Свежий взгляд на классические подходы к защите рабочих станций

Кадыков Иван
Руководитель направления
Отдел развития продуктов ИнфоТеКС

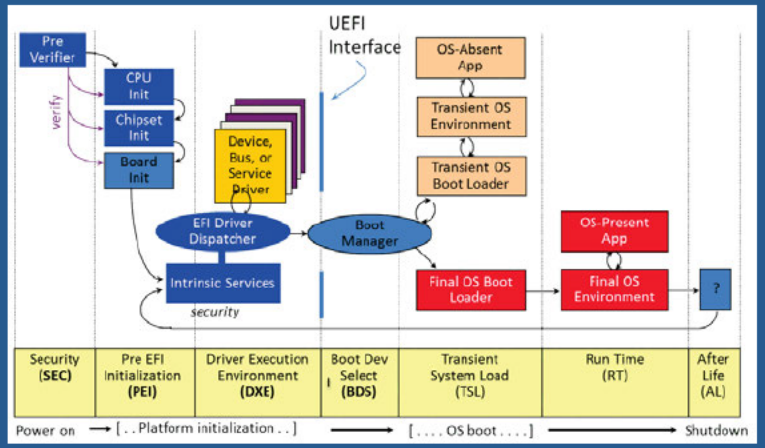
Доверие к платформе.
Доверие к среде.
Доверенная загрузка.

Включаем компьютер

Считанные секунды — и загрузилась операционная система.

- Что происходит за эти секунды?
- Что может произойти за эти секунды?

Фазы инициализации платформы



SEC (от Security) – проверка сигнатур, ключей и т.д. в чипе UEFI и на других NVRAM-носителях

PEI (Pre-EFI Initialization) – процедура инициализации системной памяти

DXE (Driver Execution Environment) – инициализация ресурсов системной платы, похожей на позднюю и финальную фазу BIOS POST

BDS (Boot Device Selection) – выбор загрузчика из доступных

TSL (Transient System Load) - старт загрузки ОС, но выполняется еще как UEFI приложение

Зловреды, атаки, уязвимости…

Cr4sh/**PeiBackdoor**

PEI stage backdoor for UEFI compatible firmware

2016

LOJAX

First UEFI rootkit found in the wild, courtesy of the Sednit group

2018

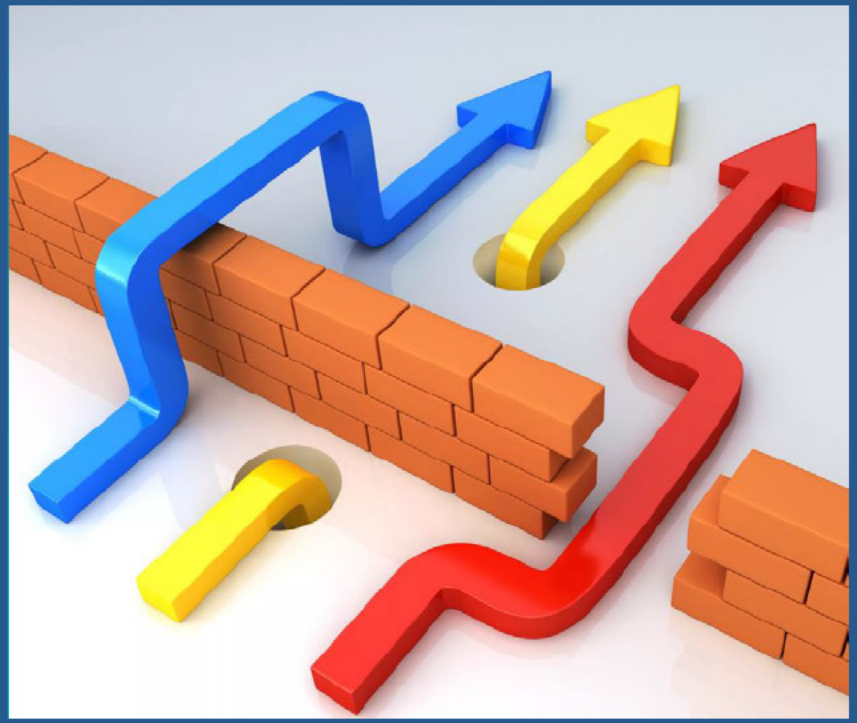
BootHole

2020

MosaicRegressor: Lurking in the Shadows of UEFI

2020

История повторяется



- Исследования безопасности среды
- Размещение на общедоступных ресурсах буткитов, руткитов и прочего malware
- Поиск и публикация уязвимостей
- Обнаружение malware «in the wild»
- Обнаружение «глобальных зловредов», с попыткой оценить масштабы трагедии

И это еще не конец…

Compliance – соответствие

Соответствие:

- Федеральным законам
- Требованиям регуляторов
- Внутриотраслевым стандартам
- Внутрикорпоративным стандартам

ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS.

