Платформа FireEye для защиты от APT

Рагушин Дмитрий, региональный менеджер, Россия и СНГ
Dmitry.Ragushin@FireEye.com
Белоглазов Алексей, системный инженер, Россия и СНГ
Aleksey.Beloglazov@FireEye.com

Сколько вендоров предлагают защиту от APT?

200+

Что все продают?

Что в итоге?

Dear Fellow Shareholders,

Jamie Dimon,
Chairman and
Chief Executive Officer

What a year. Despite tremendous challenges, your company earned $17.9 billion in net income on revenue of $96.6 billion in 2013. Our financial results reflected strong underlying performance across our four main businesses – unfortunately marred by significant legal settlements largely related to mortgages. These legal expenses cost the company $8.6 billion after-tax. Excluding these expenses and some one-time positive benefits from reserve reductions (which we never have considered true earnings) and one-time gains on the sale of assets, your company earned about $23 billion.

As tough as the year was – the company was under constant and intense pressure – I can hardly express the admiration, even pride, I feel because of the enduring resolve and resiliency of our management team and our employees. They never wavered as they attacked our problems while maintaining a relentless focus on serving our clients. We all owe them a great deal of gratitude.

The bad news was bad. The most painful, difficult and nerve-wracking experience that I have ever dealt with professionally was trying to resolve the legal issues we had this past year with multiple government agencies and regulators as we tried to get many large and risky legal issues behind us, including the Chief Investment Office (CIO) situation (that happened in 2012) and mortgage-related matters (that happened

2

Банк J.P.Morgan после взлома

«К концу 2014 года мы будем тратить на безопасность более 250 миллионов долларов в год».

«Мы добились хорошего прогресса, но интенсивность атак в киберпространстве нарастает по всему миру. Это будет непрекращающаяся борьба, но, к сожалению, не все битвы можно выиграть. Тем не менее, будьте уверены, что мы делаем все возможное».

Source: http://files.shareholder.com/downloads/ONE/3430314926x0x742267/e2efaf60-814f-430e-869e-6889ba3ec0ec/2013AR_Chairman-CEO_letter.pdf

