Т.к. Immunity работает лишь с x86,

для первых образцов возьмём найденные в сети

исходные коды вирусов и скомпилируем их под

соответствующую платформу.

UPDATE: удалось найти 3 сайта, бесплатно предоставляющих уже готовые образцы.

Мониторинг API, пути:

1. Перехватывающая вызовы API DLL (пр.: Microsoft Detours);

В том числе : AppInit\_DLL – но лишь при использовании user32.dll.

1. Перехватывающий вызовы API драйвер (пр.: Process Hacker);
2. В отладчике.
3. Процедуры, выполняющие уведомления о создании процесса/ потока/ загрузке образа в память (пр.: ProcMon, Process и Thread events).