Typical Mining Family Series Analysis 3

——Sysrv-hello Mining Worm

Antiy CERT

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

Draft completed: December 12, 2022, 4:40 p.m.

First published: January 12, 2023, 5:44 p.m.

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

Contents

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 that continue to operate mining Trojans, other black industry organizations that do not 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[1], which clearly required the rectification of virtual currency mining activities and 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, mining Trojan families such as Hezb, "1337" and Kthmimu.

Antiy CERT will compile a special report on the typical popular mining Trojan families that have been tracked and stored in recent years, and will release it in the next few months, and continue 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 the organization's 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 seek more illegal profits.

3 Sysrv-hello Mining Worm

Sysrv-hello is a mining worm that exploits multiple vulnerabilities to spread on both Windows and Linux platforms. Its main purpose is to spread the mining worm and then realize mining profits. The mining worm was first disclosed on December 31, 2020. Since the master file names of a large number of captured samples are mainly composed of the string " sysrv", and the function or module paths used in the samples all contain the string "hello", researchers named it Sysrv-[2]. The files spread by the Sysrv-hello mining worm mainly include the core script, the worm master and the mining program. The core script file types include Shell and PowerShell, which are mainly responsible for downloading and executing worms. The Linux script functions include ending competing products, defense evasion, persistence, and lateral propagation. The PowerShell script focuses more on defense evasion and persistence. The worm matrix is written in GO language and uses various vulnerabilities to spread the core script, thereby achieving its own indirect propagation. The mining program is responsible for hijacking the computing resources of the target host to implement mining. The program is mainly released and executed through the worm matrix, but there is a period of time when the core script is responsible for downloading and executing it.

The Sysrv-hello mining worm are mainly reflected in the core script and the worm matrix. The iteration of the worm matrix is most obvious in the number of vulnerability exploitation components, and there is a phenomenon of trying some vulnerabilities and eliminating them. So far, it has used more than 20 vulnerabilities, and more than 18 are commonly used . The iteration of the core script that can be clearly observed has reached more than 13 times.

The Sysrv-hello mining worm is different from other mining Trojans in that it does not focus on maintaining access to the target system during propagation. Instead, it focuses on improving its propagation capabilities by adding new vulnerability exploitation components to achieve continuous growth and maintain highly stable mining revenue.

4 Sysrv-hello Mining Worm

The Sysrv-hello mining worm was first disclosed on December 31, 2020. It spreads through vulnerabilities, has no targeted targets, and has frequently updated worm samples. It is a dual-platform mining worm active on Windows and Linux. Based on its activities in the past two years, its development can be divided into three stages: early attempt to spread, mid-term expansion of spread, and late focus on defense, avoidance, and maintaining spread. From the analysis of samples in the three stages, it can be seen that the black industry organization behind it does not attach importance to maintaining access to the target host. It only adds the function of implanting the SSH public key in the target system in the mid-term and late Redis vulnerability exploitation; it pays more attention to profit and expands and maintains its propagation capabilities as much as possible. Since its later mining pool connection method uses a mining pool proxy, its comprehensive profit situation cannot be obtained, but during March 2021, it earned an average of one Monero every two days [3]. According to the market price at the time, it earned an average of US$100 per day.

Table 4-1 Basic information of Sysrv-hello mining worm

Family name	Sysrv-hello	
First disclosure time	December 31, 2020	
Reason for naming	The master file names of a large number of captured samples are mainly composed of the string"sysrv", and the function or module paths used in the samples all contain the string "hello"[2].	
Threat types	Mining, worms	
Target	No special target, worm propagation targets are randomized, including cloud hosts	
Transmission method	SSH private keys stored on the victim host	
Propagation components	Laravel Debug mode RCE (CVE-2021-3129)	XXL-JOB executor unauthorized access vulnerability
	Jenkins RCE Vulnerability (CVE-2018-1000861)	Jupyter Unauthorized Access Vulnerability
	Nexus Repository Manager 3 RCE Vulnerability (CVE-2019-7238)	ThinkPHP5 RCE Vulnerability
	WebLogic RCE Vulnerability (CVE-2020-14882)	Hadoop YARN REST API Unauthorized Vulnerability
	Supervisord RCE Vulnerability (CVE-2017-11610)	Wordpress - XMLRPC Brute Force

	JBOOS Deserialization Vulnerability (CVE-2017-12149)	SSH weak password brute force cracking
	PostgreSQL RCE Vulnerability (CVE-2019-9193)	Tomcat weak password brute force cracking
	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396)	Brute force cracking of Redis weak password
	Apache Struts2 RCE Vulnerability (CVE-2017-5638)	Nexus weak password brute force cracking
	PHPUnit RCE Vulnerability (CVE-2017-9841)	Jupyter weak password brute force cracking
	Spring Cloud Gateway Actuator RCE vulnerability (CVE-2022-22947)	Jenkins weak password brute force cracking
	GitLab CE/EE RCE Vulnerability (CVE-2021-22205)	MySQL weak password brute force cracking

