

Title:

Proof of Concept (PoC) – Decryption and Recovery of BTCWare and Cerber v1 Ransomware-Infected Systems

Name: Shubhalaxmi Rout

Organization: Digisuraksha Internship
Program 2025

Intern ID: 320

Project Duration: July 2025

→ Abstract

Ransomware continues to be one of the most damaging and sophisticated cyber threats. This Proof of Concept (PoC) explores the effectiveness of decryption and recovery tools for two specific ransomware families: BTCWare and Cerber v1. BTCWare, known for its decryptable early versions, is analyzed using tools such as Avast BTCWare Decryptor. Cerber v1, notorious for strong encryption, is shown to be non-decryptable without backups. Through controlled simulations and recovery trials in isolated environments, this PoC highlights best practices in ransomware response and mitigation strategies.

→ Table of Contents

1. Introduction
2. Objectives
3. Tools and Test Setup
4. BTCWare Ransomware Analysis
5. Cerber v1 Ransomware Analysis
6. How to Recover Cerber Files
7. Comparison Summary Tables

8. Key Findings

9. Conclusion

1. Introduction

Ransomware encrypts critical user data and demands a ransom for decryption keys. BTCWare and Cerber v1 have caused widespread disruption due to their unique attack vectors and encryption mechanisms. BTCWare relies on leaked keys for early decryption, while Cerber v1 remains one of the most resilient variants.

2. Objectives

- Simulate BTCWare and Cerber v1 ransomware infections.
 - Test decryption tools and recovery utilities.
 - Evaluate the effectiveness of backup restoration.
 - Provide recommendations to mitigate future attacks.
-

3. Tools and Test Setup

Decryption Tools:

- **Avast BTCWare Decryptor** – Trusted for early BTCWare variants.
- **Michael Gillespie's BTCWareDecrypter** – Targets specific BTCWare strains.

Recovery Tools:

- **ShadowExplorer** – Restores Volume Shadow Copies.
- **PhotoRec / EaseUS** – Recovery tools for corrupted files.

Environment:

- Virtual Machine (VM) isolated test bed
 - Sample encrypted file types: `.docx`, `.xlsx`, `.jpg`
 - Simulated RDP brute-force attacks
-

4. BTCWare Ransomware Analysis

BTCWare is a ransomware strain that first appeared in March 2017. Since then, we observed five variants that can be distinguished by encrypted file extension. The ransomware uses two different encryption methods – RC4 and AES 192.

Filename changes:

Encrypted file names will have the following format:

`foobar.docx.[sql772@aol.com].theva`

`foobar.docx.[no.xop@protonmail.ch].cryptobyte`

`foobar.bmp.[no.btc@protonmail.ch].cryptowin`

`foobar.bmp.[no.btcw@protonmail.ch].btcware`

`foobar.docx.onyon`

Furthermore, one of the following files can be found on the PC

`Key.dat` on `%USERPROFILE%\Desktop`

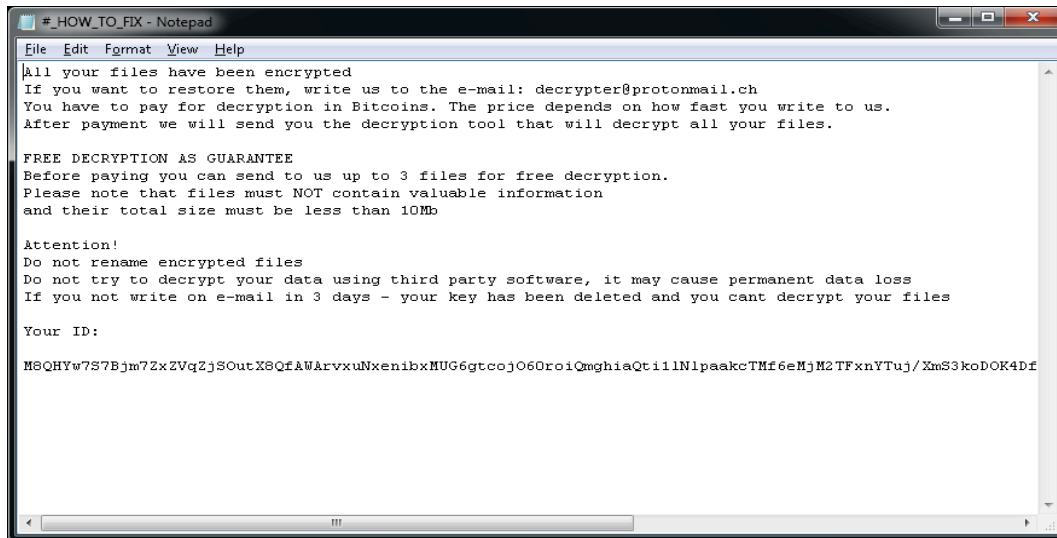
`1.bmp` in `%USERPROFILE%\AppData\Roaming`

