AVSOFT

AVSOFT ATHENA

Система выявления и анализа вредоносного ПО

О КОМПАНИИ

Компания «АВ Софт» существует с 2010 года.
Основными направлениями нашей деятельности являются разработка программного обеспечения и консалтинг в сфере информационной безопасности.

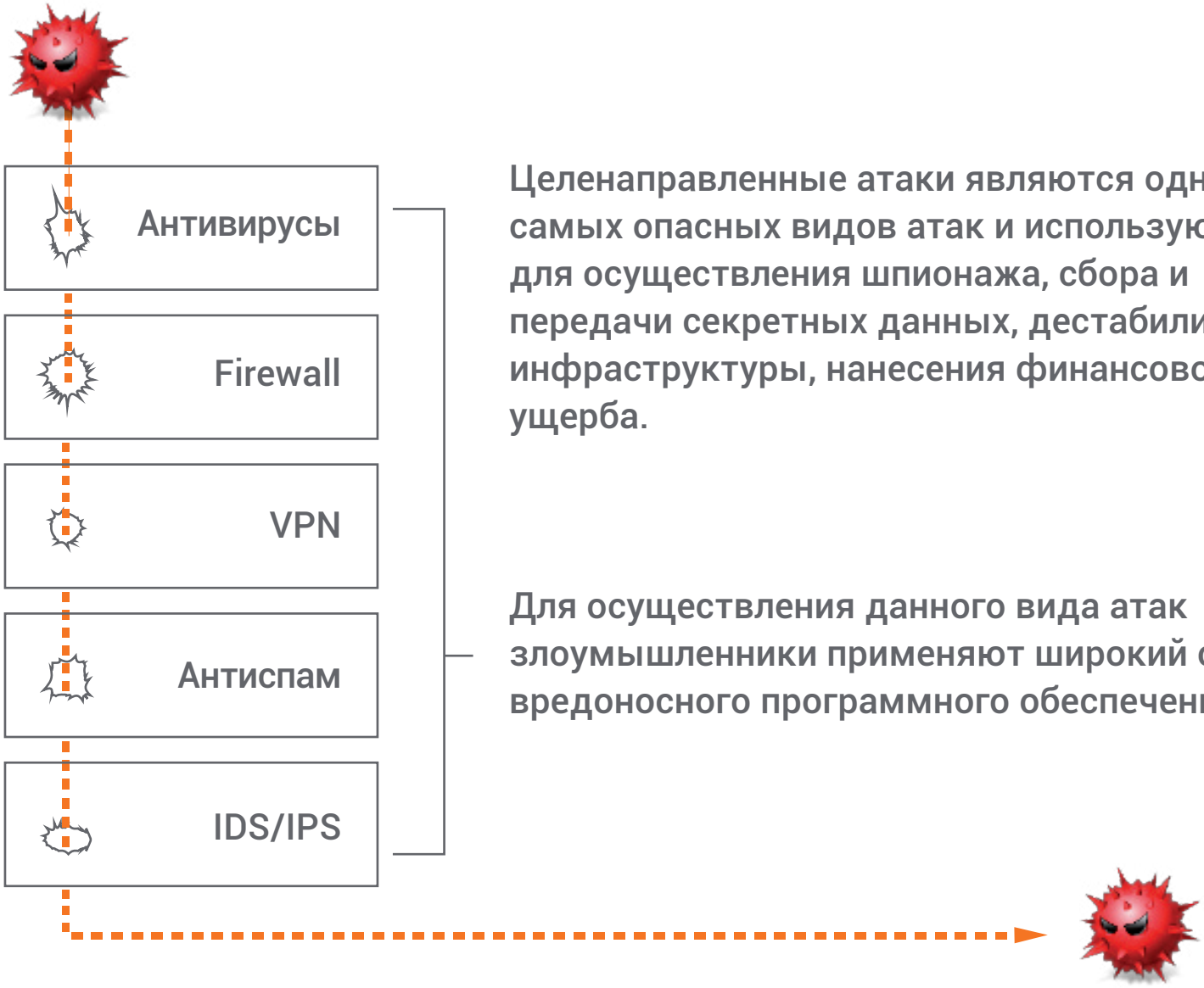
Анализ вредоносного ПО

Расследование инцидентов ИБ

Консалтинг в области ИБ

Разработка ПО

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ



Целенаправленные атаки являются одним из самых опасных видов атак и используются для осуществления шпионажа, сбора и передачи секретных данных, дестабилизации инфраструктуры, нанесения финансового ущерба.

