a74d12c0bb3594965b51d0e45b6f，流量监控系统提示它和IP45.9.150.144产生了SSL流量，而且双方都使用了伪造的Kaspersky证书，这引起了我们的关注。经过分析，我们确认它由CIA被泄露的Hive项目server源码改编而来。这是我们首次捕获到在野的CIA HIVE攻击套件变种，基于其内嵌Bot端证书的CN=xdr33，我们内部将其命名为xdr33。关于CIA的Hive项目，互联网中有大量的源码分析的文章，读者可自行参阅，此处不再展开。概括来说，xdr33是一个脱胎于CIA Hive项目的后门木马，主要目的是收集敏感信息，为后续的入侵提供立足点。从网络通信来看，xdr33使用XTEA或AES算法对原始流量进行加密，并采用开启了Client-Certificate Authentication模式的SSL对流量做进一步的保护；从功能来说，主要有beacon, trigger两大任务，其中beacon是周期性向硬编码的Be



· Jan 9, 2023 · 17 min read

Botnet

快讯：使用21个漏洞传播的DDoS家族WSzero已经发展到第4个版本

概述 近期，我们的BotMon系统连续捕获到一个由Go编写的DDoS类型的僵尸网络家族，它用于DDoS攻击，使用了包括SSH/Telnet弱口令在内的多达22种传播方式。短时间内出现了4个不同的版本，有鉴于此，我们认为该家族未来很可能继续活跃，值得警惕。下面从传播、样本和跟踪角度分别介绍。传播分析 除了Telnet/SSH弱口令，我们观察到wszero还使用了如下21个漏洞进行传播： VULNERABILITY AFFECTED CVE_2014_08361 Realtek SDK CVE_2017_17106 Zivif Webcams CVE_2017_17215 Huawei HG532 CVE_2018_12613 phpMyAdmin 4.8.x before 4.8.2 CVE_2020_10987 Tenda AC15 AC1900



· Dec 7, 2022 · 7 min read

Botnet

Fodcha Is Coming Back, Raising A Wave of Ransom DDoS

Background On April 13, 2022, 360Netlab first disclosed the Fodcha botnet. After our article was published, Fodcha suffered a crackdown from the relevant authorities, and its authors quickly responded by leaving "Netlab pls leave me alone I surrender" in an updated sample. No surprise, Fodcha's authors



· Oct 31, 2022 · 16 min read

Botnet

卷土重来的DDoS狂魔：Fodcha僵尸网络再次露出獠牙

背景 2022年4月13日，360Netlab首次向社区披露了Fodcha僵尸网络，在我们的文章发表之后，Fodcha遭受到相关部门的打击，其作者迅速做出回应，在样本中留下Netlab pls leave me alone I surrender字样向我们投降。本以为Fodcha会就此淡出江湖，没想到这次投降只是一个不讲武德的假动作，Fodcha的作者在诈降之后并没有停下更新的脚步，很快就推出了新版本。在新版本中，Fodcha的作者重新设计了通信协议，并开始使用xxtea和chacha20算法对敏感资源和网络通信进行加密，以躲避文件&流量层面的检测；同时引入了OpenNIC域名做为主选C2，ICANN域名做为后备C2的双C2方案。这种冗余机制，既能防止C2被接管，又有良好的健壮性，能够维持其主控网络的稳定。依托于背后团队强大的N-day漏洞整合能力，卷土重来的Focha与之前对比可谓有过之而无不及。在我们的数据视野中，从规模来看，Fodcha再次发展成日活Bot节点数超过60K，C2域名绑定40+IP，可以轻松打出超过1Tbps流量的大规模僵尸网络；就活跃程度而言，



· Oct 27, 2022 · 23 min read

Botnet

PureCrypter is busy pumping out various malicious malware families

In our daily botnet analysis work, it is common to encounter various loaders. Compared to other types of malware, loaders are unique in that they are mainly used to "promote", i.e., download and run other malware on the infected machine. According to our observations, most loaders are



· Aug 29, 2022 · 12 min read

loader

PureCrypter Loader持续活跃，已经传播了10多个其它家族

在我们的日常botnet分析工作中，碰到各种loader是常事。跟其它种类的malware相比，loader的特殊之处在于它主要用来“推广”，即在被感染机器上下载并运行其它的恶意软件。根据我们的观察，大部分loader是专有的，它们和推广的家族之间存在绑定关系。而少数loader家族会将自己做成通用的推广平台，可以传播其它任意家

