PoC Report : SNSLocker & SpartCrypt Decryptor Tools
Reported By: Swadhin Das
Intern ID: 396
Tool ID: 175,176

Objective
To test ransomware decryption using two publicly available decryptor tools: SNSLocker and SpartCrypt in a controlled lab environment.

This PoC validates the tools' behavior and setup using simulated encrypted files.

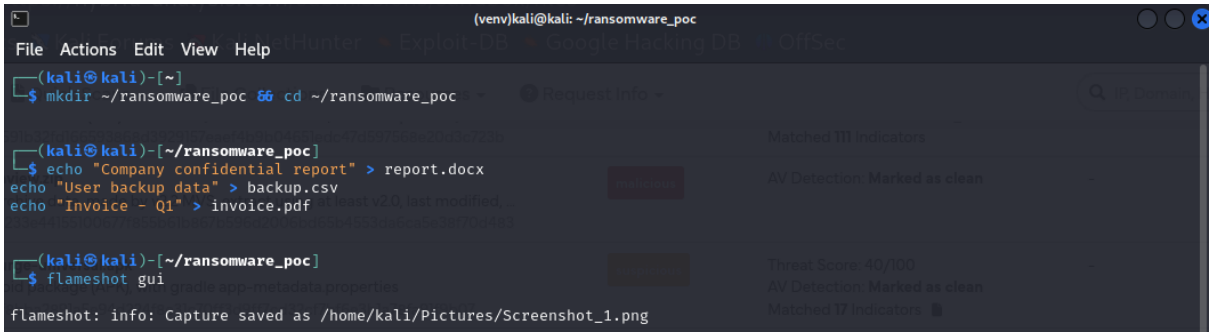
Environment
OS: Kali Linux
Platform: VMware Workstation
Decryption Tools:
RansomwareFileDecryptor 1.0.1668 MUI.exe` (SNSLocker)
decrypt_SpartCrypt.exe` (SpartCrypt)

Test Setup (Simulated Encryption)
1. Prepare wine environment:
sudo apt update
sudo apt install wine -y

2. Simulate Encrypted File
sns_test.txt.encrypted
sns_test.txt.locked
sns_test.txt.RSNSLocker

3. Run SNSLocker Decryptor Tool(RansomwareFileDecryptor 1.0.1668 MUI.exe)
wine 'RansomwareFileDecryptor 1.0.1668 MUI.exe'

