JiaYu

Beijing

en

Threat Alert: z0Miner Is Spreading quickly by Exploiting ElasticSearch and Jenkins Vulnerabilities

Overview In recent months, with the huge rise of Bitcoin and Monroe, various mining botnet have kicked into high gear, and our BotMon system detects dozens of mining Botnet attacks pretty much every day, most of them are old families, some just changed their wallets or propagation methods, and z0Miner

· Mar 8, 2021 · 3 min read

Botnet

威胁快讯：z0Miner 正在利用 ElasticSearch 和 Jenkins 漏洞大肆传播

 概述 最近几个月受比特币、门罗币大涨的刺激，各种挖矿家族纷纷活跃起来，我们的 BotMon 系统每天都能检测到几十上百起的挖矿类 Botnet 攻击事件。根据我们统计，它们多数是已经出现过的老家族，有的只是换了新的

钱包或者传播方式，z0Miner 就是其中一例。 z0Miner 是去年开始活跃的一个恶意挖矿家族，业界已有公开的分析。z0Miner 最初活跃时，利用 Weblogic 未授权命令执行漏洞进行传播。 近期，360 网络安全研究院 Anglerfish 蜜罐系统监测到 z0Miner 又利用 ElasticSearch 和 Jenkins 的远程命令执行漏洞进行大肆传播，近期活跃趋势如下： 漏洞利用情况 ElasticSearch RCE 漏洞 CVE-2015-1427 虽然是个

· Mar 7, 2021 · 4 min read

en

Blackrota, a heavily obfuscated backdoor written in Go

The most obfuscated Go-developed ELF-formatted malware we've found to date. Overview Recently, a malicious backdoor program written in the Go language that exploits an unauthorized access vulnerability in the Docker Remote API was caught by the our Anglerfish honeypot. We named it Blackrota, given that its C2 domain

· Nov 24, 2020 · 7 min read

Import 2022-11-30 11:16

Blackrota, 一个Go开发的高度混淆的后门

概述 最近，我们通过 Anglerfish 蜜罐捕获到一个利用 Docker Remote API 未授权访问漏洞来传播的 Go 语言编写的恶意后门程序，鉴于它上线的 C2 为 blackrota.ga ，我们把它命名为 Blackrota。 Blackrota 后门程序目前只有 Linux 版，为 ELF 文件格式，支持 x86/x86-64 两种 CPU 架构。Blackrota 基于 geacon 配置并编译，geacon 是一个 Go 语言实现的 CobaltStrike Beacon，它可以作为 CobalStrike 的 Beacon 与 CobaltStrike 交互来控制失陷主机： 不过它只实现了原生 CobaltStrike

· Nov 20, 2020 · 9 min read

Import 2022-11-30 11:16

HEH Botnet, 一个处于开发阶段的 IoT P2P Botnet

概述 近期 360Netlab 未知威胁检测系统捕获到一批未知恶意家族的样本，这一批样本支持的 CPU 架构有 x86(32/64), ARM(32/64), MIPS(MIPS32/MIPS-III) 以及 PPC，经过我们分析，将其命名为 HEH Botnet。 HEH 是一个由 Go 语言编写的 IoT P2P Botnet，它的 P2P 协议不基于公开的任何 P2P 协议，而是自研协议。 HEH 现阶段会通过暴力破解 23/2323 两个端口的 Telnet 服务来传播，而不针对特定设备。 基于以下两点，我们认为它还处于开发测试阶段： 1. 整个僵尸网络的运作机制还不太成熟； 2. 部分指令还未实现。 根据

· Nov 9, 2020 · 10 min read

en

HEH, a new IoT P2P Botnet going after weak telnet services

Overview Recently, 360Netlab threat detection system captured a batch of unknown samples. The CPU architectures supported by this batch of samples are broad, including x86(32/64), ARM(32/64), MIPS(MIPS32/MIPS-III) and PPC, it is spreading through brute force of the Telnet service on ports 23/2323, which

· Oct 7, 2020 · 8 min read

Botnet

DDG的新征程——自研P2P协议构建混合P2P网络

1. 概述 DDG Mining Botnet 是一个活跃已久的挖矿僵尸网络，其主要的盈利方式是挖 XMR。从 2019.11 月份至今，我们的 Botnet 跟踪系统监控到 DDG Mining Botnet 一直在频繁跟新，其版本号和对应的更新时间如下图所示： 其中，v4005~v4011 版本最主要的更新是把以前以 Hex 形式硬编码进样本的 HubList 数据，改成了 Gob 序列化的方式；v5009 及以后的版本，则摒弃了以前基于 Memberlist 来构建 P2P 网络的方式，改用自研的 P2P 协议来构建混合模式 P2P 网络 。简化的网络结构如下： 右边服务器是 C&C Server，DDG

· May 7, 2020 · 20 min read

en

DDG botnet, round X, is there an ending?

