



Genshen Ye



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ldm，

 · Dec 11, 2021 · 5 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

CVE-2021-26855

Microsoft Exchange Vulnerability (CVE-2021-26855) Scan Analysis

Background On March 2, 2021, Microsoft disclosed a remote code execution vulnerability in Microsoft Exchange server[1]。 We customized our Anglerfish honeypot to simulate and deploy Microsoft Exchange honeypot plug-in on March 3, and soon we started to see a large amount of related data, so far, we have

already



· Mar 25, 2021 · 12 min read

CVE-2021-26855

Microsoft Exchange 漏洞 (CVE-2021-26855) 在野扫描分析报告

背景介绍 2021年3月2号，微软披露了Microsoft Exchange服务器的远程代码执行漏洞[1]。2021年3月3号开始，360网络安全研究院Anglerfish蜜罐开始模拟和部署Microsoft Exchange蜜罐插件，很快我们搜集到大量的漏洞检测数据，目前我们已经检测到攻击者植入Webshell，获取邮箱信息，甚至进行XMRig恶意挖矿(<http://178.62.226.184/run.ps1>)的网络攻击行为。根据挖矿文件路径名特征，我们将该Miner命名为Tripleone。2021年3月6号开始，ProjectDiscovery和微软CSS-Exchange项目相继披露了漏洞检测脚本[2][3]。Microsoft Exchange服务器的远程代码执行漏洞利用步骤复杂，一般从PoC公布到黑色产业攻击者利用需要一定的时间，我们看到这个攻击现象已经开始了。CVE-2021-26855 植入Webshell POST /ecp/j2r3.js
HTTP/1.1 Host: {target} Connection: keep-alive



· Mar 25, 2021 · 13 min read

QNAP

QNAP NAS users, make sure you check your system

Background On March 2, 2021, 360Netlab Threat Detection System started to report attacks targeting the widely used QNAP NAS devices via the unauthorized remote command execution vulnerability (CVE-2020-2506 & CVE-2020-2507)[1], upon successful attack, the attacker will gain root privilege on the device and perform malicious mining activities. Due to



· Mar 5, 2021 · 4 min read

QNAP

QNAP NAS在野漏洞攻击事件2

背景介绍 2021年3月2号，360网络安全研究院未知威胁检测系统监测到攻击者正在使用台湾QNAP Systems, Inc.公司的网络存储设备诊断程序(Helpdesk)的未授权远程命令执行漏洞 (CVE-2020-2506 & CVE-2020-2507)，获取到系统root权限并进行恶意挖矿攻击。我们将此次挖矿程序命名为UnityMiner，值得注意的是攻

击者专门针对QNAP NAS设备特性，隐藏了挖矿进程，隐藏了真实的CPU内存资源占用信息，使用户无法在Web管理界面看到系统异常行为。2020年10月7号，QNAP Systems, Inc.公司发布安全公告QSA-20-08[1]，并指出已在Helpdesk 3.0.3和更高版本中解决了这些问题。目前，互联网上还没有公布CVE-2020-2506和CVE-2020-2507的漏洞详细信息，由于该漏洞威胁程度极高，为保护尚未修复漏洞的QNAP NAS用户，我们不公开该漏洞技术细节。我们推测仍有数十万个在线的QNAP NAS设备存在该漏洞。此前我们曾披露了另一起QNAP NAS在野漏洞攻击事件[2]。



· Mar 5, 2021 · 6 min read

Botnet

Fbot is now riding the traffic and transportation smart devices

Background Fbot, a botnet based on Mirai, has been very active ever since we first blogged about it here[1][2], we have seen this botnet using multiple 0 days before(some of them we have not disclosed yet) and it has been targeting various IoT devices, now, it is



· Mar 3, 2021 · 5 min read

Botnet

Fbot僵尸网络正在攻击交通和运输智能设备

背景介绍 Fbot是一个基于Mirai的僵尸网络，它一直很活跃，此前我们曾多次披露过该僵尸网络[1][2]。我们已经看到Fbot僵尸网络使用了多个物联网（Internet of things）设备的N-day漏洞和0-day漏洞（部分未披露），现在它正在攻击车联网（Internet of Vehicles）领域的智能设备，这是一个新现象。2021年2月20号，360网络安全研究院未知威胁检测系统监测到攻击者正在使用美国Iteris, Inc.公司的Vantage Velocity产品的远程命令执行漏洞（CVE-2020-9020）[3][4]，传播Fbot僵尸网络样本。据维基百科介绍[5]，Iteris, Inc.公司为智能移动基础设施管理提供软件和咨询服务，包括软件即服务以及托管和咨询服务，并生产记录和预测交通状况的传感器和其他设备。结合Vantage Velocity产品用途，并从受影响的设备上发现AirLink GX450 Mobile Gateway产信息，因此我们推测受影响设备是路边设备系统。CVE-2020-9020漏洞分析 通过360 F



