Synology C3RB3R Data Recovery: How to Recover .L0CK3D Files Without Paying

TechRounder PDF Edition

Live article: https://www.techrounder.com/how-to/synology-c3rb3r-data-recovery/

By Vipin PG | Published November 5, 2026 | Updated November 5, 2026 | Format: Guide | 19 min read

Quick answer

If the files on your Synology NAS suddenly have a .L0CK3D extension and you find a ransom note called read-me3.txt, your NAS may have been hit by C3RB3R ransomware. The attackers encrypt stored files and demand payment for a decryptor, leaving owners searching for ways to get their data back.

If the files on your Synology NAS suddenly have a ‘.L0CK3D‘ extension and you find a ransom note called ‘read-me3.txt‘, your NAS may have been hit by C3RB3R ransomware. The attackers encrypt stored files and demand payment for a decryptor, leaving owners searching for ways to get their data back.

There are some recovery options that do not involve paying. Researchers and affected users have reported recovering files by extracting encryption keys from a running ransomware process, restoring older Btrfs data blocks, and using existing snapshots. The results vary considerably. A NAS that is still running may offer recovery opportunities that disappear after a restart.

The situation is especially difficult on an EXT4 volume when the NAS has already been rebooted and no backup exists. There is no verified method that can fully recover every file in that situation.

The steps below explain how to assess an infected NAS, preserve the data that remains, and decide which recovery techniques are worth investigating. They also cover what researchers have learned about C3RB3R’s encryption and the DSM vulnerabilities reported during the October 2026 attacks.

Before doing anything: do not restart an infected NAS that is still running.

The ransomware process may still contain usable encryption keys in memory. Restarting, shutting down, upgrading DSM, or terminating that process can remove the chance to recover them. Isolate the NAS from untrusted networks and preserve its current state before attempting repairs.

What happened in the Synology C3RB3R ransomware attacks?

C3RB3R is part of the Cerber ransomware family. During October 2026, attackers targeted internet-accessible Synology NAS devices, encrypted files stored on them, and demanded a ransom for a tool called C3rb3r Decryptor.

Synology issued a warning on October 29, 2026, urging customers to update outdated DiskStation Manager (DSM) installations. The campaign received wider attention after BleepingComputer reported the attacks on November 2.

Three signs appear repeatedly in victim reports:

- Files have been renamed with the extension ‘.L0CK3D‘ . The character after L is the number zero.
- A ransom note named ‘read-me3.txt‘ appears in affected locations.
- The note refers to a paid decryption utility and directs victims to the attackers’ payment system.

Image: Figure 1: Example of a folder affected by C3RB3R

Finding these filenames is a strong indication of an infection, but it does not tell you how much of each file was encrypted. Some C3RB3R samples encrypt entire files while others modify selected regions. This affects what can be recovered when the decryption key is unavailable.

What to do immediately after finding .L0CK3D files

It is natural to try restarting the NAS when files stop opening or DSM behaves unexpectedly. In this case, restarting can make recovery harder. The safest first actions are aimed at stopping further access while preserving the current system state.

1. Isolate the NAS without shutting it down

Disconnect the device from untrusted networks so attackers cannot continue accessing it and other devices cannot write to its shared folders.

You can isolate the NAS through router or switch rules, remove external port forwarding, or physically disconnect its network connection. If you need local access for evidence collection, use a controlled connection.

Check IPv6 exposure as well as IPv4. A NAS can remain reachable through IPv6 even after IPv4 port forwarding has been removed. VPN access, reverse proxies, and externally published applications also need attention.

2. Preserve the ransomware process if it is still active

The community project soimy/c3rb3r-rescue documents cases where investigators recovered encryption material from the memory of a running C3RB3R process.

Some reported processes used names such as ‘libgld‘, although malware filenames can vary. A matching name alone is not enough to identify a process safely.

Investigators may suspend a confirmed malicious process and collect a memory dump before continuing recovery. Avoid killing processes or running unfamiliar commands without first understanding their effects. On a NAS containing irreplaceable data, this work is better handled by an experienced incident responder.

3. Keep the encrypted files and ransom note

Do not delete the ‘.L0CK3D‘ files simply because they no longer open. They may still be needed if a working key is recovered or a compatible recovery technique becomes available.

Preserve the ransom note, DSM logs, suspicious files, and information about when the attack began. Keep copies of any unaffected originals found on other devices.

If you plan to investigate the disks directly, arrange a forensic image of the storage first. Copying visible files through File Station does not preserve deleted data or old filesystem blocks that might be useful for recovery.

