Современные Руткит/Антируткит технологии

Дмитрий Варшавский,
Ведущий программист ОДО «ВирусБлокАда»

Руткиты: общие сведения

Руткит – программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

Системы: **Windows**, Unix

Уровень привелегий: User Mode, **Kernel Mode**

Сокрытие: захват кода, модификация данных (в памяти и на диске)

Руткиты: эволюция

- Джефри Рихтер: методы внедрения DLL, создание удалённых потоков и т.п.
- Vanquish
- FU, NtRootKit, ресурс rootkit.com (Грег Хогланд, Джеймс Батлер)
- …
- Rustock
- …
- TDL v3, MAX++ и т.п.

Руткиты: задачи

- Сокрытие вредоносного ПО, осуществляющего удалённое управление компьютером, сбор информации, кражу информации, подмену поисковых запросов и т.п.
- Сокрытие сопутствующей сетевой активности

Руткиты: актуальность

- Руткит – коммерческий продукт

```
[main]
quote=You people voted for Hubert Humphrey, and you killed Jesus
version=3.27
botid=105ef377-e1a7-42d0-a324-30096d7a9bf1
affid=20223
subid=0
installdate=25.2.2010 13:59:41
builddate=24.2.2010 17:25:9
[injector]
*=tdlcmd.dll
[tdlcmd]
servers=https://d45648675.cn/;https://d92378523.cn/;https://91.212.226.65/
wspservers=http://jook877x.cc/;http://b11335599.cn/
popupservers=http://m3131313.cn/
version=3.741
```

Антируткиты

- **PoC**
  - Klister
  - Process Hunter
- **Независимые разработчики**
  - GMER
  - RkU
  - XueTr
- **Вендоры**
  - Vba32 Arkit

Варианты присутствия

- Собственный файл на диске
  (48EfX3lq.sys; msinfox.sys; userinit.exe)
- Модифицированный системный либо пользовательский файл (atapi.sys, руткит TDL3; AdobeUpdater.exe)
- Модифицированный загрузчик (буткит Sinowal/Mebroot)

Методы сокрытия

- Захват кода
- Модификация данных

Пример. Скрытый процесс

- Задача 1. Скрыть процесс из диспетчера задач

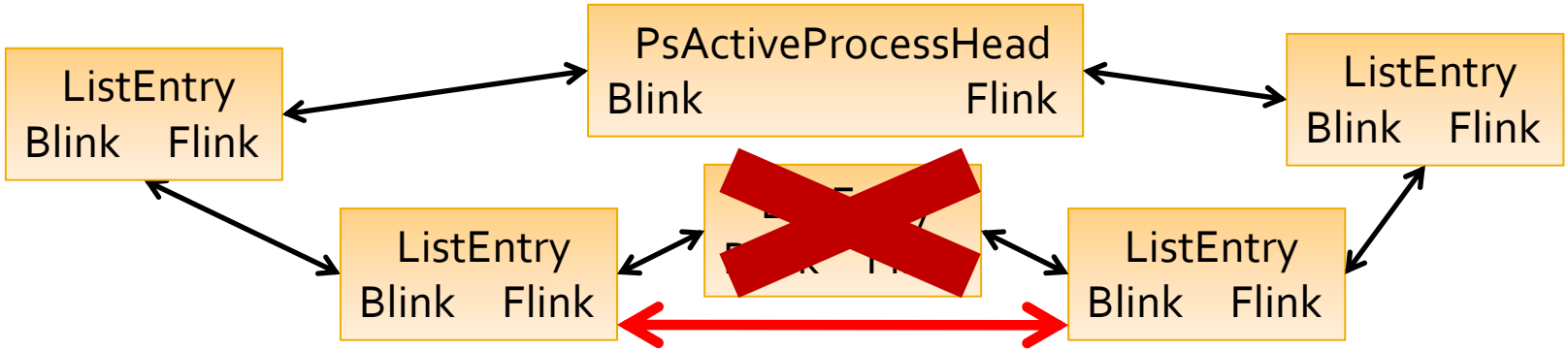
- Задача 2. Скрыть процесс от антируткита

Методы сокрытия: процессы

- Перехват системных функций на различных уровнях
  NtQuerySystemInformation (SystemProcessInformation,…)
  - Сплайсинг NtQuerySystemInformation в ntdll.dll
  - Перехват int 2E / SysEnter
  - Подмена сервиса в таблице SSDT, сплайсинг в ядре