族，实现所谓的malware-as-a-service (MaaS)。跟专有loader相比，MaaS类型显然更危险，更应该成为我们的首要关注目标。本文介绍我们前段时间看到的一个MaaS类型的loader，它名为PureCrypter，今年非常活跃，先后推广了10多个其它的家族，使用了上百个C2。因为zscaler已经做过详细的样本分析，本文主要从C2和传播链条角度介绍我们看到的PureCrypter传播活动，分析其运作过程。本文要点如下： * PureCrypter是一款使用C#编写的loader，至少2021年3月便已出现，能传播任意的其它家族。 * PureCrypter今年持续活跃，已经传播了包括Formbook、SnakeKeylog



· Aug 29, 2022 · 14 min read

Botnet

A new botnet Orchard Generates DGA Domains with Bitcoin Transaction Information

DGA is one of the classic techniques for botnets to hide their C2s, attacker only needs to selectively register a very small number of C2 domains, while for the defenders, it is difficult to determine in advance which domain names will be generated and registered. 360 netlab has long focused



· Aug 5, 2022 · 13 min read

Botnet

DGA家族Orchard持续变化，新版本用比特币交易信息生成DGA域名

DGA是一种经典的botnet对抗检测的技术，其原理是使用某种DGA算法，结合特定的种子和当前日期，定期生成大量的域名，而攻击者只是选择性的注册其中的极少数。对于防御者而言，因为难以事先确定哪些域名会被生成和注册，因而防御难度极大。360 netlab长期专注于botnet攻防技术的研究，维护了专门的DGA算法和情报库，并通过订阅情报的方式与业界分享研究成果。近期我们在分析未知DGA域名时发现一例不但使用日期，还会同时使用中本聪的比特币账号交易信息来生成DGA域名的例子。因为比特币交易的不确定性，该技术比使用时间生成的DGA更难预测，因而防御难度更大。该技术发现于一个名为Orchard的botnet家族。自从2021年2月份首次检测到该家族以来，我们发现它至少经历了3个版本的变化，中间甚至切换过编程语言。结合长期的跟踪结果和其它维度的信息，我们认为Orchard会是一个长期活跃、持续发展的botnet家族，值得警惕。本文将介绍Orchard的最新DGA技术，以及它这3个版本的发展过程。本文要点如下： * Orchard是一个使用了DGA技术的botnet家族，核心功能



· Aug 5, 2022 · 18 min read

Botnet

Fodcha, a new DDos botnet

Overview Recently, CNCERT and 360netlab worked together and discovered a rapidly spreading DDoS

botnet on the Internet. The global infection looks fairly big as just in China there are more than 10,000 daily active bots (IPs) and also more than 100 DDoS victims being targeted on a daily basis. We named



· Apr 13, 2022 · 7 min read

Botnet

新威胁：闷声发大财的Fodcha僵尸网络

本报告由国家互联网应急中心（CNCERT）与三六零数字安全科技集团有限公司共同发布。概述 近期，CNCERT和三六零数字安全科技集团有限公司共同监测发现一个新的且在互联网上快速传播的DDoS僵尸网络，通过跟踪监测发现其每日上线境内肉鸡数（以IP数计算）已超过1万、且每日会针对超过100个攻击目标发起攻击，给网络空间带来较大威胁。由于该僵尸网络最初使用的C2域名folded.in，以及使用chacha算法来加密网络流量，我们将其命名为Fodcha。僵尸网络规模 通过监测分析发现，2022年3月29日至4月10日Fodcha僵尸网络日上线境内肉鸡数最高达到1.5万台，累计感染肉鸡数达到6.2万。每日境内上线肉鸡数情况如下。Netlab按：根据国外合作伙伴的数据，我们估算该家族全球日活肉鸡数量应该在5.6w+ Fodcha僵尸网络位于境内肉鸡按省份统计，排名前三位的分别为山东省（12.9%）、辽宁省（11.8%）和浙江省（9.9%）；按运营商统计，联通占59.9%，电信占39.4%，移动占0.5%。传播方式 通过跟踪监测，



· Apr 13, 2022 · 9 min read

Botnet

New Threat: B1txor20, A Linux Backdoor Using DNS Tunnel

Background Since the Log4J vulnerability was exposed, we see more and more malware jumped on the wagon, Elknot, Gafgyt, Mirai are all too familiar, on February 9, 2022, 360Netlab's honeypot system captured an unknown ELF file propagating through the Log4J vulnerability. What stands out is that the network



· Mar 15, 2022 · 11 min read

Botnet

新威胁：使用DNS Tunnel技术的Linux后门B1txor20正在通过Log4j漏洞传播

背景 自从Log4J漏洞被曝光后，正所谓“忽如一夜漏洞来，大黑小灰笑开怀”。无数黑产团伙摩拳擦掌加入了这个“狂欢派对”，其中既有许多业界非常熟悉的恶意软件家族，同时也有一些新兴势力想趁着这股东风在黑灰产上分一杯羹。360Netlab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

