**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. проф. М. А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра «Защищенные системы связи»

Дисциплина «Компьютерные вирусы»

# Лабораторная работа № 2

**«** **Malware Static Analysis»**

Выполнил: Громов А.А.

Миколаени М.С.

ИКТЗ-83

Проверил: Косов Н. А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург

2021

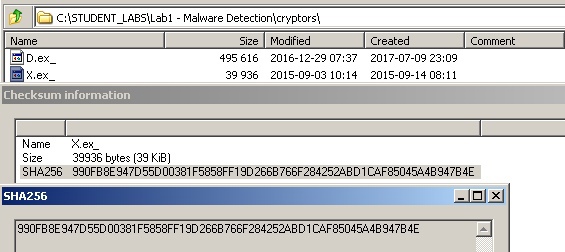
**Часть 1**

Рис. 1 Посчитали sha-256

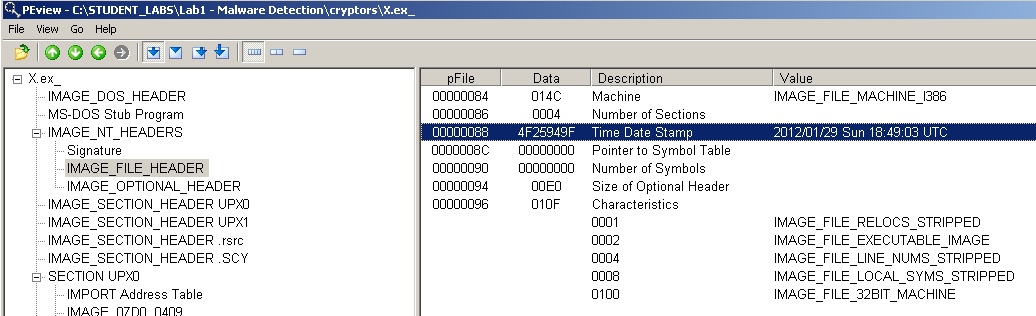


Рис. 2 Открыли X.exe в PEview.

