2018年云上挖矿分析报告

阿里云安全技术 / 2019-02-01 17:22:00 / 浏览数 1486 安全技术 技术讨论 顶(0) 踩(0)

近日，阿里云安全团队发布了《2018年云上挖矿分析报告》。该报告以阿里云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

报告指出，尽管加密货币的价格在2018年经历了暴跌，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，越来越多的0-Day/N-Day漏洞在公布后的极短时间内

以下是报告部分内容，请关注"阿里云安全"公号后，回复"报告"二字获取完整版报告下载链接。

报告主笔：悟泛

其他内容贡献者：桑铎、董云、穆如、乐枕、燚矗、刘洪亮、南浔

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

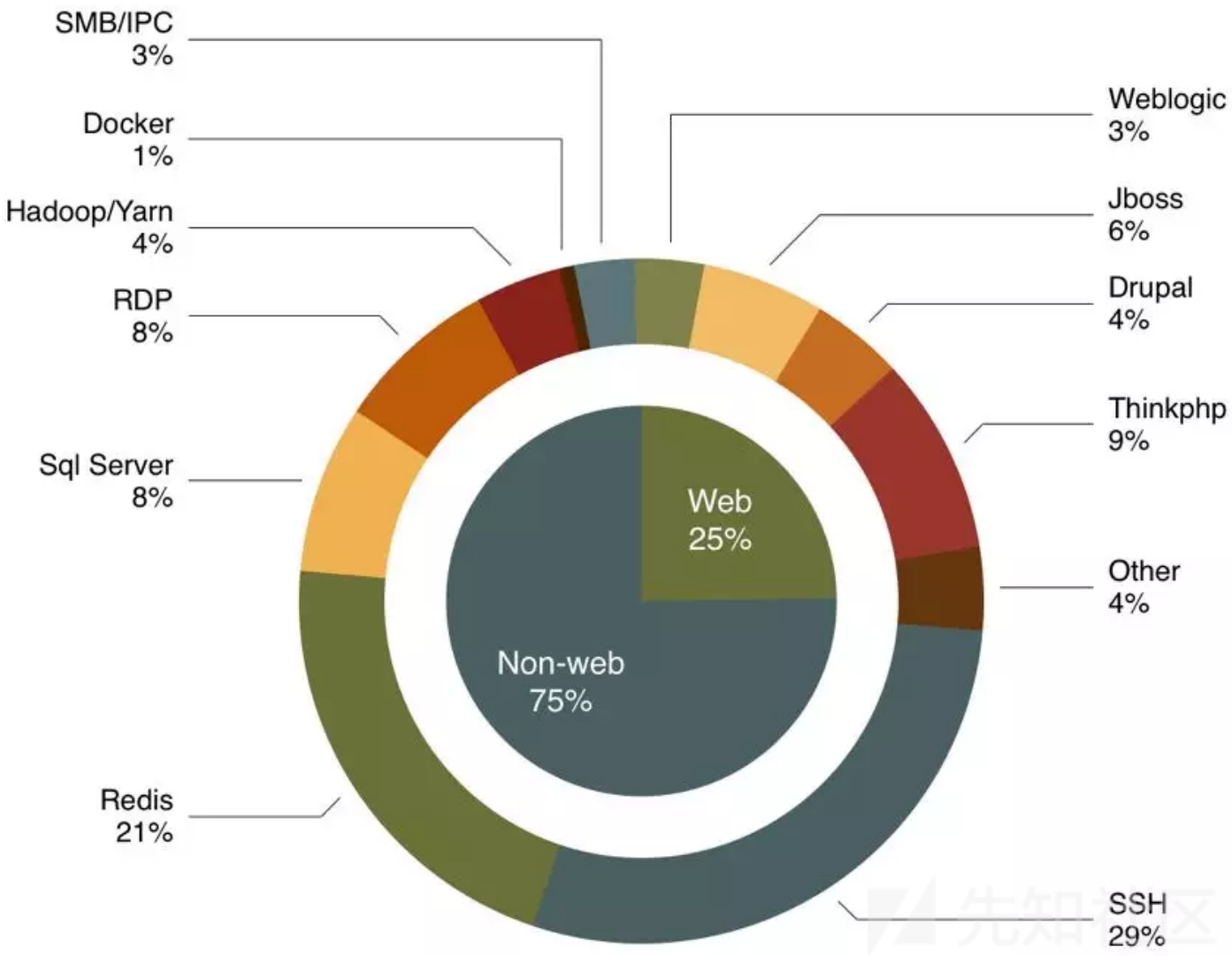
同时阿里云观察到，0-Day漏洞从披露到大规模利用之间的时间间隔越来越小。因此在高危0-Day漏洞爆出后未能及时修复的用户，容易成为恶意挖矿的受害者。

