Antiy IEP for Linux Effectively Defends Against Sorry Ransomware

This report is a machine-translated version.

1. Overview

On August 10, 2026, the National Computer Virus Emergency Response Center, in collaboration with the National Engineering Laboratory for Computer Virus Prevention and Control Technology, released Early Warning Report on "Sorry" Ransomware, disclosing multiple attacks involving Sorry ransomware detected within China. This malicious code is a new ransomware family that emerged in 2026, written in Go, and primarily targets publicly exposed Linux web servers.

The attack process typically involves exploiting a authorization flaw in WebPros cPanel (CNNVD-202604-5641/CVE-2026-41940) to gain root administrative privileges on the server, deploying ransomware and launching the attack without the victim's knowledge. This vulnerability affects all versions of cPanel from version 11.42 (released March 4, 2014) to the patched version on May 1, 2026. Attackers weaponized the vulnerability and launched it in a large-scale attack within 48 hours of its public disclosure. This ransomware possesses dual ransomware characteristics of "data theft + file encryption". **Antiy CERT , relying on the Antiy AVL Code Agent and based on Antiy LanDi VILLM, conducts sample analysis, completes malicious code parsing, and outputs a special analysis report.**

Verification has shown that Antiy Intelligent Endpoint Protection System （IEP） for Linux can effectively detect and remove this ransomware and provide robust protection for user terminals.

2. Technical Analysis

Sorry ransomware first appeared in March 2026, with two waves of attacks peaking in mid-April. **Since its initial outbreak, this malware has rapidly grown into a**

leading high-risk ransomware family in China. In May 2026, its Linux version was confirmed to have spread on a large scale by exploiting the cPanel vulnerability (CVE-2026-41940).

Table 1 Steps Taken by the Attacker to Carry Out the Attack

Stage	Behavior Description
Initial Access	By exploiting the cPanel authorization bypass vulnerability (CVE-2026-41940) to gain server administrative privileges; deploys and runs without the victim's knowledge, disguising itself as a common sshd process to evade detection.
Information Gathering	Generate a unique victim identifier (including username, hostname, number of CPUs, operating system information, active network interfaces, etc.) and send the relevant information back to the attacker.
Defense Evasion	Terminate services related to databases, security protection, and backups
Data Theft	Bulk theft of business data, configuration files and various internal files
Data Encryption	User files are encrypted using the AES algorithm, and the AES decryption key is double-encrypted using the RSA algorithm.
Lateral Movement	Scan SSH ports 22, 2222, and 22222, and attempts lateral movement to other Linux hosts by exploiting weak passwords.

2.1 Sample Analysis

The Sorry ransomware family sample is a Linux ransomware written in Go, featuring a complete ransomware attack chain: stopping the database/SSH service → generating an RSA+AES encryption scheme → traversing and encrypting files from the root directory → writing a ransom note → reporting victim information via C2.

Table 2 Sample Labels

Virus Name	Trojan/Linux.Sorry[Ransom]
MD5	01896FBB58E8EDEFC5A8392E467C2260
File Size	5.08MB (5,329,044 bytes)
File fFormat	ELF
Target Platform	Linux
Compiled Languages	Go
VT First Upload Time	2026-04-30 16:42:14
Encryption Extensions	.sorry、.sorry_exist

Ransom Note	README.md
Victim ID	sorry_id_%v%v、/tmp/.sorry_
Contact Information	TOX

The program has two modes: encryption (enc) and decryption (dec). It parses command-line parameters and supports specifying the encryption/decryption directory in enc/dec mode.

Figure 2-1 Command-Line Parameter Mode Execution

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

Calling syscall.Flock locks the file to prevent encryption conflicts caused by multiple processes running simultaneously.

Figure 2-2 Create a File Lock

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

Before encryption, stop the database service to ensure that the database file is not occupied and can be fully encrypted.

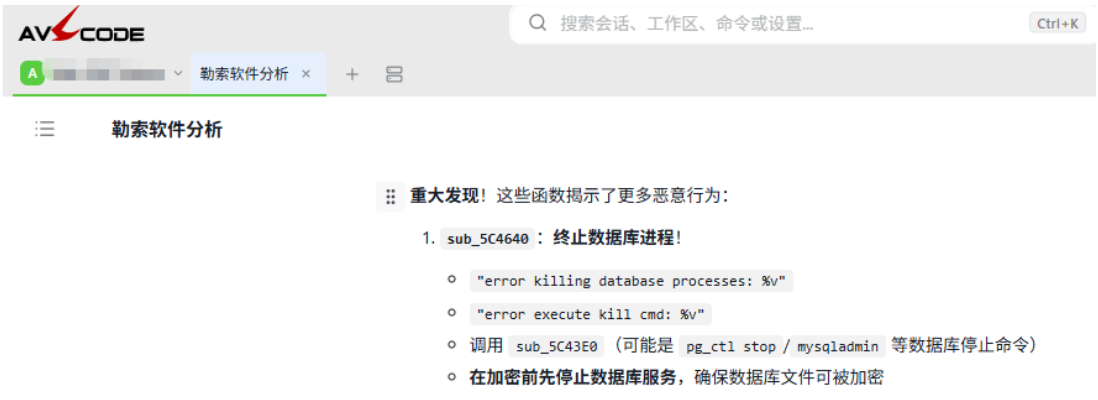

Figure 2-3 Stop a Specific Database Service

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

Table 3 Stop Specific Database

Database	Stop Command (String)
MySQL	service mysql stop, service mysqld stop, systemctl stop mysql, /etc/init.d/mysqld stop, systemctl disable "mysql*"
PostgreSQL	service postgresql stop, systemctl stop postgresql, systemctl disable "postgresql*"

Execute four SSH stop commands (adapted to different distributions) using `/bin/bash//bin/sh -c` to cut off the remote management channel and prevent administrators from intervening during encryption.