Простая истина

100% защиты не бывает

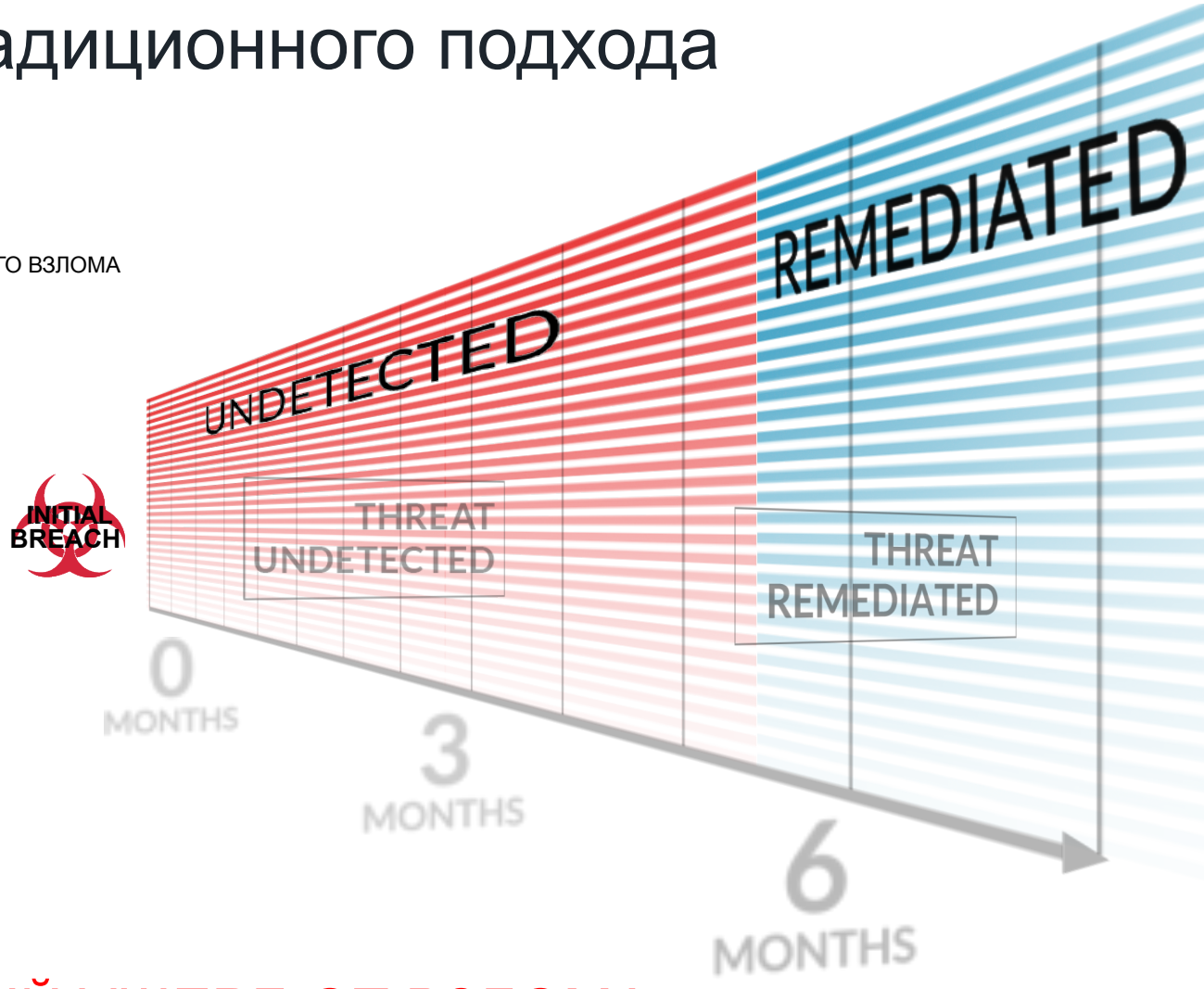
Недостатки традиционного подхода

146 ДНЕЙ
СРЕДНЕЕ ВРЕМЯ ОБНАРУЖЕНИЯ УСПЕШНОГО ВЗЛОМА

32 ДНЯ
НА УСТРАНЕНИЕ ПОСЛЕДСТВИЙ

53%
УЗНАЛИ О КОМПРОМЕНТАЦИИ ИЗ ВНЕШНИХ ИСТОЧНИКОВ

100%
ИСПОЛЬЗОВАЛИ МЕЖСЕТЕВЫЕ ЭКРАНЫ И АНТИВИРУСЫ С АКТУАЛЬНЫМИ ОБНОВЛЕНИЯМИ



$3.5M СРЕДНИЙ УЩЕРБ ОТ ВЗЛОМА

SOURCE: MANDIANT M-TRENDS REPORT, PONEMON COST OF DATA BREACH STUDY

FireEye

Еще одна простая истина

APT – это не ЧТО,

Это - КТО

Проблема не в кирпиче, проблема в том, кто его бросил

Мотивация атакующего (и профиль жертвы)

	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	DESTRUCTIVE ATTACK
Objective	Access & Propagation	Economic, Political Advantage	Financial Gain	Defamation, Press & Policy	Disrupt Operations
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Delete Data
Targeted	✗	☑	☑	☑	☑
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven

О том, кто вам противостоит

ЭТО “КТО”, А НЕ “ЧТО”

