

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.

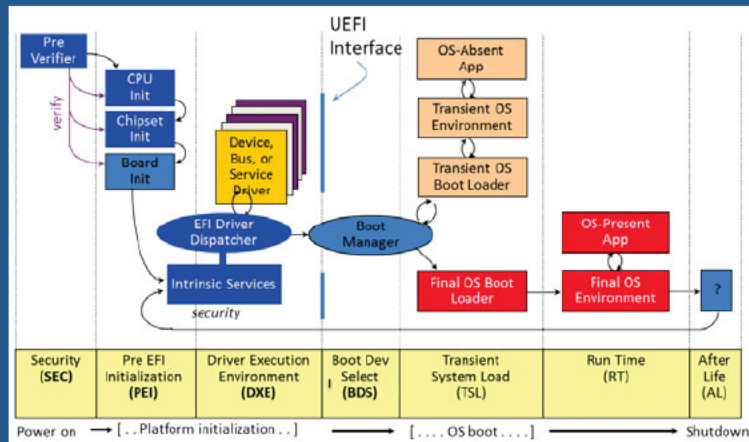


Включаем компьютер

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

2018



BootHole

2020



2016



LOJAX

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

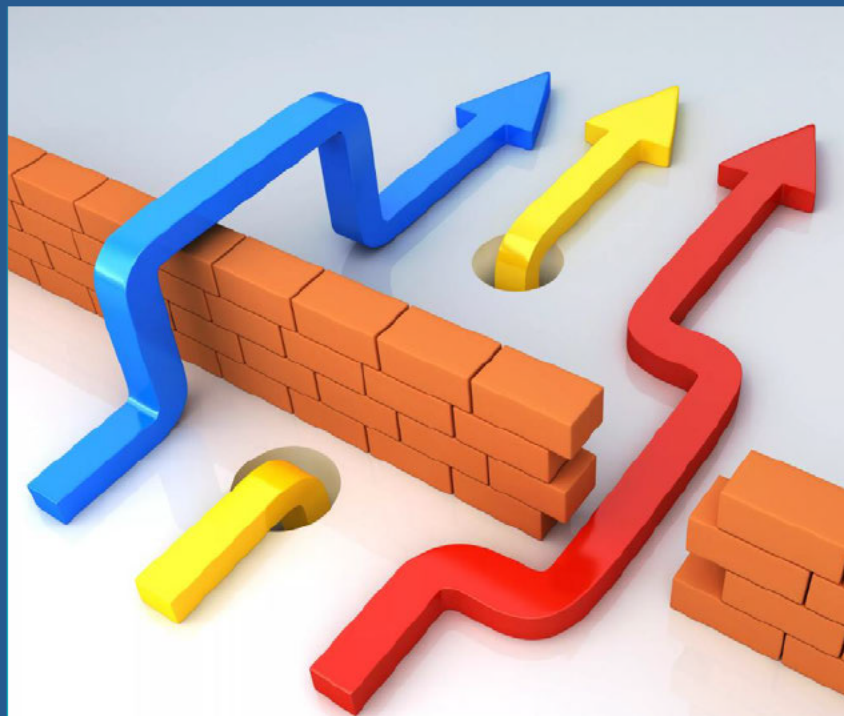


2020



MosaicRegressor:
Lurking in the
Shadows of UEFI

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
- Внутрикorporативным 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.

Организация доверенной загрузки

Контроль целостности

Разграничение доступа

UEFI BIOS

MBR

Таблицы ACPI,
SMBIOS, карты
распределения
памяти

Файлов

CMOS

Двухфакторная
аутентификация

Авторизация
в AD/LDAP

С начала года поставляли ViPNet SafeBoot версии 2.0



Ключевые нововведения:

