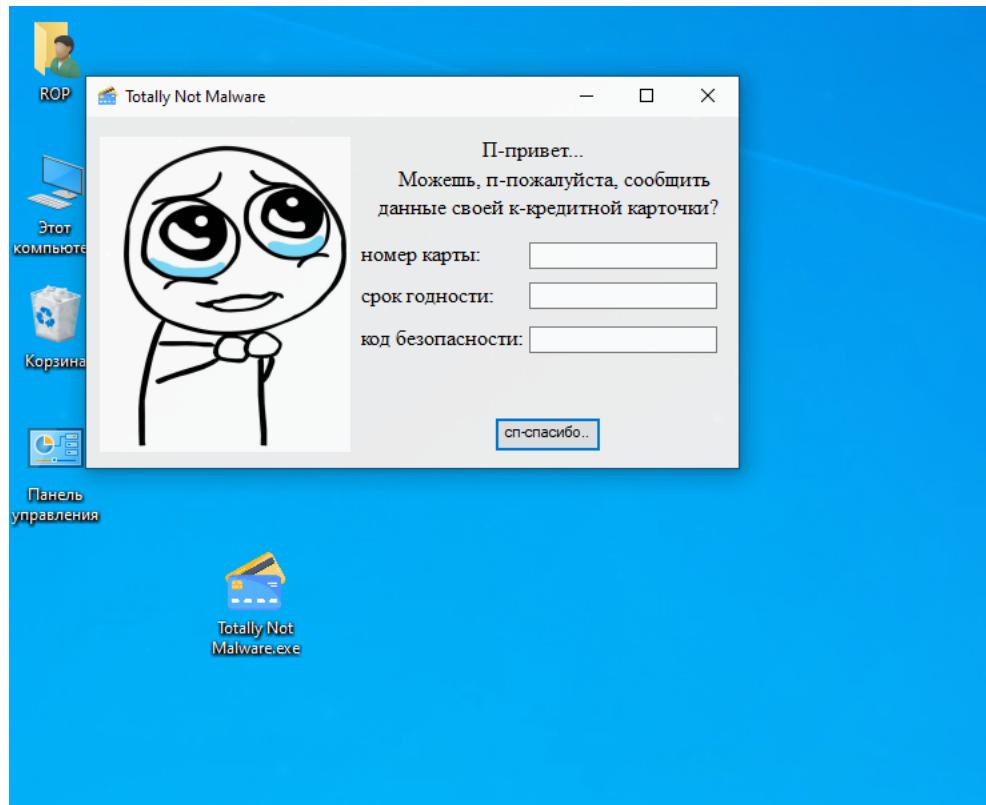




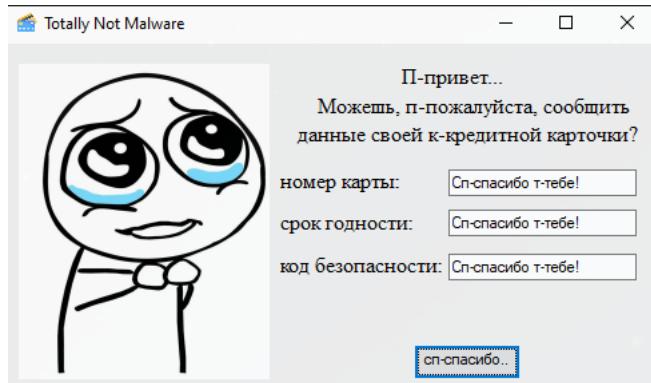
|            |  |
|------------|--|
| Название:  | П-пожалуйста, запусти этот файл                        |
| Категория: | Реверс-инжиниринг                                      |
| Уровень:   | Легко  |
| Очки:      | 250  |
| Описание:  | Я п-прошу тебя зап-п-пусти этот файл и в-введи данные. |
| Теги:      | .NET Framework   |
| Автор:     | ROP  |

Прохождение:

