**Отчёт**

Процесс: **eicar.exe**

PID: **11816**

PID: **12204**

|  |
| --- |
| eicar.exe (12204) C:\Users\elk\Desktop\eicar.exe <graph> WIN10\elk "C:\Users\elk\Desktop\eicar.exe" 18.03.2024 16:29:36 18.03.2024 16:29:44 |

|  |
| --- |
| eicar.exe (11816) C:\Users\elk\Desktop\eicar.exe <graph> NT AUTHORITY\СИСТЕМА C:\Users\elk\Desktop\eicar.exe 18.03.2024 16:00:00 n/a |





**Активность:**

- Создал: cmd.exe, conhost.exe

- Путь: C:\Users\elk\Desktop\eicar.exe

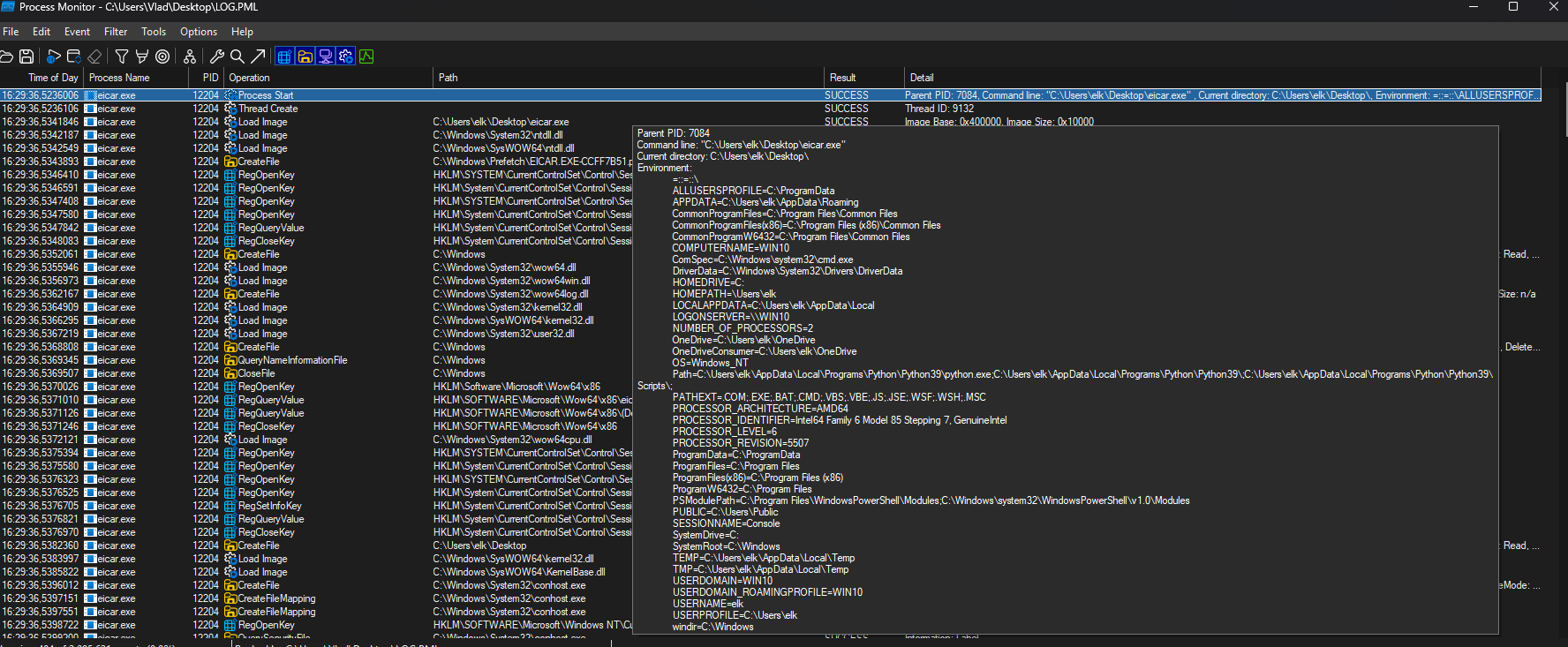
- Файлы: C:\Users\elk\AppData\Local\Temp\CVTUDCB6.bat

- Старт: 18.03.2024 16:00:00 | 18.03.2024 16:29:36

- Конец: n/a | 18.03.2024 16:29:44

- Реестр: HKLM\System\CurrentControlSet\Services\bam\UserSettings\...\eicar.exe

- Сеть: Отсутствует



**Хронология:**

---------------------------------------------------------------------------------------

Инициатор: Explorer.EXE

Процесс: eicar.exe (PID: 12204)

Путь: C:\Users\elk\Desktop\eicar.exe

Командная строка: "C:\Users\elk\Desktop\eicar.exe"

---------------------------------------------------------------------------------------

Действие: Process Create

Родитель: eicar.exe (12204)

Процесс: conhost.exe (PID: 8924)

Командная строка: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Назначение: Создание консоли для выполнения команд

---------------------------------------------------------------------------------------

Действие: Process Create

Родитель: eicar.exe (12204)

Процесс: cmd.exe (PID: 12748)

Командная строка: C:\Windows\Sysnative\cmd.exe /c ""C:\Users\elk\AppData\Local\Temp\CVTUDCB6.bat" "C:\Users\elk\Desktop\eicar.exe" "

---------------------------------------------------------------------------------------

16:29:44,5441457 - cmd.exe регистрируется в BAM

Путь: HKLM\System\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-3169843388-1045293179-3196199937-1001\\Device\HarddiskVolume4\Windows\System32\cmd.exe

16:29:44,5463478 - eicar.exe регистрируется в BAM

Путь: HKLM\System\CurrentControlSet\Services\bam\UserSettings\S-1-5-21-3169843388-1045293179-3196199937-1001\\Device\HarddiskVolume4\Users\elk\Desktop\eicar.exe

---------------------------------------------------------------------------------------

**Классификация:**

- Тип: Тестовый файл

- Уровень угрозы: Низкий

- Логика: Проверка антивирусной системы

**Причина:**

1. Нестандартное расположение файла

|  |
| --- |
| Путь: C:\Users\elk\Desktop\eicar.exe |
| Проблема: Легитимные программы не запускаются с рабочего стола |
| Норма: Program Files, System32, Windows |

2. Использование временных файлов

|  |
| --- |
| Действие: Запуск BAT-файла из Temp |
| Путь: C:\Users\elk\AppData\Local\Temp\CVTUDCB6.bat |
| Проблема: Легитимные программы не используют временные BAT-файлы |

3. Работа через командную строку

|  |
| --- |
| Действие: Создание cmd.exe |
| Команда: C:\Windows\Sysnative\cmd.exe /c "..." |
| Проблема: Пользовательские приложения не запускают cmd.exe |

5. Регистрация в системном мониторинге

|  |
| --- |
| Раздел: HKLM\System\CurrentControlSet\Services\bam\UserSettings\ |
| Процессы: eicar.exe и cmd.exe |
| Проблема: Легитимные программы не прописываются в BAM |

Вывод: Исходя из проанализированной информации об активности, данное ВПО принадлежит к виду: **Тестовый файл**. (EICAR-Test-File)