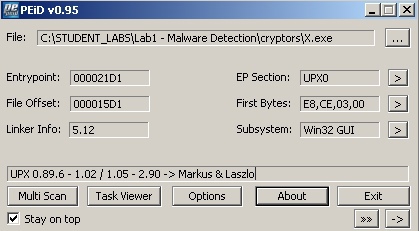


Рис.3 Открыли X.exe в PEID

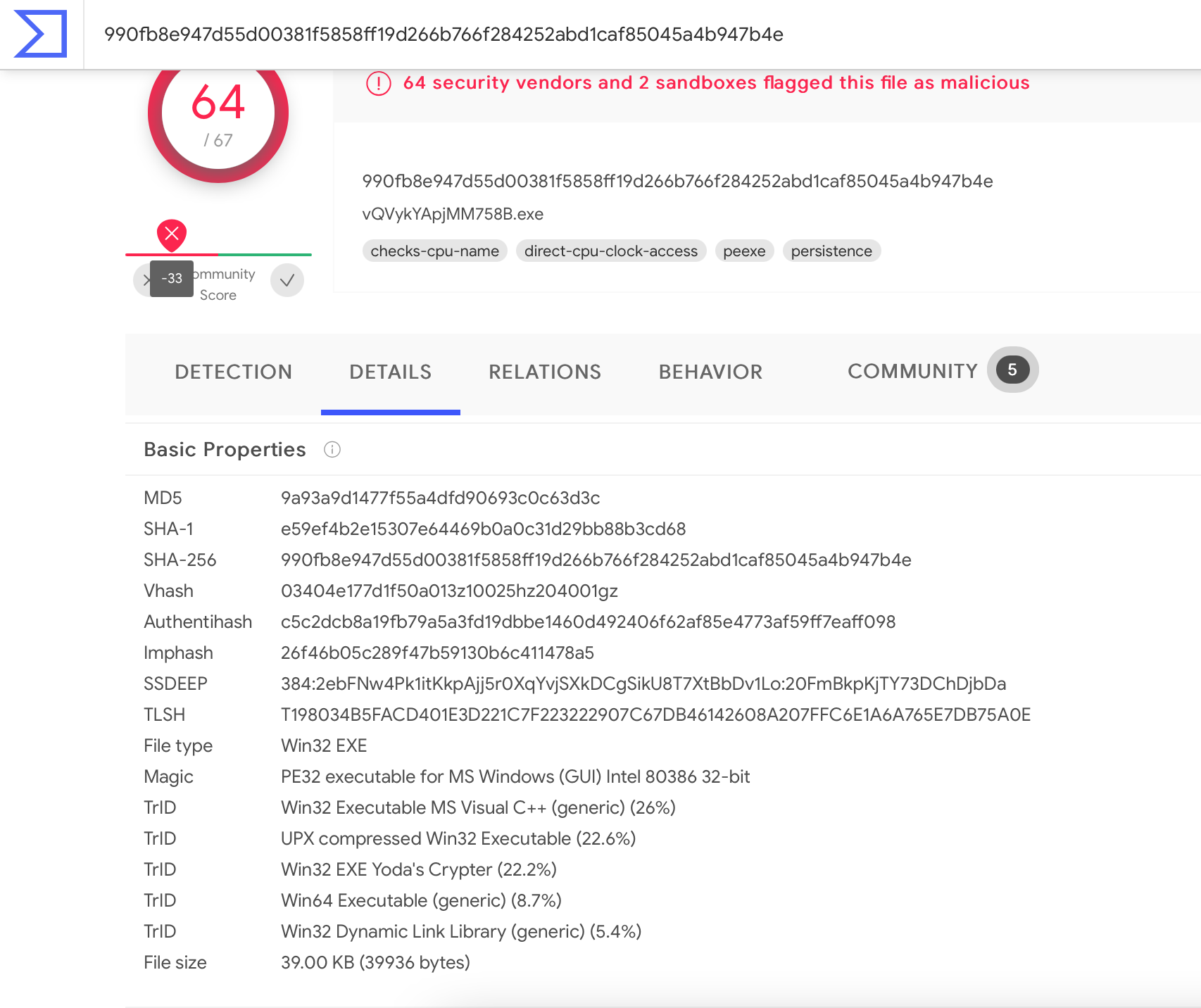


Рис. 4 Узнали язык программирования вируса

|  |  |
| --- | --- |
| File name | x.exe |
| Filesize | 40KB |
| Hash | 9a93a9d1477f55a4dfd90693c0c63d3c E59EF4B2E15307E64469B0A0C31D29BB88B3CD68 990FB8E947D55D00381F5858FF19D266B766F284252ABD1CAF85045A4B947B4E |
| Imports | Addres table, Name table, Directory table, Hints/Names&DLL Names |
| Exports | - |
| Time Date Stamp | 2012/01/29 |
| Sections | UPX0, UPX1, .rsrc, .SCY |
| Subsystem | IMAGE\_SUBSYSTEM\_WINDOWS\_GUI |
| Resources | Несколько картинок |
| Packer | UPX packer |
| Compiler/Language | MS Visual C++ |
| Detection | 64/67 |