#_README_#.inf or !_DECRYPT_#!.inf in each folder with at least one encrypted file.

**All your files have been encrypted
If you want to restore them
write us to the e-mail: decrypter@protonmail.ch**

Ransom message:

After encrypting your files, the desktop wallpaper is changed to the following:



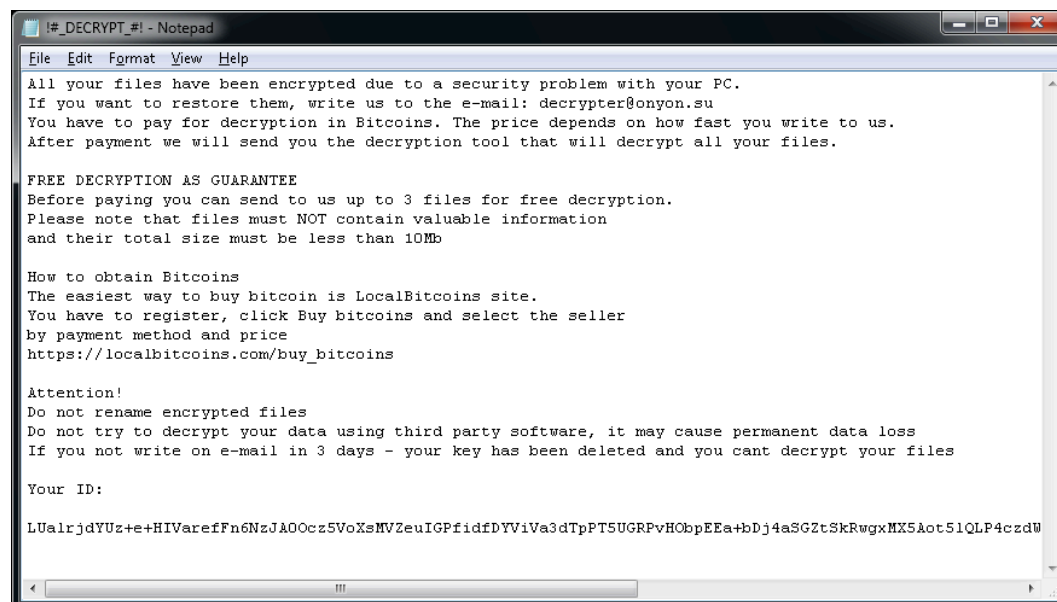
```
#_HOW_TO_FIX - Notepad
File Edit Format View Help
All your files have been encrypted
If you want to restore them, write us to the e-mail: decrypter@protonmail.ch
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.

FREE DECRYPTION AS GUARANTEE
Before paying you can send to us up to 3 files for free decryption.
Please note that files must NOT contain valuable information
and their total size must be less than 10Mb

Attention!
Do not rename encrypted files
Do not try to decrypt your data using third party software, it may cause permanent data loss
If you not write on e-mail in 3 days - your key has been deleted and you cant decrypt your files

Your ID:
M8QHYw7S7Bjm7ZxZVqZjSOutX8QfAWArvxuNxenibxMUG6gtcojO6OroiQmghiaQt11lNlpaakcTMf6eHjM2TFxnYTuj/XmS3koDOK4df
```