ЗА КАЖДОЙ АТАКОЙ СТОЯТ КОНКРЕТНЫЕ ЛЮДИ

ОНИ АДАПТИРУЮТ АТАКИ ПОД ВАШУ ИНФРАСТРУКТУРУ

ИХ ЦЕЛЬ – ИМЕННО ВЫ

ОНИ ПРОФЕССИО-НАЛЬНЫ И ОРГАНИЗОВАНЫ

У НИХ ЕСТЬ ФИНАНСИРОВАНИЕ

ОНИ МОГУТ ИСПОЛЬЗОВАТЬ УНИКАЛЬНЫЙ ИНСТРУМЕНТАРИЙ

ОНИ МОГУТ РАБОТАТЬ ГОДАМИ

ОНИ ПОЧТИ ВСЕГДА ВОЗВРАЩАЮТСЯ

У НИХ ЕСТЬ ЧЕТКО ОПРЕДЕЛЕННЫЕ ЦЕЛИ

ОНИ ДОБИВАЮТСЯ ПОСТОЯННОГО ПРИСУТСТВИЯ

ОНИ ХОТЯТ ОБЕСПЕЧИТЬ БЕСПРЕПЯТСТВЕННЫЙ ДОСТУП В ВАШУ СЕТЬ

Все говорят про threat intelligence, а как же threat actors?

Конкуренты

- Телеметрия
- R&D

FireEye

- Телеметрия
- R&D
- Сотни тысяч часов Incident Response в год, включая Target, Sony, Swift и пр.
- Отслеживание деятельности более чем 17000 хакеров и хакерских группировок

И еще один момент

В слове APT ключевое слово – persistent

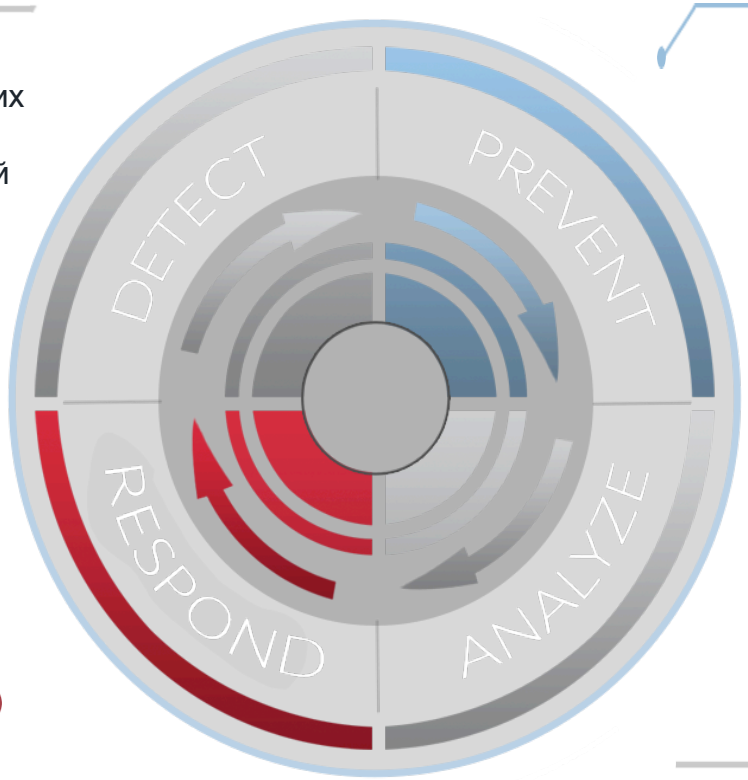
Непрерывный цикл защиты от APT

Обнаружить

Динамически без сигнатур, эмуляция трафика нескольких потоков в контексте с использованием базы знаний об инструментах и тактиках злоумышленников

Предотвратить

Установка в разрыв, предотвращение угроз «нулевого» дня, включая первоначальное заражение для отдельных векторов, распространение и каналы управления



Отреагировать

Восстановить после атаки, удалить все инструменты и блокировать пути возврата злоумышленников с учетом их профиля, целей и методов

Расследовать

Изоляция скомпрометированных станций, анализ активности вредоносного ПО и удаленных злоумышленников на уровне сети и конечных точек