【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、SQLSer

【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



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。这些挖矿木马传播速度较快，且

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

【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:

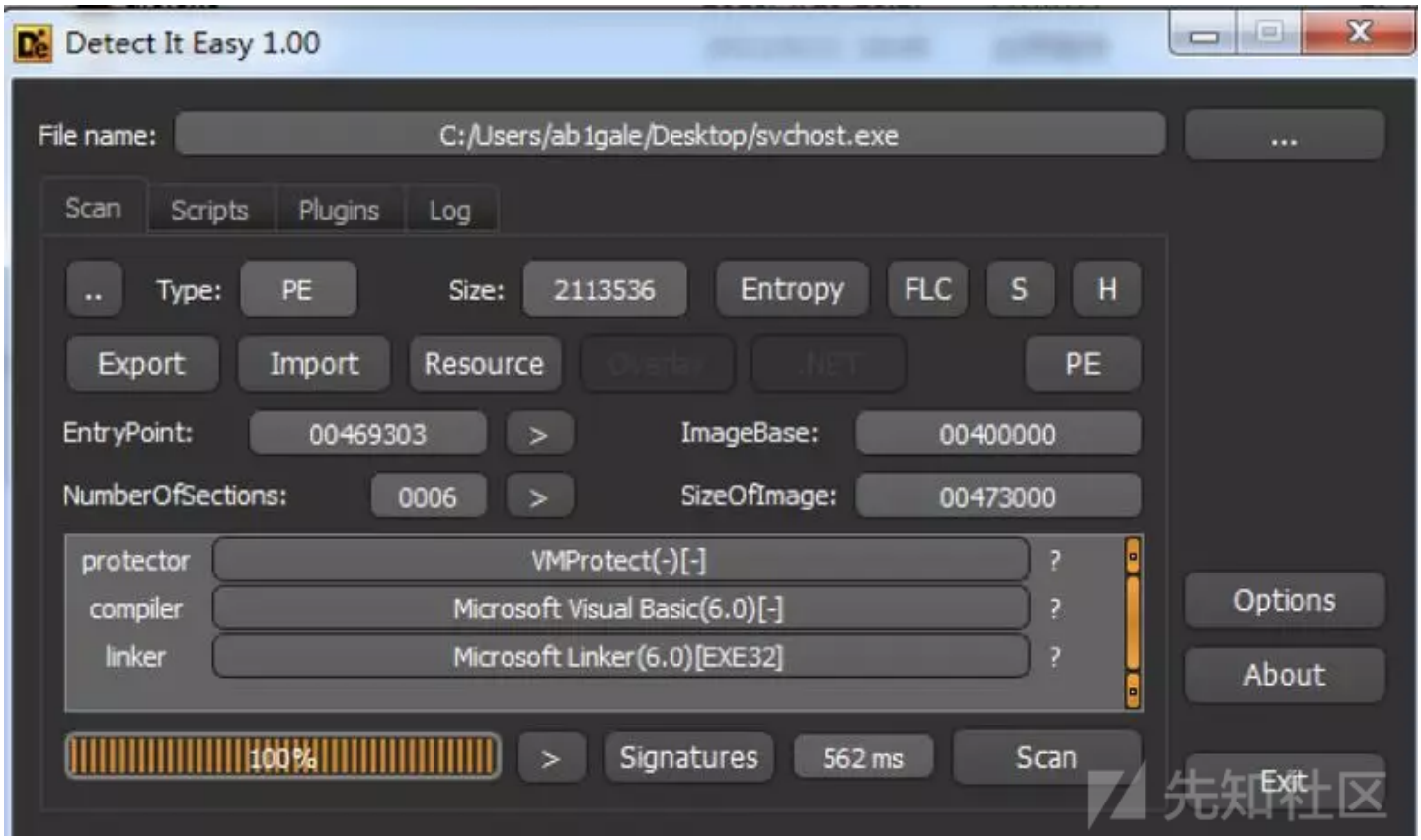
```
cmd /c schtasks /create /sc minute /mo 1 /tn "Miscfost" /ru system /tr "cmd /c C:\Windows\ime\scvsots.exe"
```