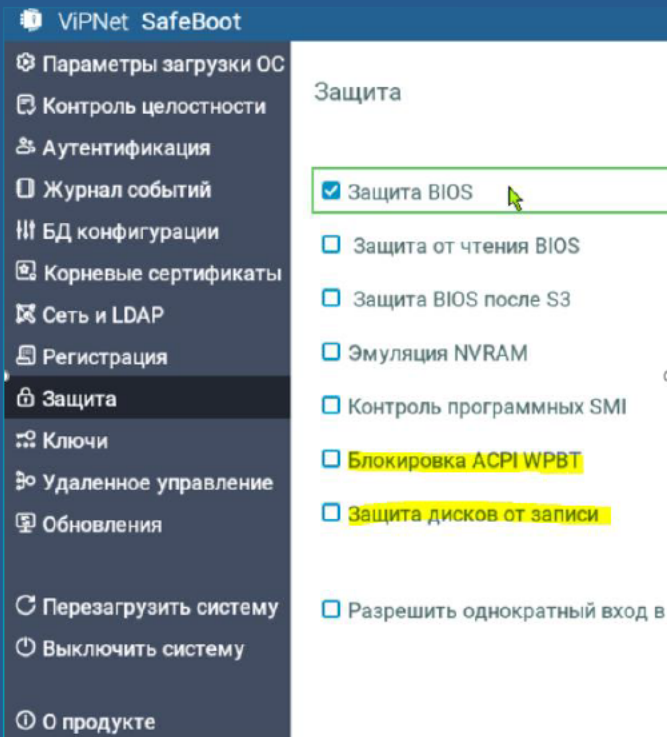
- Новый графический интерфейс
- Защита на уровне SMM – Фильтрация программных SMI(system management interrupt и ограничение их функциональности).

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, ASEDdrive 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.0001.01Б100**

**СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823**

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

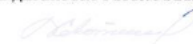
Выдан: 14 ноября 2017 г. Переоформлен: 25 октября 2021 г.
Действителен до: 14 ноября 2020 г.
Срок действия продлён до: 14 ноября 2025 г.

Настоящий сертификат удостоверяет, что программный комплекс «Программный модуль доверенной загрузки VPNet SafeNet», разработанный и произведённый АО «Ифотекс», 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), «Профилю защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты ИТСДВ.УЕ2.П» (ФСТЭК России, 2013) при выполнении условий по эксплуатации, приведенных в формуляре ФРКЕ.00180-02.30.01.ФО.

Сертификат выдан на основании технического заключения от 26.07.2017, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦНИ» (статус аккредитации от 11.04.2016 № СИ RU.0001.01Б100.0004), экспертного заключения от 12.10.2017, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СИ RU.0001.01Б100.0002), технических заключений от 16.04.2021 и 11.10.2021, оформленных испытательной лабораторией ООО «ЦНИ», и экспертного заключения от 28.05.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заявитель: АО «Ифотекс»
Адрес: 127063, г. Москва, ул. Мясная, д. 56, стр. 2, эт. 2, помещение ПХ, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ


В.Лютиков

Программный комплекс «Программный модуль доверенной загрузки, разработанный и произведённый АО «Ифотекс», 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), «Профилю защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты ИТСДВ.УЕ2.П» (ФСТЭК России, 2013) при выполнении условий по эксплуатации, приведенных в формуляре ФРКЕ.00180-02.30.01.ФО.