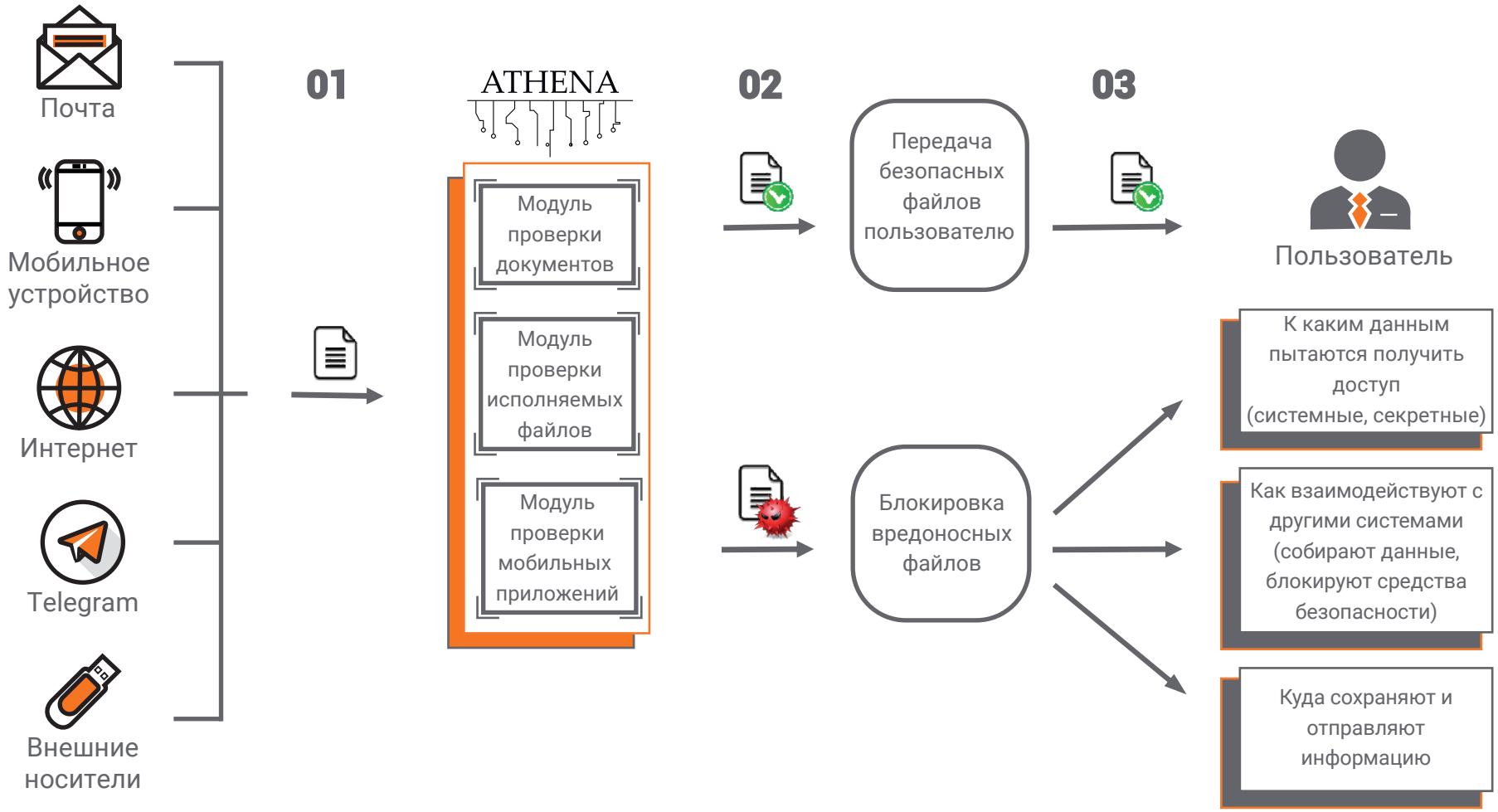
Для осуществления данного вида атак злоумышленники применяют широкий спектр вредоносного программного обеспечения.