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

【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、taskmg

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



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。

xmr.enjoytopic.tk/d/ps3.txt

```
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">
    window.resizeTo 0,0
    window.MoveTo -100,-100
        Dim OremkplPWQdwlnIx, fmqzhrxtRYABlzVD, VTkTfqwEWaZCcFvO
        sUb WiCfVBxZLfommLtk
        oReMkplPWqdwLnIx = "-3133+3220*-6518+6623*-6095+6205*-3145+3245*-155+266*-1425+1544*5902-
5856*-4234+4316*-5595+5696*-1780+1863*-3549+3654*-4447+4569*452682/4482*-223+307*7729-7618*261568/8174*-4717+4765*-6424+646
5798*5517-5417*-4343+4454*-2721+2840*390494/8489*-1243+1352*-5712+5823*7900-7782*-477+578*1986-1902*264624/2384*1160-1128*1
3875*5713-5668*-643+693*-557+605*925-877*1803-1755*-5946+5978*79990/7999*249480/3564*-3923+4040*249040/2264*-3413+3512*916-
7205*369667/3811*-4286+4400*4781-4686*891-789*-2329+2446*239250/2175*-4011+4110*-4938+4978*15867/387*-2892+2902*-3207+3216*
1542*120360/1020*-253+350*2475-2361*-5874+5969*133745/1163*6247-6143*1842-1741*9707-9599*2623-2515*9057-9047*-9394+9403*930
4681*1034604/8919*171424/5357*416186/3527*132405/1365*5220-5106*5585-5490*-157+272*-1894+1998*1233-1132*-6686+6794*-5942+60
5398*-7401+7515*214019/2119*65378/674*973124/8389*740229/7329*584916/7404*153860/1570*-555+661*-8761+8862*2159-2060*-3704+3
2007*-7254+7369*56232/568*-2738+2852*736470/7014*658560/5880*2308-2192*82754/1799*488704/5888*7586-7482*412585/4085*5940-
5832*-2460+2568*276930/8145*391304/9544*-9898+9908*-4212+4221*766-648*1979-1882*-2652+2766*235505/2479*1016140/8836*7043-
6939*197657/1957*-5832+5940*816156/7557*77924/1694*1108650/9725*3735-3618*-983+1093*123808/3869*-9082+9116*6270-6158*376956
1414*-8903+9004*215352/1994*-9106+9214*197202/4287*-7390+7491*663360/5528*9628-9527*-2760+2792*234360/5208*2031-
```

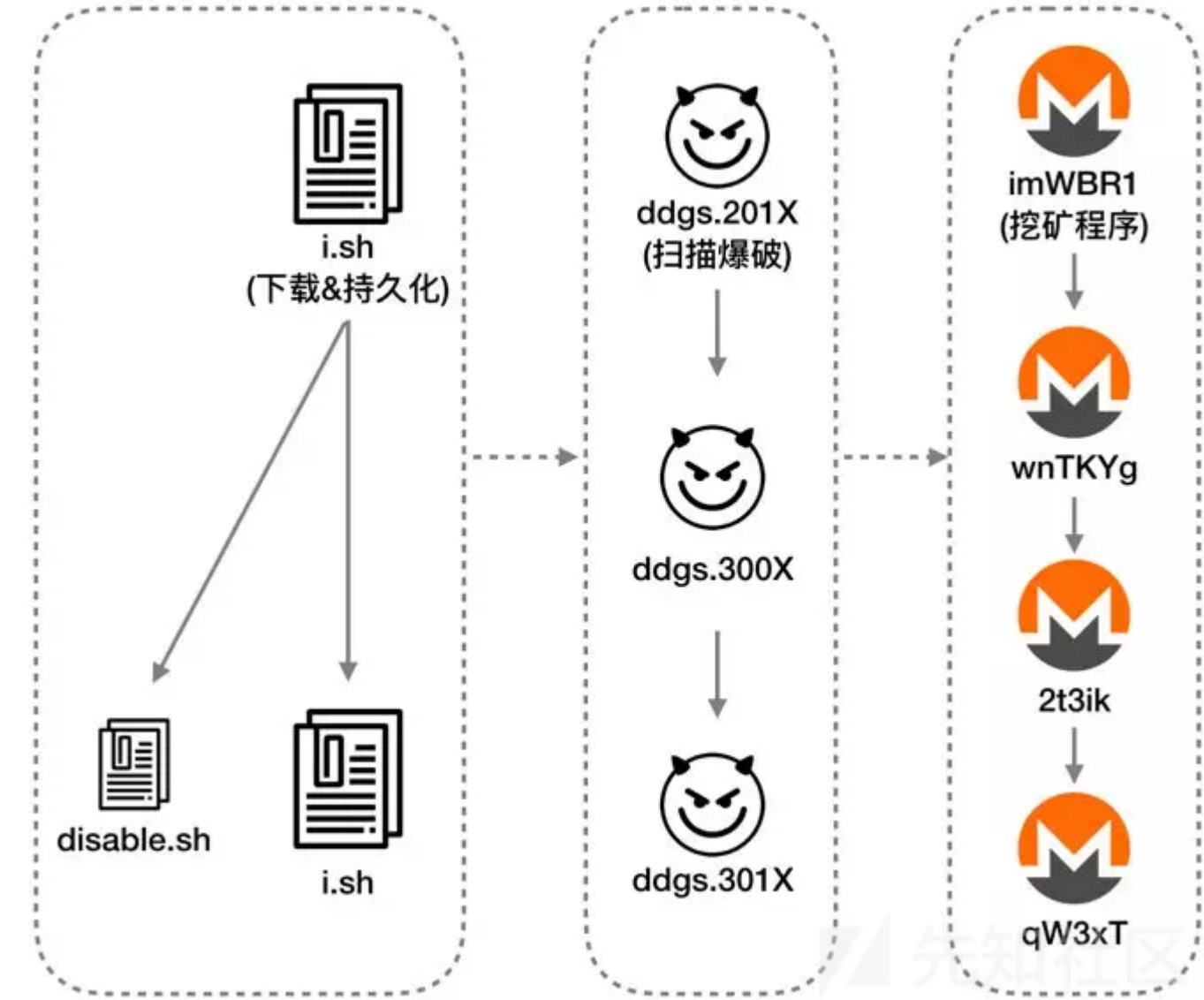
尽管人工分析时可以通过多种手段去混淆或解密，但加密和混淆对逃避杀毒软件而言，仍是非常有效的手段。