The Sysrv-hello mining worm can be divided into three stages based on its updates, sample functions, and mining modes in the past two years. The early stage is mainly propagation, which should be the attacker's attempt to propagate the worm; the mid-term expansion of the propagation intensity, the number of vulnerabilities has also greatly increased, and the specific scope of infection can also be inferred from the revenue in March; the later stage focuses on avoiding and maintaining the propagation ability, further increasing the number of vulnerabilities, and focusing on defense avoidance from aspects such as mining pool addresses, vulnerability module names, and sample implementation names.

5 ATT&CK Mapping of Sysrv-hello Mining Worm

The distribution diagram of technical features corresponding to Figure 5-1.

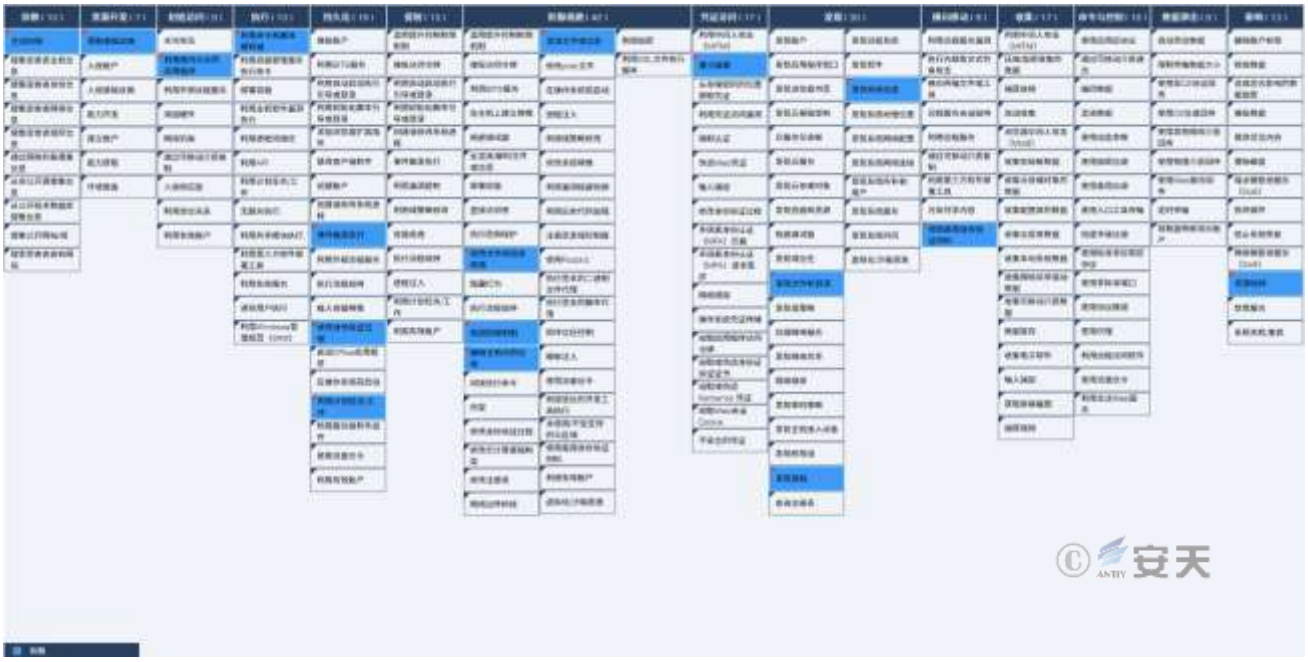

Figure 5-1 Mapping of technical features to ATT&CK

The specific description of ATT&CK technical behavior is shown in 错误!未找到引用源。resist analysis by security researchers) .