FireEye

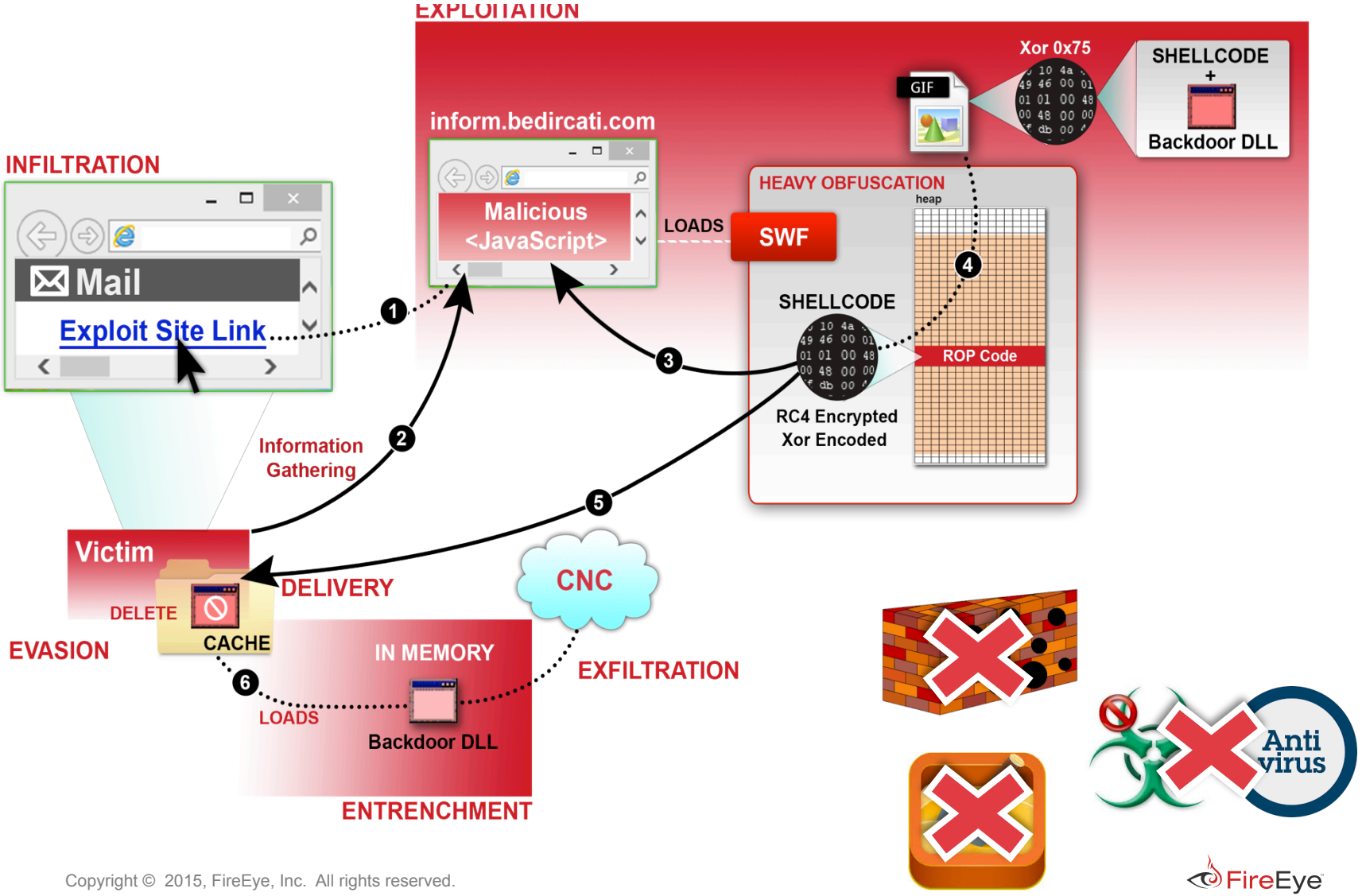
Как строится современная составная атака (Multi-Flow Attack)

SECURITY REIMAGINED

Этапы составной атаки (Kill-Chain)

FireEye

Пример 1: Clandestine Fox (2014), Wolf (2015) Китайская хакерская группа (APT3)