哪些僵尸网络利用，期间我们看到了Elknot, Gafgyt, Mirai等老朋友的从不缺席，也见证了一些新朋友的粉墨登场。2022年2月9日，360Netlab的蜜罐系统捕获了一个未知的ELF文件通过Log4J漏洞传播，此文件在运行时产生的网络流量引发了疑似DNS Tunnel的告警，这引起了我们的兴趣。经过分析，我们确定是一个全新的僵尸网络家族，基于其传播时使用的文件名“b1t”，XOR加密算法，以及RC4算法秘钥长度为20字节，它被我们命名为B1txor20。简单来说，B1txor20是一个针对Linux平台的后门木马，它利用DNS Tunnel技术构建C2通信信道，除了传统的后门功能，B1txor20还有开启Socket5代理，远程下载安装Rootkit，反



· Mar 15, 2022 · 14 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

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

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lmd，



· Dec 11, 2021 · 5 min read

DDoS

EwDoor僵尸网络，正在攻击美国AT&T用户

背景介绍 2021年10月27日，我们的BotMon系统发现有攻击者正通过CVE-2017-6079漏洞攻击Edgewater Networks设备，其payload里有比较罕见的mount文件系统指令，这引起了我们的兴趣，经过分析，我们确认这是一个全新的僵尸网络家族，基于其针对Edgewater产商、并且有Backdoor的功能，我们将它命名为

EwDoor。最初捕获的EwDoor使用了常见的硬编码C2方法，同时采用了冗余机制，单个样本的C2多达14个。Bot运行后会依次向列表中的C2发起网络请求直到成功建立C2会话。这些C2中多数为域名形式，有趣的是它们多数还未来得及注册，因此我们抢注了第二个域名iunno.se以获取Bot的请求。但一开始连接到我们域名的Bot非常少，因为大多数Bot都成功和第一个C2(185.10.68.20)建立连接，这让我们有些许“沮丧”。转机发生在2021年11月8日，当天7点到10点EwDoor的第一个C2185.10.68.20发生了网络故障，瞬间大量Bot连接到我们注册的C2域名，这使得我们成功的测绘了EwDoor僵尸网络的规模&感染范



· Dec 1, 2021 · 18 min read

DDoS

EwDoor Botnet Is Attacking AT&T Customers

Background On October 27, 2021, our Botmon system ided an attacker attacking Edgewater Networks' devices via CVE-2017-6079 with a relatively unique mount file system command in its payload, which had our attention, and after analysis, we confirmed that this was a brand new botnet, and based on it'



· Nov 30, 2021 · 14 min read

DNS

The Pitfall of Threat Intelligence Whitelisting: Specter Botnet is 'taking over' Top Legit DNS Domains By Using ClouDNS Service

Abstract In order to reduce the possible impact of false positives, it is pretty common practice for security industry to whitelist the top Alexa domains such as www.google.com, www.apple.com, www.qq.com, www.alipay.com. And we have seen various machine learning detection models that bypass



· Nov 18, 2021 · 6 min read

DDoS

Abcbot, an evolving botnet

Background Business on the cloud and security on the cloud is one of the industry trends in recent years. 360Netlab is also continuing to focus on security incidents and trends on the cloud from its own expertise in the technology field. The following is a recent security incident we observed,



· Nov 9, 2021 · 10 min read

DDoS

僵尸网络Abcbot的进化之路

背景 业务上云、安全上云是近年来业界的发展趋势之一。360Netlab 从自身擅长的技术领域出发，也在持续关注云上安全事件和趋势。下面就是我们近期观察到的一起，被感染设备IP来自多个云供应商平台的安全事件。

2021年7月14日，360BotMon系统发现一个未知的ELF文件(a14d0188e2646d236173b230c59037c7)产生了大量扫描流量，经过分析，我们确定这是一个Go语言实现的Scanner，基于其源码路径中"abc-hello"字串，我们内部将它命名为Abcbot。Abcbot在当时的时间节点上功能比较简单，可以看成是一个攻击Linux系统的扫描器，通过弱口令&Nday漏洞实现蠕虫式传播。一个有意思的事情是，Abcbot的源码路径中有"dga.go"字串，但是在样本中并没有发现相关的DGA实现，我们推测其作者会在后续的版本中补上这个功能，这让我们对这个家族多了几分留意。随着时间的推移，Abcbot也在持续更新，如我们所料，它在后继的样本中加入了DGA特性。如今Abcbot除了拥有蠕虫式传播的能力，还有自更新，Webserver，DDoS等功



· Nov 9, 2021 · 13 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