Table 5-1List of worm master vulnerabilities

Application Domain	Custom Vulnerability Coding	CVE Number	Vulnerability Description
Current samples and other historical samples	a7545b	none	XXL-JOB executor unauthorized access vulnerability
	a7ed26	none	Jupyter Notebook Unauthorized Access Vulnerability
	a7ee93	CVE-2021-3129	Laravel Debug mode RCE
	b42207	CVE-2018-1000861	Jenkins RCE Vulnerability
	bd788f	CVE-2019-7238	Nexus Repository Manager 3 RCE Vulnerability
	bf714e	CVE-2020-14882	WebLogic RCE Vulnerability
	da8317	CVE-2017-11610	Supervisord RCE Vulnerability
	e39dc2	CVE-2017-12149	JBOOS Deserialization Vulnerability
	e59d60	none	ThinkPHP5 RCE Vulnerability
	e7945e	CVE-2019-9193	PostgreSQL RCE Vulnerability
	e838f9	CVE-2019-3396	Confluence Unauthorized RCE Vulnerability
	ea25a9	CVE-2017-5638	Apache Struts2 RCE Vulnerability

	ebb056	CVE-2017-9841	PHPUnit RCE Vulnerability
	f9edaa	none	Hadoop YARN REST API Unauthorized Vulnerability
	le0943	CVE-2021-22205	GitLab CE/EE RCE Vulnerability
	e842c5	none	SSH weak password brute force cracking
	b0f895	none	Tomcat weak password brute force cracking
	c41954	none	Brute force cracking of Redis weak password
	fa39c1	none	Wordpress - XMLRPC Brute Force
	7d85fa	none	Vulnerability Exploitation Common Module
	7eb18b	none	Vulnerability Exploitation Common Module
Other historical samples	p3e874	CVE-2022-22947	Spring Cloud Gateway Actuator RCE vulnerability
	mysql	none	MySQL weak password brute force cracking
	Nexus	none	Nexus weak password brute force cracking
	jupyter	none	Jupyter weak password brute force cracking
	jenkins	none	Jenkins weak password brute force cracking

5.1.1 Mining Delivery Module

MD5 value of the mining program file in the master sample, and the process management will end the old version of the mining process.d

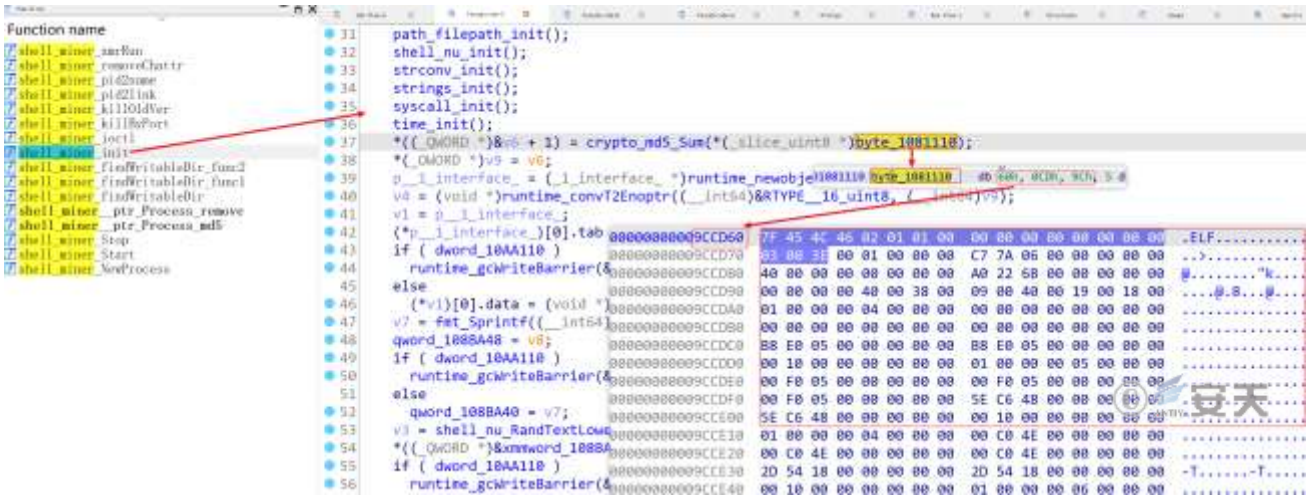

Figure 5-2Mining delivery module

The mining pool proxy address and port are 194.38.23.2:8080, and the previous version is 194.145.227.21:5443.


```
data:00000000007EB97D                db '        "hw-aes": null,',0Ah
data:00000000007EB97D                db '        "priority": null,',0Ah
data:00000000007EB97D                db '        "memory-pool": false,',0Ah
data:00000000007EB97D                db '        "yield": true,',0Ah
data:00000000007EB97D                db '        "max-threads-hint": 100,',0Ah
data:00000000007EB97D                db '        "asm": true,',0Ah
data:00000000007EB97D                db '        "argon2-impl": null,',0Ah
data:00000000007EB97D                db '        "astrobwt-max-size": 550,',0Ah
data:00000000007EB97D                db '        "cn/0": false,',0Ah
data:00000000007EB97D                db '        "cn-lite/0": false,',0Ah
data:00000000007EB97D                db '        "kawpow": false',0Ah
data:00000000007EB97D                db '    },',0Ah
data:00000000007EB97D                db '    "donate-level": 0,',0Ah
data:00000000007EB97D                db '    "donate-over-proxy": 0,',0Ah
data:00000000007EB97D                db '    "log-file": null,',0Ah
data:00000000007EB97D                db '    "pools": [ { "url": "194.38.23.2:8080" } ],',0Ah
data:00000000007EB97D                db '    "retries": 5,',0Ah
data:00000000007EB97D                db '    "retry-pause": 5,',0Ah
data:00000000007EB97D                db '    "syslog": false,',0Ah
```