You may also see one of the following ransom notes:notes:



```
!#_DECRYPT_#! - Notepad
File Edit Format View Help
All your files have been encrypted due to a security problem with your PC.
If you want to restore them, write us to the e-mail: decrypter@onyon.su
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.

FREE DECRYPTION AS GUARANTEE
Before paying you can send to us up to 3 files for free decryption.
Please note that files must NOT contain valuable information
and their total size must be less than 10Mb

How to obtain Bitcoins
The easiest way to buy bitcoin is LocalBitcoins site.
You have to register, click Buy bitcoins and select the seller
by payment method and price
https://localbitcoins.com/buy_bitcoins

Attention!
Do not rename encrypted files
Do not try to decrypt your data using third party software, it may cause permanent data loss
If you not write on e-mail in 3 days - your key has been deleted and you cant decrypt your files

Your ID:
LUalrjdYUz+e+HIVarefFn6NzJA0Ocz5VoXsMVZeuIGPfidfDYViVa3dTpPT5UGRPvHObpEEa+bDj4aSGZtSkRvgxMX5Aot51QLP4czdW
```

Observed Variant: .cryptobyte

Encryption Algorithms: RC4 / AES-192

File Naming Format: foobar.docx.[email].cryptobyte

Behavior:

- Encrypted user files with specific extensions.
- Generated ransom note `#_RESTORE_FILES_#.txt`.
- Deleted shadow copies.

Decryption Test:

- **Tool Used:** Avast BTCWare Decryptor
- **Result:** 100% decryption success (100 files, 4 minutes)

Recommendations:

- Disable open RDP ports; use VPN access.
 - Maintain frequent offline backups.
 - Use only verified decryptor tools.
-

5. Cerber v1 Ransomware Analysis

Observed Variant: Files renamed with random characters.

Encryption Algorithm: AES-256 + RSA-2048 hybrid encryption

Ransom Notes: `README.hta`, `DECRYPT MY FILES.html`

Behavior:

- File contents scrambled using hybrid encryption.
- System audio played a ransom message.
- No shadow copy recovery possible.

Decryption Test:

- **Tools Attempted:** Check Point's CerberDecrypt, Trend Micro Decryptor (Deprecated)

- **Result:** No successful decryption

Recovery Test:

- **Backup Restoration:** Offline backup recovery was successful

Recommendations:

- Regular offline and cloud backups.
 - Disable SMBv1 and restrict RDP access.
 - Educate users on phishing and malicious downloads.
-

6. How to Recover Cerber Files

A. Restore from Windows Previous Versions

1. Open "My Computer" or "Windows Explorer".
2. Right-click on the infected file.
3. Click "Restore previous versions".
4. Choose from available restore points.
5. Click open, copy, or restore to overwrite the encrypted file.

B. Recover with iMyFone AnyRecover

If restore points are unavailable, recovery software can be used:

1. Open AnyRecover and select "Deleted Files Recovery" mode.
2. Choose the location of the lost files.
3. Select file types and start scan.
4. Preview and select files to recover.