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。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

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

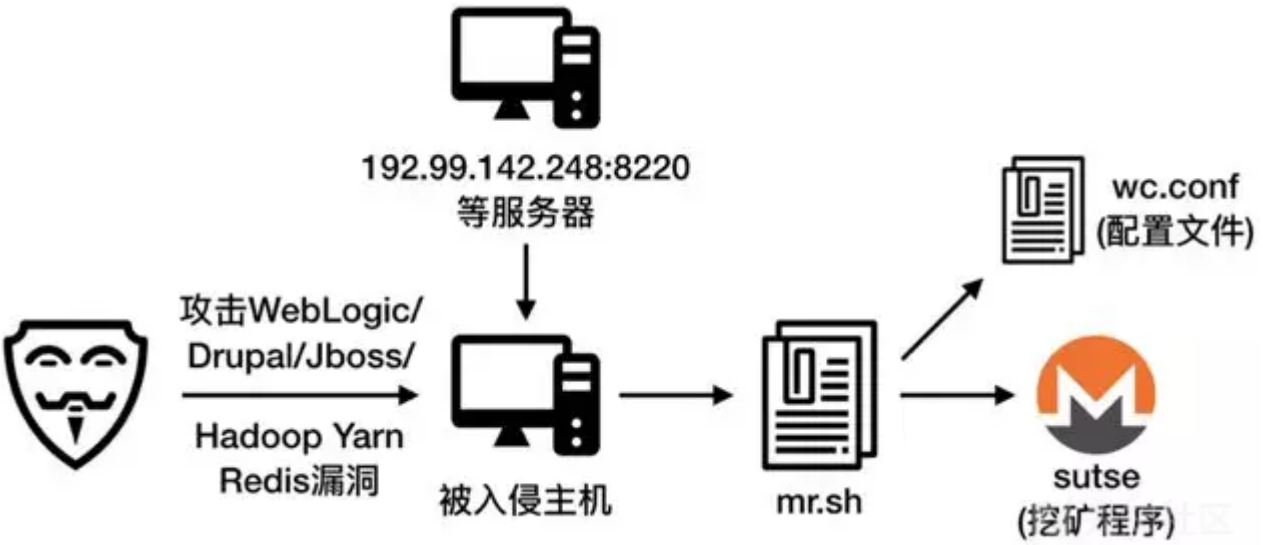


DDG（3019）各模块结构功能

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。

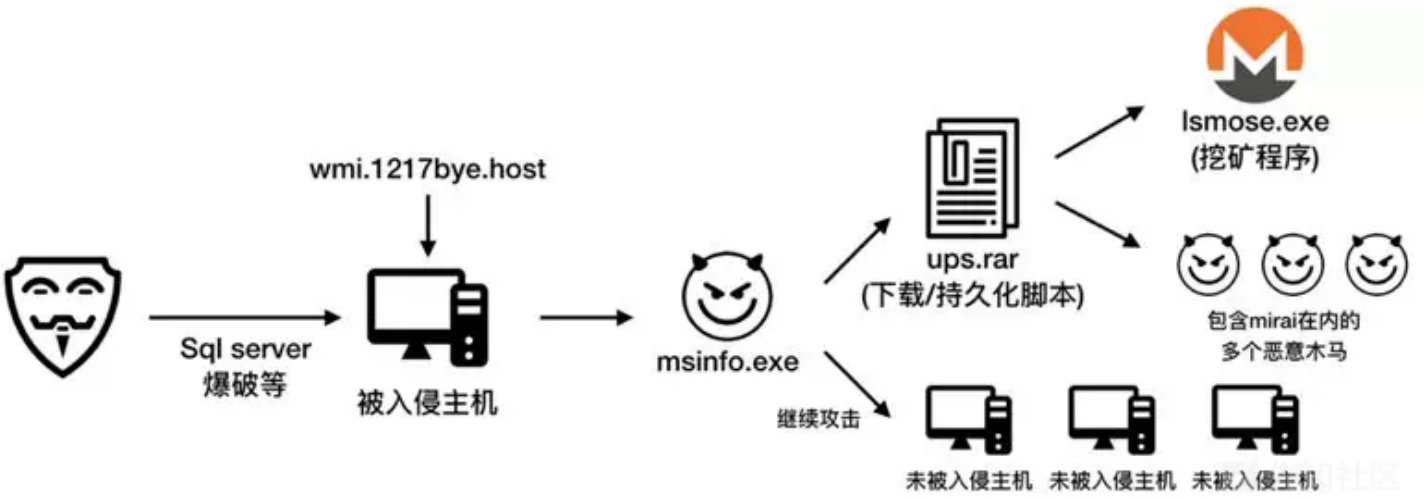
这种方式理论上传播速度较慢，相较于蠕虫型传播的僵尸网络也更难存活，但8220挖矿团伙仍以这种方式获取了较大的感染量。



