# **Proof Of Concept Report**

**INTERN NAME : SIDDHI SUNIL BENSEKAR.**

**INTERN ID : 344**

**1] Tool Name :**

**ZIP Password Recovery Tool**

**Description:**

ZIP Password Recovery Tool is a software application designed to help users recover or decrypt lost passwords from encrypted ZIP files. It supports various password recovery techniques, including brute force, dictionary, and mask-based attacks, to recover passwords for ZIP archives protected by standard encryption methods (ZipCrypto) or more advanced encryption (AES-256).

**What Is This Tool About?**

This tool is primarily used for recovering the password to encrypted ZIP files, whether users have forgotten the password or lost access to the file. It works by using different attack strategies to guess or crack the password. The tool supports modern encryption methods (AES-256) commonly used in ZIP archives, making it effective for recovering passwords from files created with tools like WinRAR, 7-Zip, and WinZip.

**Key Characteristics / Features:**

* **Brute Force Attack**: Tries all possible combinations to guess the correct password.
* **Dictionary Attack**: Uses a predefined list of common passwords (or a custom dictionary) to recover the password quickly.
* **Mask Attack**: If the user knows part of the password (e.g., the first few characters), they can define a mask pattern to narrow down the number of combinations tested.
* **AES-256 Support**: Supports breaking AES-256 encryption used in modern ZIP files, offering high-level security bypass.
* **Multi-Core Processing**: The tool can utilize multiple CPU cores, speeding up password recovery, especially in brute force scenarios.
* **GPU Acceleration**: Utilizes GPU power to speed up password recovery significantly, especially for lengthy or complex passwords.
* **Real-Time Progress Monitoring**: Tracks and displays the progress in terms of attempts made, estimated time, and recovery status.
* **Resume Capability**: Can pause and resume the password recovery process, allowing users to stop and restart without losing progress.
* **User-Friendly Interface**: Easy-to-use interface that doesn’t require advanced technical skills to operate.

**Types / Modules Available:**

* **Brute Force Attack**: This method tests all possible password combinations without any assumptions.
* **Dictionary Attack**: The tool uses a list of potential passwords to try and unlock the ZIP file.
* **Mask Attack**: Users can define a pattern (for example, known parts of the password like the first letter or length) to focus the attack.
* **Hybrid Attack**: Combines dictionary and brute force to improve recovery chances (i.e., trying words from the dictionary and modifying them based on rules).

**How Will This Tool Help?**

* **Forensic Investigations**: Helps investigators recover important data that is locked in encrypted ZIP files found during an investigation.
* **Password Recovery**: Assists users who’ve forgotten the password to their encrypted ZIP archives and need to recover files.
* **Data Access**: Enables access to vital files stored in old or inaccessible ZIP backups when passwords are lost.
* **Auditing and Security Testing**: Useful for testing the strength of passwords used in ZIP files for security audits.

By using multiple recovery techniques, the tool maximizes the likelihood of successfully recovering the password for encrypted ZIP files.

**Proof of Concept (PoC) Images:**

While I cannot directly generate or show images here, I can provide a typical workflow visualization:

1. **Step 1**: The ZIP Password Recovery Tool is launched, and the encrypted ZIP file is selected.
2. **Step 2**: The user selects an attack method—either brute force, dictionary, or mask.
3. **Step 3**: The tool begins the attack, displaying a progress bar showing the number of attempts, estimated time remaining, and any other relevant information.
4. **Step 4**: After a set amount of time, the tool displays the recovered password, unlocking the ZIP file.

**8-Liner Summary:**

* ZIP Password Recovery Tool is a powerful utility designed for recovering lost passwords from encrypted ZIP files.
* It supports multiple decryption methods, such as brute force, dictionary, and mask attacks, and can handle both standard and advanced AES-256 encryption.
* The tool offers GPU acceleration for faster processing and uses multi-core support for better performance.
* Its intuitive interface is user-friendly and does not require advanced technical skills.
* Users can track the progress of the decryption process in real-time and pause/resume if needed.
* It’s particularly useful in forensic investigations, data recovery, and password audits.
* However, longer passwords and stronger encryption may take considerable time to crack.
* The tool is ideal for both individual and professional use, especially for those needing to recover critical files from encrypted ZIP archives.

**Time to Use / Best Case Scenarios:**

* **Best Time to Use**:
  + When you’ve forgotten the password to a ZIP file containing important files or backups.
  + During a forensic investigation when encrypted ZIP files are found, and the password needs to be cracked.
  + When testing the strength of passwords used for ZIP archives in an organizational environment.
* **Best Case Scenarios**:
  + **Forensics**: Investigating and extracting evidence from encrypted ZIP files found in evidence.
  + **Data Recovery**: Recovering files from encrypted ZIP backups where the password is unknown.
  + **Security Auditing**: Testing how strong the passwords are in ZIP archives used by an organization.