Figure 5-3Mining pool proxy address

6 Sysrv-hello Mining Worm Iteration

6.1 Iterative Update of Core Scripts

6.1.1 Core Script Introduction

Sysry-hello is a mining worm that runs on both Windows and Linux platforms. The worm body is mainly executed through core scripts, so there are two types of script files, PowerShell scripts and shell scripts. Based on the characteristics of the mining worm's series of activities, the process of spreading Sysrv-hello mining worm can be divided into three stages: the early stage is mainly spread, the middle stage is to expand the spread, and the late stage is to focus on avoiding and maintaining the spread ability.

6.1.2 File Name Changes

The Sysrv-hello mining worm and the master name in the download link of the master sample remain basically unchanged. The master name of the core script remains consistent. The Windows platform is "ldr.ps1", the Linux platform is "ldr.sh", and the master name of the master sample is mainly sysrv and sysrvv. However, the file name of the target system where the master file implements shows the characteristics of the continuous iteration of the mining worm, mainly sysrv, sysrv001-sysrv013, and 6-12 random strings, which are reflected in the code written by the core script to implant the master sample into the target system.

Table 6-1File name changes

Stages	System Type	State	Core Script File Name	master File Name	Mining Program File name
Early stage	Windows	Before implementation	ldr.ps1	sysrv.exe	xmr32.exe xmr64.exe
		After implementation	none	sysrv.exe	network01.exe
	Linux	Before implementation	ldr.sh	sysrv sysrvv	xmr32 xmr64
		After implementation	none	sysrv sysrvv sysrv00[1-2]	network01 network001
Middle stage	Windows	Before implementation	ldr.ps1	unknown	none
		After implementation	none	sysrv00[3-13]	network00[0-1]
	Linux	Before implementation	none	sysrv sysrvv	xmr32
		After implementation	ldr.sh	sysrv00[3-13]	sysrv010
Late stage	Windows	Before implementation	ldr.ps1	sys.exe	none
		After implementation	none	6-12 random character string (lowercase letters and numbers) .exe	network01
	Linux	Before implementation	none	unknown	none
		After implementation	ldr.sh	6-12 random character string (lowercase letters and numbers) .exe	unknown

6.1.3 Core Script Function Iteration

The iterative changes in the core script functions fully reflect the characteristics of the development stage of the Sysrv-hello mining worm.

Table 6-2Core script function iteration

Stage	Script Type	Function

Early stage	PowerShell	Terminate the old version of the worm matrix and mining program, install the corresponding mining program according to the system bit number, download and execute the worm matrix
	Shell	Encapsulate the functions of downloading and ending processes, download and execute mining and worms, create scheduled tasks related to worms, uninstall cloud host security components and services, and end other mining processes (open source, docker, etc.)
Middle stage	PowerShell	Terminate the old version of the worm matrix and mining program, install the corresponding mining program according to the system bit number, download and execute the worm matrix
	Shell	Encapsulate the download function, end the mining process, download and execute the worm master
Late stage	PowerShell	Disable all firewall configuration files, download and execute the worm matrix, create a new WMI object and store the carrier, scheduled tasks, and registry startup items to achieve the persistence of the worm matrix
	Shell	Download function encapsulation, terminate own malicious processes and other malicious processes, clear logs, modify related command file names, uninstall cloud host security components and services, and clear open source mining pool domain names in hosts files Utilize the SSH private key obtained from the victim host to achieve lateral spread

6.1.4 C2 Address Change

The following are the changes in the implemented file names of the master samples involved in the core script and the corresponding C2 addresses. The Sysrv-hello mining worm uses a rich infrastructure and frequently deploys samples.