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



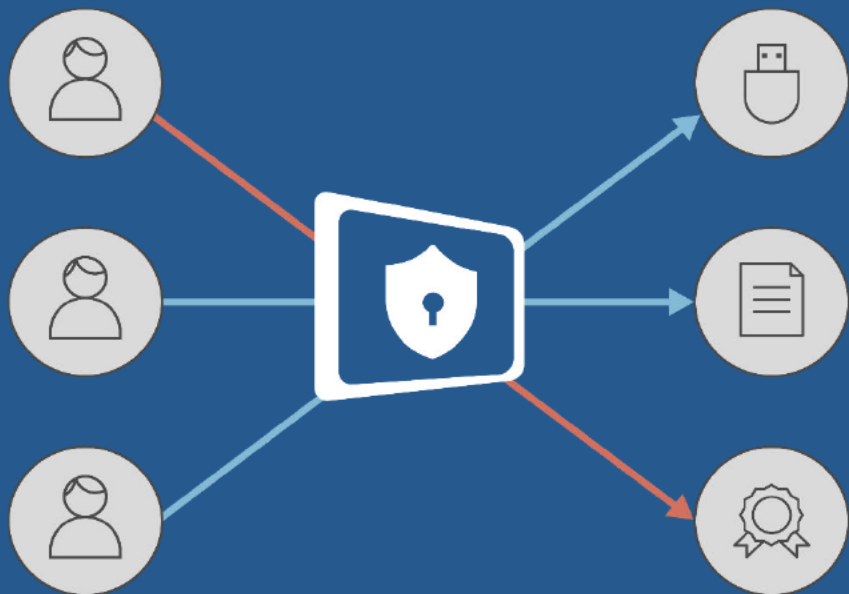
Разграничение доступа

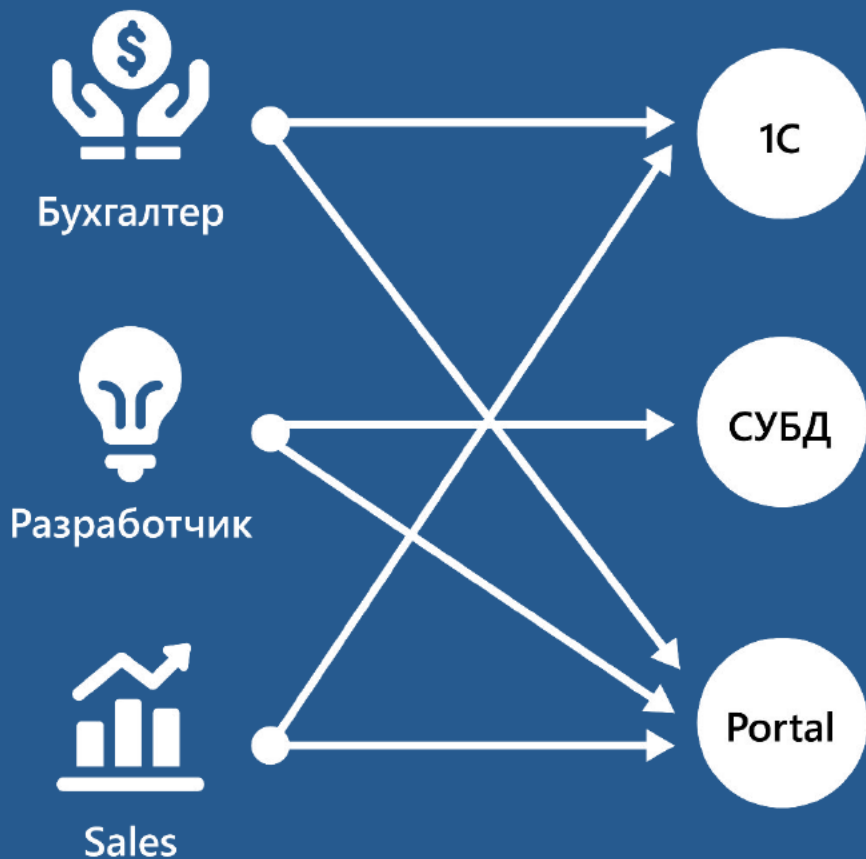
- После прохождения идентификации и аутентификации, в соответствии с требованиями, необходимо организовать разграничение доступа для данного пользователя, чтобы:
 - Работал только с тем ПО, которое разрешено
 - Мог работать только с теми файлами/документами для которых хватает прав(полномочий)
 - В системе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

Защита от
модификации
запускаемых
модулей (РПД)

Ограничение по
каталогам
запуска
(РПД)
`%SystemRoot%`
`%ProgramFiles%`

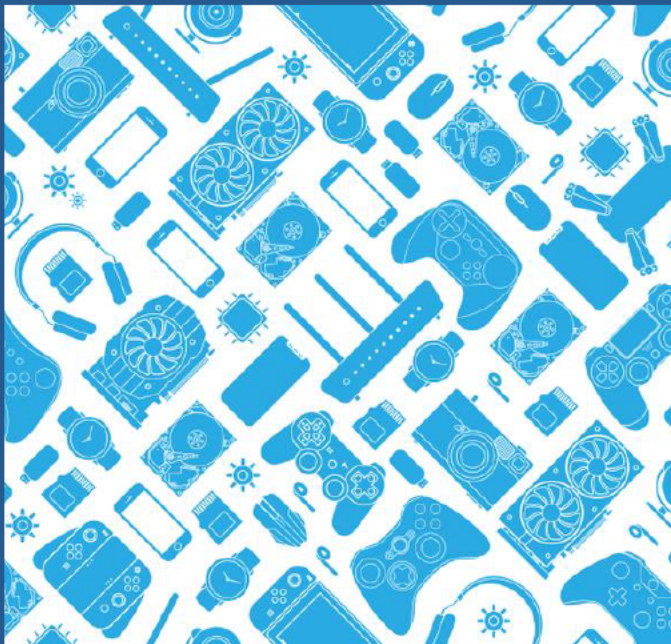
Контроль
запуска
скриптов (по
расширениям
или хост-
процессу)

Разрешенные
процессы
`%SystemRoot%`
`ProgramFiles`

Обязательные
процессы
(Пользователь
+ командная
строка)

Расписание
работы
(Процесс +
День
недели,
Начало,
Окончание,
Максимум,
Аудит)

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).