4. Avoid repair and storage maintenance operations

Do not initialize the storage pool, rebuild the RAID array, format disks, or run aggressive filesystem repair tools. Avoid Btrfs balance and defragmentation operations, TRIM or discard, and other unnecessary writes.

These actions can remove data that recovery tools might otherwise find. Record the position of every drive before removing disks from a multi-bay NAS.

5. Identify the filesystem and backup situation

Once the system is safe to inspect, determine whether the affected volume uses Btrfs or EXT4. Also check whether you have snapshots, Hyper Backup archives, an external disk backup, or another copy of the files.

If DSM is accessible and inspection will not interfere with evidence preservation, the filesystem can generally be checked in Storage Manager under the volume's details. The exact location depends on the DSM release.

Which recovery method should you try?

The state of the NAS is more useful than its model number when choosing a recovery method. First establish whether the encryption process may still be running. Then check for backups and identify the filesystem.

Image: Figure 2: Choosing a C3RB3R recovery method

NAS condition: Encryptor still running | Recovery approach: Memory-based key recovery | Limitation: Usable key material must remain available

NAS condition: Rebooted, Btrfs | Recovery approach: Snapshots or older CoW extents | Limitation: Old blocks may have been released or reused

NAS condition: Rebooted, EXT4 | Recovery approach: Original copies, forensic remnants, partial file salvage | Limitation: No verified general method for complete recovery

NAS condition: Clean backup available | Recovery approach: Restore to a trusted system | Limitation: Backup must predate the attack and be intact

NAS condition: Only fully encrypted data remains | Recovery approach: Usable encryption keys or a compatible decryptor | Limitation: No universal public C3RB3R decryptor is verified

Method 1: Recover encryption keys from the NAS memory

Memory-based recovery has produced some of the strongest reported results from this campaign. It requires a narrow set of conditions, particularly that the original ransomware process is still present and its memory can be preserved.

While ransomware encrypts files, it must use cryptographic material to perform the operation. Some of that material may remain in the process memory long enough for investigators to collect it.

The c3rb3r-rescue repository describes identifying the encryptor, preserving its state, collecting memory and testing recovered keys against encrypted file copies.

Image: Figure 3: How memory-based recovery works

How to investigate this recovery method

1. Keep the infected NAS isolated and powered on.
2. Have the suspected encryption process positively identified. Do not rely on a filename alone.
3. Preserve the process state and collect memory using a suitable forensic procedure.
4. Follow the recovery project's documentation to analyze the captured memory.
5. Test any recovered key material using copies of affected files.
6. Compare recovered files with known originals or trusted checksums where available.

The repository reports a recovery involving approximately 49 GiB of GitLab backup data from a Proxmox guest. The recovered backup matched a historical digest and was used to restore 80 projects in an isolated environment.

Another documented test involved a physical Synology DS920+. Investigators recovered two files that matched their originals byte for byte, along with a readable PDF. These tests support the feasibility of memory recovery on physical Synology hardware as well as virtual machines.

There are limits. A process may have exited before the infection was discovered, memory may have been overwritten, or the available material may not be enough to decrypt the affected files. The project also records unsuccessful searches for keys after the encryptor had stopped.

Method 2: Recover files from Btrfs without a decryption key

Btrfs may preserve older copies of modified data blocks through its Copy-on-Write (CoW) behavior. When an application changes a file, Btrfs can write modified data to new locations instead of overwriting the old blocks immediately.

During a ransomware attack, that behavior can leave some of the original data behind. Recovery software may be able to locate those older extents and rebuild files from them.

The method is useful even after a reboot because it relies on disk contents rather than the original ransomware process's memory. However, old blocks do not remain available indefinitely, and Btrfs recovery can be affected by NoCOW settings, snapshots and later storage writes.

Image: Figure 4: Why Btrfs can leave recoverable original data

Using a Btrfs recovery project

The open-source crt106/c3rb3r-btrfs-recovery project documents recovering files from surviving Btrfs data blocks without obtaining the ransomware's encryption key.

The author reports recovering 35,445 files totaling about 229.9 GB on a Synology system running DSM 7.2.1 with SHR storage. The case study includes SHA-based comparisons and Btrfs checksum validation.

The same documentation describes recovering another approximately 6,100 files totaling 346 GB from a NoCOW-related scenario involving earlier snapshot history.

These numbers come from the project's published tests. They describe specific storage conditions and should not be used to predict how much data another NAS owner will recover.