ОБЩАЯ СХЕМА РАБОТЫ AVSOFT ATHENA

01 Фильтрация файлов на проверку

02 Исследование файлов в системе AVSOFT ATHENA статическим и динамическим анализом

03 Получение результатов анализа



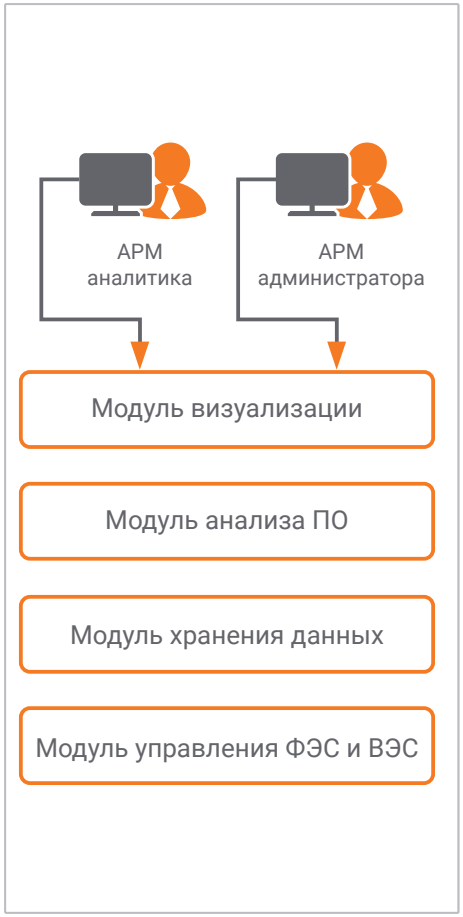
ПРОВЕРКА МОБИЛЬНЫХ УСТРОЙСТВ

1 шаг	2 шаг	3 шаг	4 шаг
Проверка мобильных устройств с ОС: Android iOS Windows Mobile	Считывание пользовательских приложений с мобильного устройства	Передача файлов на анализ в интерфейс системы «AVSOFT ATHENA»	Подробная информация о проверке мобильного устройства и приложений
			
Мобильное устройство	Программа анализа мобильного устройства	Интерфейс AVSOFT ATHENA	Отчет о проверке