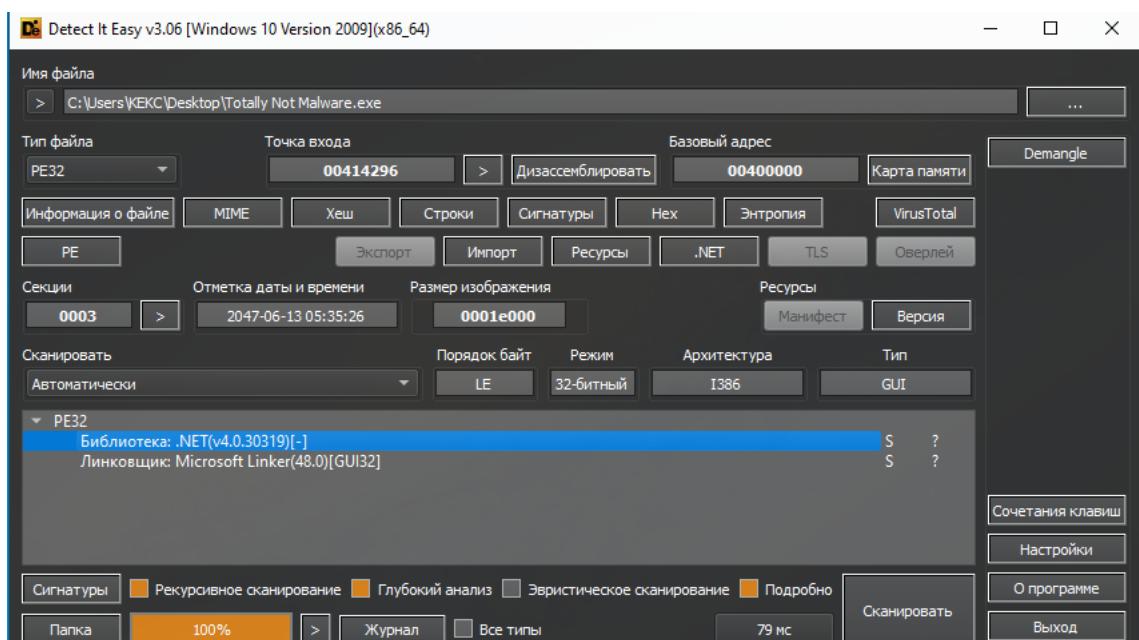
Распаковываем архив и пробуем запустить.



Нас просят данные карты. Окей.



Ничего не получаем. Идём в DIE.



Имя файла  
C:\Users\KEKC\Desktop\Totally Not Malware.exe

Тип файла  
PE32

Точка входа  
00414296

Базовый адрес  
00400000

Карта памяти

Demangle

Информация о файле  
MIME  
Хеш  
Строки  
Сигнатуры  
Нек  
Энтропия  
VirusTotal

РЕ

Экспорт  
Импорт  
Ресурсы  
.NET  
TLS  
Оверлей

Секции  
0003  
Отметка даты и времени  
2047-06-13 05:35:26

Размер изображения  
0001e000

Ресурсы  
Манифест  
Версия

Сканировать  
Автоматически

Порядок байт  
LE

Режим  
32-битный

Архитектура  
I386

Тип  
GUI

РЕ32

Библиотека: .NET(v4.0.30319)[-]  
Линковщик: Microsoft Linker(48.0)[GUI32]

Сочетания клавиш  
Настройки  
О программе  
Выход

Сигнатуры  
Рекурсивное сканирование  
Глубокий анализ  
Эвристическое сканирование  
Подробно

Папка  
Журнал  
Все типы

100%  
79 мс

Сканировать

.NET. Хорошо, идём в DnSpy.