Решаемые задачи ViPNet SafeBoot

Организация доверенной загрузки

Контроль целостности

- UEFI BIOS
- MBR
- Таблицы ACPI, SMBIOS, карты распределения памяти
- Файлов
- CMOS

Разграничение доступа

- Двухфакторная аутентификация
- Авторизация в AD/LDAP

С начала года поставляли ViPNet SafeBoot версии 2.0

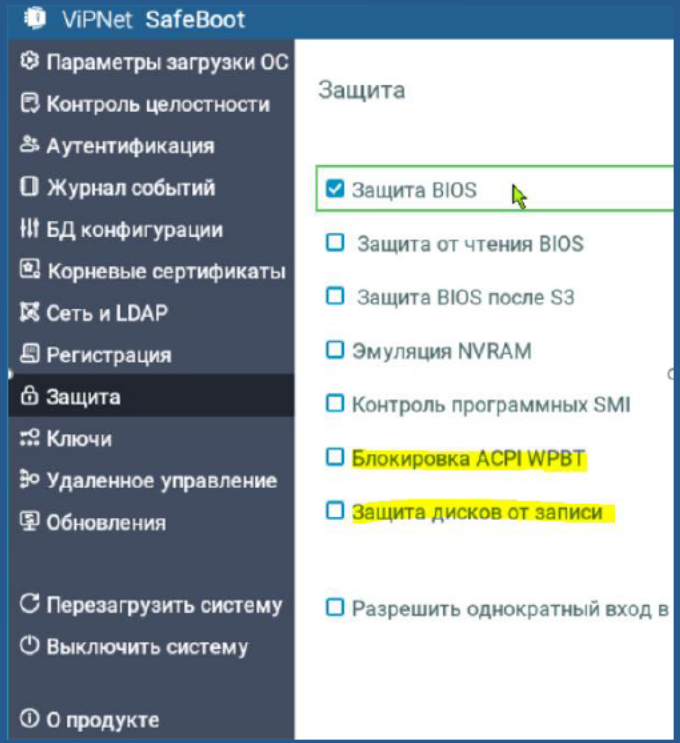
Ключевые нововведения:

- Новый графический интерфейс
- Защита на уровне SMM – Фильтрация программных SMI(system management interrupt и ограничение их функциональности.

Релиз 2.1 завершил контроль изменений! Что нового?

- Защита от malware в UEFI BIOS
- Активация защиты на платформах AMD
- Поддержка токена Rutoken S
- Поддержка работы со считывателями смарт-карт – ACR38, JCR721, ASEDrive IIIe
- Поддержка SSO для входа в операционную систему и ViPNet SafePoint v.1.2
- Поддержка сенсорных экранов, реализация сенсорной клавиатуры под UEFI
- Базовая поддержка ARM-архитектуры

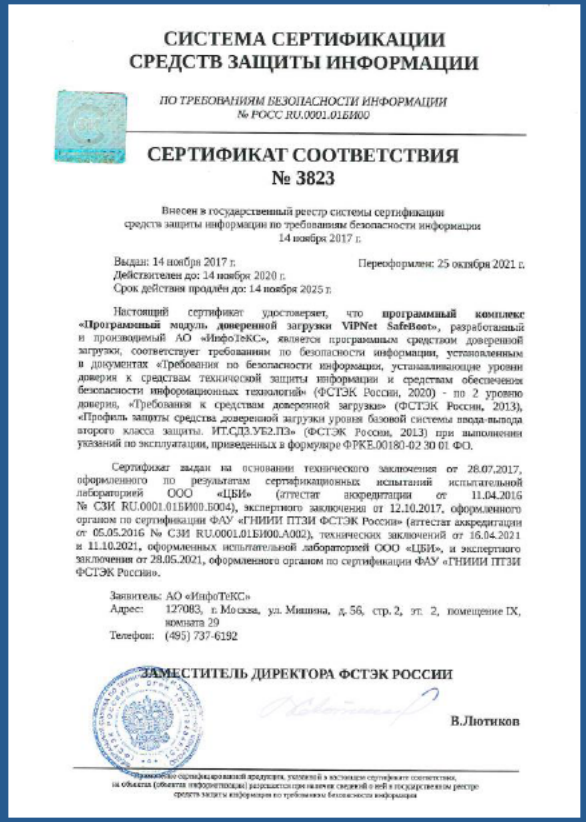
Защита от Malware



Как действует malware?

