

Hypersight Rootkit Detector

Антируткит нового поколения

North Security Labs

www.northsecuritylabs.com

Введение

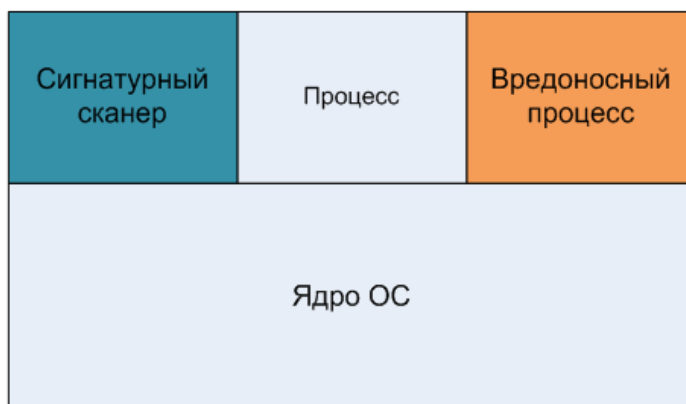
В последнее время наблюдается устойчивый рост использования руткит-технологий во вредоносных программах. Руткит-технология – это набор методов для скрытия программного обеспечения на компьютере. Сами по себе руткит-технологии вреда не несут, но они могут использоваться для недопущения обнаружения вредоносных программ, что и происходит на практике. Эти технологии достаточно сложны, но в последнее время хакеры успешно их осваивают и применяют в своих вирусах (банковских троянцах, спам-ботах, adware и пр.)

Ситуация осложняется тем, что до сих пор не разработаны универсальные методы борьбы с руткитами режима ядра. Все существующие на данный момент системы информационной безопасности не способны эффективно обнаруживать вредоносные программы этого типа и противодействовать им.

Классификация систем информационной безопасности

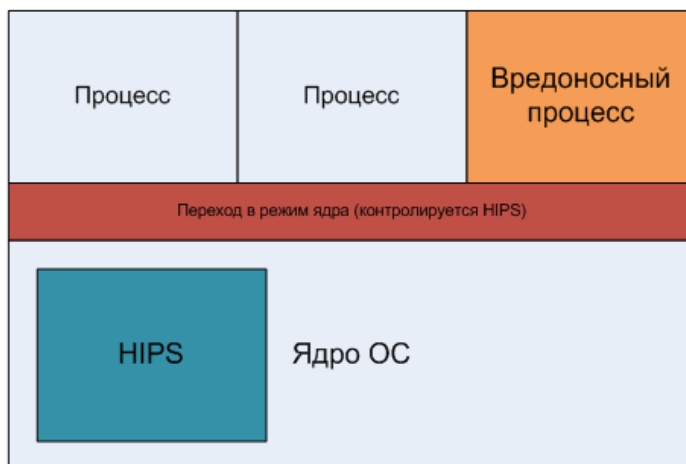
Системы информационной безопасности делятся на несколько типов. Это разделение нечеткое, возможны сочетания нескольких типов в одном и том же программном продукте.

1. Сигнатурные сканеры.



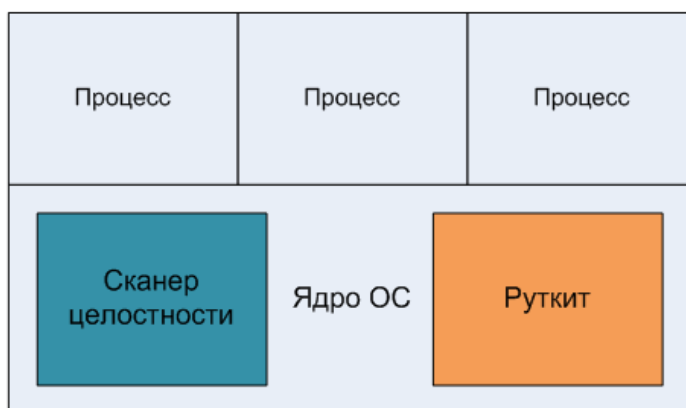
Это классические антивирусы. Они анализируют код в памяти и на диске с целью найти вредоносные программы по сигнатурам, контрольным суммам или эвристическим путем. Это самое первое поколение систем информационной безопасности. К сожалению, они неспособны обнаружить даже самые элементарные руткиты, поскольку те используют техники скрытия кода как на диске, так и в памяти.

2. Системы предупреждения вторжений (Host Intrusion Prevention Systems, HIPS).



Блокирующие антируткиты. Они работают в режиме ядра и блокируют вредоносные действия программ, выполняющихся в пользовательском режиме. Эти антируткиты показывают неплохие результаты против руткитов пользовательского режима, а также не допускают установки руткитов режима ядра. Однако они бессильны против уже запущенных в системе руткитов режима ядра.