Table 6-3C2 address changes

Date	Changes in the file name of the master sample implemented	C2
December 2020 - February 2021	sysrv sysrvv	185.239.242.71 195.58.39.46
February 2021 - June 2021	sysrv001	45.145.185.85
	sysrv002	45.145.185.85
	sysrv003	185.239.242.70
	sysrv004	31.210.20.120
	sysrv005	31.42.177.123
	sysrv006	194.40.243.98 185.239.242.70
	sysrv007	194.40.243.98
	sysrv008	31.210.20.181

		185.239.242.70
	sysrv009	unknown
	sysrv010	194.145.227.21
	sysrv011	194.145.227.21
	sysrv012	unknown
	sysrv013	194.145.227.21
July 2021 - Present	Random string	194.145.227.21

6.2 Iterative Update of Master Sample

6.2.1 Master Sample Introduction

The Sysrv -hello master file is a mining worm for Windows and Linux written in GO language. The samples dropped are all packed with UPX, and the UPX versions used are inconsistent. The master file has attack and detection behaviors such as port scanning, brute force cracking, and vulnerability exploitation. After success, it implants commands to download and execute core scripts, and uses core scripts to download and execute master files to achieve self-propagation. At the same time, the master file also has the function of installing mining programs.

6.2.2 Master Module Changes

The changes in module functions reflect the attacker's intentions. The early boundary device detection module is encapsulated in the mid- and late-stage basic functions, and the hello string in the module is modified to shell in the later stage. It is not ruled out that this is a simple evasion after a large number of manufacturers disclosed their activities.

Table 6-4Master module changes

Modules	The beginning name of the previous module	Mid-term module title	The beginning name of the later module
Basic function encapsulation	hello_src_nu	hello_src_nu	shell_nu
Linux network edge device detection module	hello_src_gateway	This independent module is cancelled	This independent module is cancelled
Port scanning Mmodule	hello_src_scan	hello_src_scan	shell_scanner
Exploit module	hello_src_exp	hello_src_exp	shell_exploit
Mining program deployment module	hello_src_work hello_controller_xmrig	This independent module is cancelled	shell_miner

6.2.3 Vulnerability Module Changes

Table 6-5Vulnerability module changes

Stage	Exploit component name	Number of exploits	Event
Early stage	Plain text representation	3 -6	Sysrv-hello New mining method emerges [2]
Middle stage	Plain text representation	6-14	The Sysrv-hello mining worm continues to spread and persists [3]
Late stage	6-8 represents a string like "c 41954 "	18- 2 0	New vulnerability in [4]

6.2.4 Mining Module Changes

Table 6-6Mining module changes

sStage	Delivery method	Mining pool address	Wallet address	Income
Early stage	Released via master (stored in gzip format)	pool.minexmr.com:5555 xmr.f2pool.com:13531	49dnvYkWkZNPrDj3KF8fR1BHLBfiVArU6Hu61N9gtrZWgbRptntwht5JUrXX1ZeofwPwC6fXNxPZfGjNEChXttwWE3WGURa	unknown
Middle stage	Download via core script	xmr-eu1.nanopool.org:14444 f2pool.com:13531 minexmr.com:5555		During March 2021, an average of one Monero was mined every two days
Late stage	Released via the master (master executable file storage)	194.145.227.21:5443		unknown

7 Association Analysis

7.1 The Phenomenon of "Black Eating Black"

A suspicious core script was found in the captured samples. Its functions and code style are inconsistent with those of the Sysrv-hell o mining worm core script. The most prominent feature is that it has the function of writing the SSH public key in the target system, and the URL splicing method for downloading the mining worm master file is different.

Figure 7-1Analysis of abnormal core script

The functions and codes of the downloaded master file are consistent with those of the master sample of the Sysrv-hello mining worm, but a wallet address is hard-coded, which has never appeared in the master sample of the Sysrv-hello mining worm iteration.

Figure 7-2Hardcoded wallet address

The IP address in the master file download link is also hard-coded in the master file.

Figure 7-3Hardcoded C2 address

The IP addresses, wallet addresses, and SSH public keys involved, they all point to the Clean fda mining trojan. Antiy CERT speculates that this phenomenon may be that the attacker of the Cleanfda mining trojan captured a version of the Sysrv-hello mining worm master body (this version has 7 vulnerability exploit components), and then replaced the C2 address and wallet address in it , stored it in its own server, and wrote the corresponding core script to hijack the propagation capability.

7.2 EternalBlue Vulnerability Propagation

In a captured late-stage sample, it was found that it had the EternalBlue vulnerability exploit component, which was capable of releasing related exploit components and spreading the Sysrv-hello mining worm. However, the vulnerability exploit module was not retained continuously, which should be an attempt made by the attacker. At the same time, it is not ruled out that other vulnerability exploit modules appeared in the historical propagation stage and were eliminated in the later stage.