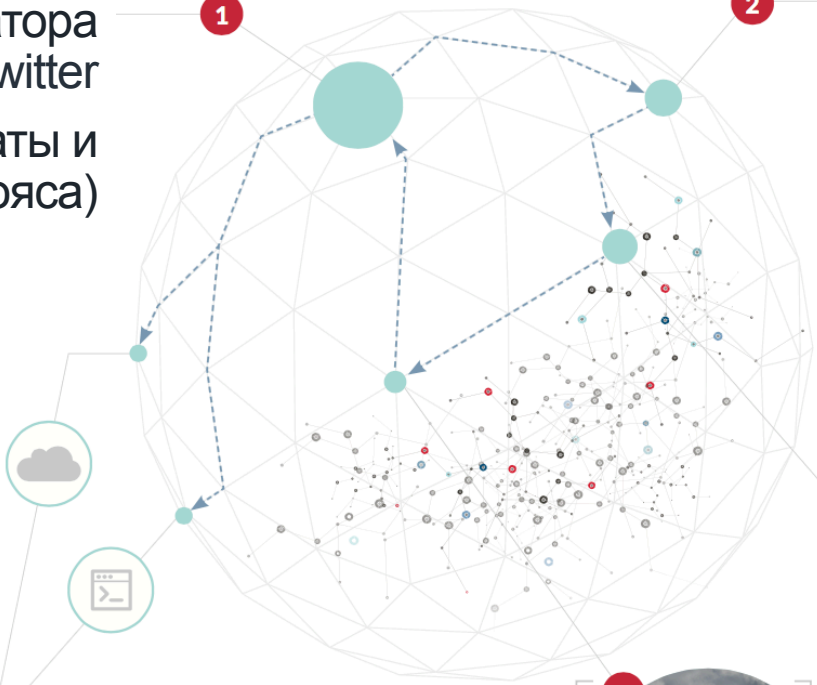


FireEye

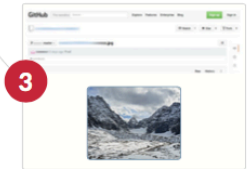
Пример 2: HAMMERTOSS (2015)
Русскоязычная хакерская группа (APT29)

Автоматическая ежедневная генерация идентификатора пользователя Twitter

(зависит от даты и часового пояса)



Посещение страницы Twitter, поиск URL (в т.ч. на GitHub) и хэш-тега с частью ключа

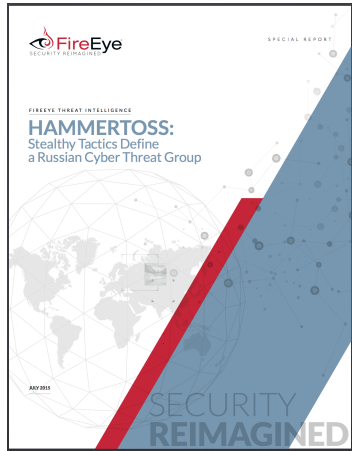


Скачивание изображения

В изображении зашифрованы инструкции (стеганография)

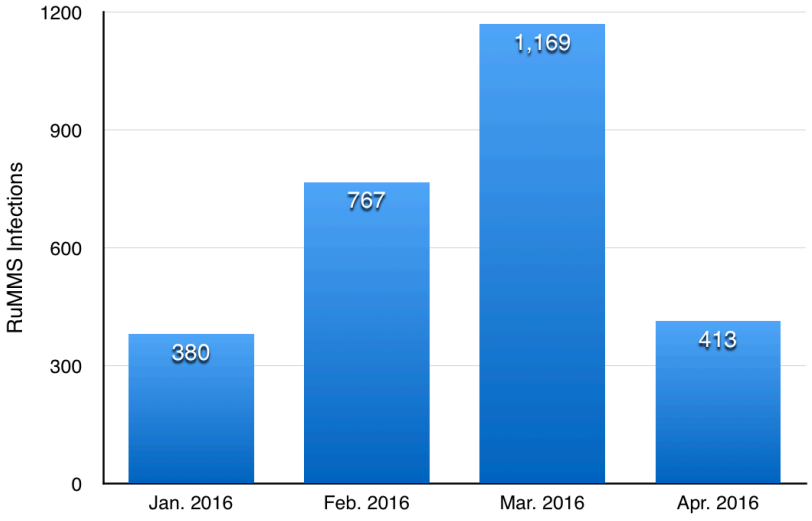
Выполнение инструкций, включая команды PowerShell, отправка данных в облако