**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 заданию 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**

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 фишки:

- 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





**VIPNet EndPoint
Protection
версия 1.5**

Новые защитные механизмы

Контроль приложений



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

AntiMalware

Обнаружение вредоносных файлов

Введите название устройства

Наименование

Все устройства > Главная

DESKTOP-ID9FDVG

DESKTOP-ID9FDVG

Запустить сканирование

<input type="checkbox"/>	Время начала	Время завершения
<input type="checkbox"/>	21.09.2021 18:54:12	21.09.2021 18:54:16
<input type="checkbox"/>	21.09.2021 18:47:53	21.09.2021 18:48:00
<input type="checkbox"/>	21.09.2021 18:41:52	21.09.2021 18:42:00
<input type="checkbox"/>	21.09.2021 18:36:56	21.09.2021 18:37:00
<input type="checkbox"/>	21.09.2021 18:36:32	21.09.2021 18:36:36
<input type="checkbox"/>	21.09.2021 18:36:14	21.09.2021 18:36:18
<input type="checkbox"/>	21.09.2021 10:30:30	21.09.2021 10:30:34
<input type="checkbox"/>	21.09.2021 18:28:46	21.09.2021 18:28:50
<input type="checkbox"/>	21.09.2021 18:27:48	21.09.2021 18:27:52
<input type="checkbox"/>	21.09.2021 18:27:32	21.09.2021 18:27:36

Детали отчёта

Время начала: 21.09.2021 18:54:12

Время завершения: 21.09.2021 18:54:16

Сканирование: Выборочное

Проверено: 112

Опасных: 57

Неудачно: 0

Результат: Завершено

Поиск по путям

Файл (57) Опасность

<input checked="" type="checkbox"/>	★ C:\Program Files\My program\Keylogger.exe	1,00
<input checked="" type="checkbox"/>	★ C:\Program Files\My program\PE_exec32bit.exe	1,00
<input checked="" type="checkbox"/>	★ C:\Program Files\My program\malware.exe	1,00
<input checked="" type="checkbox"/>	★ C:\Program Files\My program\trhghfghTRHTHT...	1,00
<input checked="" type="checkbox"/>	★ C:\Program Files\My program\dqlkdlllIOJOIBO...	1,00
<input checked="" type="checkbox"/>	★ C:\Program Files\My program\Bad process.exe	1,00

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.





Мониторинг

Информанель

События

Управление защитой

Устройства

Базы правил

Доверенная загрузка

Обнаружение аномалий

Критерии обнаружения аномалий

Поведенческий анализ

AntiMalware

Сервис

Журналы

Конфигурация

Параметры системы

Учетные записи

Передача данных

Политика аудита

О программе

Выход

События

Введите идентификатор события: Обновить

<input type="checkbox"/>	Дата, время	Идентификатор	Описание
<input type="checkbox"/>	21.09.2021 19:40:30	5000001	Разрешен запуск разрешенного
<input type="checkbox"/>	21.09.2021 19:40:10	5000001	Разрешен запуск разрешенного
<input type="checkbox"/>	21.09.2021 19:39:50	5000001	Разрешен запуск разрешенного
<input type="checkbox"/>	21.09.2021 19:39:29	5000001	Разрешен запуск разрешенного
<input checked="" type="checkbox"/>	21.09.2021 19:39:17	7000006	Аномалия в событии удаления
<input type="checkbox"/>	21.09.2021 19:39:17	7000006	Аномалия в событии удаления
<input type="checkbox"/>	21.09.2021 19:39:17	7000005	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000005	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:17	7000004	Аномалия в событии создания
<input type="checkbox"/>	21.09.2021 19:39:09	400070	Удаление задачи планировщика
<input type="checkbox"/>	21.09.2021 19:39:09	300023	Удаление задачи (командная с
<input type="checkbox"/>	21.09.2021 19:39:09	400029	Установлена задача планиров
<input type="checkbox"/>	21.09.2021 19:39:09	304000	Правило для модуля поведенч
<input type="checkbox"/>	21.09.2021 19:39:09	300022	создание задачи (командная с
<input type="checkbox"/>	21.09.2021 19:39:09	300001	Создание процесса
<input type="checkbox"/>	21.09.2021 19:39:09	5000001	Разрешен запуск разрешенного
<input type="checkbox"/>	21.09.2021 19:38:49	5000001	Разрешен запуск разрешенного
<input type="checkbox"/>	21.09.2021 19:37:06	400014	Отправка DNS запроса