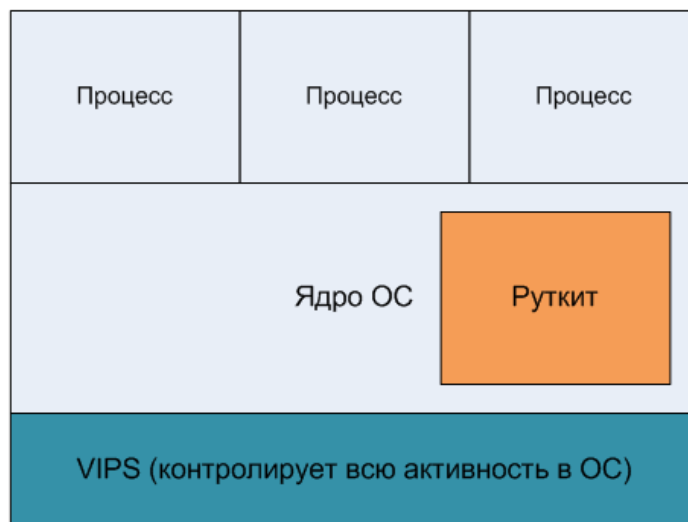
3. Сканеры целостности ядра (Integrity Scanners).



Это недавно появившийся класс антируткитов. Они пытаются обнаружить работающие руткиты режима ядра по результатам их деятельности (а именно, по изменениям кода или системных структур). Основные недостатки этих антируткитов: уязвимость, сложность и отсутствие универсальности. Современные ОС очень сложны и число участков кода/данных, которые нужно контролировать, исчисляется сотнями и тысячами. Поскольку сканеры целостности работают с тем же уровнем привилегий, что и вредоносное ПО режима ядра, они, в общем случае, бесполезны. В противостоянии между двумя программами, работающими с одним и тем же набором привилегий, победителя определяет мастерство и интеллект их авторов. Не составляет труда, располагая информацией о сканере целостности, разработать невидимый для него руткит. Кроме того, сканеры целостности не изолированы от руткитов режима ядра, поэтому они сравнительно легко могут быть заблокированы руткитами.

Мы предлагаем новый тип систем информационной безопасности.

4. Виртуальная система предупреждения вторжений (Virtual Intrusion Prevention System, VIPS).



Система использует технологию аппаратной виртуализации. Она работает в режиме гипервизора на процессорах, поддерживающих эту технологию. При этом операционная система работает в виртуальной машине, а все события в ней контролируются VIPS. Действия, свойственные вредоносным программам, перехватываются VIPS с целью оповещения пользователя, затем вредоносный код может быть изолирован в «песочнице» (sandbox). В идеальном случае работа такой системы незаметна для вредоносного ПО.

Hypersight Rootkit Detector – первый шаг на пути реализации VIPS

Hypersight Rootkit Detector – программа, предназначенная для обнаружения вредоносной активности в режиме ядра ОС Windows NT. Поддерживаются следующие версии ОС: Windows 2000, Windows XP, Windows Server 2003.

Hypersight RD – это монитор виртуальной машины. Ядро Hypersight RD запускается в режиме гипервизора при старте компьютера. Оно контролирует критические операции и работает прозрачно для операционной системы и всех программ, запущенных в ней.

Hypersight RD перехватывает следующие потенциально опасные действия:

- Модификация таблицы страниц. Данный тип активности свойственен руткитам, скрывающим себя в памяти (тип руткитов, известный как shadow walker)
- Модификация секций исполняемых модулей режима ядра, доступных только для чтения. Это свойственно большинству руткитов

- Модификация GDT, IDT. Это используется руткитами типа shadow walker, а также иными руткитами

Вышеприведенные действия являются недопустимыми с точки зрения Microsoft и не используются драйверами, получившими Windows Logo. Однако они используются в руткитах, а также в некоторых системах информационной безопасности и защитах от копирования.

Любое из этих действий перехватывается Hypersight RD, после чего пользователь оповещается о том, какой драйвер его пытался выполнить. Таким образом решается задача обнаружения руткитов режима ядра (стоит заметить, что сканеры целостности ядра не способны в общем случае ее решить).

Способы, применяемые руткитами для обхода защиты памяти от записи:

- Сброс бита защиты от записи (CR0.WP)
- Отображение участка памяти с правами на запись (вызовы MmMapLockedPages, MmMapLockedPagesSpecifyCache)
- Доступ к физической памяти через системный объект \Device\PhysicalDrive

Все эти варианты обхода защиты от записи перехватываются ядром Hypersight RD.

Кроме этого, Hypersight RD перехватывает и блокирует попытки перехода в режим гипервизора. Данный тип активности свойственен руткитам, использующим аппаратную виртуализацию (Blue Pill, Vitriol).

Перспективы VIPS

Виртуальные системы предотвращения вторжений (VIPS) способны успешно бороться с большинством руткитов режима ядра. Аппаратная виртуализация – достаточно мощная технология. Ее использование позволяет не только обнаруживать вредоносные действия руткитов (как это делает Hypersight RD), но и предотвращать их. Однако было бы неправильно считать, что аппаратная виртуализация может обеспечить полную защиту ПК. Комплексная защита должна сочетать методы, применяемые в системах безопасности 1-го, 2-го, 3-го и 4-го типов.