挖矿网络结构

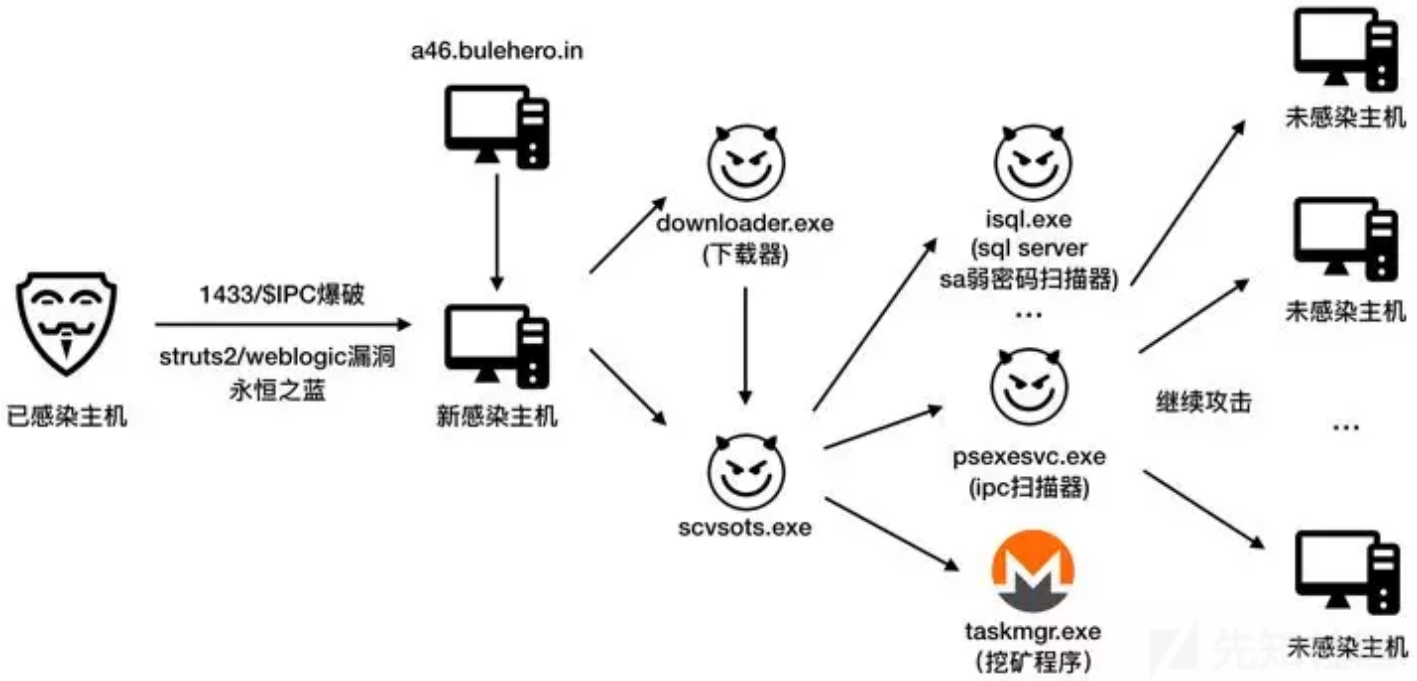
3.Mykings(theHidden)挖矿团伙

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



挖矿网络结构