- запись файлов malware из UEFI на диск посредством встроенного (собственного) драйвера файловой системы
- использование технологии Windows Platform Binary Table (WPBT)

Продукт сертифицирован



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
14 ноября 2017 г.

Выдан: 14 ноября 2017 г. Переоформлен: 25 октября 2021 г.
Действителен до: 14 ноября 2020 г.
Срок действия продлён до: 14 ноября 2025 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Программный модуль доверенной загрузки ViPNet SafeBoot»**, разработанный и производимый АО «ИнфоТеКС», является программным средством доверенной загрузки, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 2 уровню доверия, «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00180-02 30 01 ФО.

Сертификат выдан на основании технического заключения от 28.07.2017, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), экспертного заключения от 12.10.2017, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технических заключений от 16.04.2021 и 11.10.2021, оформленных испытательной лабораторией ООО «ЦБИ», и экспертного заключения от 28.05.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Сертификат соответствия продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) размещается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Сертифицирован:

- По требованиям к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса
- По требованиям по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по 2 уровню доверия

Разграничение доступа
Защита данных
Замкнутая программная среда

ViPNet SafePoint

Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации.

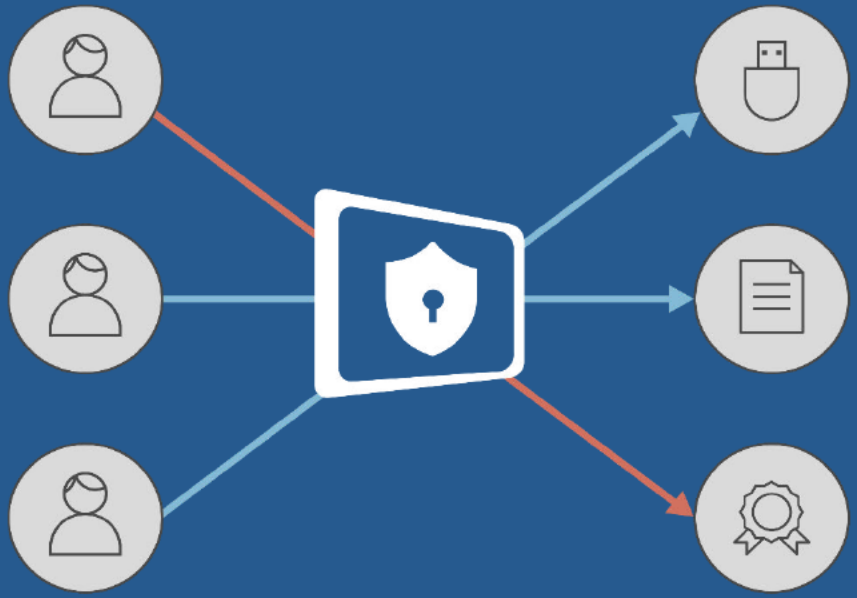
Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

Ключевая функциональность

- Двухфакторная аутентификация пользователей
- Поддержка USB-токенов и смарт-карт:
  - JaCarta ГОСТ
  - JaCarta PKI
  - JaCarta LT
  - Rutoken S
  - Rutoken Lite
  - Rutoken ЭЦП

Разграничение доступа

- После прохождения идентификации и аутентификации, в соответствии с требованиями, необходимо организовать разграничение доступа для данного пользователя, чтобы:
  - Работал только с тем ПО, которое разрешено
  - Мог работать только с теми файлами/документами для которых хватает прав(полномочий)
  - В системе запускались, только разрешённые процессы
  - Не модифицировал(-ись) важные модули