DDG is a mining botnet that we first blogged about in Jan 2018, we reported back then that it had made a profit somewhere between 5.8million and 9.8million RMB(about 820,000 to 1.4Million US dollar)，we have many follow up blogs about this botnet after that,

· Apr 8, 2020 · 2 min read

Botnet

SystemdMiner,when a botnet borrows another botnet's infrastructure

Update(2019.4.26 17:30) About 3 hours after the release of this article, we found that the attacker took down the URL of some Payload downloads, the following URL has expired: aptgetgxqs3secda.onion.ly/systemd-cron.sh aptgetgxqs3secda.onion.pet/systemd-cron.sh

aptgetgxqs3secda.onion.ly/systemd-login-ddg aptgetgxqs3secda.onion.pet/

· May 7, 2019 · 16 min read

Botnet

systemdMiner 借鸡下蛋，通过 DDG 传播自身

1. 概述 在最近的关于 DDG.Mining.Botnet v3021/v3022 版本的 威胁快讯 一文中，我们提到了 DDG 最近在用的主 C2: 119.9.106.27 AS45187|RACKSPACE-AP Rackspace IT Hosting AS IT Hosting Provider Hong Kong, HK|Hong Kong|China 2019.4.19 日凌晨，我们发现 DDG 更新了其配置数据(CfgVer:23)和恶意 Shell 脚本 i.sh，在 i.

· Apr 11, 2019 · 22 min read

Botnet

“双枪”木马的基础设施更新及相应传播方式的分析

1. 引述 2018.12.23 日，我们的 DNSMon 系统监测到以下三个异常的域名，经过研判这些域名属于 双枪 木马的网络基础设施。考虑到这些域名仅在最近才注册并启用，我们认为双枪木马近期在更新其基础设施，建议安全社区加以关注。 white[.]gogo23424.com www[.]src135.com www[.]x15222.com 双枪 木马是目前我们见过的最复杂的恶意程序之一，最早由 360 安全卫士团队披露，并对其木马工作原理做了详细的技术分析。双枪木马本身集 Rootkit 和 Bootkit(同时感染 MBR 和 VBR)于一身，还有诸多对抗措施。除此之外，双枪木马恶意活动相关的网络基础设施十分庞杂，感染路径繁琐、传播手段多样，涉及的黑灰产业务种类也五花八门。 之前对双枪木马的公开披露内容主要涉及双枪木马本身的工作原理、涉及的黑灰产业务以及部分溯源。对其传播过程的技术细节少有涉及。在双枪木马多种多样的传播方式中，按照我们的统计，

· Dec 28, 2018 · 25 min read

Import 2022-11-30 11:16

威胁快讯：DDG 3013 版本

DDG 是一个专注于扫描控制 SSH 、 Redis数据库 和 OrientDB数据库 服务器，并攫取服务器算力挖矿（门罗币）的僵尸网络。我们在2017年10月25日首次感知到 DDG僵尸网络，并在随后发布了多份报告。最近的一篇报告 发布于 2018-06，当时 DDG 的版本更新到 3012。 今晨，我们注意到 DDG 更新到版本 3013。 IoC C2 149.56.106.215:8000 Canada/CA Pierrefonds "AS16276 OVH SAS" 下载URL hxxp://149.56.106.215:8000/i.sh

· Aug 1, 2018 · 1 min read

Import 2022-11-30 11:16

Threat Alert: DDG 3013 is Out

DDG is a mining botnet mainly focusing on SSH, Redis databases and OrientDB database servers. We captured the first DDG botnet on October 25, 2017, and subsequently released several reports. A recent report was released in 2018-06, which reflected the newest version of DDG 3012 at that time. This morning,

· Aug 1, 2018 · 1 min read

Import 2022-11-30 11:16

僵尸永远不死，DDG拒绝凋零

DDG 是一个专注于扫描控制 SSH 、 Redis数据库 和 OrientDB数据库 服务器，并攫取服务器算力挖矿（门罗币）的僵尸网络。我们在2017年10月25日首次感知到 DDG僵尸网络，并在随后展开了持续的分析和跟踪。在这期间，我们注意到该僵尸网络有两个内部保留域名尚未注册，我们抢注了这两个域名，并利用到这两个域名的流量精确记录了该僵尸网络感染的 4,391 个IP地址。在那段时间中，DDG 的主要流行版本是 2020、2021。以上内容详细记录在我们 2018年2月发布的 报告中。 有些僵尸网络的作者，会在我们发布分析报告之后悄然离去，比如 http81（persirai），但是 ddg 的作者选择留在场上。 DDG首份报告发布后3个月，2018年5月，我们意识到 DDG 有更新。这一次卷土重来，DDG更换了其主控IP地址，以期逃避安全研究员的跟踪。不过我们依旧定位到了 DDG 的两个新版本 3010和3011，并监控到作者对 3011