Steps to assess Btrfs recovery

1. Preserve the original storage pool or create forensic images before testing anything.
2. Confirm the volume uses Btrfs and check the project's supported configurations.
3. Look for existing snapshots first. They may offer a simpler restoration path.
4. Review the project's read-only scanning procedures and storage requirements.
5. Save any recovered data to separate storage, never back to the affected volume.
6. Test recovered files and verify their contents using checksums or known originals where possible.

A separate project, hjs785053766/c3rb3r-btrfs-recovery, reports an overall recovery of about 65% excluding thumbnails in one case. Its results varied considerably between file categories.

Another community case discussed in the recovery research reported recovering 17,893 of 24,142 files, approximately 74%. That result was primarily validated at file-format level rather than through complete comparisons with original files.

A file that opens successfully may still contain missing or damaged content. Keep such files separate from those that have been verified against trusted originals.

Method 3: Restore files from Synology snapshots and backups

Before trying filesystem reconstruction, check whether a clean copy of the data already exists. A snapshot captured before the attack can restore the original files without decrypting the ransomware's modified copies.

Synology Snapshot Replication supports snapshots on compatible Btrfs shared folders. Hyper Backup and independent external backups may also contain older versions of the files.

How to check for usable snapshots

1. Preserve evidence from the compromised NAS before attempting restoration.
2. Access Snapshot Replication in a trusted or appropriately isolated DSM environment.
3. Check the affected shared folders for recovery points dated before encryption began.
4. Choose a snapshot that predates the attack.
5. Restore a small sample to a separate location if the available recovery procedure supports it.
6. Verify the files and restore the remaining data to a clean environment.

Exact options vary by DSM version, NAS model and snapshot configuration. Refer to Synology's official knowledge base for the recovery procedure supported by your device.

In one reported DS1621+ case, snapshots protected four of twelve shared folders. The user restored those four folders, while the remaining data required other recovery methods.

That case illustrates a common limitation: a NAS can have Snapshot Replication installed without every important shared folder being covered.

Also check older computers, cloud backups and external drives. If the ransomware compromised credentials or backup destinations, verify that the copies are clean before restoring them.

Method 4: Recovery on EXT4 after the NAS has been rebooted

EXT4 presents a different problem. It generally writes modified file data in place, although the exact behavior depends on the application and storage configuration. When encryption overwrites the original blocks, the original content may no longer exist on the volume.

After a reboot, the original ransomware process's volatile memory is also normally gone. Without a backup or another copy of the original data, complete recovery can be extremely difficult.

The Synology DS420j case

A GitHub discussion opened in early November 2026 describes a DS420j owner facing exactly this problem.

The NAS had four 4 TB disks and approximately 5.2 TB of stored data, much of it family photos and videos. It used EXT4 with a redundant disk arrangement described as RAID 5 or SHR, although the exact configuration was not confirmed.

The owner discovered the infection, restarted the NAS and upgraded DSM before learning about memory-based recovery. No snapshots or backups were available.

The user had not formatted the disks or rebuilt the array and planned to make complete sector-by-sector images before further investigation.

At the time of the discussion, the project maintainer knew of no successful full recovery method for that exact situation: EXT4, already rebooted, and no backups or snapshots.

What can still be recovered?

There are a few possibilities worth checking, especially if the data is irreplaceable.

- Other copies of the files: Look in computer libraries, phone storage, photo synchronization folders, cloud accounts, exported albums and external drives.
- Deleted data remnants: A forensic examination may locate original blocks or deleted copies that the ransomware did not overwrite.
- Unencrypted sections: Some larger files may retain readable data if the ransomware used partial encryption.
- Original and encrypted sample pairs: If an original is found elsewhere, preserve it alongside the encrypted version. Such pairs help investigators test recovery techniques.

Conventional file-recovery applications such as PhotoRec can sometimes locate surviving data, but they cannot reverse encryption. If original file bytes have genuinely been overwritten with ciphertext, carving software cannot recreate them from nothing.

For this type of EXT4 case, preserving the original disks is more useful than repeatedly running recovery software against the live storage pool.

How C3RB3R encrypts files and why recovery results differ

Technical analysis of the Synology-targeting samples provides some insight into why one victim may recover most files while another gets very little back.

Qihoo 360’s ransomware analysis describes ChaCha8 file encryption, with key material protected through RSA-2048. Its report also describes a set of 187 priority file extensions that receive full encryption.