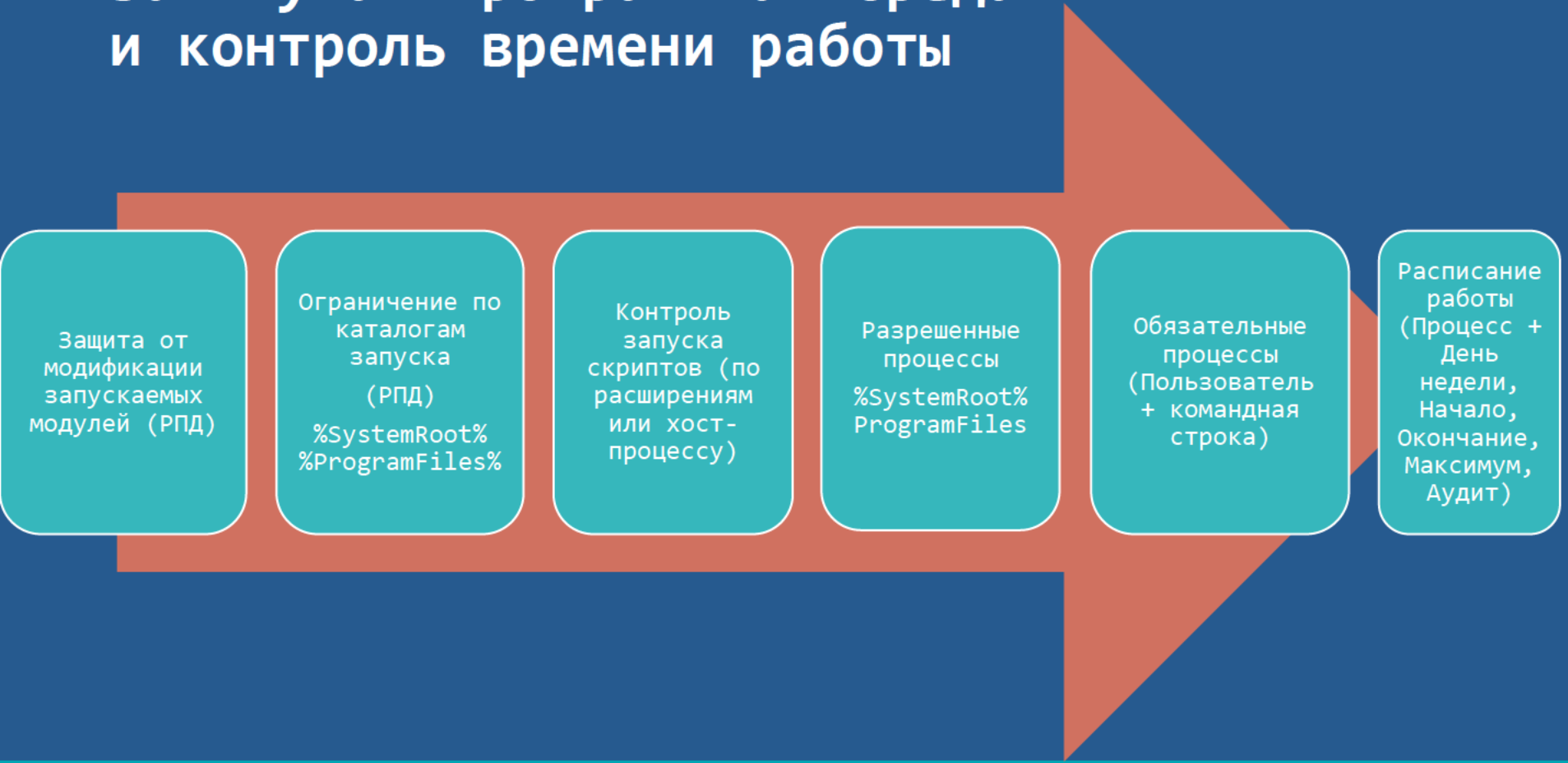
Дискреционный контроль доступа пользователей