4. Run SpartCrypt Decryptor Tool(decrypt_SpartCrypt.exe)
wine decrypt_SpartCrypt.exe



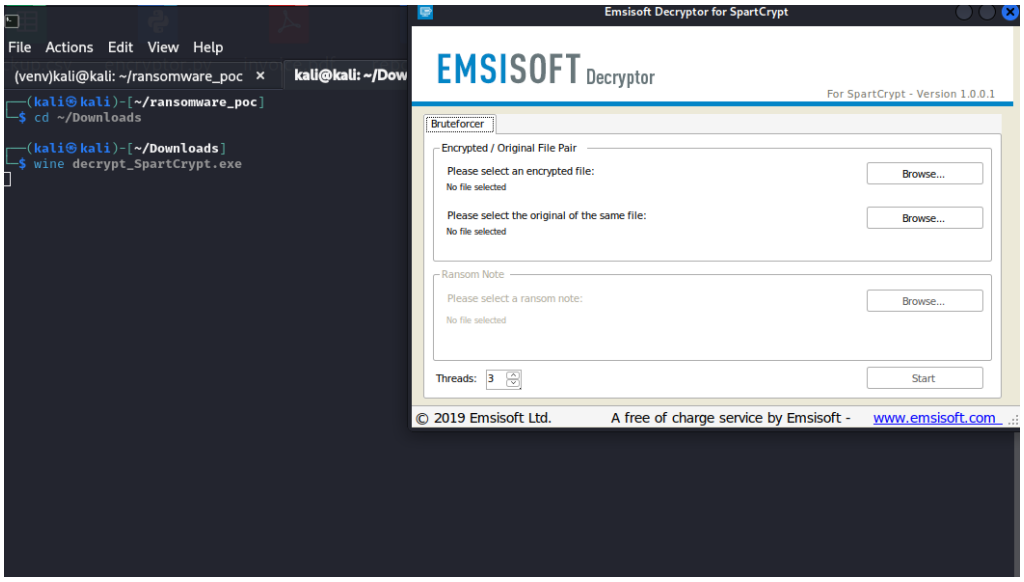
Simulated Test Data

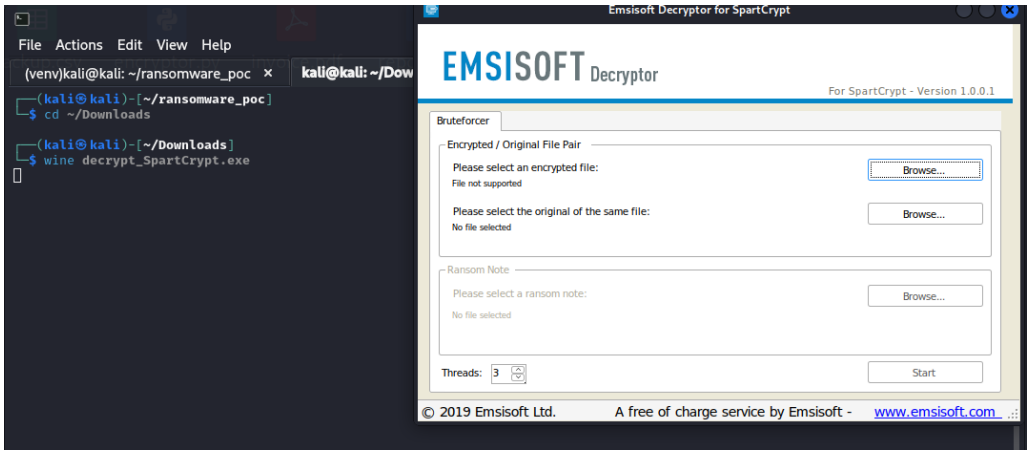
Created dummy `sns_test.txt` files and renamed with .encrypted`, .locked, .RSNSLocker extensions to mimic ransomware behavior.
Create encrypted file through
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes
import os
# Generate a random 16-byte key
key = get_random_bytes(16)

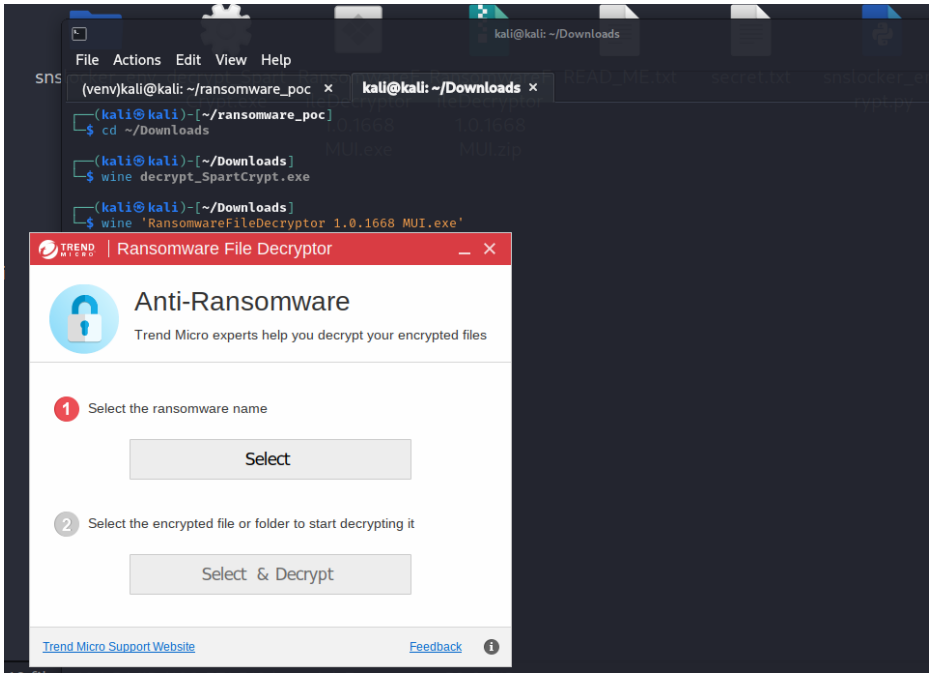
Save the key to file (for manual decryption later)
with open("aes_key.bin", "wb") as kf:
    kf.write(key)