Мы не нашли флаг в DnSpy, но нашли это.

```

Form1.cs
69     string text3 = this.textBox3.Text;
70     string text4 = "C0DEBY{ThIs_15_a_N0t_F1@g}";
71     string text5 = "C0DEBY{ThIs_15_a_N0t_F1@g}";
72     string text6 = "41 is a key";
73     byte[] array = new byte[]
74     {
75         2,
76         14,
77         5,
78         4,
79         3,
80         24,
81         58,
82         2,
83         50,
84         41,
85         32,
86         51,
87         17,
88         30,
89         50,
90         115,
91         49,
92         4,
93         51,
94         30,
95         18,
96         53,
97         51,
98         0,
99         47,
100        6,
101        115,
102        60
103    };
104    char c = text6[0];
105    byte b = array[0];
106    char c2 = text4[0];
107    char c3 = text5[0];

```

Ложные флаги, строка, говорящая о том, что 41 - ключ и массив байт. Идём в кибершеф.

<https://cyberchef.org/>

2, 14, 5, 4, 3, 24, 58, 2, 50, 41, 32, 51, 17, 30, 50, 115, 49, 4, 51, 30, 18, 53, 51, 0, 47, 6, 115, 60

Берём файл "Totaly Not Hint.txt". Вот информация из него:

```

00110110 00110101 00100000 00110110 00110011 00100000 00110100 00110000 00100000 00110110 0011
0101 00100000 00110110 00110011 00100000 00110100 00110000 00100000 00110110 00110011 00100000
00110110 00110010 00100000 00110100 00110000 00100000 00110110 00110101 00100000 00110110 0011
0100 00100000 00110100 00110000 00100000 00110111 00110001 00100000 00110111 00110000 00100000
00110100 00110000 00100000 00110110 00110011 00100000 00110110 00110010 00100000 00110100 0011
0000 00100000 00110110 00110101 00100000 00110110 00110001 00100000 00110100 00110000 00100000
00110110 00110101 00100000 00110110 00110111 00100000 00110100 00110000 00100000 00110110 0011
0011 00100000 00110110 00110010 00100000 00110100 00110000 00100000 00110110 00110101 00100000
00110110 00110011 00100000 00110100 00110000 00100000 00110110 00110101 00100000 00110110 0011
0111

```

Опытным путём декодируем сообщение:

[https://cyberchef.org/#recipe=From\\_Binary\('Space',8\)From\\_Octal\('Space'\)From.Decimal\('Space',false\)Za-z0-%2B%3D',true,false\)&input=MDAxMTAxMTAgMDAxMTAxMDEgMDAxMDAwMDAgMDAxMTAxMTAgMDAxMTAwMTEgMDAxMDAwMI](https://cyberchef.org/#recipe=From_Binary('Space',8)From_Octal('Space')From.Decimal('Space',false)Za-z0-%2B%3D',true,false)&input=MDAxMTAxMTAgMDAxMTAxMDEgMDAxMDAwMDAgMDAxMTAxMTAgMDAxMTAwMTEgMDAxMDAwMI)

Получили: ROX

Читаем задом-наперёд и получаем XOR.

Пробуем ключ 41 в CyberChef.

The screenshot shows the CyberChef interface version 10.4.0. The left sidebar contains a list of operations under the 'Operations' category, including xor, XOR, XOR Brute Force, XKCD Random Number, Hex to Object Identifier, Unicode Text Format, Text Encoding Brute Force, Lorenz, and Magic. A 'Favourites' section is also present. The main workspace is titled 'XOR' and shows a 'From Decimal' recipe. The input field contains the decimal numbers 2, 14, 5, 4, 3, 24, 58, 2, 50, 41, 32, 51, 17, 30, 50, 115, 49, 4, 51, 30, 18, 53, 51, 9, 47, 6, 115, 60. The output field displays the resulting hex values: +1, -1, +5, +4, +3, +24, +58, +2, +50, +41, +32, +51, +17, +30, +50, +115, +49, +4, +51, +30, +18, +53, +51, +9, +47, +6, +115, +60. A green button labeled 'BAKE!' is visible at the bottom of the workspace.

Это не 10-ая система. Это 16-ая система! А там уже флаг