**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 № 3

**«** **Malware Dynamic Analysis »**

Выполнил: Громов А.А.

Миколаени М.С.

ИКТЗ-83

Проверил: Косов Н. А.

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

Санкт-Петербург

2021

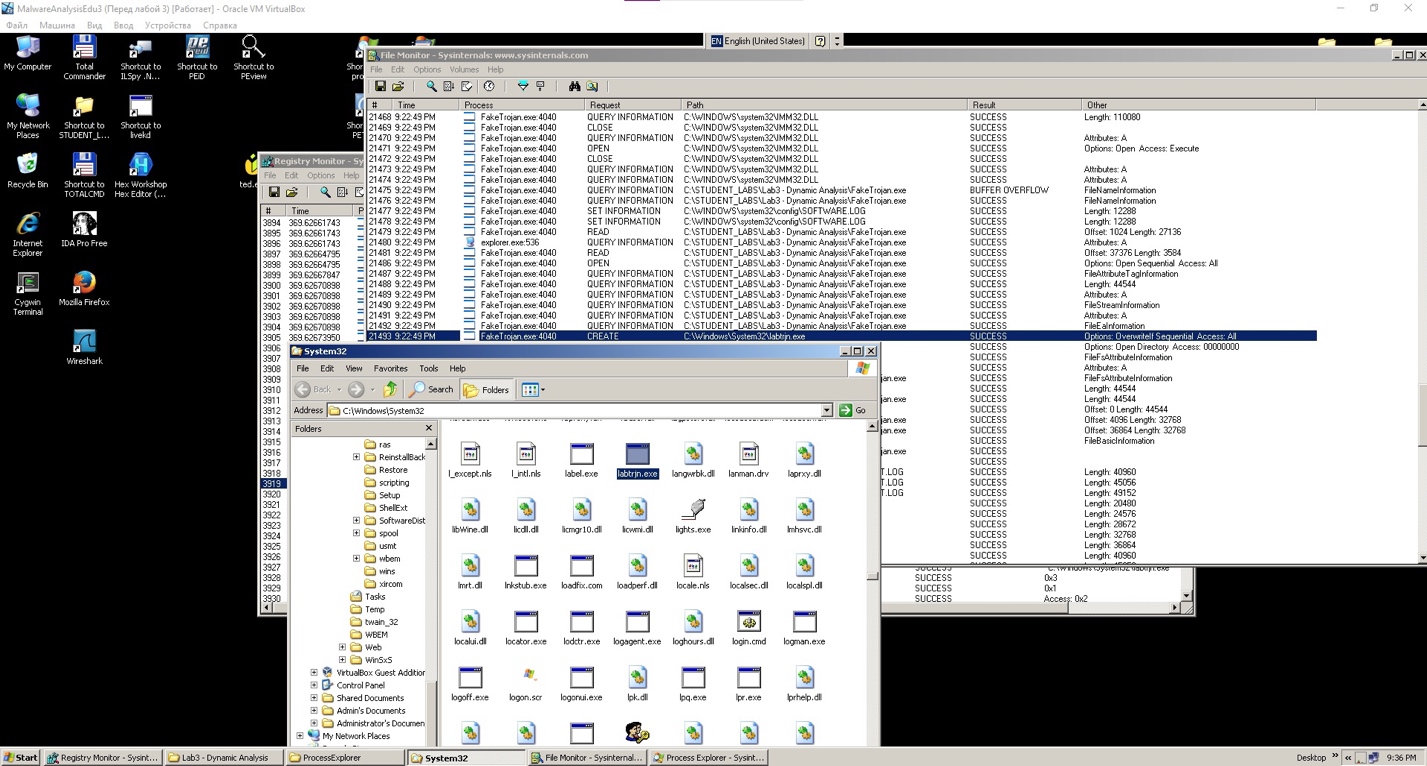


Рис. 1 Нашли labtrjn.exe в папке C:\Windows\System32