Разграничительная политика
на основе матрицы доступа

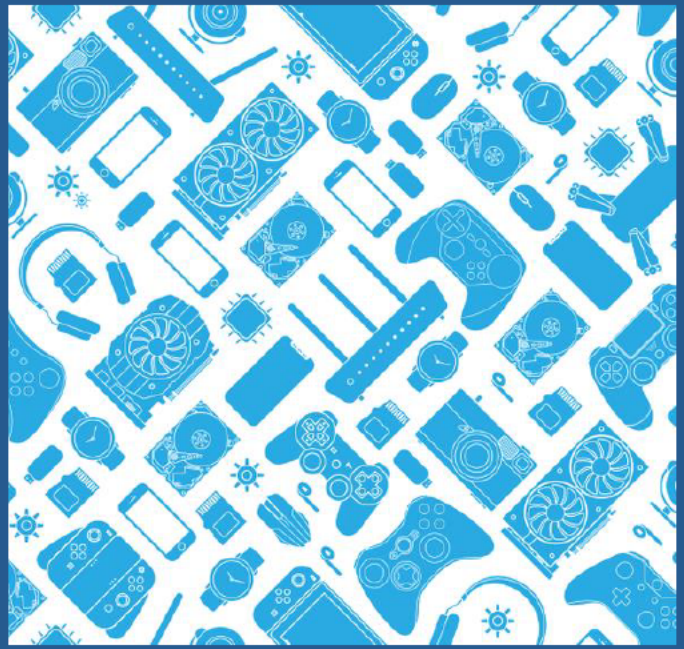
Мандатный контроль доступа пользователей и процессов

Разграничительная политика
на основе меток безопасности

Замкнутая программная среда и контроль времени работы



Контроль устройств



- Контроль и разграничение доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам

Решаемые задачи (дополнительные возможности)

- Защита от внедрения и выполнения вредоносных программ и кода
- Защита от атак на повышение привилегий
- Защита данных от атак на уязвимости системного ПО
- Защита от инсайдеров
- Защита данных от атак на уязвимости прикладного ПО

Последний актуальный кейс

- В Windows найдена уязвимость CVE-2021-41379
- Выявлена специалистами из Cisco Talos
- «Повышение привилегий в Microsoft Windows»
- 22.11.2021 выложен эксплоит на GitHub
- Один их вариантов эксплуатации – использование списка управления дискреционным доступом (DACL) в Microsoft Edge Elevation Service

ViPNet SafePoint использует свою дискреционную модель доступа, запрещает запуск того, что создано или изменено пользователем(элемент ЗПС).

СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4468

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
18 октября 2021 г.

Выдан: 18 октября 2021 г.
Действителен до: 18 октября 2026 г.

Настоящий сертификат удостоверяет, что **изделие «ViPNet SafePoint»**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014), «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014), «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности и задании по безопасности ФРКЕ.00240-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00240-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 15.07.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 05.10.2021, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

infotecs

Сертифицировано

- 5 класс защищенности СВТ
- 4 класс защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 класс ТДБ

Что дальше?

У нас есть релиз ViPNet SafePoint 1.2, а там новые фичи:

- Одновременная работа нескольких администраторов с сервером безопасности
- Возможность создания учетных записей главного и подчиненных администраторов с заданным набором их прав и ролей
- Отправка событий на электронную почту в внешние SIEM-системы
- Возможность блокировки учетных записей пользователей при попытке несанкционированного отключения заданных устройств
- Контроль передачи данных через OLE (Object Linking & Embedding) и Drag and Drop (перетаскивание объектов), он дополняет возможность управления доступом к буферу обмена
- Поддержка работы в среде Citrix XenApp и XenDesktop
- Реализована технология единого входа SSO (Single Sign-On) с ViPNet SafeBoot версии 2.1
- Поддержка новых электронных ключей и смарт-карт - JaCarta ГОСТ, JaCarta-2 SE, JaCarta-2 ГОСТ и JaCarta-2 PRO/ГОСТ

ViPNet SafePoint 1.2

Будет передан на контроль изменений в течение декабря

Завершения контроля изменений ожидаем в Q2 2022

Защита от внешних угроз
Предотвращение атак

ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия. Ключевыми модулями системы являются персональный межсетевой экран, система обнаружения и предотвращения вторжений, а также контроль приложений.