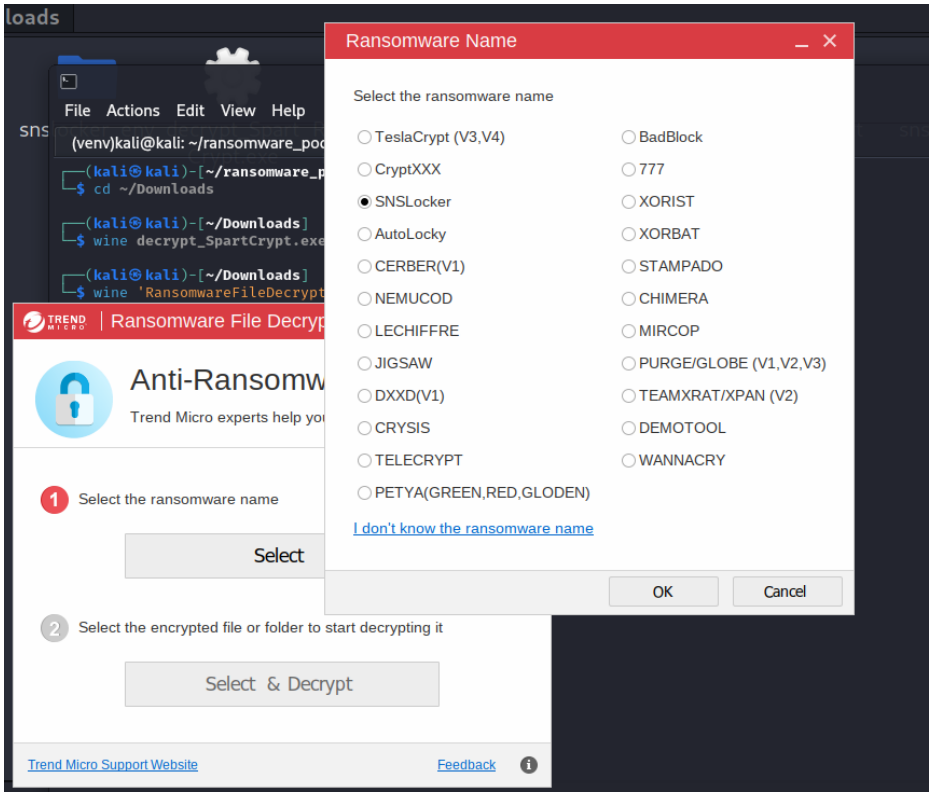
Encrypt all files in current folder (skip .py files)