- Модификация внутренних структур операционной системы (DKOM)

nt!PsActiveProcessHead - Unlink



Методы сокрытия: процессы

```
dt nt!_EPROCESS
  +0x000 Pcb          : _KPROCESS
  +0x0b4 UniqueProcessId  : Ptr32 Void
  +0x0b8 ActiveProcessLinks : _LIST_ENTRY
  ...
  +0x0f4 ObjectTable     : Ptr32 _HANDLE_TABLE
  +0x0f8 Token          : _EX_FAST_REF
  ...
  +0x0e4 SessionProcessLinks : _LIST_ENTRY
  ...
  +0x1f0 Vm           : _MMSUPPORT
    +0x000 WorkingSetMutex  : _EX_PUSH_LOCK
    +0x004 ExitGate       : Ptr32 _KGATE
    +0x008 AccessLog      : Ptr32 Void
    +0x00c WorkingSetExpansionLinks : _LIST_ENTRY
    ...
  ...
  +0x25c MmProcessLinks   : _LIST_ENTRY
  ...
```

```
dt nt!_HANDLE_TABLE
  +0x000 TableCode      : Uint4B
  +0x004 QuotaProcess    : Ptr32 _EPROCESS
  +0x008 UniqueProcessId  : Ptr32 Void
  +0x00c HandleLock      : _EX_PUSH_LOCK
  +0x010 HandleTableList  : _LIST_ENTRY
  +0x018 HandleContentionEvent : _EX_PUSH_LOCK
```

CSRSS Handle Table

PspCidTable

Scheduler's lists

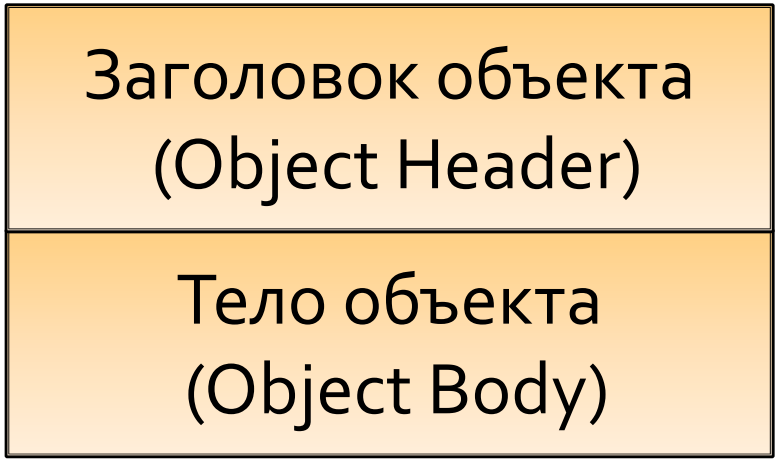
Balance manager's lists

Методы сокрытия: объекты ОС

Adapter	Event	PcwObject	TmRm
ALPC Port	EventPair	PowerRequest	TmTm
Callback	File	Process	TmTx
Controller	FilterCommunicationPort	Profile	Token
DebugObject	FilterConnectionPort	Section	TpWorkerFactory
Desktop	IoCompletion	Semaphore	Type
Device	IoCompletionReserve	Session	UserApcReserve
Directory	Job	SymbolicLink	WindowStation
Driver	Key	Thread	WmiGuid
EtwConsumer	KeyedEvent	Timer	
EtwRegistration	Mutant	TmEn	

Методы сокрытия: объекты ОС

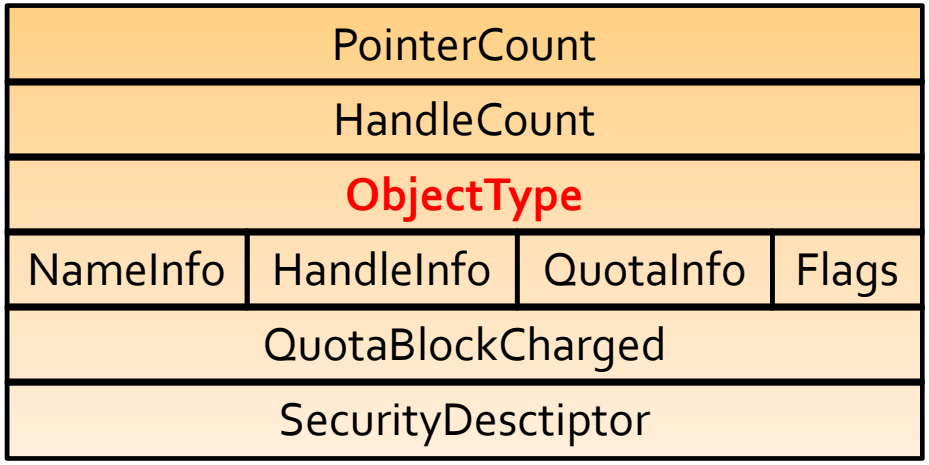
- Модификация заголовка объекта
- Модификация тела объекта