Аномалия в событии удаления задачи

21.09.2021 19:39:17

Сработавшее правило [Подробнее](#)

Тип правил:	Аномальная активность
Идентификатор правила:	7000006
Уровень события:	Важное
Превышение порога (RE/IREth):	6.60/1.05
Описание:	Аномалия в событии удаления задачи
Модуль:	BA
Устройство:	DESKTOP-ID9FDWG
Попытки:	1
Дата:	21.09.2021 16:39:09
База правил на устройстве:	3.0.0
Тип правил:	Системная активность (Windows)
Идентификатор правила:	400070
Уровень события:	Опасное
Описание:	Удаление задачи планировщика
Модуль:	HIDS
Попытки:	2
Категория:	Подозрительная, потенциально опасная активность
Описание категории:	События данной категории могут свидетельствовать о компрометации системы либо указывать на факт компрометации, например: установка подозрительных служб/драйверов, изменение типа запуска служб, изменения в системном каталоге, изменения в группах пользователей, создание/удаление учетных записей, множественные неудачные попытки логина и т.д.
Рекомендуемые действия:	Рекомендуемые действия: провести корреляцию с другими событиями ИБ.

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



ViPNet EndPoint Protection Server

Назад к редактору

Категории угроз

Правила HIPS (Windows)

- Усиленный
- Базовый
- Минимальный

Локальные правила HIPS (Windows)

- Бесфайловые атаки

Правила HIPS (Linux)

Редактор правил - Обнаружение и предотвращение вторжений - Бесфайловые атаки

Глобальные

Найти

+ Добавить

Правило	Действие	Тип хука	Маска процесса
<input type="checkbox"/> Allow explorer	Разрешать	Клавиату...	?**\explorer.exe
<input type="checkbox"/> Allow cmd	Разрешать	Окна	*cmd.exe
<input type="checkbox"/> Block keylogger	Блокировать	Клавиату...	***keylogger.exe
<input type="checkbox"/> Block *consent.exe	Блокировать	Прочее	*consent.exe
<input type="checkbox"/> Block all	Блокировать	Клавиату...	^

Обнаружение и предотвращение бесфайловых атак

ViPNet EndPoint Protection Server

Администратор

Мониторинг

- Информация
- События
- Управление защитой
- Устройства
- Базы правил
- Доверенная загрузка
- Обнаружение аномалий
- Критерии обнаружения аномалий
- Поведенческий анализ
- Anti-Malware

События

Введите идентификатор события:

Обновить

Дата, время	Идентификатор	Описание
19.08.2021 18:14:19	5000001	Разрешен запуск разрешенной программы
19.08.2021 18:13:59	400069	Обновление задачи планировщика
19.08.2021 18:13:59	5000001	Разрешен запуск разрешенной программы
19.08.2021 18:13:38	6381008	Блокирование Keylogging
19.08.2021 18:13:38	400069	Обновление задачи планировщика
19.08.2021 18:13:38	400014	Отправка DNS запроса
19.08.2021 18:13:38	5000001	Разрешен запуск разрешенной программы
19.08.2021 18:13:18	6381008	Блокирование Keylogging
19.08.2021 18:13:18	400014	Отправка DNS запроса
19.08.2021 18:13:18	5000001	Разрешен запуск разрешенной программы

Блокирование Keylogging

19.08.2021 18:13:38

Сработавшее правило: Подробнее

База правил на устройстве: 2.0.0

Тип правила: Предотвращение бесфайловых атак (Windows)

Идентификатор правила: 6381008

Уровень события: Опасное

Описание: Блокирование Keylogging

Модуль: HIPS

Устройство: DESKTOP-ID9FDVG

Попытки: 3

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



ViPNet SafePoint

Разграничение
доступа и защита
данных



ViPNet Client 4U

Обеспечение
защищённых
коммуникаций



ViPNet EndPoint
Protection

Защита от
внешних атак и
угроз