



## Alex.Turing



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

## 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



· 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

## 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厂商、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

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

DNS

## 白名单之殇：Specter僵尸网络滥用ClouDNS服务，github.com无辜躺枪

摘要 威胁情报的应用，始终存在着“漏报”和“误报”的平衡，为了减少可能的误报带来的业务影响，你的威胁情报白名单中是否静静的躺着 www.apple.com、www.qq.com、www.alipay.com 这样的流行互联网业务域名呢？你的机器学习检测模型，依照历史流量，是否会自动对 .qq.com、.alipay.com 这样的流量行为增加白权重呢？但安全是对抗，白帽子想“判黑”，黑客想“洗白”。我们看到的白，不一定是真的白，可能只是黑客想让我们以为的白。我们BotnetMon最近的跟踪发现，Specter僵尸网络家族的样本，会使用api.github.com这种域名作为CC域名来通信，通过“可定制化”的DNS服务，将“白域名”引导到黑IP上来实现自己恶意指令通信。这种“过白”手法，在流量检测的场景下，



· Nov 18, 2021 · 11 min read

Import 2022-11-30 11:16

## Malware uses namesilo Parking pages and Google's custom pages to spread

Abstract Recently, we found a suspicious GoELFsample, which is a downloader mainly to spread mining malwares. The interesting part is that we noticed it using namesilo's Parking page and Google's user-defined page to spread the sample and configuration. Apparently this is yet another attempt to hide



· Nov 12, 2021 · 3 min read

Import 2022-11-30 11:16

## 快讯：利用namesilo Parking和Google的自定义页面来传播恶意软件

摘要 近期，我们发现一个GoELF可疑样本，分析得知是一个downloder，主要传播挖矿。有意思的地方在于传播方式，利用了namesilo的Parking页面，以及Google的用户自定义页面来传播样本及配置，从而可以躲避跟踪。该样本最开始被友商腾讯安全团队捕获，不过传播链条分析中，对namesilo parking域名的分析不太准确。往往大家以为，域名停靠期间(Domain Parking)，页面显示内容是被域名停靠供应商强制限定的，域名实际拥有者并不能修改其页面内容。但在这个案例中，域名停靠供应商允许域名拥有者自定义停靠页面。攻击者利用了这一点，再加上Google提供的自定义页面来传播自己的木马。这样做有两个显而易见的好处：一方面攻击者几乎不需要为恶意代码的传播付出任何带宽和服务器的费用；另一方面攻击者将自己的恶意行为隐藏在大型互联网基础服务供应商的巨大流量中，所谓大隐于市，以此隐藏自己的行踪使得更难被检测和追踪。在我们的DNSMon/DTA监测数据中显示，这种趋势在最近几月有上升迹象，值得安全社区注意。缘起 在10.13号，我们的BotnetM



· Nov 11, 2021 · 5 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

Backdoor

## 窃密者Facefish分析报告

背景介绍 2021年2月，我们捕获了一个通过CWP的Nday漏洞传播的未知ELF样本，简单分析后发现这是一个新botnet家族的样本。它针对Linux x64系统，配置灵活，并且使用了一个基于Diffie–Hellman和Blowfish的私有加密协议。但因为通过合作机构（在中国区有较好网络通信观察视野）验证后发现对应的C2通信命中为0，所以未再深入分析。2021年4月26号，Juniper发布了关于此样本的分析报告，我们注意到报告中忽略了一些重要的技术细节，所以决定将漏掉的细节分享出来。该家族的入口ELF样本

MD5=38fb322cc6d09a6ab85784ede56bc5a7是一个Dropper，它会释放出一个Rootkit。因为Juniper并未为样本定义家族名，鉴于Dropper在不同的时间点释放的Rootkit有不同的MD5值，犹如川剧中的变脸，并且该家族使用了Blowfish加密算法，我们将它命名为Facefish。Facefish概览 Facefish由Dropper和Rootkit 2部分组成，主要功能由Rootkit模块决定。Rootki



· May 28, 2021 · 17 min read

Backdoor

## Analysis report of the Facefish rootkit

Background In Feb 2021, we came across an ELF sample using some CWP's Ndays exploits, we did some analysis, but after checking with a partner who has some nice visibility in network traffic in some China areas, we discovered there is literally 0 hit for the C2 traffic. So



· May 27, 2021 · 13 min read