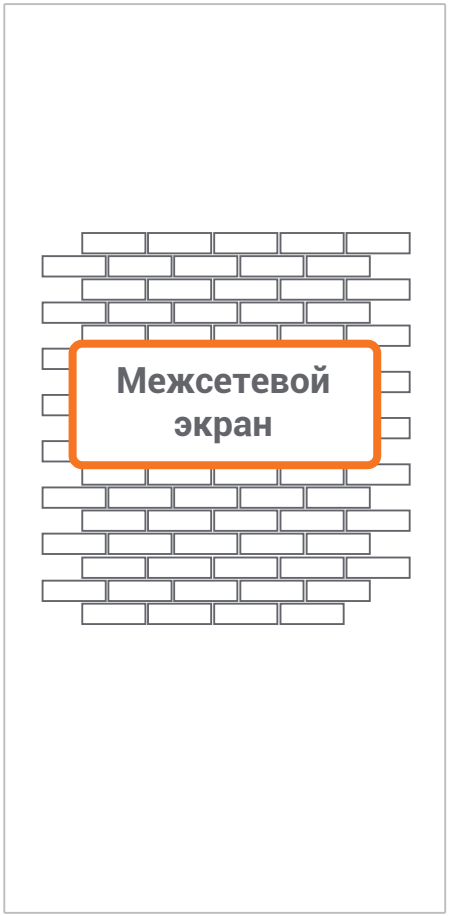
АНАЛИЗ ПОЧТОВОГО ТРАФИКА

АРХИТЕКТУРА СИСТЕМЫ

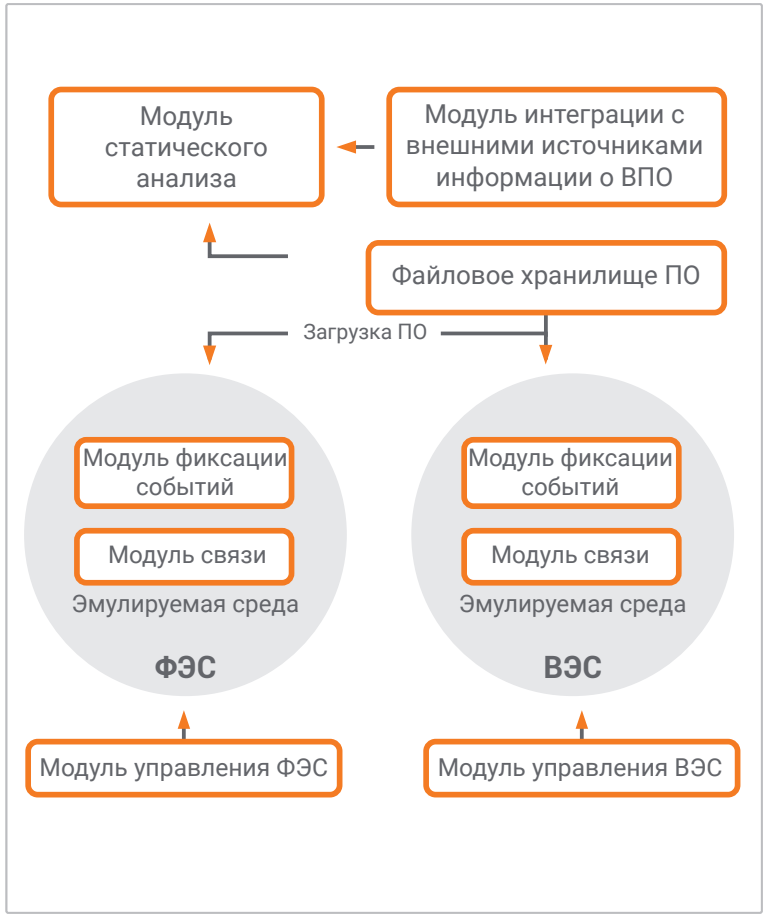
Подсистема анализа и управления



Подсистема обеспечения сетевой безопасности



Подсистема исследования ПО «Песочница»



ПО - программное обеспечение
ВПО - вредоносное программное обеспечение

ВЭС - виртуальная эмулируемая среда
ФЭС - физическая эмулируемая среда

ВИДЫ АНАЛИЗА ФАЙЛОВ

Система «AVSOFT ATHENA» усиливает защиту информационной инфраструктуры от целенаправленных кибератак путем использования двух видов анализа ПО: статического и динамического.

СТАТИЧЕСКИЙ АНАЛИЗ

Запуск файлов на анализ

Исследования файлов

Проверка в 15 локальных антивирусах

Статический анализ файлов

Проверка во внешних ресурсах

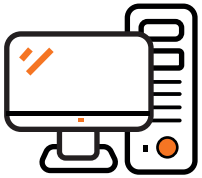
Результаты анализа

- Анализ манифестов мобильных приложений на требуемые разрешения
- Анализ атрибутов, структуры и контента файлов на наличие подозрительных признаков (сжатие, обфускация и т.п.)
- Анализ офисных файлов на наличие активных элементов (макросы, скрипты и пр.)

ДИНАМИЧЕСКИЙ АНАЛИЗ

Исследования файлов в «песочницах»