Community researchers have identified three encryption modes in observed files. The mode affects how much original content remains available for recovery without a key.

Mode: ‘0x24‘ | Observed encryption: Entire file encrypted | Recovery implication: Keyless carving cannot retrieve intact content from the encrypted copy

Mode: ‘0x26‘ | Observed encryption: First 1 MiB encrypted in reported samples | Recovery implication: Later data may remain, but file headers can be damaged

Mode: ‘0x25‘ | Observed encryption: Separate regions encrypted across the file | Recovery implication: Some original content may remain between encrypted regions

Image: Figure 5: Full encryption compared with partial encryption

Why partial encryption does not guarantee file recovery

In some segmented encryption cases, around 88% of the file’s bytes may remain untouched. That figure describes the unencrypted data, not the percentage of the file that can be restored to usable condition.

A video may have intact media data but lack the information needed to play it. A PDF may contain recoverable embedded images while the original document structure is damaged. Some archives and databases cannot be reconstructed if critical internal sections are missing.

In a BleepingComputer forum discussion, a participant reported recovering most pages of a partially encrypted PDF by extracting intact JPEG streams. This was partial reconstruction of the document's content, rather than decryption of the original file.

Are JPG, HEIF, MP4 and MOV files fully encrypted?

Qihoo 360 reported that the malware gives full-encryption priority to 187 file extensions. The original research includes the extension list as an image, but the individual entries have not all been independently verified in this guide.

For that reason, it would be misleading to assume that family photos and videos are only partially encrypted. A file's extension, size and observed encryption mode need to be checked against the relevant malware sample.

If a photograph or video belongs to the full-encryption group, carving intact content directly from that encrypted file is unlikely to work. Btrfs recovery or an independent original copy may still be useful because those methods can retrieve data that existed before encryption.

Recovery results reported by researchers and victims

The available reports show that recovery is possible under certain conditions, but the success figures come from different tools and storage environments.

Reported case: Proxmox guest with GitLab backup | Method: Memory key recovery | Result: About 49 GiB recovered, 80 projects restored | Verification: Historical digest comparison reported

Reported case: Physical Synology DS920+ | Method: Memory key recovery | Result: Two byte-identical files and a valid PDF | Verification: Limited file comparison

Reported case: Btrfs Synology case | Method: CoW extent recovery | Result: 35,445 files, about 229.9 GB | Verification: SHA comparison reported

Reported case: NoCOW-related recovery | Method: Filesystem reconstruction | Result: About 6,100 files, 346 GB | Verification: Project case report

Reported case: Additional community Btrfs case | Method: Keyless reconstruction | Result: 17,893 of 24,142 files | Verification: Mostly file-format checks

Reported case: DS420j, EXT4, rebooted | Method: No established complete recovery route | Result: No verified full recovery | Verification: Open victim discussion

The reports are documented in the memory recovery repository, the Btrfs recovery project, and related GitHub issues. The results are not independently established recovery rates for the wider campaign.

Open-source C3RB3R recovery projects

Several community projects appeared after the attacks. They address different recovery situations, so choosing the correct tool matters more than trying every repository.

soimy/c3rb3r-rescue

soimy/c3rb3r-rescue on GitHub documents memory preservation, cryptographic key recovery, test decryption and related recovery work.

It is particularly relevant if the original encryptor is still running or investigators have already collected useful process memory.

crt106/c3rb3r-btrfs-recovery

crt106/c3rb3r-btrfs-recovery on GitHub focuses on reconstruction from older Btrfs extents. Its case study includes reported checksum-verified recovery from physical Synology storage.

The technique is intended for compatible Btrfs systems. It does not provide the same recovery method for EXT4.

hjs785053766/c3rb3r-btrfs-recovery

hjs785053766/c3rb3r-btrfs-recovery on GitHub contains another Btrfs recovery approach with reported recovery results across different file categories.

Its case study is useful for understanding how strongly encryption mode affects the outcome.

penv13/c3rb3r-inplace-rescue

penv13/c3rb3r-inplace-rescue on GitHub explores restoration methods designed to reduce additional storage requirements. The project documents a large recovery case, but its in-place operations require particular caution.

Do not use in-place modification tools on the only surviving copy of affected data. Preserve the original files or disks and test unfamiliar recovery methods separately.

Is there a free decryptor for C3RB3R .L0CK3D files?

No verified universal public decryptor was identified in the research reviewed through November 5, 2026. The community tools discussed above work under specific technical conditions, rather than decrypting every affected file automatically.