shell_exploit_eternalblue_init_0	.text	00673C70	000004B8	0000015C
shell_exploit_eternalblue_Run	.text	00674130	0000020C	0000004C
shell_exploit_eternalblue_bindataFileInfo_Name	**.text**	**00674340**	**0000002A**	**00000000**
shell_exploit_eternalblue_bindataFileInfo_Size	**.text**	**00674370**	**0000002A**	**00000000**
shell_exploit_eternalblue_bindataFileInfo_Mode	**.text**	**006743A0**	**00000022**	**00000000**
shell_exploit_eternalblue_bindataFileInfo_ModTime	**.text**	**006743D0**	**00000032**	**00000000**
shell_exploit_eternalblue_bindataFileInfo_IsDir	**.text**	**00674410**	**0000002A**	**00000000**
shell_exploit_eternalblue_bindataFileInfo_Sys	**.text**	**00674440**	**0000002A**	**00000000**
shell_exploit_eternalblue_eternalblueDoublepulsar131Exe	.text	00674470	000001D9	000000C4
shell_exploit_eternalblue_eternalblueDoublepulsar131Xml	.text	00674650	000001D9	000000C4
shell_exploit_eternalblue_eternalblueEternalblue220Exe	.text	00674830	000001D9	000000C4
shell_exploit_eternalblue_eternalblueEternalblue220Xml	.text	00674A10	000001D9	000000C4
shell_exploit_eternalblue_eternalblueCnli1Dll	.text	00674BF0	000001D9	000000C4
shell_exploit_eternalblue_eternalblueColi0Dll	.text	00674DD0	000001D9	000000C4
shell_exploit_eternalblue_eternalblueCrli0Dll	.text	00674FB0	000001D9	000000C4
shell_exploit_eternalblue_eternalblueExma1Dll	.text	00675190	000001D9	000000C4
shell_exploit_eternalblue_eternalblueLibeay32Dll	.text	00675370	000001D9	000000C4
shell_exploit_eternalblue_eternalblueLibxml2Dll	.text	00675550	000001D9	000000C4
shell_exploit_eternalblue_eternalblueMs17010Dll	.text	00675730	000001D9	000000C4
shell_exploit_eternalblue_eternalbluePosh0Dll	.text	00675910	000001D9	000000C4
shell_exploit_eternalblue_eternalblueSsleay32Dll	.text	00675AF0	000001D9	000000C4
shell_exploit_eternalblue_eternalblueTibe2Dll	.text	00675CD0	000001D9	000000C4
shell_exploit_eternalblue_eternalblueTrch1Dll	.text	00675EB0	000001D9	000000C4
shell_exploit_eternalblue_eternalblueTrfo2Dll	.text	00676090	000001D9	000000C4
shell_exploit_eternalblue_eternalblueTucl1Dll	.text	00676270	000001D9	000000C4
shell_exploit_eternalblue_eternalblueUclDll	.text	00676450	000001D9	000000C4
shell_exploit_eternalblue_eternalblueXdvl0Dll	.text	00676630	000001D9	000000C4
shell_exploit_eternalblue_eternalblueZlib1Dll	.text	00676810	000001D9	000000C4
shell_exploit_eternalblue_Asset	.text	006769F0	00000255	00000054
shell_exploit_eternalblue_init	.text	00676C50	00001893	0000002C

Figure 7-4EternalBlue vulnerability exploit module

8 Self-Inspection and Disposal

8.1 Windows Platform

1. Check the system process list to see if there is a process with the process name containing the strings "network", "kthreadd", or "sysrv". If so , terminate the process.
2. Check the system process list to see if there is a process with a name containing a 6-12 random string like "ylket8pfrj5", " goj57n3", or "bp5ovz" . If so, terminate the process.
3. Check the system startup items and see if the corresponding payload file name contains a 6-12 random string such as "ylket8pfrj5", "sgoj57n3", or "bp5ovz". If it does, delete the startup item.
4. Check the system scheduled tasks to see if there is a scheduled task named "BrowserUpdate". The corresponding path of the payload is the temporary directory. If it exists, delete it.

8.2 Linux Platform

1. Check the system process list to see if there is a process with the process name containing the strings "network", "kthreadd", or "sysrv". If so , terminate the process.
2. Check the system process list to see if there is a process with a name containing a 6-12 random string similar to "5c46403e1d", "ce368c626", or "ce368c626". If so, terminate the process.
3. Check whether there is a download link in the scheduled task, and whether the downloaded file name is "ldr.sh" . If it exists, delete the corresponding scheduled task.