· Mar 3, 2021 · 7 min read

0-day

Another LILIN DVR 0-day being used to spread Mirai

Author: Yanlong Ma, Genshen Ye Background Information In March, we reported[1] that multiple botnets, including Chalubo, Fbot, Moobot were using a same 0 day vulnerability to attack LILIN DVR devices, the vendor soon fixed the vulnerability. On August 26, 2020, our Anglerfish honeypot detected that another

new LILIN DVR/



· Dec 3, 2020 · 5 min read

0-day

LILIN DVR/NVR 在野0-day漏洞攻击报告2

本文作者：马延龙，叶根深 背景介绍 2020年8月26号，360网络安全研究院Anglerfish蜜罐系统监测到有攻击者，使用Merit LILIN DVR/NVR 默认密码和0-day漏洞，传播Mirai僵尸网络样本。2020年9月25号，Merit LILIN联络人在收到漏洞报告后，快速地响应并提供了固件修复程序(4.0.26.5618 firmware version for NVR5832)。此前，我们曾向Merit LILIN报告了另一个0-day漏洞[1][2]。时间线 2020年9月21号，我们邮件联系Merit LILIN厂商并报告了漏洞详情以及在野攻击PoC。2020年9月22号，Merit LILIN联络人邮件回复已经连夜修复该问题。2020年9月25号，Merit LILIN联络人提供固件修复程序4.0.26.5618 firmware version for NVR5832。影响范围 360 FirmwareTotal系统通过对Merit LILIN



· Dec 3, 2020 · 6 min read

0-day

Ttint: An IoT Remote Access Trojan spread through 2 0-day vulnerabilities

Author: Lingming Tu, Yanlong Ma, Genshen Ye Background introduction Starting from November 2019, 360Netlab Anglerfish system have successively monitored attacker using two Tenda router 0-day vulnerabilities to spread a Remote Access Trojan (RAT) based on Mirai code. The conventional Mirai variants normally focus on DDoS, but this variant is different.



· Oct 1, 2020 · 10 min read

0-day

Ttint: 一款通过2个0-day漏洞传播的IoT远控木马

本文作者：涂凌鸣，马延龙，叶根深 背景介绍 从2019年11月开始，360Netlab未知威胁检测系统Anglerfish蜜罐节点相继监测到某个攻击者使用2个腾达路由器0-day漏洞传播一个基于Mirai代码开发的远程控制木马(RAT)。常规的Mirai变种基本都是围绕DDoS做文章，而这个变种不同，在DDoS攻击之外，它针对路由器设

备实现了Socket5代理，篡改路由器DNS，设置iptables，执行自定义系统命令等多达12个远程控制功能。此外，在C2通信层面，它使用WSS (WebSocket over TLS) 协议，一方面这样在流量层面可以规避非常成熟的Mirai流量检测，另一方面可以为C2提供安全加密通信。在C2本身，攻击者最开始使用了一个Google的云服务IP，其后切换到位于香港的一台托管主机，但是当我们使用网站证书，样本，域名及IP在我们的DNSmon系统里深入扩展关联后，我们看到更多的基础设施IP，更多的样本，和更多的C2域名。两个0 day，网关设备的12种远控功能，加密流量协议，多次更换的基础设施IP，我们怀疑这个也许不是普通玩