**Часть 2**

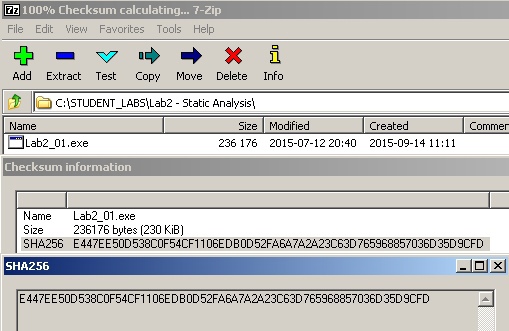


Рис. 5 Посчитали sha-256

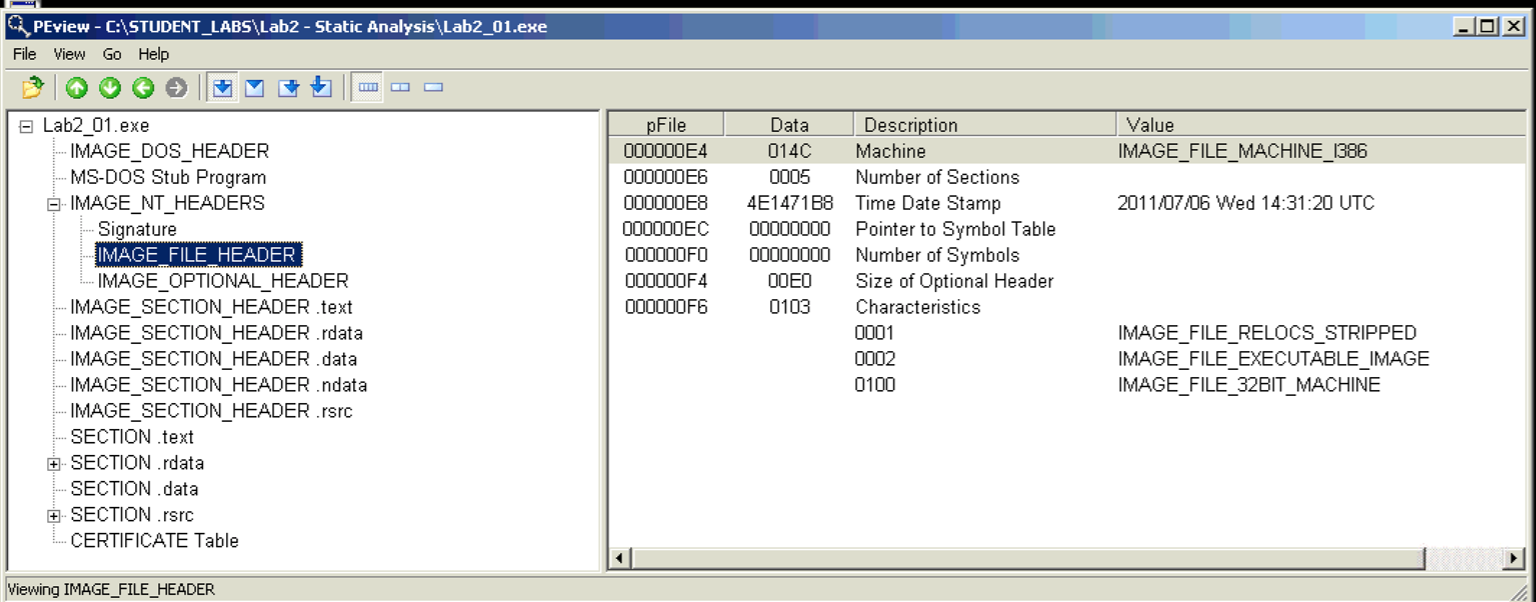
****

Рис. 6 Открыли Lab2\_01.exe в PEview.