Запуск файлов на анализ



Физическая

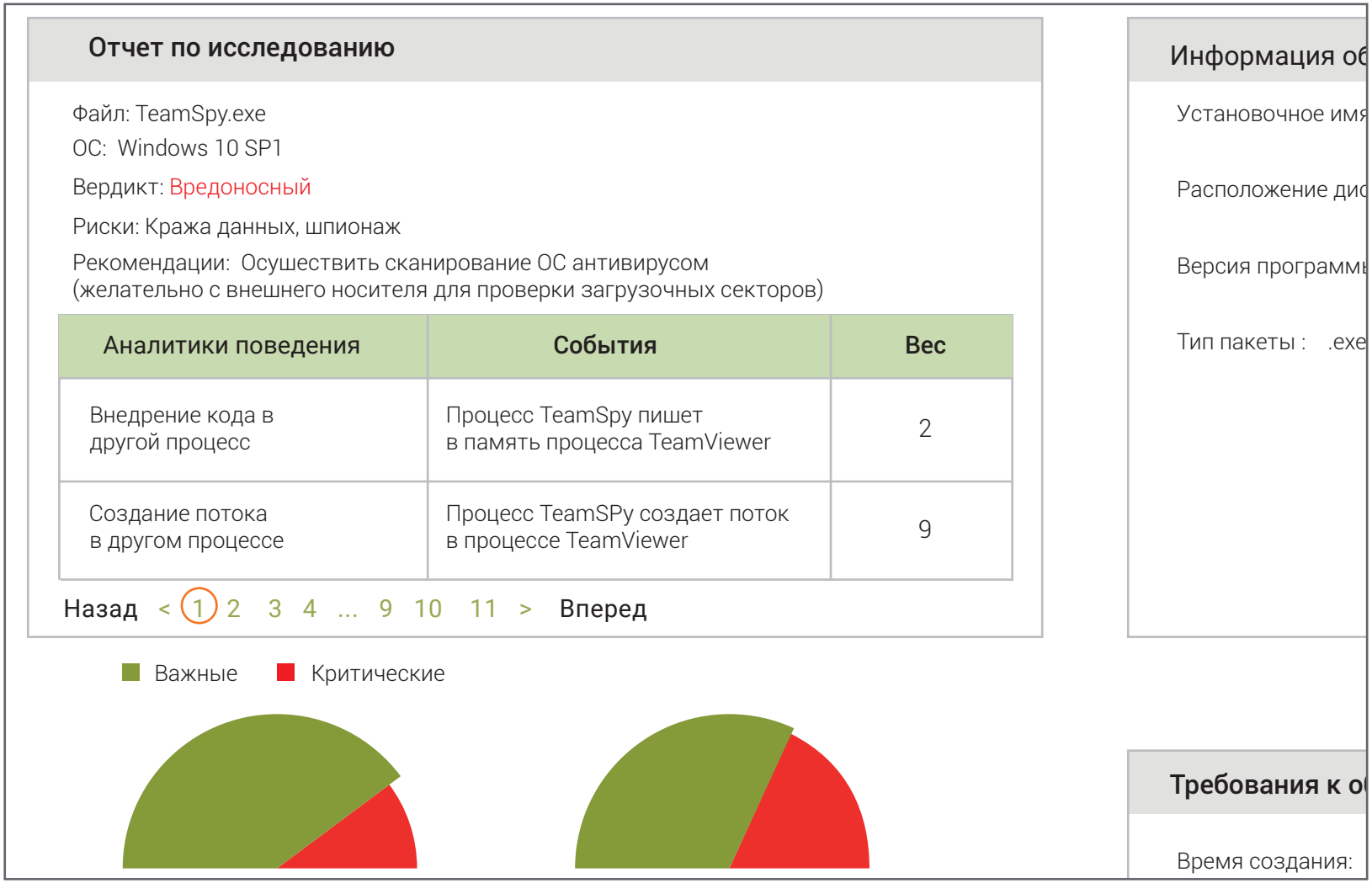
Виртуальная

Результаты анализа

- события в файловой системе;
- события в реестре;
- события в процессах;
- события в сети (зафиксированные IP-адреса и домены проходят проверку в базах данных вредоносных IP-адресов и доменов).

ОТЧЕТ ПО ФАЙЛУ

Система «AVSOFT ATHENA» предоставляет подробный отчет с ключевой информацией по результатам исследования файла.



Отчет по исследованию

Файл: TeamSpy.exe

ОС: Windows 10 SP1

Вердикт: Вредоносный

Риски: Кража данных, шпионаж

Рекомендации: Осушествить сканирование ОС антивирусом (желательно с внешнего носителя для проверки загрузочных секторов)

Аналитики поведения	События	Вес
Внедрение кода в другой процесс	Процесс TeamSpy пишет в память процесса TeamViewer	2
Создание потока в другом процессе	Процесс TeamSPy создает поток в процессе TeamViewer	9

Назад < 1 2 3 4 ... 9 10 11 > Вперед

Важные Критические

Информация об

Установочное имя

Расположение дис

Версия программы

Тип пакеты : .exe

Требования к о

Время создания:

ОСНОВНЫЕ ВОЗМОЖНОСТИ AVSOFT ATHENA

Анализ различных типов файлов

Офисные документы, исполняемые файлы, скрипты и т.д.

Анализ почтового трафика

Выявление вредоносных вложений в письмах и их удаление из писем до получения адресатом

Проверка файлов со съемных носителей

USB-накопители, внешние диски (HDD), CD/DVD, карты памяти и др.