Модули


Система обнаружения и предотвращения вторжений
Контроль приложений
Межсетевой экран

ViPNet EndPoint Protection версия 1.5

Новые защитные механизмы

Контроль приложений

Персональный межсетевой экран

Эвристический Antimalware движок

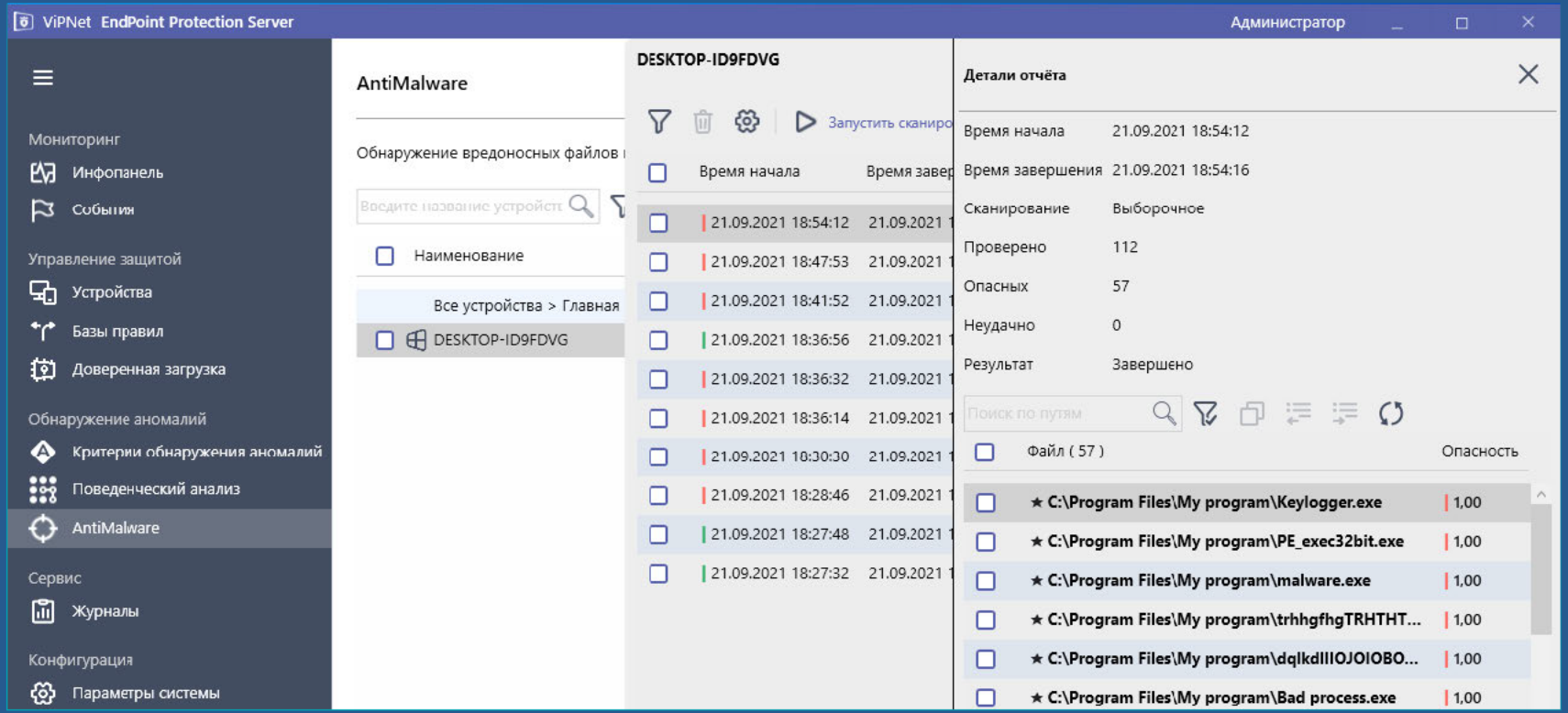
Система обнаружения и предотвращения вторжений

Модуль поведенческого анализа

Эвристический Antimalware движок

- Возможность сканирования исполняемых файлов и библиотек с целью выявления зловреда
- Эвристический Antimalware использует собственную модель построенную с помощью машинного обучения
- Модель постоянно обновляется в рамках подписки на БРП