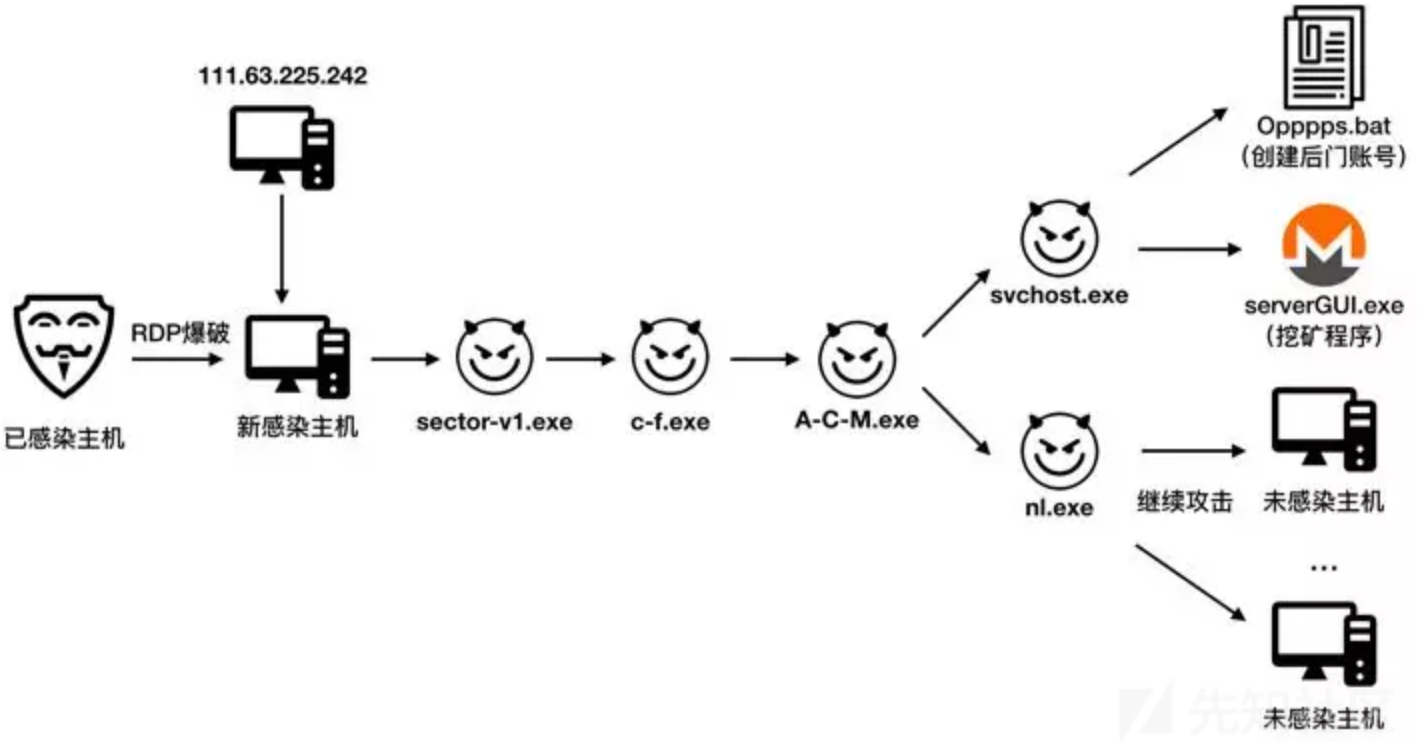
4.Bulehero挖矿团伙



挖矿网络结构

5.RDPMiner挖矿团伙

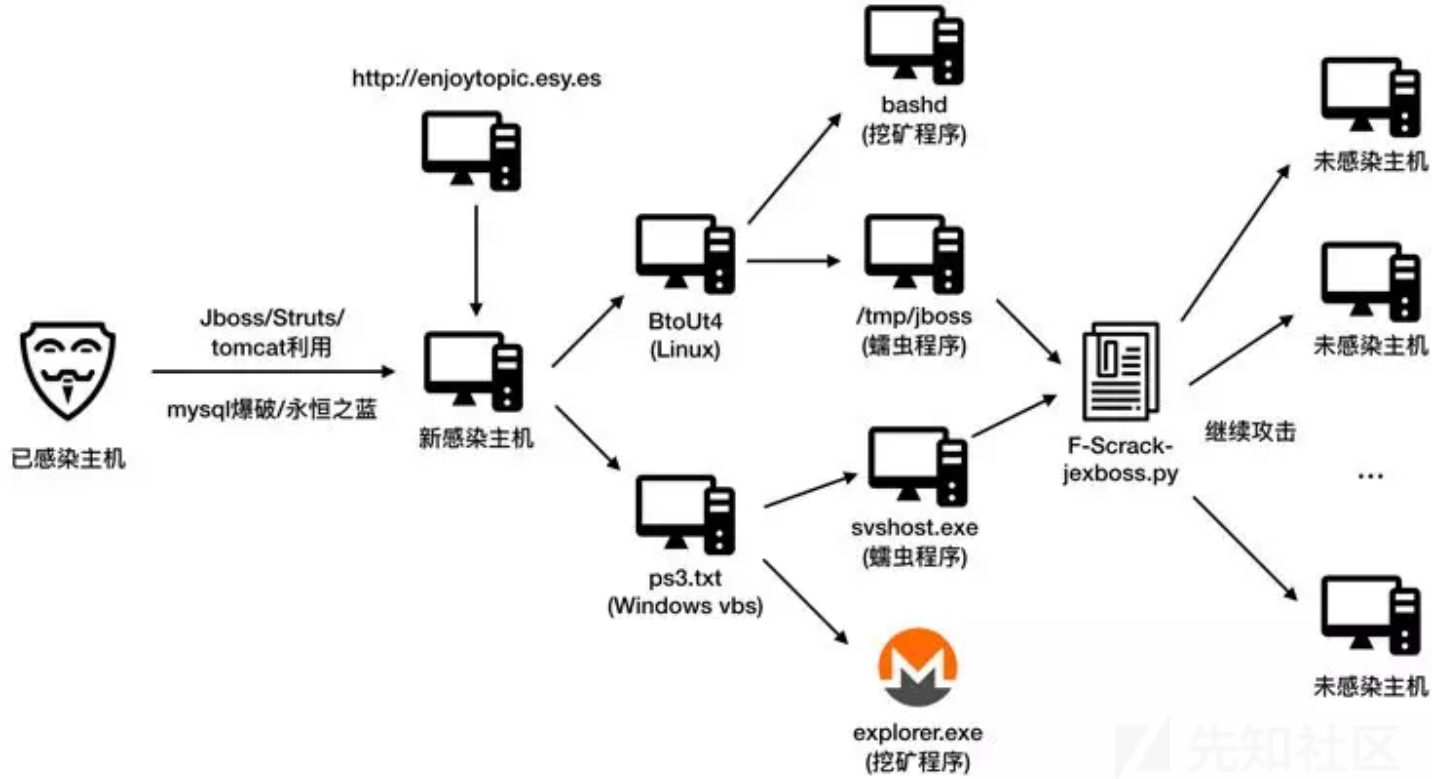
该挖矿僵尸网络自2018年10月开始蔓延，之后多次更换挖矿程序名称。



挖矿网络结构