Гибкая настройка сценариев исследования

Любая конфигурация параметров исследования файлов

Интерфейс для отправки файлов из других систем

Присутствует API-интерфейс, который позволяет отправлять файлы на проверку из других систем

Интеграция в существующую инфраструктуру

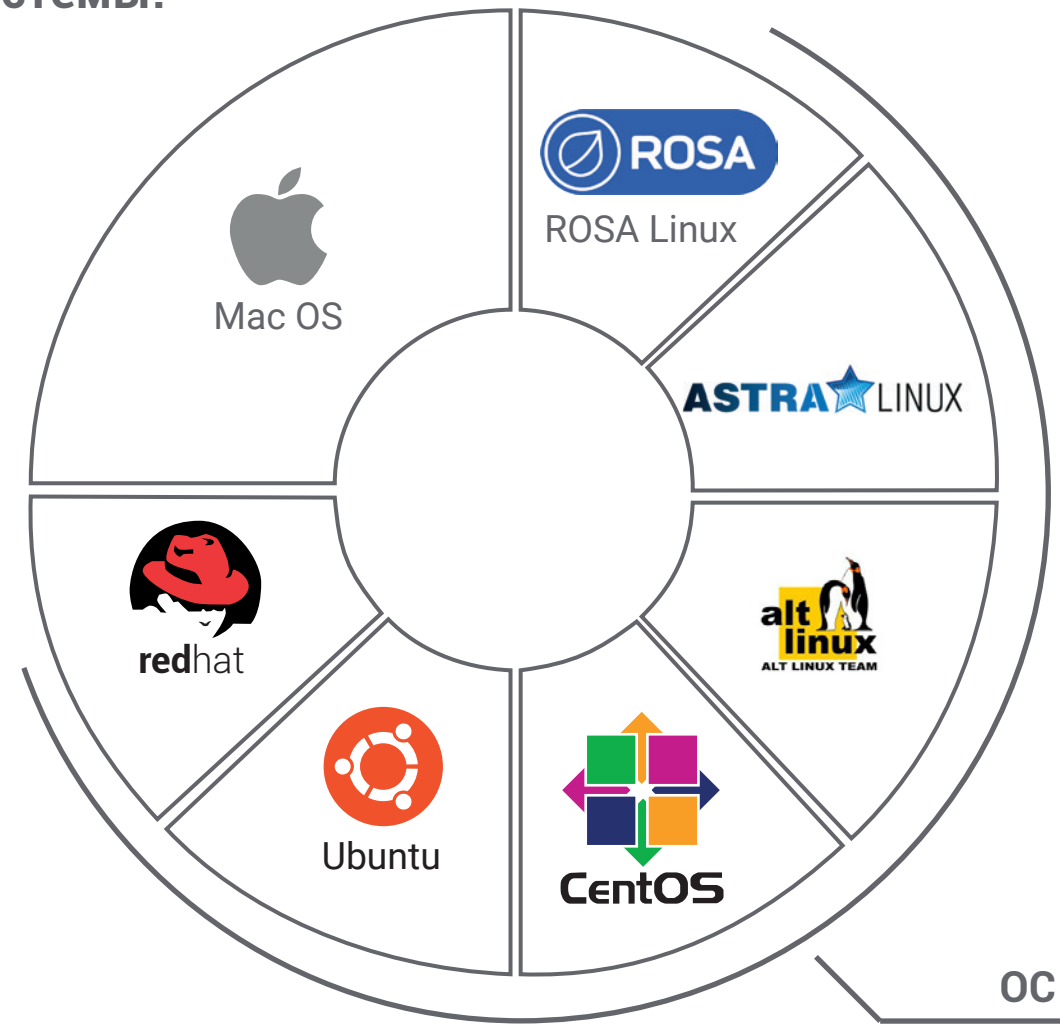
Не требует установку дополнительного оборудования

ПРЕИМУЩЕСТВА СИСТЕМЫ

Параметры	SandBlast	JOESecurity	FortiSandbox	FireEye	ThreatGRID	WildFire	ATHENA
Имитация сознательной работы пользователя в автоматическом режиме	✗	✗	✗	✗	✗	✗	✓
Имитация корпоративных приложений и данных (кастомизация «песочницы»)	✗	✗	✓	✗	✗	✗	✓
Экспертный режим работы с детальной настройкой имитационной среды	✗	✗	✗	✗	✗	✗	✓
Анализ файлов без отправки данных за периметр организации	✓	✓	✓	✓	✓	✓	✓
Динамический анализ мобильных приложений ОС Android и iOS	✓	✓	✓	✓	✗	✗	✓

БЛИЖАЙШИЕ РЕЛИЗЫ

Готовятся к выходу версии системы:



ОС на базе ядра Linux

+7 (495) 988-92-25

office@avsw.ru

127106, Москва,
ул. Гостиничная, д.5

www.avsw.ru

AVSOFT

ATHENA