You can check the No More Ransom project for legitimate ransomware decryption utilities. However, a tool designed for an older Cerber ransomware variant should not be assumed to work with the Synology-targeting C3RB3R samples.

Will removing the .L0CK3D extension work?

No. Renaming ‘photo.jpg.L0CK3D‘ to ‘photo.jpg‘ does not change the encrypted contents. The file will remain damaged or unreadable until its original data is restored or successfully decrypted.

Should you pay the ransom?

Payment offers no guarantee of recovery. Attackers may supply a defective decryptor, refuse to provide a working key, or demand additional payment.

Even if a decryptor works, the underlying compromise remains. The attackers may have copied data, created additional access routes or changed system settings.

Some victims have reported that the attackers’ free sample decryption worked. That demonstrates the ability to decrypt a particular sample, but it does not establish that all affected files can be recovered or that payment will be honored.

Which DSM vulnerability was used in the attacks?

Two different vulnerability explanations appeared during the October 2026 campaign.

Synology attributed the attacks to a flaw patched in December 2024 and referred customers to Synology-SA-24:20. That advisory includes CVE-2024-10441 and other DSM security issues.

Qihoo 360's analysis instead attributed the campaign to CVE-2026-13639 and CVE-2026-13684, which were addressed in September 2026 under Synology-SA-26:13.

Source: Synology | Vulnerabilities identified: 2024 vulnerability group, including CVE-2024-10441 | Advisory: SA-24:20

Source: Qihoo 360 | Vulnerabilities identified: CVE-2026-13639 and CVE-2026-13684 | Advisory: SA-26:13

Both advisories are real, but the published evidence does not establish a single entry point for every infected NAS. Different incidents may have involved different vulnerabilities, compromised credentials or exposed software.

One reported case also raised questions about a NAS running a recent DSM build, although that report did not establish a DSM zero-day. An exposed package, container or compromised account remained possible explanations.

Why the exact DSM build number matters

A DSM installation can include the 2024 fixes while still missing the security updates released in September 2026.

For DSM 7.2.2, the two advisories specify different minimum fixed builds:

Image: Figure 6: Comparing two DSM 7.2.2 security updates

The September 2026 advisory lists the following minimum fixed versions:

DSM branch: DSM 7.4 | Minimum fixed build for SA-26:13: '7.4-90075'

DSM branch: DSM 7.3 | Minimum fixed build for SA-26:13: '7.3.2-86009-4'

DSM branch: DSM 7.2.2 | Minimum fixed build for SA-26:13: '7.2.2-72806-9'

DSM branch: DSM 7.2.1 | Minimum fixed build for SA-26:13: '7.2.1-69057-12'

For an uninfected NAS, check the latest compatible DSM release and install applicable security updates. An already compromised NAS should be assessed and evidence preserved before an upgrade that requires restarting the system.

How to secure the NAS after recovery

Recovering files does not remove the original security problem. Before returning the NAS to normal use, investigate how the attackers gained access and rebuild or clean the system as appropriate.

Update DSM and installed packages

Install the latest supported DSM security updates after preserving evidence. Check installed packages, containers and applications for outdated or vulnerable components.

For a confirmed compromise, rebuilding from trusted software and restoring clean data is generally safer than assuming the system is clean after deleting a suspicious executable.

Restrict remote access

Remove unnecessary port forwarding and avoid exposing the DSM administration interface directly to the internet.

Review firewall rules, IPv6 connectivity, reverse proxy routes and VPN access. When remote administration is required, use a secured connection with appropriate authentication and access restrictions.

Review user accounts and credentials

Change credentials that may have been exposed. Disable unused accounts and enable multifactor authentication where supported.

Examine unfamiliar administrative accounts, scheduled tasks, SSH keys, startup scripts and installed services. Any evidence of persistence should be handled as part of the incident investigation.

Keep independent, tested backups

Snapshots can help with accidental changes and some ransomware incidents, but backup copies should also exist outside the affected NAS. Offline or immutable copies are particularly useful when an attacker gains administrative access.

Use more than one backup destination for important data, and periodically test restoration. For configuration guidance, consult Synology’s backup and security documentation.

Frequently asked questions

Can C3RB3R .L0CK3D files be recovered without paying?

Yes, in some situations. Reported recoveries have used memory-based key extraction, older Btrfs extents, snapshots and clean backups. The appropriate method depends on the condition of the NAS and the affected files.

Is recovery possible after rebooting a Synology NAS?