6.JbossMiner挖矿团伙

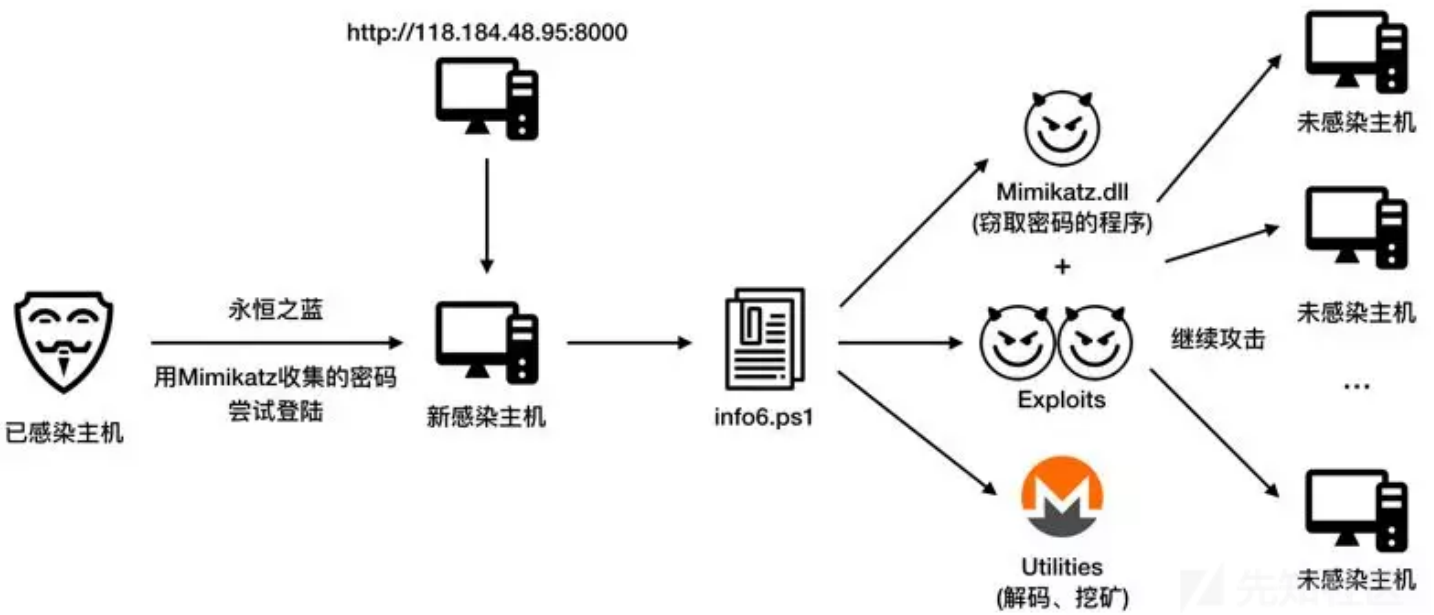
阿里云安全团队于2018年3月报道过，从蜜罐中捕获到JbossMiner的恶意程序样本，该样本由py2exe打包，解包反编译后是一套由Python编写的完整攻击程序，包含源码及