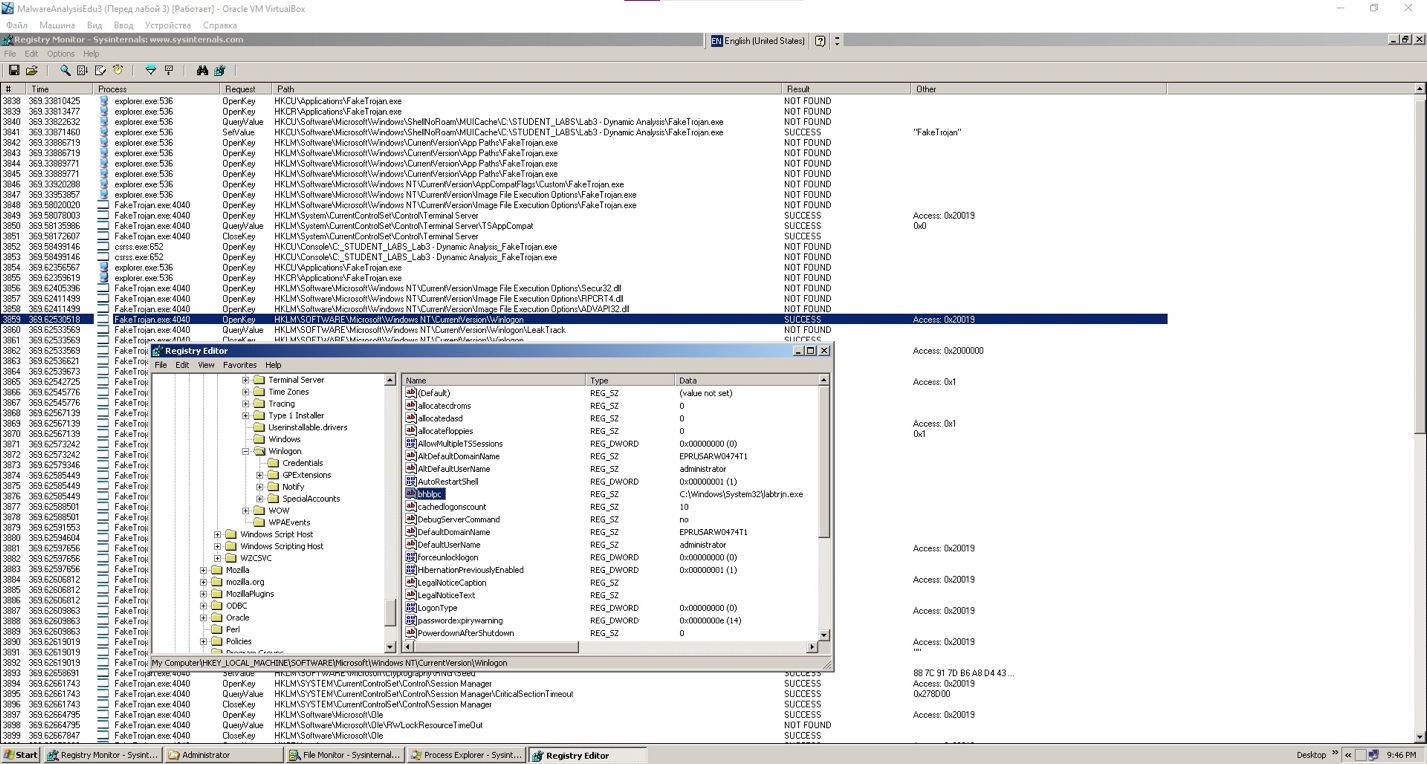


Рис. 2 Добавление пути к вирусу в winlogon

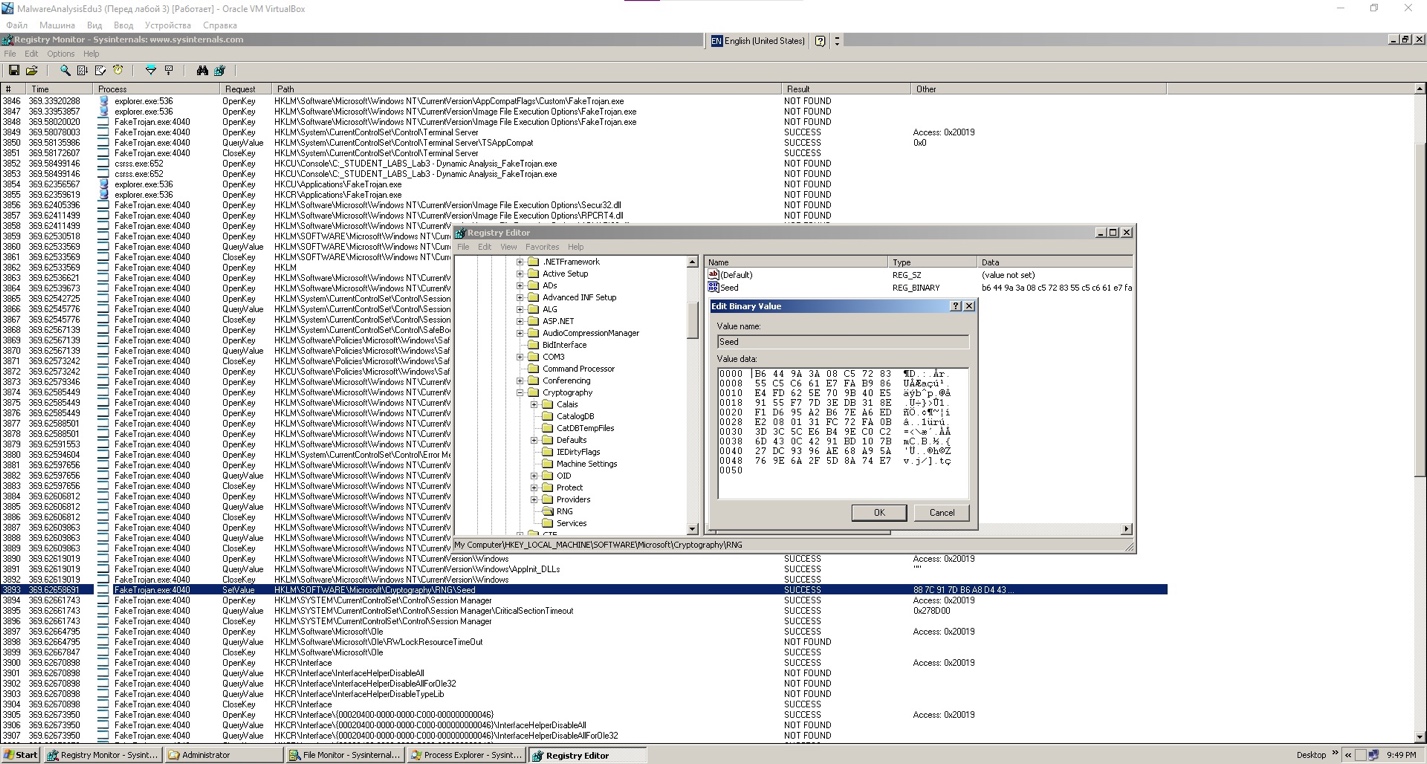


Рис.3 добавление seed

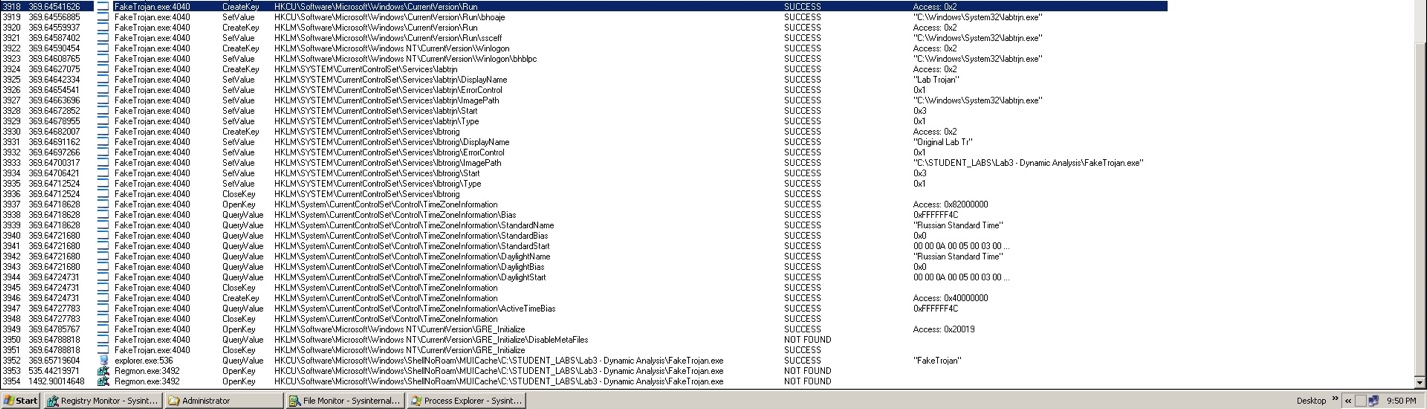


Рис. 4 Проводит манипуляции с TimeZone

При запуске файла faketrojan.exe он производит следующие действия:  
1) Создает в папке C:/Windows/System32 файл labtrjn.exe  
2) Вносит его в ветку реестра HKLM/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon  
3) Создает seed в hklm/software/microsoft/cryptography/rng/seed  
4) Заносит себя в HKCU/SOFTWARE/Microsoft/Windows/CurrentVersion/Run, HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Run, HKLM/SYSTEM/CurrentControlSet/Services