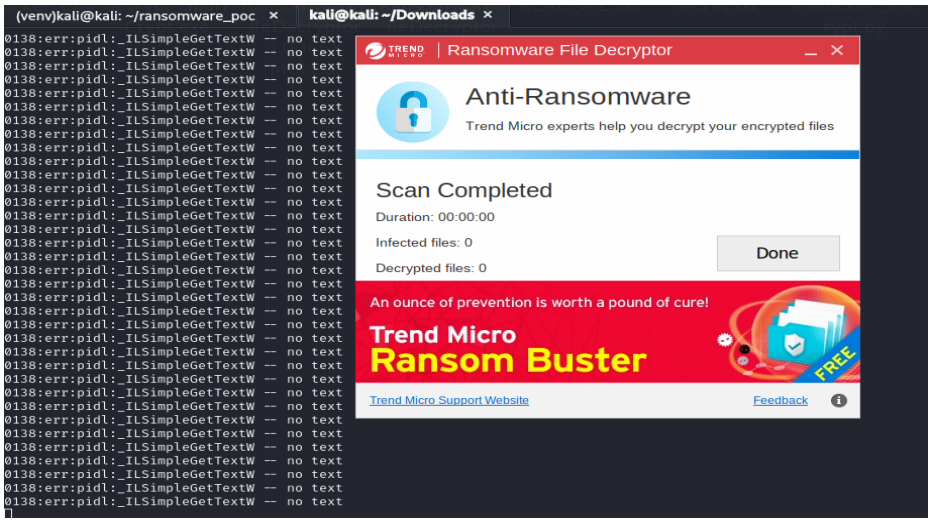
```
for filename in os.listdir():
    if filename.endswith(".py") or filename.endswith(".bin") or filename.endswith(".enc"):
        continue

    if os.path.isfile(filename):
        with open(filename, "rb") as f:
            data = f.read()

        cipher = AES.new(key, AES.MODE_EAX)
        ciphertext, tag = cipher.encrypt_and_digest(data)

        with open(filename + ".enc", "wb") as f:
            f.write(cipher.nonce + tag + ciphertext)

        os.remove(filename)
```




File Actions Edit View Help
(venv)kali@kali: ~/ransomware_poc
kali@kali: ~/Dow
(kali㉿kali)-[~/ransomware_poc]
$ cd ~/Downloads
(kali㉿kali)-[~/Downloads]
$ wine decrypt_SpartCrypt.exe
Emsisoft Decryptor for SpartCrypt
EMSISOFT Decryptor
For SpartCrypt - Version 1.0.0.1
Bruteforcer
Encrypted / Original File Pair
Please select an encrypted file:
File not supported
Browse...
Please select the original of the same file:
No file selected
Browse...
Ransom Note
Please select a ransom note:
No file selected
Browse...
Threads: 3
Start
© 2019 Emsisoft Ltd.
A free of charge service by Emsisoft -
www.emsisoft.com


kali@kali: ~/Downloads
File Actions Edit View Help
(venv)kali@kali: ~/ransomware_poc
kali@kali: ~/Downloads
(kali㉿kali)-[~/ransomware_poc]
$ cd ~/Downloads
(kali㉿kali)-[~/Downloads]
$ wine decrypt_SpartCrypt.exe
(kali㉿kali)-[~/Downloads]
$ wine 'RansomwareFileDecryptor 1.0.1668 MUI.exe'
Ransomware File Decryptor
Anti-Ransomware
Trend Micro experts help you decrypt your encrypted files
1 Select the ransomware name
Select
2 Select the encrypted file or folder to start decrypting it
Select & Decrypt
Trend Micro Support Website
Feedback


Ransomware Name
Select the ransomware name
TeslaCrypt (V3,V4)
CryptXXX
SNSLocker
AutoLocky
CERBER(V1)
NEMUCOD
LECHIFFRE
JIGSAW
DXXD(V1)
CRYSIS
TELECRYPT
PETYA(GREEN,RED,GLODEN)
BadBlock
777
XORIST
XORBAT
STAMPADO
CHIMERA
MIRCOP
PURGE/GLOBE (V1,V2,V3)
TEAMXRAT/XPAN (V2)
DEMOTOOL
WANNACRY
I don't know the ransomware name
OK
Cancel
Select the encrypted file or folder to start decrypting it
Select & Decrypt
Trend Micro Support Website
Feedback



Conclusion:

- Tools executed successfully using Wine in a Kali Linux environment.
- SpartCrypt Decryptor did not recognized the file due to real encrypted payload or keys.
- RansomwareFileDecryptor 1.0.1668 MUI.exe run but couldn’t decrypt.
- Tools ran but couldn't decrypt (no real key/data).
- Simulated encrypted files were created using AES and file extension spoofing.
- Decryptors failed to process files without real ransomware payload or keys.
- This PoC verifies that the test environment and tools are **ready for analysis of real ransomware** samples in the future.