Figure 2-4 Prevent Interference with Encryption

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

Generate an RSA key pair (the attacker retains the private key), generate a unique Sorry-ID for the victim (16-byte random → 32-bit hex), and write the ~/.sorry_exist

flag to the user's home directory (to prevent repeated infection: exit if it already exists).

Figure 2-5 Partial Encryption Features

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

Construct a ransomware configuration structure, including:

• Encryption extensions: .sorry

• Ransom note filename: README.md

• Hard-code the attacker's RSA public key: 3D7889AEC00F... (used to encrypt the symmetric key, which the victim cannot decrypt).

Figure 2-6 Encryption Features

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

File traversal and encryption functions:

• Recursively traverse from the root directory (filepath.Walk, walkfail:%v/skipeverythingandstopthewalk)

• 30 goroutines concurrent encryption

• Skip system files (thumbs.db, desktop.ini, autorun.inf, etc.) to avoid damaging the system.

• Perform actual encryption via function pointer 0x5c3d20 (encryption)

Figure 2-7 Partial Encryption Functions

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

For the encryption algorithm, a hybrid encryption method is used: AES (CBC/CTR/GCM) is used to encrypt the file data, and RSA is used to encrypt the AES key. `GetPrivateKeyEncrypted` indicates that the symmetric key is encrypted with the RSA public key, the attacker holds the private key, and the victim cannot decrypt it themselves.

Figure 2-8 Encryption Algorithm

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

Generate ransom note content, collect system usernames and network interface IP addresses, fill them into the ransom note, write it into README.md, and test network connectivity.

Figure 2-9 Ransom Note and Connectivity Test

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

In the C2 communication section, the C2 server address 68.183.190.253:80 is hardcoded, and victim information (username|hostname|...) is concatenated and sent to C2.

Figure 2-10 C2 Communication

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

After Sorry ransomware main program starts, it parses the runtime parameters, adds a single-instance runtime lock, and shuts down the database and SSH service. It generates an RSA key pair and a device-specific Sorry-ID, and writes them to the infection marker file. The program uses 30 lightweight coroutines to concurrently execute a full-disk directory recursive traversal task. This multi-task synchronous

scanning significantly reduces the full-disk processing time. During execution, it automatically skips system-protected directories. For ordinary business files, it employs a dual encryption scheme: AES encryption of file content and RSA protection of session keys. After encryption, it appends the ".sorry" suffix to the file. After full encryption, it stores the ransom note file, reports the victim host information to the C2 server, and continuously probes the C2 network connectivity. The overall process sequence diagram is shown below.

Figure 2-11 Overall Process Sequence Diagram

(Analysis and generation by Antiy AVL Code Agent based on Antiy LanDi VILLM)

3. Mitigation Recommendations

In response to this ransomware, Antiy recommends that individuals and businesses take the following protective measures:

3.1 Individual Protective Measures

1. **Strengthen endpoint protection: Install antivirus software. Antiy IEP users are advised to enable the ransomware defense module (enabled by default);**

2. Strengthen 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. Also, avoid using the same password for multiple servers;

3. Timely patch updates: It is recommended to enable automatic updates and install system patches. The server should be updated with system patches in a timely manner;

4. Close high-risk ports: Close unused high-risk ports such as 3389, 445, 139, and 135;

5. Disable PowerShell: If you do not use the PowerShell command-line tool, it is recommended to disable it;

6. Regular data backup: Regularly back up important files, and the backup data should be isolated from the host computer.

3.2 Enterprise Protective Measures

1. **Enable logging: Enable critical log collection functions (security log, system log, PowerShell log, IIS log, error log, access log, transmission log, and cookie log) to provide a foundation for tracing and attributing security incidents;**

2. Configure IP whitelist rules: Configure Windows Firewall with Advanced Security, set inbound rules for remote desktop connections, add the IP address or range of IP addresses used to the rules to prevent brute-force attacks from IPs outside the rules;

3. Host hardening: Perform penetration testing and security hardening on the system;

4. Deploy an Intrusion Detection System (IDS): Deploy traffic monitoring software or devices to facilitate timely detection and tracing of ransomware. It is recommended to deploy Antiy Persistent Threat Detection System (PTD) , which analyzes network traffic and can accurately detect a massive amount of known malicious code and network attack activities, effectively identifying suspicious network behavior, assets, and various unknown threats;

5. Disaster Recovery Plan: Establish a security disaster recovery plan to ensure that backup business systems can be quickly activated;

6. Antiy Service: If you are attacked by ransomware, we recommend disconnecting from the internet immediately and securing the scene while a security engineer inspects your computer. Antiy 24/7 service hotline: 400-840-9234.

Antiy Endpoint Detection and Response System (EDR) is an endpoint security protection product for devices such as office computers, servers, and virtualized hosts. Relying on Antiy's self-developed AVL SDK threat detection engine and massive threat intelligence, IEP EDR creates a comprehensive and integrated endpoint security depth protection system that is "manageable", "aware", "protectable", and "responsive" across all scenarios through multiple capabilities such as asset management, threat detection and analysis, ransomware-specific protection, host control, software management, and distributed firewall.

Currently, Antiy Intelligent Endpoint Protection System (IEP) for Linux can effectively detect and remove this ransomware. It has also been tested with the domestic Tongxin operating system and Kylin operating system, both of which provide effective protection.

Figure 3-1 Antiy IEP Blocks Encryption Activities

4. IoC

IoCs
01896fbb58e8edefc5a8392e467c2260
68.183.190.253:80

References

Early Warning Report on "Sorry" Ransomware

https://mp.weixin.qq.com/s/YP3Qp2fbhnkKzfk5MYHzfw