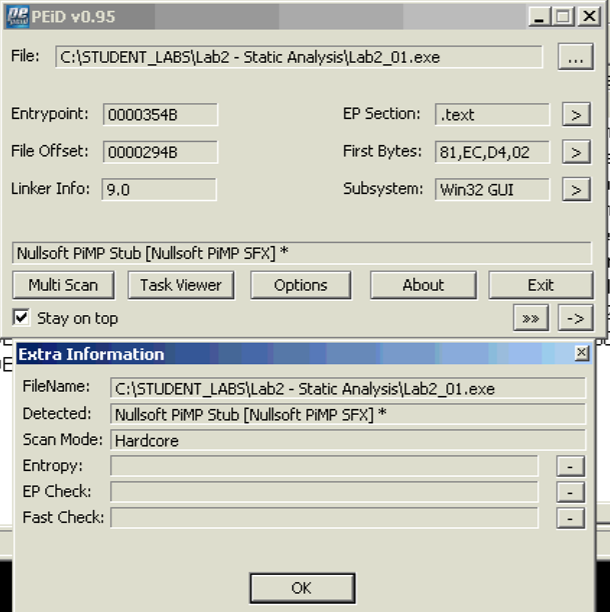


Рис. 7 Открыли Lab2\_01..exe в PEID

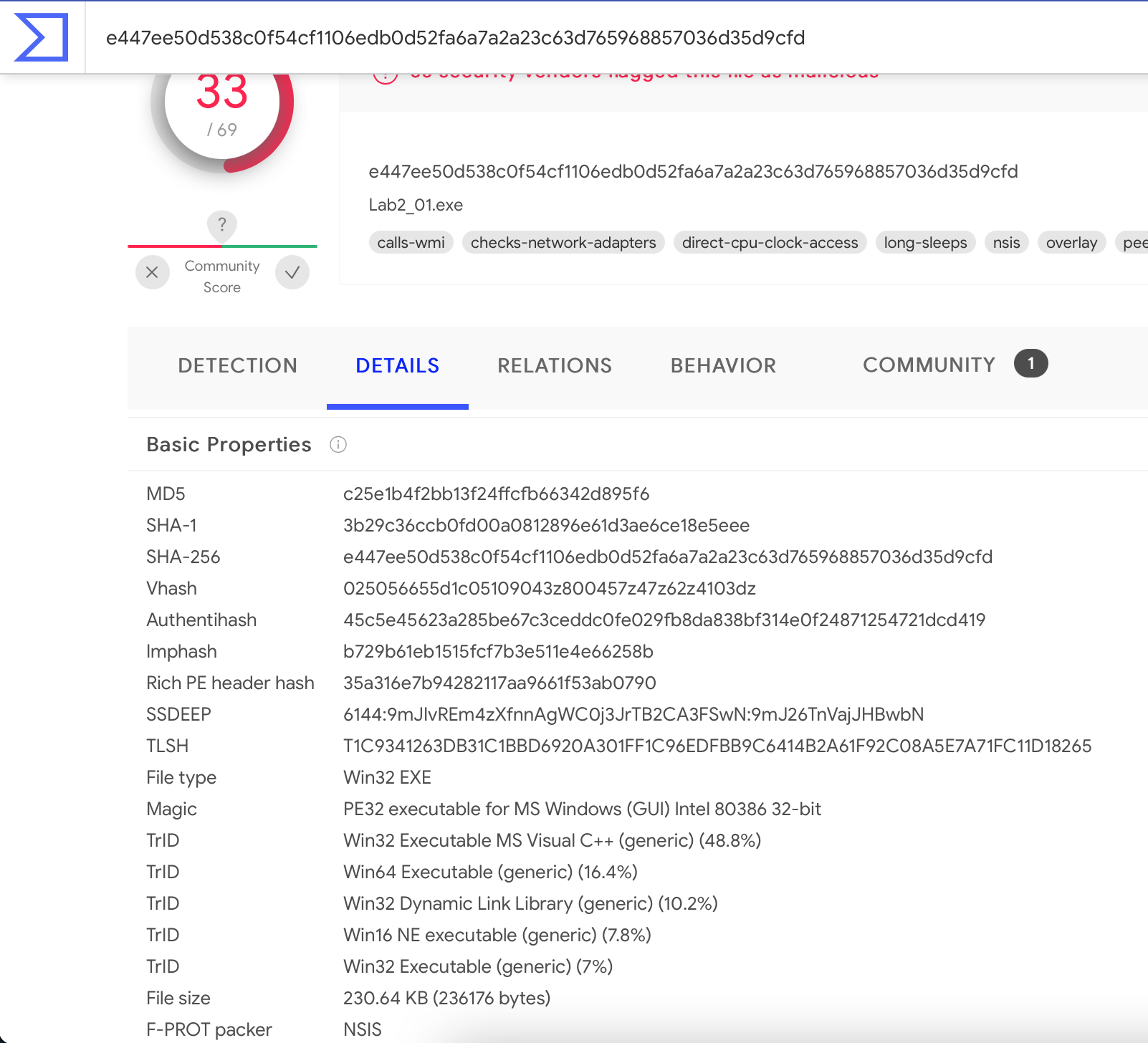


Рис. 8 Узнали язык программирования вируса

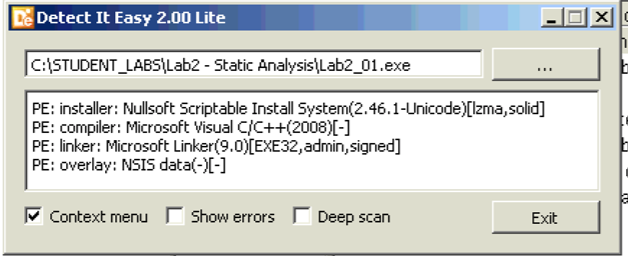


Рис. 9 Убедились, что язык программирования С++

|  |  |
| --- | --- |
| File name | Lab2\_01.exe |
| Filesize | 230KB |
| Hash | c25e1b4f2bb13f24ffcfb66342d895f63B29C36CCB0FD00A0812896E61D3AE6CE18E5EEEE447EE50D538C0F54CF1106EDB0D52FA6A7A2A23C63D765968857036D35D9CFD |
| Imports | Addres table, Name table, Directory table, Hints/Names&DLL Names |
| Exports | - |
| Time Date Stamp | 2011/07/06 |
| Sections | .text, .data, .rsrc, .rdata, .ndata |
| Subsystem | IMAGE\_SUBSYSTEM\_WINDOWS\_GUI |
| Resources | Несколько картинок |
| Packer | Nullsoft PiMP Stub [Nullsoft PiMP SFX] \* |
| Compiler/Language | MS Visual C++ |
| Detection | 33/69 |