

DDoS

A collection of 57 posts

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Fodcha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

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

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

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

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

0-day

Mirai_ptea_Rimasuta variant is exploiting a new RUIJIE router 0 day to spread

Overview In July 2021 we blogged about Mirai_ptea, a botnet spreading through an undisclosed vulnerability in KGUARD DVR. At first we thought it was a short-lived botnet that would soon disappear so we just gave it a generic name. But clearly we underestimated the group behind this family, which



· Sep 28, 2021 · 10 min read

0-day

Mirai_ptea_Rimasuta变种正在利用RUIJIE路由器在野0DAY漏洞传播

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 2021年7月我们向社区公布了一个通过KGUARD DVR未公开漏洞传播的僵尸网络Mirai_ptea，一开始我们认为这是一个生命短暂的僵尸网络，不久就会消失不见，因此只给了它一个通用的名字。但很显然我们小看了这个家族背后的团伙，事实上该家族一直非常活跃，最近又观察到该家族正在利用RUIJIE NBR700系列路由器的在野0day漏洞传播。比较有意思的是，该家族的作者曾经在某次更新的样本中加入了这么一段话吐槽我们的mirai_ptea命名： -_- you guys didnt pick up on the name? really??? its ``RI-MA-SU-TA``. not MIRAI_PTEA this is dumb name. 出于对作者的"尊重"，以及对该团伙实力的重新评估，我们决定将其命名为 Mirai_

 · Sep 28, 2021 · 14 min read

Botnet

The Mostly Dead Mozi and Its' Lingering Bots

Background It has been nearly 2 years since we (360NETLAB) first disclosed the Mozi botnet in December 2019, and in that time we have witnessed its development from a small-scale botnet to a giant that accounted for an extremely high percentage of IOT traffic at its peak. Now that Mozi&

 · Aug 30, 2021 · 10 min read

Botnet

Mozi已死，余毒犹存

背景 360NETLAB于2019年12月首次披露了Mozi僵尸网络，到现在已有将近2年时间，在这段时间中，我们见证了它从一个小规模僵尸网络发展为巅峰时占据了极高比例IOT流量巨无霸的过程。现在Mozi的作者已经被执法机关处置，其中我们也全程提供了技术协助，因此我们认为后续在相当长的一段时间内它都不会继续更新。但我们知道，Mozi采用了P2P网络结构，而P2P网络的一大“优点”是健壮性好，即使部分节点瘫痪，整个网络仍然能工作。所以即使Mozi作者不再发布新的更新，它仍然会存活一段时间，残余的节点仍然会去感染其它存在漏洞的设备，所以我们现在仍然能看到Mozi在传播，正可谓“百足之虫，死而不僵”。许多安全厂商都对Mozi进行了跟踪分析，但从我们的角度而言，或多或少有些遗漏，甚至有错误。今天我们将对Mozi的看法总结在下面这篇文章里，以补充安全社区的分析；同时也为我们对Mozi僵尸网络的持续关注画上一个句号。本文将回答以下问题： 1: Mozi除Bot节点外还有别的功能节点吗？ 2: Mozi Bot模块有新功能吗？ 3: Mozi僵尸网络还在更新吗？ M

 · Aug 27, 2021 · 14 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

Necro

Necro upgrades again, using Tor + dynamic domain DGA and aiming at both Windows & Linux

Overview Back in January, we blogged about a new botnet Necro and shortly after our report, it stopped spreading. On March 2nd, we noticed a new variant of Necro showing up on our BotMon tracking radar. On March 2nd, the BotMon system has detected that Necro has started spreading again, in



• Mar 18, 2021 • 12 min read

New Threat

New Threat: ZHtrap botnet implements honeypot to facilitate finding more victims

Overview In the security community, when people talk about honeypot, by default we would assume this is one of the most used toolkits for security researchers to lure the bad guys. But recently we came across a botnet uses honeypot to harvest other infected devices, which is quite interesting. From



• Mar 12, 2021 • 11 min read

New Threat

新威胁：ZHtrap僵尸网络分析报告

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2021年2月28日起，360网络安全研究院的BotMon系统检测到IP(107.189.30.190)在持续传播一批未知ELF样本。经分析，我们确认这些样本隶属于一个新的botnet家族，结合其运行特点，我们将其命名为ZHtrap，本文对其做一分析，文章要点如下：1. ZHtrap的传播使用了4个Nday漏洞，主要功能依然是DDoS和扫描，同时集成了一些后门功能。2. Zhtrap能将被感染设备蜜罐化，目的是提高扫描效率。3. Zhtrap感染受害主机后会禁止运行新的命令，以此实现彻底控制和独占该设备。4. 在C2通信上，ZHtrap借鉴了套娃，采用了Tor和云端配置。ZHtrap全情介绍 ZHtrap的代码由Mirai修改而来，支持x86, ARM, MIPS等主流CPU架构。但相对Mirai，ZHtrap变化较大，体现在如下方面：* 在指令方面，加入了校验机制 * 在扫描传播方面，增加了对真实设备和蜜