**When to Use During Investigation:**

* **Forensics**:
  + Use this tool if a ZIP file is discovered in a suspect’s computer and it is encrypted with an unknown password.
  + If an investigator needs to gain access to evidence files in ZIP format but cannot open them without the password.
* **Evidence Decryption**: When encrypted ZIP files contain files critical for an investigation (e.g., documents, images, and logs) and need to be accessed as part of a larger investigation.

**Best Person to Use This Tool & Required Skills:**

* **Best Person to Use**:
  + **Forensic Investigators**: Professionals working in cybercrime investigations or digital forensics.
  + **System Administrators**: Admins responsible for handling encrypted ZIP files or recovering encrypted backups.
  + **Data Recovery Technicians**: Technicians who work to restore encrypted files for businesses or individuals.
* **Required Skills**:
  + **Basic Understanding of Encryption**: Familiarity with how ZIP file encryption works (ZipCrypto, AES).
  + **Basic Computer Security Knowledge**: Awareness of password recovery techniques and decryption methods.
  + **Familiarity with Forensic Tools**: Experience in using various password recovery or forensic tools.

**Flaws / Suggestions to Improve:**

**Flaws**:

1. **Long Time for Strong Passwords**: Brute force attacks can take a considerable amount of time for long or complex passwords.
2. **Limited File Format Support**: Works only for ZIP files and does not support other formats like RAR, 7z, or encrypted disk images.
3. **Dependency on Hardware**: Decryption time is highly dependent on the hardware (CPU/GPU). It may be slow on older systems.

**Suggestions for Improvement**:

* **Support for More Formats**: Extend support to other encrypted file formats (e.g., RAR, 7z).
* **Cloud-Based Cracking**: Integration with cloud-based services to leverage more computational power for faster decryption.
* **Progressive Mode**: Include an adaptive attack mode that adjusts depending on the results from earlier attempts (e.g., if a partial password is found).

**Good About the Tool:**

* **Fast Processing**: With GPU acceleration and multi-core support, it speeds up the password recovery process considerably.
* **Multiple Attack Methods**: The ability to choose between brute force, dictionary, and mask-based attacks offers flexibility.
* **Easy to Use**: The intuitive interface makes it suitable for both beginners and experts.
* **AES-256 Encryption Support**: Can handle modern encryption methods like AES-256, making it effective for newer ZIP files.
* **Real-Time Monitoring**: Provides progress updates, helping users understand the status of password recovery.

**Conclusion:**

ZIP Password Recovery Tool is an invaluable asset for anyone needing to recover a forgotten password from encrypted ZIP archives. Whether you're a forensic investigator, data recovery professional, or a regular user trying to recover old files, this tool offers efficient and reliable methods for cracking ZIP file passwords. While it may struggle with long and complex passwords, its combination of brute force, dictionary, and mask attacks makes it highly versatile and useful in various recovery and investigation scenarios.

**2] Tool Name:**

**FortuneCrypt Decrypting Tool**

**Description:**

The **FortuneCrypt Decrypting Tool** is a tool designed to decrypt files encrypted by the **FortuneCrypt** ransomware. This ransomware variant typically encrypts files and appends a specific file extension to them. The decrypting tool works by utilizing the ransomware’s weak points or flaws, such as identifying encryption keys or using known patterns from ransomware decryption techniques.

**What Is This Tool About?**

This tool is aimed at restoring files that have been encrypted by the **FortuneCrypt** ransomware. FortuneCrypt is a type of malware that typically encrypts data and demands a ransom payment from victims for a decryption key. However, certain ransomware variants leave vulnerabilities or encryption flaws that allow for decryption tools to break the encryption without paying the ransom.

**Key Characteristics / Features:**

* **Ransomware Detection**: The tool first identifies files encrypted by the FortuneCrypt ransomware by scanning for specific file extensions or known encryption patterns.
* **Decryption Methods**: Utilizes specific decryption algorithms or known encryption flaws in FortuneCrypt to decrypt files.
* **Automatic Decryption**: After detecting the encrypted files, the tool automatically attempts to recover the files without manual intervention.
* **Log Files**: It generates detailed logs for users to track the decryption process and confirm successful decryption.
* **Offline Decryption Support**: In many cases, FortuneCrypt ransomware may not require online communication with the ransomware operators, allowing the decryption to be carried out offline.
* **No-Ransom Requirement**: It’s designed to offer a method to decrypt files without requiring any payment, ensuring that victims do not fund the criminal operation.
* **User-Friendly Interface**: Easy-to-use interface for both experienced and non-experienced users.
* **File Recovery**: Focused on recovering documents, media, and other critical files encrypted by the ransomware.