9 IoCs

URL
hxxp://185.239.242.71/ldr.ps1
hxxp://185.239.242.71/ldr.sh
hxxp://185.239.242.71/sysrv
hxxp://185.239.242.71/sysrv.exe
hxxp://185.239.242.71/xmr32

hxxp://185.239.242.71/xmr32.exe
hxxp://185.239.242.71/xmr64
hxxp://185.239.242.71/xmr64.exe
hxxp://194.145.227.21/ldr.ps1
hxxp://194.145.227.21/ldr.sh
hxxp://194.145.227.21/sys.exe
hxxp://194.145.227.21/sys.x86_64
hxxp://194.145.227.21/sysrv
hxxp://194.40.243.98/ldr.ps1
hxxp://194.40.243.98/ldr.sh
hxxp://195.58.39.46/asap
hxxp://31.210.20.120/ldr.sh
hxxp://31.210.20.120/sysrv.exe
hxxp://31.210.20.120/sysrvv
hxxp://31.210.20.181/ldr.sh
hxxp://31.42.177.123/sysrv.exe
hxxp://31.42.177.123/sysrvv
hxxp://45.145.185.85/sysrv.exe
hxxp://45.145.185.85/ldr.ps1
hxxp://45.145.185.85/ldr.sh
hxxp://45.145.185.85/sysrv
hxxp://45.145.185.85/sysrv.exe
hxxp://194.38.23.2/ldr.sh
hxxp://194.38.23.2/ldr.ps1
hxxp://194.38.23.2/sys.x86_64
hxxp://194.38.23.2/sys.exe
hxxp://finalshell.nl/ldr.ps1
hxxp://finalshell.nl/ldr.sh
hxxp://finalshell.nl/sysrv
hxxp://finalshell.nl/sysrv.exe

hxxp://finalshell.nl/sysrvv
Domain&IP
finalshell.nl
185[.]239.242.71
185[.]239.242.70
194[.]145.227.21
194[.]40.243.98
195[.]58.39.46
31[.]210.20.120
31[.]210.20.181
31[.]42.177.123
45[.]145.185.85
194[.]38.23.2
HASH
49CE7EFA66788D06CA73067C8BECA6AD
41E46A59C9B1F7F33C26C58FC6AD4A5A
71D473E09C8A0F3B61028409207B445B
AE6CAA7B2A81738F3287E202F0E132E1
005E88BA30B9A99B82237DB071EAEFC4
020AD95CF1AF6812CCF20395F59F4551
030231D96234F06AE09CA18D621241E5
074C9C0865F7E76EED921BAE2362CDA3
0964D7889A46C5339D813AA286506286
0B50031BC84FD33287E259CD45A86444
0CF1D07E1407F64B3F7347BA5C1BDC46
15417A0D16E8E7EFA70DF037502A76A0
16BCC0E077314DAB3595465F829DEB6A
16E46C567FE1F9A18CD8B1EB3DB34CDA
1CC8DFBCAB6D59734C39A8EAAE4998FA
1D59BA6A5EDC6E0A1B7C30E4250A1980

2170F4C7CE9B443E7A21AEAB52807864
219787F32DEFC4850F981A19472FB705
2B4039026364318CE24BA2B8D25C9590
2C5A971F9359145AE44ACBC7A0425B6C
2C8BAB7B072DDBCF3E5816C08CBE5C85
2E3655A405E6111B401295071CF7B77E
30135CFA92B3D220FD37F5F5ABEB25D9
3147300F1C143399586A9950C08C4BDE
3226C3F8D984CB50484270B48B97B8D4
333182A045996AE215729958A3ED9CFE
371AF7E3F03AEEC3C277FB4C677740D4
38D932661825E340321DFBC1B23533CA
3DDCC1CC534BDB10F275AB91EC894BF1
3FA0C08CB6D360636679FF8E899475C7
405DEE8A93FF734A9D9D2BB6C34186AD
409E3743B6557B291EE0D300FADC75AA
47F542E14CC8307842FD622BD4496E53
48E278EA6600C481C5E2B1D6CB4AEC34
4AA6AA8AACFF31D0C445699A6E0475D1
4B4825DF79233D71F441100353661CD0
4C6354A25EF95462D628D58C1C9FAEE4
4F468AF0409670F94DD56CBA1D928966
5160C9236515D14FDC9D1CB739CB5637
518038589BA147888834966B7F5B6FEF
575D17DE7D97DF2CC83AA9BCC30886BE
5C1DDF4E0A174DF5488036F95987E1EF
5CB91E6B2047C211C0CCADCF82DB21AD
6142CDCCB22D23365E056CAFBCD0CF18
620E54B0252D8179A7FF90967B643889
6296080A1920F1AAC69D25E481A69179