5. Use "All-Round Recovery" mode if needed.



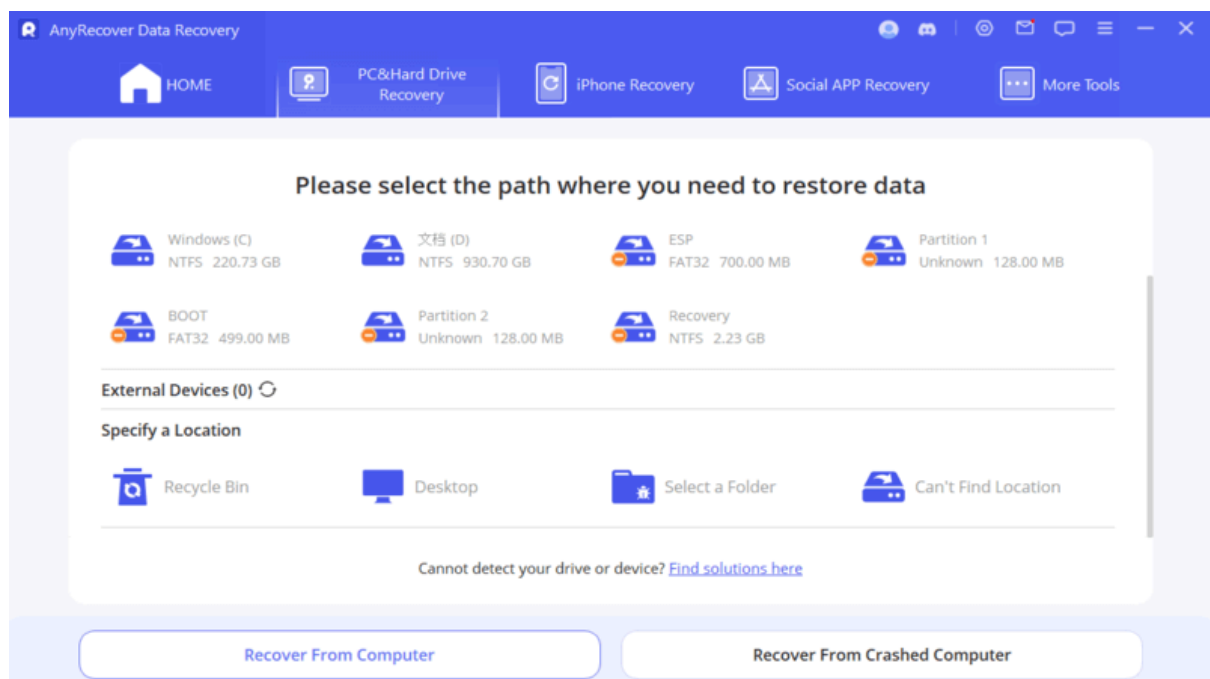
Note: Avoid saving recovered files in the original infected location.

Features of AnyRecover:

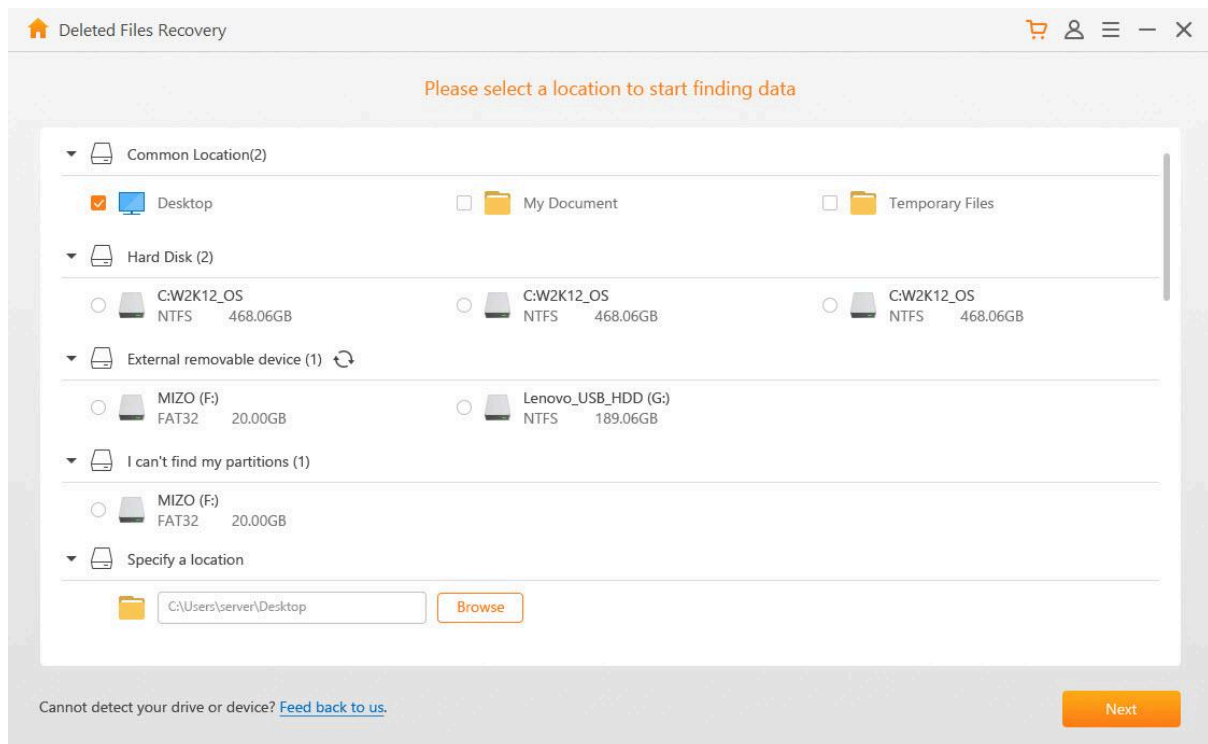
- Recovers files lost due to ransomware, system crash, or formatting.
- Supports all major file types and storage media.
- Compatible with Windows and macOS.