· Sep 30, 2020 · 12 min read

honeypot

360网络安全研究院杭州开点招聘

团队简介 360网络安全研究院（360Netlab）于2014年成立。不同于传统网络安全主要基于规则，数据分析是团队的主要方向。团队持续专注于DNS和僵尸网络领域，并在领域内保持领先地位。从2014年开始，团队在DNS方向上建设了国内历史最久、覆盖范围最广的PassiveDNS基础数据库，及其附属其它基础数据库，持续分析产出威胁情报并应用于360网络安全大脑，并在多个DNS领域内的技术会议上做公开报告。在僵尸网络领域内，团队多年来持续致力于发现跟踪僵尸网络活动，披露了包括Mirai、Satori在内的若干重大安全威胁，并因为其中针对Mirai僵尸网络的持续分析工作得到美国FBI、美国司法部的致谢。360网络安全研究院计划在杭州新成立一个产品团队，把我们的安全数据和技术产品化，探索网络安全行业未知威胁检测难题，为360安全大脑添砖加瓦。从一次平凡的网络扫描，到漏洞、样本、安全事件分析，再到0-day漏洞检测、未知恶意软件检测、高级威胁追踪，我们致力于通过数据驱动安全，构建网络安全看得见的能力。更多信息：

<https://netlab.360.com> 简历投



· Sep 8, 2020 · 6 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 漏洞原因：通过360 FirmwareTotal系统分析，我们发现这个漏洞出现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

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

0-day

Two zero days are Targeting DrayTek Broadband CPE Devices

Author: Yanlong Ma, Genshen Ye, Hongda Liu Background From December 4, 2019, 360Netlab Threat Detection System has observed two different attack groups using two 0-day vulnerabilities of DrayTek[1]

Vigor enterprise routers and switch devices to conduct a series of attacks, including eavesdropping on device's network traffic, running SSH



· Mar 27, 2020 · 5 min read

0-day

DrayTek Vigor企业级路由器和交换机设备在野0-day 漏洞分析报告

本文作者：马延龙，叶根深，刘宏达 背景介绍 从2019年12月4开始，360Netlab未知威胁检测系统持续监测到两个攻击团伙使用DrayTek Vigor企业级路由器和交换机设备0-day漏洞，窃听设备网络流量，开启SSH服务并创建系统后门账号，创建Web Session后门等恶意行为。2019年12月25号，我们在Twitter[1][2]上披露了DrayTek Vigor在野0-day漏洞攻击IoC特征，并给相关国家CERT提供技术支持。2020年2月10号，厂商DrayTek发布安全公告[3]，修复了该漏洞并发布了最新的固件程序1.5.1。漏洞分析 我们根据Firmware Total系统[4]进行DrayTek Vigor在野0-day漏洞定位和模拟漏洞验证。其中2个0-day漏洞命令注入点keyPath，rtick已经被厂商修复，它们均位于/www/cgi-bin/mainfunction.cgi程序中，对应的Web Server程序为/usr/sbin/lighttpd。keyPath 命令注入漏洞分析 漏洞类型：未授权远程命



· Mar 27, 2020 · 6 min read

LILIN DVR

LILIN DVR 在野0-day 漏洞分析报告

本文作者：马延龙，涂凌鸣，叶根深，刘宏达 当我们研究Botnet时，我们一般看到的是攻击者通过N-day漏洞植入Bot程序。但慢慢的，我们看到一个新的趋势，一些攻击者开始更多地利用0-day漏洞发起攻击，利用手段也越发成熟。我们希望安全社区关注到这一现象，积极合作共同应对0-day漏洞攻击威胁。背景介绍 从2019年8月30号开始，360Netlab未知威胁检测系统持续监测到多个攻击团伙使用LILIN DVR 0-day漏洞传播Chalubo[1]，FBot[2]，Moobot[3]僵尸网络。在2020年1月19号，我们开始联系设备厂商LILIN。在2020年2月13号，厂商修复了该漏洞[4]，并发布了最新的固件程序2.0b60_20200207[5]。漏洞分析 LILIN 0-day漏洞主要包括：硬编码登陆账号密码，/z/zbin/dvr_box命令注入漏洞和/z/zbin/net_html.cgi任意文件读取漏洞。其中/z/zbin/dvr_



· Mar 20, 2020 · 5 min read

LILIN DVR

Multiple botnets are spreading using LILIN DVR 0-day

Author: Yanlong Ma, Lingming Tu, Genshen Ye, Hongda Liu When we talk about DDos botnet, we tend to think the typical scenario, some mediocre, code-borrowing scripts target old vulnerabilities. But things

actually have started to change, we noticed more and more attackers beginning to use 0-day vulnerabilities. Background Starting from



· Mar 20, 2020 · 4 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，我们认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