Внешний вид Antimalware

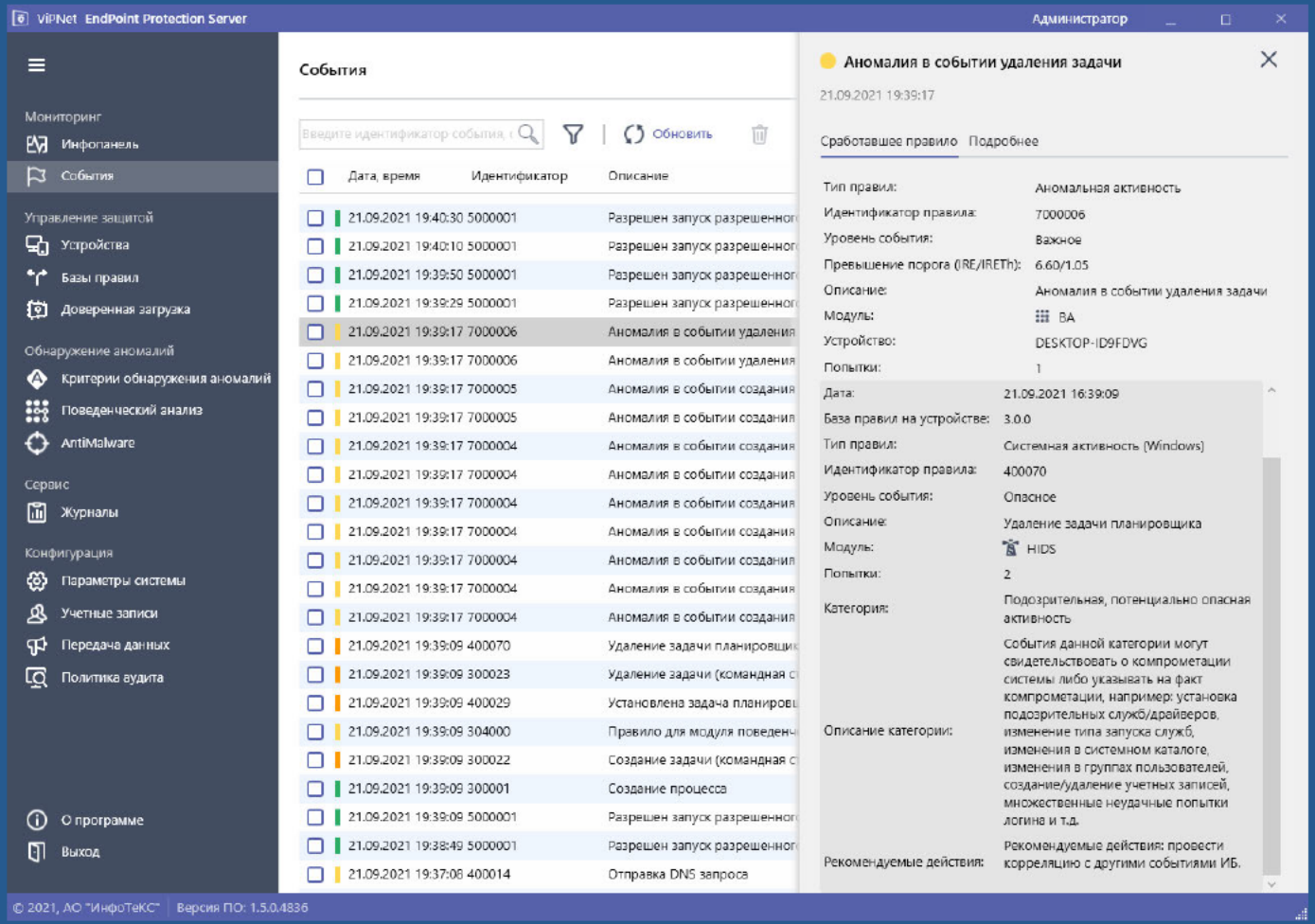


Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенной с помощью машинного обучения.

Выявляем различного рода аномалии, например:

- Аномальный вход в систему
- Аномалия в создании процесса
- Аномалия в создании задачи планировщику
- Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т.д.



Выявление аномалий

Обнаружение и предотвращение бесфайловых атак

Расширение возможностей модуля обнаружения и предотвращения вторжений

Отслеживаем техники Keylogging и Process injection

- Credential API Hooking (T1056.004)
- Process Hollowing (T1055.012)
- Process Doppelganging (T1055.013)
- Dynamic-link library injection (T1055.001)
- Portable Executable Injection (T1055.002)

