Ransomware

Description

Ransomware causes a lot of headache and money each year. Your task is to experiment with ransomware.

On your windows 7 vm, you will download the ransomware found here. Extract it. Try to run the .sln file, windows will have you download an appropriate program to run it with (VisualStudio). You can choose to install a package from the web. Install VisualStudio 2019. You should install the .Net Desktop package when prompted. After installation (10 minutes), you should be able to open the sln file. You will want to right click on the form and view code. The only line of code that you should change should be the targetURL string. Point it to the ip of your kali machine or another website under your control. (Make sure you are NOT using https)

Before you build the project, you should navigate to the folder where this project is located. Find the form1.cs file and the form1.resx. Right click on them -> properties. Click `unblock` at the bottom of the general properties.

You can build the project by clicking on `build`-> `build solution`. Your new executable should be found in, the obj->debug directory. Don't run the executable until you do a few more things.

Create the Web site - Kali should have all the packages installed that you need but if not, install apache2, libapache2-mod-php, php7. In your document root (/var/www/html) you need to put the script that your code is looking for `write.php`. It should consist of the following code:

```
<?php
$x = $_GET['info'];
file_put_contents('foo.txt', $x );
?>
```

You need to also create foo.txt in that document root and chmod it 666. Also do a `service apache2 start` to start the webserver.

Create a `test` directory on your windows desktop. Any file you place in this directory will be encrypted by the ransomware.

You will then be able to run the ransomware encrypt/decrypt.

I had to rebuild the decrypter software and it was successfully able to decrypt.

TO pass off

Prove that you can do this.