How to Recover Cerber Files with AnyRecover

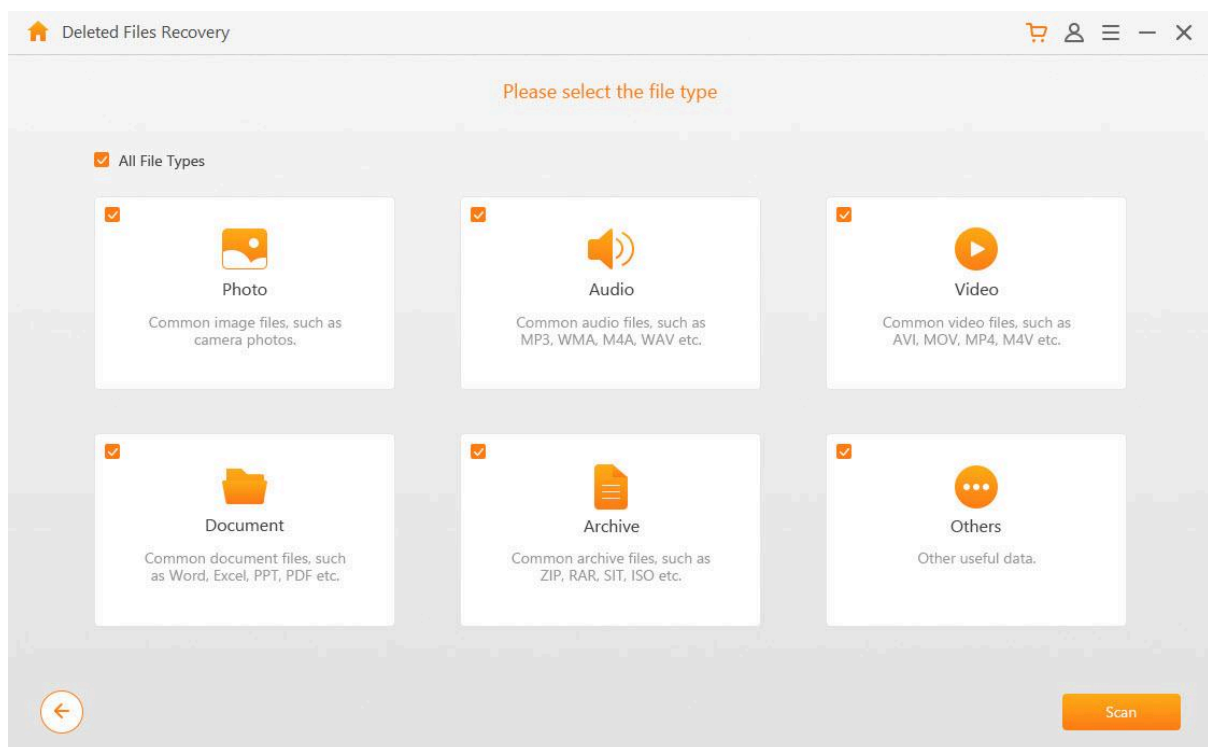
Step 1. Open AnyRecover on your computer and choose the "Deleted Files Recovery" mode.