 · Mar 12, 2021 · 15 min read

Necro

Gafgtyt_tor, Necro作者再次升级“武器库”

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。概述自2021年2月15号起，360Netlab的BotMon系统持续检测到Gafgtyt家族的一个新变种，它使用Tor进行C2通信以隐藏真实C2，并对样本中的敏感字符串做了加密处理。这是我们首次发现使用Tor机制的Gafgtyt变种，所以将该变种命名为Gafgtyt_tor。进一步分析发现该家族与我们1月份公开的Necro家族有紧密联系，背后为同一伙人，即所谓的keksec团伙[1] [2]。检索历史样本发现该团伙长期运营Linux IoT botnet，除了Necro和Gafgtyt_tor，他们还曾运营过Tsunami和其它Gafgtyt变种botnet。本文将介绍Gafgtyt_tor，并对该团伙近期运营的其它botnet做一梳理。本文关键点如下：1. Gafgtyt_tor使用Tor来隐藏C2通信，可内置100多个Tor代理，并且新样本在持续更新代理列表。2. Gafgtyt_tor跟keksec团伙之前分发的Gafgtyt样本同源，核心功能依

 · Mar 5, 2021 · 15 min read

Necro

Gafgtyt_tor and Necro are on the move again

Overview Since February 15, 2021, 360Netlab's BotMon system has continuously detected a new variant of the Gafgtyt family, which uses Tor for C2 communication to hide the real C2 and encrypts sensitive strings in the samples. This is the first time we found a Gafgtyt variant using the

 · Mar 4, 2021 · 12 min read

DDoS

New Threat: Matryosh Botnet Is Spreading

Background On January 25, 2021, 360 netlab BotMon system labeled a suspicious ELF file as Mirai, but the network traffic did not match Mirai's characteristics. This anomaly caught our attention, and after

analysis, we determined that it was a new botnet that reused the Mirai framework, propagated through



· Feb 2, 2021 · 8 min read

DDoS

新威胁：能云端化配置C2的套娃（Matryosh）僵尸网络正在传播

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。背景 2021年1月25日，360网络安全研究院的BotMon系统将一个可疑的ELF文件标注成Mirai，但网络流量却不符合Mirai的特征。这个异常引起了我们的注意，经分析，我们确定这是一个复用了Mirai框架，通过ADB接口传播，针对安卓类设备，主要目的为DDoS攻击的新型僵尸网络。它重新设计了加密算法，通过DNS TXT的方式从远程主机获取TOR C2以及和C2通信所必须的TOR代理。这个僵尸网络实现的加密算法以及获取C2的过程都是一层层嵌套，像俄罗斯套娃一样，基于这个原因，我们将它命名为Matryosh。每天都有脚本小子拿着Mirai的源码进行魔改，想着从DDoS黑产赚上一笔。Matryosh会是这样的作品吗？随着分析的深入，更多细节浮出水面，根据C2指令的相似性，我们推测它是当下非常活跃的Moobot团伙的又一个尝试。Matryosh没有集成扫描，漏洞利用的模块，主要功能为DDoS攻击，支持 tcpraw, icmpecho,



· Feb 2, 2021 · 10 min read

DGA

Necro is going to version 3 and using PyInstaller and DGA

Overview. Necro is a classic family of botnet written in Python that was first discovered in 2015, at the beginning, it targeted Windows systems and often tagged by security vendors as Python.IRCBot and called N3Cr0m0rPh (Necromorph) by the author himself. Since January 1, 2021, 360Netlab's BoTMon system



· Jan 22, 2021 · 12 min read

DGA

Necro在频繁升级，新版本开始使用PyInstaller和DGA

概述 Necro是一个经典的Python编写的botnet家族，最早发现于2015年，早期针对Windows系统，常被报为Python.IRCBot，作者自己则称之为N3Cr0m0rPh(Necromorph)。自2021年1月1号起，360Netlab的BotMon系统持续检测到该家族的新变种，先后有3个版本的样本被检测到，它们均针对Linux系统，并且最新的版本使

用了DGA技术来生成C2域名对抗检测。本文将对最近发现的Necro botnets做一分析。本文的关键点如下：
1， Necro最新版的感染规模在万级，并且处于上升趋势。2，在传播方式上，Necro支持多种方式，并且持续集成新公开的1-day漏洞，攻击能力较强。3，最新版Necro使用了DGA技术生成C2域名，Python脚本也经过重度混淆以对抗静态分析。4，目前传播的不同版本Necro botnet背后为同一伙人，并且主要针对Linux设备。5，最新的2个版本为了确保能在没有Python2的受害机器上执行，会同时分发使用PyInstaller打包过的Python程序。在撰写本文时，我们注意



· Jan 21, 2021 · 16 min read