Как «действует» бесфайловая атака

infotecs

Initial access

Посетил ссылку, открыл почтовое вложение

Initial access

Происходит загрузка эксплоита через известную уязвимость

Execution

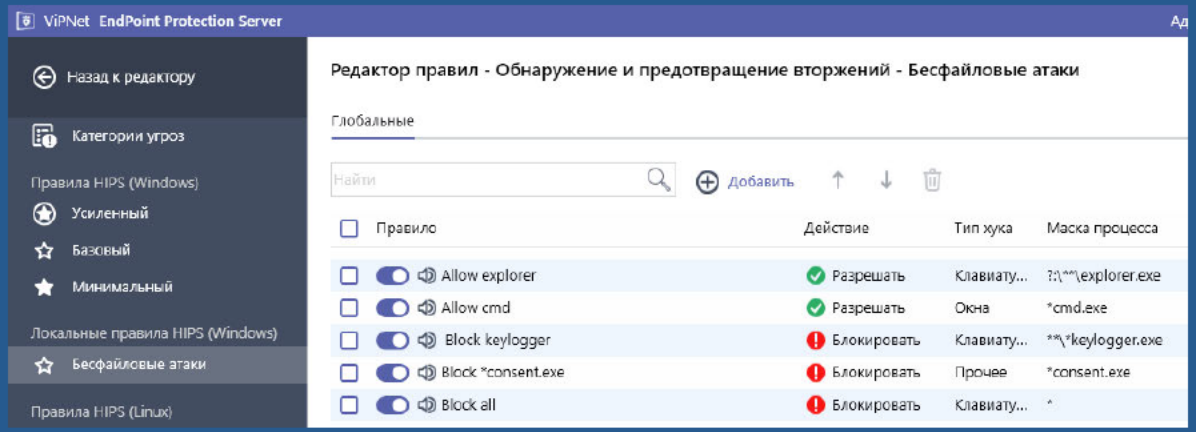
Эксплоит запускает powershell в оперативной памяти

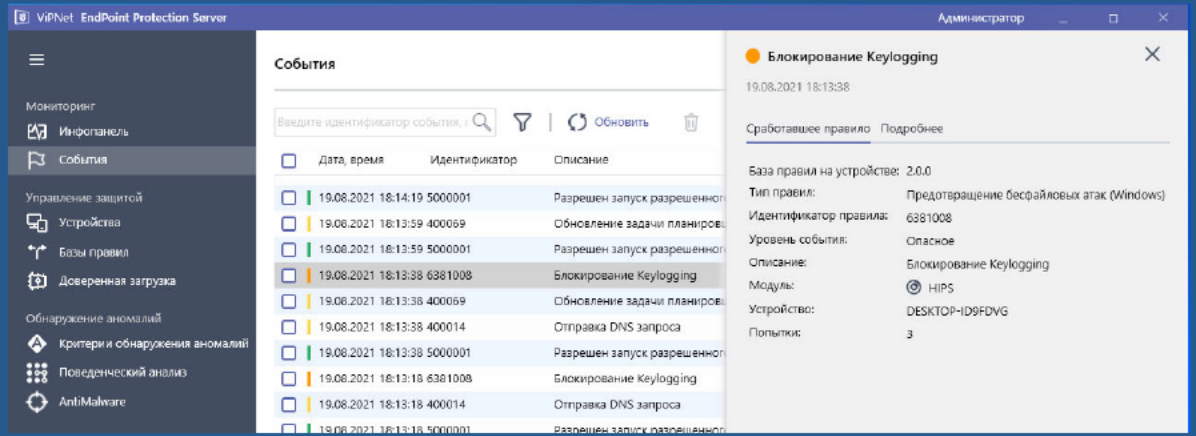
Defense Evasion

Через powershell закачивается скрипт с удалённого сервера и запускется

Command and control

Эксплоит располагается в памяти для «плохих дел»





Обнаружение и предотвращение бесфайловых атак

Входит в состав модуля «Обнаружения и предотвращения вторжений»

Поддержка Linux

Реализован ViPNet EndPoint Protection агент под следующие операционные системы:

- Astra Linux Special Edition «Смоленск» 1.6.
- РЕД ОС 7.2.
- Альт Рабочая станция 8 СП

Ожидание по сертификации

Продукт на сертификации по линии ФСТЭК России по требованиям:

- К системам обнаружения вторжений уровня узла 4 класса ИТ.СОВ.У4.ПЗ
- К межсетевым экранам типа В класса 4 (ИТ.МЭ.В4.ПЗ)
- 4 класса ТДБ

Текущая концепция защиты рабочих станций

ViPNet SafeBoot

Доверие к платформе и обеспечение доверенной загрузки ОС

Разграничение доступа и защита данных

ViPNet SafePoint

ViPNet Client 4U

Обеспечение защищённых коммуникаций

Защита от внешних атак и угроз

ViPNet EndPoint Protection