Ransomware Project - Complete Setup Guide

This documentation provides a complete setup guide for the Ransomware Proof-of-Concept (PoC) project. It explains how to configure the Command and Control (C2) server, attacker dashboard, and how to execute the ransomware on the victim machine.

---

1. Project Overview

This ransomware project demonstrates the real-world working of ransomware, including encryption of victim files, communication with a C2 server, and decryption after ransom verification. The backend dashboard for attackers is built using PHP and MySQL, hosted on a local XAMPP server.

---

2. C2 Server Setup (Attacker Side)

Step 1: Install XAMPP

- Download and install XAMPP for your OS from: https://www.apachefriends.org/download.html
- XAMPP provides Apache Web Server and MySQL database needed for the C2 server.

Step 2: Create Project Directory

- Go to the `htdocs` folder of your XAMPP installation directory.
- Create a new folder named `prjrans`.
- Copy the following folders into `prjrans`: `assets`, `public`, `includes`, `uploads`.

Step 3: Start XAMPP Services

- Start Apache and MySQL from the XAMPP control panel.
- Navigate to `http://localhost/prjrans` in your browser. If it shows the listed folders, your server setup is correct.

Step 4: Setup Database

- Go to `http://localhost/phpmyadmin`.
- Create a new database named `prjrans`.
- Then visit: `http://localhost/prjrans/includes/migrate.php` to automatically generate the required tables.

Step 5: Register and Access Attacker Dashboard

- Sign up from `http://localhost/prjrans/public/register.php`.
- Login from `http://localhost/prjrans/public/login.php`.

- View the attacker dashboard at `http://localhost/prjrans/public/dashboard.php`, where the victim's Machine ID and encryption key will be displayed.

Note: The attacker machine can run any OS as long as the XAMPP setup is correctly configured.

---

3. Ransomware Execution (Victim Side)

Requirements

- The victim PC should be Windows.
- Since the project is configured for local environment testing, it requires the attacker's IP.

Step 1: Set Attacker IP

- Open the `config.txt` file in the ransomware directory.
- Add the attacker's IP address followed by `/prjrans`. Example:
- `192.168.1.10/prjrans`

Method 1: Run Python Script

1. Install Python on the victim PC.
2. Install required libraries:

```
pip install pycryptodome pillow psutil requests
```

4. Make sure the IP is set correctly in `config.txt`.
5. Run the ransomware:

```
python rans.py
```

7. It will encrypt the victim's drives and send the Machine ID and encryption key to the C2 server.
8. For safety, it also stores `encryptionKey.txt` locally (only for PoC testing — should be removed in a real deployment).

Method 2: Run EXE File

- This method doesn't require Python or libraries.
- First, embed the attacker's IP in the `rans.py` script (`dashboard_url` variable).
- Convert the script to `.exe`:
    1. Install auto-py-to-exe:

```
pip install auto-py-to-exe
```

    3. Run:

```
auto-py-to-exe
```

    5. In the UI:
        - Select your `rans.py` file.
        - Choose "One File" and "Console Based".
        - In additional files, add the `img` folder (for desktop wallpaper).
        - Click "Convert .py to .exe".

- This will generate a standalone `.exe` file that executes the ransomware with embedded IP.

---

4. Final Notes

- Ensure attacker's IP is correctly configured in all places before execution.
- Always test in a controlled environment.
- Remove local key storage and enhance obfuscation before any public demonstration.

📄 Detection & Alert Module – Setup Documentation

📌 Project Overview

This module is designed to **monitor honeyfiles** using a GUI-based tool and **generate alerts** (PopUp, SMS, call, and email) when ransomware-like behavior (e.g., unauthorized file modification/access) is detected.

⚙️ System Requirements

- **Python 3.10**
- Internet connection (for Twilio and email alerts)
- OS: Windows AMD arch

📦 Dependency Installation

Install the required Python packages using pip:

```
pip install psutil
pip install watchdog
```

☎️ Twilio Setup (for SMS and Call Alerts)

1. Visit https://www.twilio.com/ and **create a Twilio account**.
2. After verifying your identity:
    - Go to your **Twilio Console Dashboard**
    - Note down your **Account SID** and **Auth Token**
    - Note your **Twilio phone number**
3. In your alert script, plug in these credentials and ensure your own phone number is **verified** in the Twilio dashboard (required in free-tier accounts).

4. Install Twilio SDK using:

```
pip install twilio
```

📧 Email Alert Setup (Using App Password)

To send email alerts securely using Gmail:

1. Go to your Google Account: https://myaccount.google.com
2. Navigate to **Security**.
3. Enable **2-Step Verification** if not already enabled.
4. After enabling it, go back to **Security** → scroll down to **App Passwords**.
5. Choose **App** as "Mail" and **Device** as "Other", then name it (e.g., "Ransomware Alert").
6. Click **Generate**. A 16-character app password will appear.
7. Copy this app password and use it in your alert script in place of your Gmail password.
8. Use your Gmail address as the sender and any recipient address you want.

📌 **Note:** Do not share your app password. This is more secure than using your actual Gmail login.

📁 File Descriptions

Filename	Description
`monitor_file_gui.py`	**Main file** to launch the GUI, set honeyfiles, and start monitoring.
`honeyfile_peaker.py`	Allows user to select and manage **honeyfiles** to be monitored.
`alert_generation.py`	Handles sending alerts (SMS, call, email) upon suspicious file access.

🚀 Execution Steps

1. **Run the Main Monitor Script:**

```
python monitor_file_gui.py
```

2. **Set Honeyfiles:**
   The GUI will prompt you to select one or more **honeyfiles**. These files will be monitored for suspicious activity.
3. **Start Monitoring:**
   Once you confirm, the system will continuously monitor selected files.

4. **Trigger Alert:**
   If any ransomware-like activity is detected (modification, renaming, deletion), the alert system will:
   - Send an **SMS**
   - Make a **phone call**
   - Send an **email notification**
5. **Stop Monitoring:**
   Close the GUI or stop the script to end monitoring.

🧪 Testing Tips

- To test alerts, manually open/rename/edit a honeyfile.
- **For call and SMS alert message should not be so long it will not send the message and give error in twilio account so keep it small.**
- Ensure your Twilio phone number is verified (if on free plan).
- Use the generated **Gmail app password** instead of your regular Gmail password.