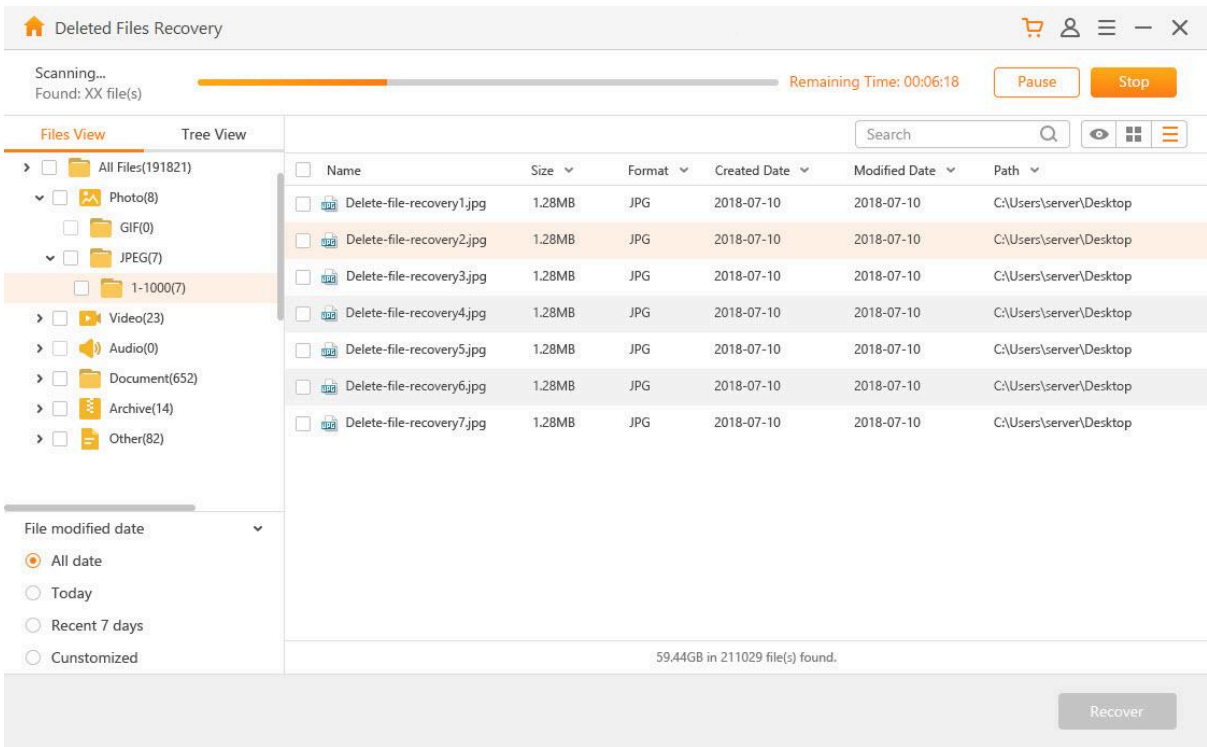
Step 2. Next, choose any location where you lost the data, then hit **"Next"**.