Методы сокрытия: объекты ОС

- **Модификация заголовка объекта**
- Модификация тела объекта

Заголовок объекта (Object Header)




```
NTSTATUS ObReferenceObjectByPointer  ( .. )
{
...
   if ( ObjectHeader->Type  !=  ObjectType )
      return  STATUS_OBJECT_TYPE_MISMATCH ;
...
```

Методы сокрытия: объекты ОС

- Модификация заголовка объекта
- **Модификация тела объекта**

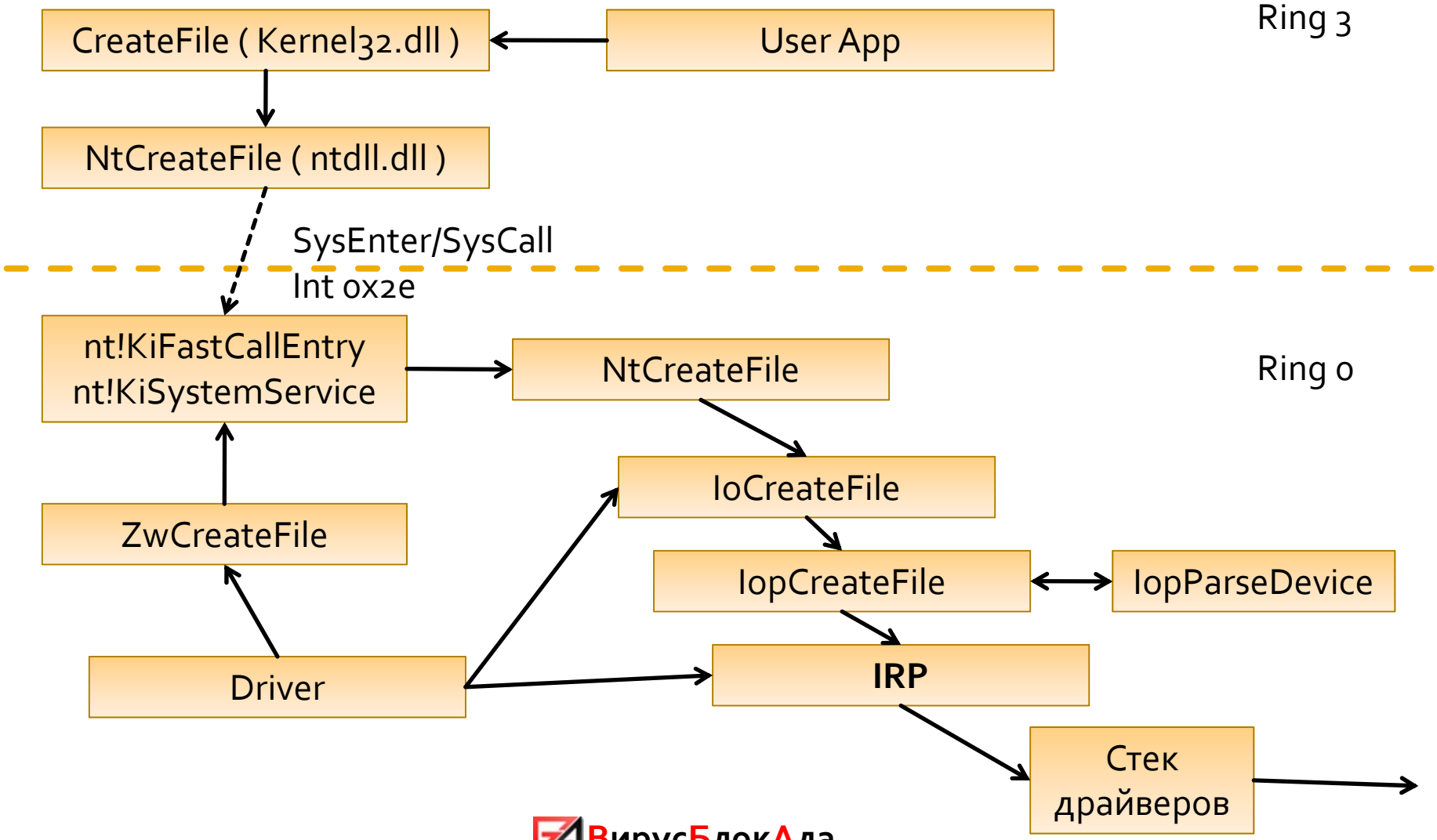
Тело объекта (Object Body)

```
dt nt!_EPROCESS
..
  +0x0b4 UniqueProcessId  : Ptr32 Void
  ..
  +0x16c ImageFileName    : [15] UChar
  ..
  +0x1ec SeAuditProcessCreationInfo :
_SE_AUDIT_PROCESS_CREATION_INFO
  ..
```