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。



挖矿网络结构

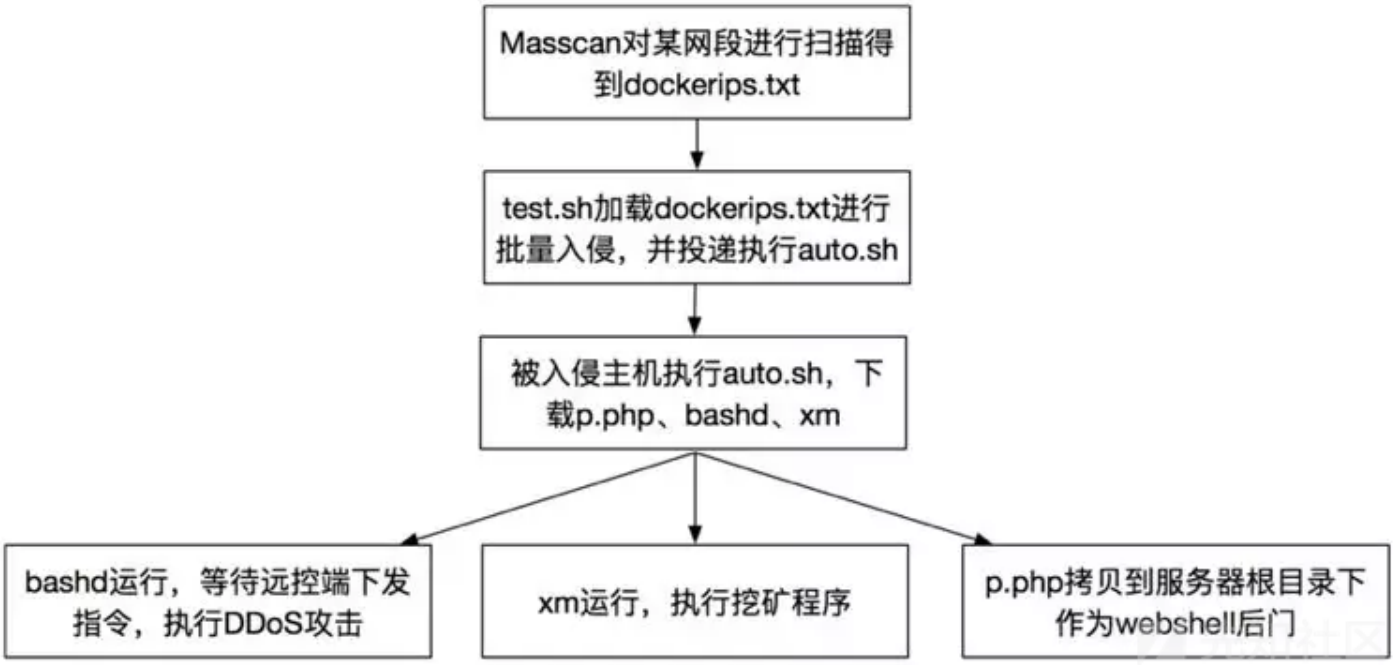
8.Kworkerd

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。

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



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

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
- 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
- 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

上一篇：某应急响应样本分析 下一篇：通过MySQL LOAD DATA...

1. 0 条回复
   - 动动手指，沙发就是你的了！