62B4AFD51D000573940373FA414709AB
6456B6E74D82EC4061F6AD6D91716549
64F7F910849BC479EC72A5E2167C8D78
6A5EB22BF8C26E577B0BAF1EA849419A
6B23697814EEED70305CE021E8A51420
6CD5CBB8906ED462589C3E64AD2167C5
6F9AF5410B1BC6DCBFA95D893B81B610
6FCF48E060381DF880A554B599BB9745
733BB2E49488E1DB42FCB7F9AFE4BD05
7383F545569C192BAB62FFBF1878EF73
7723B2EDAFAA03EB0FD455D16D56AEF3
7BEB93CC68BAC2EDEBB0C00587E13739
7C0503C53988A70E3396CD0E370B9673
7DA6B2F40E5DF2AD891668035DAF9225
7E2CD275287CED13A60D2234099A8933
85C1966C5E8EBE4FD6D05C66DC08EC97
8CF23C05302E864F96BF8CDB767D0896
96005F4E413D64AEDAAC96C65A03F352
9793A8AA5BA0DD57917F0B688456E0FE
979DD66DE1706D8057A4563CB1F740DD
9DC5150C2C77E04601D19C348205A4B2
A0086197C4F6BA51B3AE001A5AC0D803
A3B6ACA9E597D537295DD238858DEA92
A5FC20438D3C3419052CDC8CC0C9C696
A677D6AE9EEBDDAF77C7BB79A1D3FE72
A85ABA39B80BABB39742FC70479E4B50
ABB1F209477EEFE20973BFBCC27C1502
ABBB5CDB30FED6C66BAA5B44CEFD5509
AE440F9D4C32355E629DA5E55CD7486A
B31E6A543DF2C35BD9BF13C64926C327

BCBBC1971A02BDF94DE80393BD210050
BEFA8B0959809739A6A52BDF9836C8E4
BFDCC3B52E922BE3F75438B55CC5DD66
C078480C07BC0CBB4EF0DC18153CFDDA
CDB4C9AEE6A6EE93C74719CAF4F625B0
CE79447838D0DED28AE581C7F6F56462
CF17D8EA5DC01B4113250D6CCC0CCE2F
D248F62E119BFAF28A6FC12B36A1ABD5
D94E86612B89937B48E0BB85662A6A05
E372D1BA2D3A1936E3E8CDD3FEBF2038
E483BE649DA26F42C803243F0298F932
E4AF0439AA88C51F30647F2030ED1C20
EAD2CF8AB7AEF63706B40EB57D668D0A
F8D82FDF0586F5FA06584A975C5C6E88
FB355C542AF790354B17DDF02FCE4BE4
FC11FDD4B52483DDB20FEEB1EABEE33F
111EE1FA1853410E0CA002EBA4CBCFFD
3C25CB65E744F91D93BF71FC06F53857
479BD3AA6C1D5FDDFA9D4B3C4C2065AE
4B8952FE02D24406345B9C14AE4F1DD3
504B58088D1B3825674ED0F1AAEB351B
5418228A5E30F29FD6EEB30B09D7091F
5559FD6EF2B16070F088EF10B3738C5E
569C12CBFF70390E37914FC5CDE55113
5A519FB9402D43D90DF87E2FB2852CAC
5C81C90D4835A7DAD311361B999B63B5
639A2B53FDF40CB6A6E71ABCE42B497E
6FE4F2943DB66635F3C5DF328EDA9BF9
704C4EDA20B50CD919CECE80AE93BE57
73EA4CDD66B3466FC49335ED7CA7B866

8F48691B73C67F14BB378D9F97F4B5AA
9C6B60A3AEE65283DD40B4029EA99A3C
9E7FE24680C0C240EC065CDB98C5C892
A27A0C969FDB36469D17A0D5CAA40C57
AE8A20AA2EA6E32CC6D8693F64794A49
BC2530A3B8DC90ACA460A737A28CF54B
D07414166885E6765803C8ECD0E01B6A
D708A5394E9448AB38201264DF423C0A
D8081ACB7AB5B9E6E19EF666FE540245
DF209F93FCACC5BD2990953ACE28C422
F97885CADAD139D9A22C01E5A87039FC
FADC7D3ECCC2CCA29C3B8F1BD16FFE5D
FCB24F8DB0FFCCD7B70A268708767722

Appendix 1: References

[1]. Notice of the National Development and Reform Commission and other departments on regulating virtual currency "mining" activities

http://www.gov.cn/zhengce/zhengceku/2021-09/25/content_5639225.htm

[2]. Sysrv-hello New mining method emerges

https://developer.aliyun.com/article/780758?spm=a2c6h.14164896.0.0.7e0f3d89eoiqz7

[3]. Sysrv Botnet Expands and Gains Persistence

https://blogs.juniper.net/en-us/threat-research/sysrv-botnet-expands-and-gains-persistence

[4]. Dual-platform mining botnet Sysrv-hello attacks again with new vulnerability

https://www.anquanke.com/post/id/271672

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.