Rebooting usually removes the original ransomware process’s volatile memory, but it does not automatically destroy snapshots, independent backups or surviving Btrfs data. Check those options before concluding that recovery is impossible.

What if the NAS uses EXT4 and has no backups?

Full recovery is particularly difficult after a reboot. The reviewed community research does not document a verified general method for that configuration. Forensic imaging, surviving original copies and partial file salvage may still be worth investigating.

Can I use PhotoRec to recover .L0CK3D files?

PhotoRec may locate deleted or surviving file data, but it cannot decrypt C3RB3R ciphertext. It is useful only where recoverable original content still exists.

Does SHR or RAID protect against ransomware?

No. SHR and RAID provide storage redundancy against certain hardware failures. They do not prevent ransomware from encrypting files on a mounted volume, and they do not replace backups.

Can encrypted videos and photos be repaired?

Some partially encrypted files may contain recoverable images, video segments or other data. Results depend on the encryption mode and whether the file's structure can be reconstructed. Fully encrypted files require a different recovery route.

Should I update DSM as soon as I discover C3RB3R?

An uninfected NAS should receive applicable security updates promptly. If an infected NAS is still running, preserve evidence and assess memory recovery before installing an update that may restart the device.

Recovery checklist

1. Isolate the infected NAS from untrusted networks.
2. Keep it running until you determine whether volatile memory needs to be preserved.
3. Preserve the encrypted files, ransom note, logs and relevant disk evidence.
4. Check whether the original encryptor is still active.
5. Look for clean snapshots and backups.
6. Identify the affected volume's filesystem.
7. Investigate memory recovery or Btrfs reconstruction only when applicable.
8. Test recovery methods using copies of the affected data.
9. Verify restored files before relying on them.
10. Rebuild or clean the compromised system, apply updates and secure remote access.

For a NAS that is still running, the first opportunity may be the encryption material left in memory. If the system has already restarted, existing snapshots and Btrfs data can sometimes provide another way back. EXT4 recovery without keys or backups is much more limited, particularly after the original data has been overwritten.

Keep the affected disks and encrypted copies intact until the available recovery options have been assessed. Even when current tools cannot restore a file, preserving the evidence avoids losing the remaining options through unnecessary writes.

Sources and technical references

The following sources document the October and November 2026 campaign, the reported recovery cases and the relevant DSM security advisories.

- BleepingComputer: Synology warns of ongoing C3RB3R ransomware attacks
- Synology: Company security announcements
- Synology-SA-24:20: DSM security vulnerabilities
- Synology-SA-26:13: September 2026 security fixes
- Qihoo 360: Technical analysis of the Synology ransomware campaign
- GitHub: C3RB3R memory recovery and evidence preservation
- GitHub: C3RB3R Btrfs recovery research
- GitHub: Additional Btrfs recovery case study
- GitHub: DS420j EXT4 recovery discussion after reboot
- BleepingComputer Forums: C3RB3R victim reports and file recovery discussion
- No More Ransom: Ransomware identification and legitimate decryption tools

References

1. synology.com - en-global / company - https://www.synology.com/en-global/company/news

2. bleepingcomputer.com - news / security - https://www.bleepingcomputer.com/news/security/synology-warns-customers-of-ongoing-c3rb3r-ransomware-attacks/

3. github.com - soimy / c3rb3r-rescue - https://github.com/soimy/c3rb3r-rescue

4. github.com - crt106 / c3rb3r-btrfs-recovery - https://github.com/crt106/c3rb3r-btrfs-recovery

5. github.com - hjs785053766 / c3rb3r-btrfs-recovery - https://github.com/hjs785053766/c3rb3r-btrfs-recovery

6. kb.synology.com - https://kb.synology.com/

7. github.com - soimy / c3rb3r-rescue - https://github.com/soimy/c3rb3r-rescue/issues/22

8. 360.cn - n / 13055.html - https://www.360.cn/n/13055.html

9. bleepingcomputer.com - forums / t - https://www.bleepingcomputer.com/forums/t/819759/c3rb3r-nas-ransomware-encrypting-nas-devices-l0ck3d-ext-read-me3txt/page-2

10. github.com - penv13 / c3rb3r-inplace-rescue - https://github.com/penv13/c3rb3r-inplace-rescue

11. nomoreransom.org - https://www.nomoreransom.org/

12. synology.com - en-global / security - https://www.synology.com/en-global/security/advisory/Synology_SA_24_20

13. synology.com - en-global / security - https://www.synology.com/en-global/security/advisory/Synology_SA_26_13