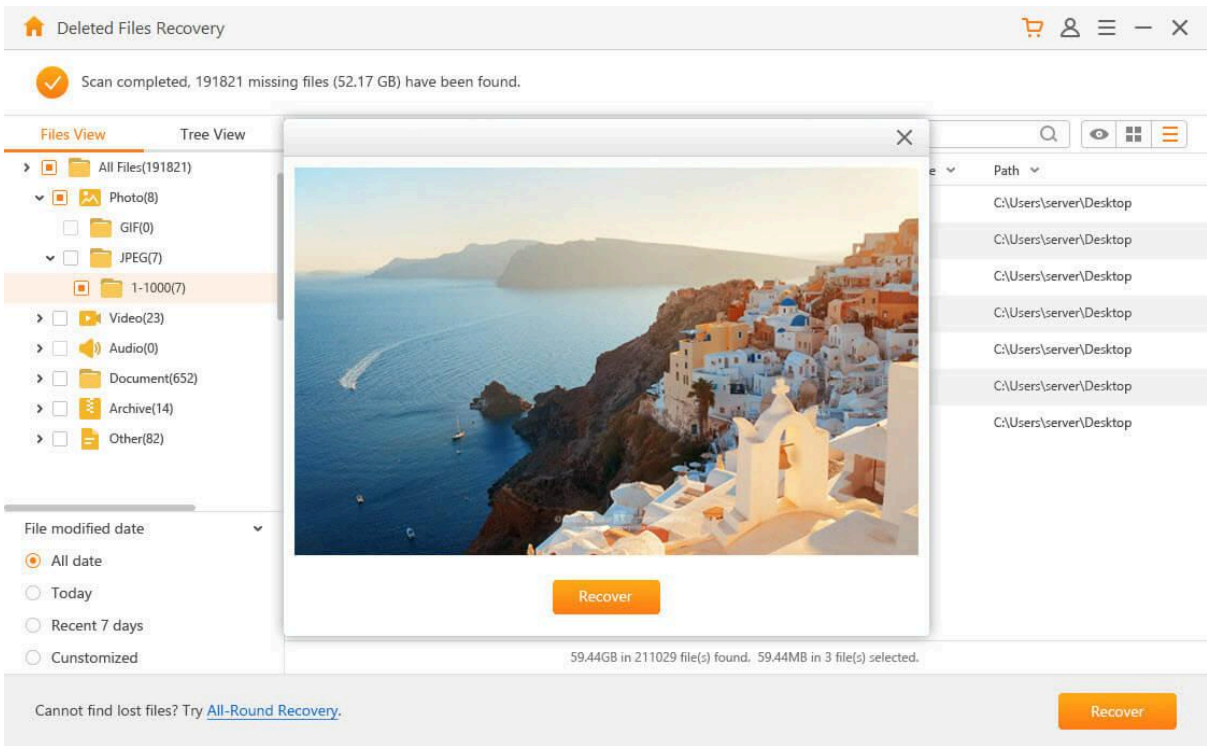
Step 3. Select the type of files you want to recover and click **"Scan"**.



Step 4. The program will scan for all the data on the location.



Step 5. Then proceed to preview the files then click "Recover" to restore your files.



Step 6. You can use the **"All-Round Recovery"** mode to conduct a deeper scan if you can't find your files on the other modes.

Note: Ensure you don't save the file to the same location before the attack or when the file was lost.

7. Comparison Summary Tables

Table 1: Decryption Availability Overview

Ransomware	Decryption Status	Tool Used	Recommendation
BTCWare	Available	Avast Decryptor	Secure RDP, Use backup and patch OS
Cerber v1	Not Available	None	Backup recovery only, system hardening

Table 2: Feature Comparison

Feature	BTCWare	Cerber v1
Free Decryptor	Yes	No
File Extension	.cryptobyte	Random rename
Shadow Copy Recovery	Possible	Rare
Encryption Type	AES-128 / RC4	AES-256 + RSA-2048
Backup Restoration	Yes	Only method

8. Key Findings

- BTCWare early variants are decryptable using free tools.

- Cerber v1 cannot be decrypted due to strong encryption.
 - Offline and cloud backups remain the most reliable recovery option.
 - RDP and SMBv1 are common attack vectors and should be restricted.
-

9. Conclusion

This PoC highlights the critical need for proactive ransomware defense. While BTCWare infections can often be mitigated using available decryptors, Cerber v1 illustrates the devastating impact of non-decryptable ransomware. Organizations must adopt a multi-layered strategy involving:

- Robust offline/cloud backup policies (3-2-1 rule)
- Timely patching and system hardening
- Employee awareness and endpoint protection

Preparedness is the only effective defense when decryption tools are unavailable.