· Jul 12, 2018 · 4 min read

Import 2022-11-30 11:16

Old Botnets never Die, and DDG REFUSE to Fade Away

DDG is a mining botnet that specializes in exploiting SSH, Redis database and OrientDB database servers. We first caught it on October 25, 2017, at that time, DDG used version number 2020 and 2021, and we noticed that the botnet has two internally reserved domain names that had not been

· Jul 12, 2018 · 3 min read

Import 2022-11-30 11:16

DDG.Mining.Botnet 近期活动分析

UPDATE(2018.6.13) 6.12 日，我们监测到 DDG.Mining.Botnet 又发布了新版本，最新版本为 v3012 ，更新概要如下： * 更换主 C2 为 69.64.32.12:8000 ； * 修改用来持久驻留的 i.sh 脚本； * 更新备用 C2 IP 列表； * 云端配置文件的结构、编码方式没有变化，只是里面涉及 C2 的内容指向最新的 C2； * 矿机程序、矿池 Proxy以

及 XMR Wallet 均未变化，Wallet 地址：
42d4D8pASAWghyTmUS8a9yZyErA4WB18TJ6Xd2rZt9HBio2aPmAAVpHcPM8yoDEYD9Fy7eRvPJhR7SKF
yTaFbSYCNZ2t3ik在矿池 supportxmr.com 中 TotalPaid

· Jun 13, 2018 · 14 min read

Import 2022-11-30 11:16

MsraMiner: 潜伏已久的挖矿僵尸网络

2017 年 11 月底，我们的 DNSMon 系统监测到几个疑似 DGA 产生的恶意域名活动有异常。经过我们深入分析，确认这背后是一个从 2017 年 5 月份运行至今的大型挖矿僵尸网络（Mining Botnet）。此僵尸网络最新的核心样本压缩包文件名为 MsraReportDataCache32.tlb ，我们将其命名为MsraMiner Botnet。 该僵尸网络的特征包括： * 运行时间：2017 年 5 月份运行至今 * 传播方式：利用 NSA 武器库来感染，通过 SMB 445 端口传播蠕虫式传播：样本自带 Web Server提供自身恶意代码下载。样本扩散主要靠失陷主机之间的 Web Server 或 Socket 传输，同时提供了 C&C 端获取样本作为后备机制；

· Mar 16, 2018 · 14 min read

Import 2022-11-30 11:16

DDG.Mining.Botnet：一个瞄准数据库服务器的挖矿僵尸网络

从 2017-10-25 开始，我们监控到有恶意代码在大规模扫描互联网上的 OrientDB 数据库服务器。进一步的分析发现，这是一个长期运营的僵尸网络，其主要目标是挖取门罗币（XMR，Monero CryptoCurrency）。我们将其命名为 DDG 挖矿僵尸网络 （DDG Mining Botnet，以下简称 DDG） ，主要原因是因为其核心功能模块的名称为 DDG。 DDG 累积挖取的门罗币数目较大。目前我们能够确认该僵尸网络累积挖取的已经超过 3,395枚门罗币，按当前价格折合人民币 ￥5,821,657 。另外因为矿池记账系统的问题，有2,428枚 XMR不能完全确认是否归属 DDG，按当前价格折合人民币 ￥4,163,179。DDG 是目前我们视野范围内门罗币收益第二大的僵尸网络，第一大的是我们之前报告的 MyKings 僵尸网络。 DDG 的结构上，除了僵尸网络中常见的 C2 和

· Feb 1, 2018 · 17 min read

Import 2022-11-30 11:16

DDG: A Mining Botnet Aiming at Database Servers

Starting 2017-10-25, we noticed there was a large scale ongoing scan targeting the OrientDB databases. Further analysis found that this is a long-running botnet whose main goal is to mine Monero CryptoCurrency. We name it DDG.Mining.Botnet after its core function module name DDG. Currently we

are able to

· Feb 1, 2018 · 11 min read

Botnet

MyKings: 一个大规模多重僵尸网络

【更新记录】 2018-01-24 原始文档首次公开，原先基于新浪blog的所有上联通道均已切断 2018-01-29 12:00 MyKings的上联通道开始使用新的blog url http://test886.hatenablog.com/entry/2018/01/26/002449，我们通过 https://twitter.com/360Netlab 发布了这一消息 2018-01-29 15:00 我们注意到上述 BLOG URL 已经被封 2018-01-29 05:00 https://twitter.com/ninoseki 告知，上述被封动作是 hantena 博客安全团队处理的。 以下是原始文章 作者 netlab.360.com MyKings 是一个由多个子僵尸网络构成的多重僵尸网络，2017

· Jan 29, 2018 · 17 min read