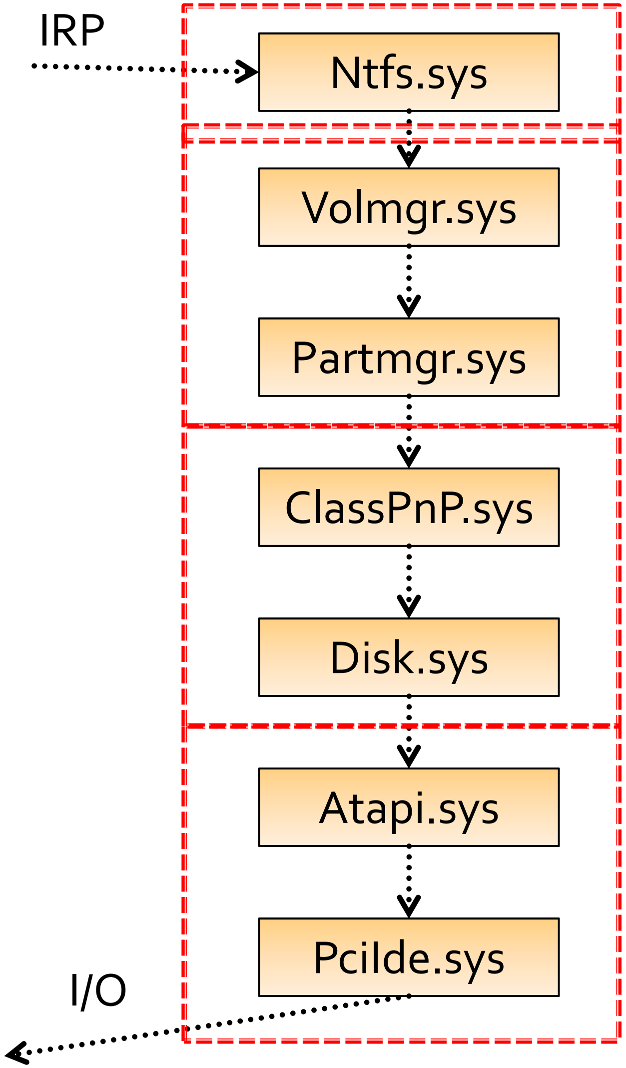
Обнаружение скрытых процессов

- Анализ двухсвязных списков SessionProcessLinks, WorkingSetExpansionLinks, MmProcessLinks и т.п.
- Поиск по списку таблиц хэндлов, а также в самих таблицах
- Поиск в PspCidTable
- Использование нотификаторов PsSetLoadImageNotifyRoutine, PsSetCreateProcessNotifyRoutine, PsSetCreateThreadNotifyRoutine
- NtQuerySystemInformation с параметром SystemObjectInformation
- Анализ списков планировщика и баллансировщика
- Перехват функций – SwapContext, KiFastCallEntry, ObCreateObject и т.п.
- Эвристический поиск структур _KTHREAD/_ETHREAD и _KPROCESS/_EPROCESS в пуле
- Поиск и анализ дублированного кода ntoskrnl.exe
- …

Файловая система



Стек драйверов: внедрение и методы противодействия



Уровень драйверов ATA/ ... PCI

Пример: TDL2 / Rustock

Пример: TDL3 / MBR Rootkit

Методы противодействия:

Восстановление перехватов

- ... файловой системы

- ... (обслуживание прерываний и т. п.)

Обсуждение и вопросы

Спасибо за внимание!

ВирусБлокАда