**Types / Modules Available:**

* **File Extension Detection Module**: This module identifies and scans files with extensions specific to FortuneCrypt.
* **Brute Force Decryption Module**: Attempts various known encryption keys or methods to recover the original files.
* **Offline Decryption Support**: Allows decryption without needing an internet connection if the ransomware doesn’t rely on a remote server for key delivery.
* **Progress Monitoring Module**: Provides users with a live update on the status of the decryption process.

**How Will This Tool Help?**

This tool can assist users who have fallen victim to the **FortuneCrypt** ransomware by providing a way to decrypt their files without paying the ransom. Forensic teams, IT admins, and even individuals can use this tool to quickly recover encrypted files, avoiding the potential financial and data loss associated with ransomware.

**Proof of Concept (PoC) Images:**

While I cannot provide PoC images, here’s an example workflow:

1. **Step 1**: The user launches the FortuneCrypt Decrypting Tool.
2. **Step 2**: The user selects the folder or disk drive where encrypted files are located.
3. **Step 3**: The tool identifies the files encrypted by FortuneCrypt.
4. **Step 4**: The decryption process begins and shows real-time progress (e.g., files decrypted, time remaining).
5. **Step 5**: Once completed, the files are accessible again in their original format.

**6-Liner Summary:**

* The **FortuneCrypt Decrypting Tool** is a software designed to decrypt files encrypted by the **FortuneCrypt ransomware** without the need to pay the ransom.
* It scans for specific file extensions and identifies encrypted files.
* Once detected, it uses decryption techniques based on vulnerabilities within the ransomware to restore the files to their original state.
* The tool offers an intuitive user interface, automatic file recovery, and generates logs to track the process.
* It supports offline decryption, making it a versatile tool for individuals and businesses.
* Users can recover critical documents, media, and other files encrypted by FortuneCrypt, providing an important asset in the fight against ransomware.

**Time to Use / Best Case Scenarios:**

* **Best Time to Use**:
  + **Immediately After Infection**: When you discover that files have been encrypted by the FortuneCrypt ransomware.
  + **No Backup Available**: When there’s no recent backup to restore from, and the ransomware has encrypted crucial files.
* **Best Case Scenarios**:
  + **Forensic Investigations**: When examining systems for traces of ransomware attacks and decrypting evidence encrypted by FortuneCrypt.
  + **Victims of Ransomware Attacks**: In cases where users or organizations want to recover files without giving in to ransom demands.

**When to Use During Investigation:**

During forensic investigations, if a system is suspected of being infected with **FortuneCrypt ransomware**, the decryption tool can be used after identifying and isolating encrypted files. It helps investigators access critical data for analysis and evidence collection, reducing the potential impact of the attack.

**Best Person to Use This Tool & Required Skills:**

* **Best Person to Use**:
  + **Cybersecurity Professionals**: Experts who are working on ransomware recovery or analysis.
  + **Forensic Investigators**: Individuals involved in investigating ransomware-related incidents.
  + **System Administrators**: IT professionals responsible for recovering encrypted files on affected systems.
  + **End Users**: People who have been infected by FortuneCrypt ransomware and need to recover their files.
* **Required Skills**:
  + **Basic Understanding of Ransomware**: Familiarity with ransomware encryption and decryption methods.
  + **File System Knowledge**: Understanding how ransomware typically affects file systems and data structures.
  + **Technical Proficiency**: Basic troubleshooting and usage of security tools.

**Flaws / Suggestions to Improve:**

**Flaws**:

1. **Limited Support for Multiple Ransomware**: This tool is designed specifically for **FortuneCrypt** and may not support other ransomware variants.
2. **Long Decryption Times**: In cases where the encryption key is highly complex, decryption can take a long time.
3. **Hardware-Dependent**: The decryption speed depends on the performance of the system’s CPU/GPU.

**Suggestions for Improvement**:

* **Add Support for Other Ransomware Variants**: Extend the tool’s compatibility to support more ransomware types, making it a more versatile decryption tool.
* **Cloud-Based Decryption**: Allow users to leverage cloud resources for faster decryption.
* **Automated Key Recovery**: Develop a system where the tool can automatically retrieve encryption keys from known sources or decryptions.

**Good About the Tool:**

* **No Ransom Payment Required**: The tool removes the need to pay the ransom to cybercriminals.
* **Ease of Use**: The tool is user-friendly, making it accessible to both technical and non-technical users.
* **Offline Decryption**: The tool allows decryption to be done offline without relying on external servers.
* **Automatic File Detection**: The tool automatically detects and identifies encrypted files, reducing the manual effort required by users.

**Conclusion:**

The **FortuneCrypt Decrypting Tool** offers a viable option for recovering files encrypted by the FortuneCrypt ransomware. With features such as offline decryption, automatic file detection, and an intuitive interface, it is an invaluable tool for victims of ransomware attacks. While it may have limitations in supporting other ransomware types, it offers users a way to avoid paying ransom demands and recover critical data during forensic investigations or after an infection.