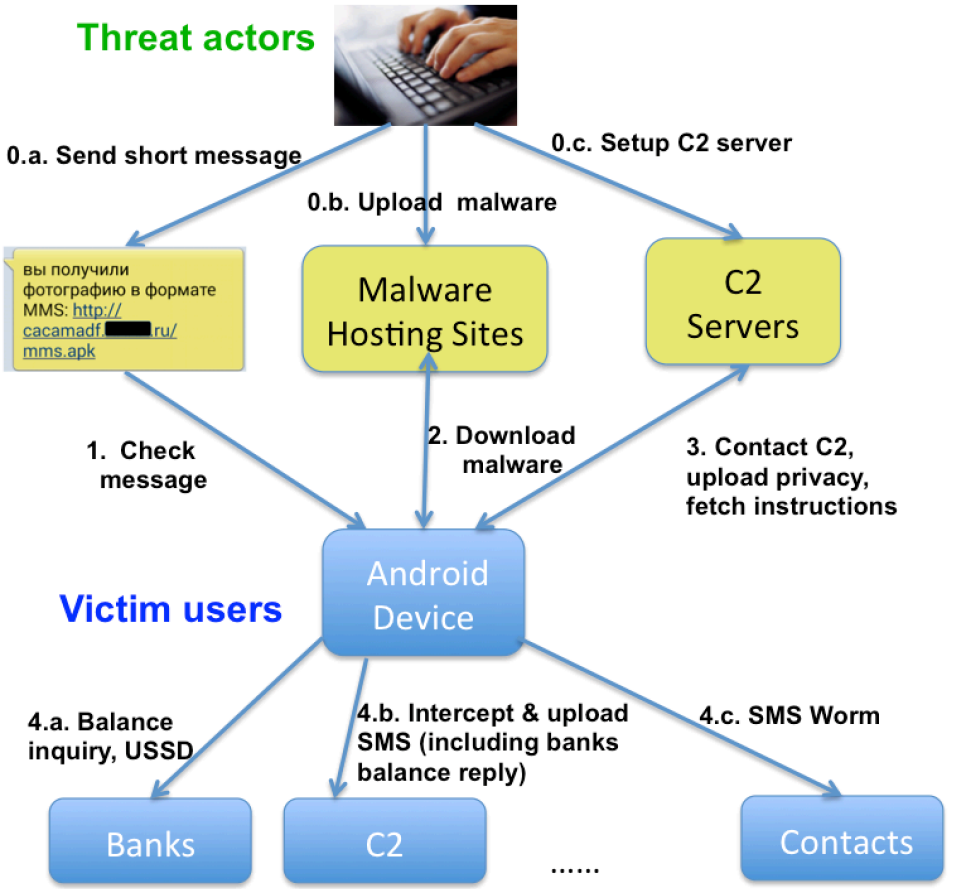
Note: The images are stock photography and were not used by the group.



Пример 3: Android malware – RuMMS (2016) СМС фишинг с российским хостингом

http://yyyyyyyy[.]XXXX.ru/mms.apk
300+ вариантов вредоносных Android APK





https://www.fireeye.com/blog/threat-research/2016/04/rumms-android-malware.html

FireEye

FireEye

MVX

Как мы обнаруживаем подобные атаки?

SECURITY REIMAGINED

MVX – ядро платформы FireEye

1 Гипервизор собственной разработки

- Защищен от обнаружения и обхода «песочницы»
- Создан для анализа вредоносного кода

2 Мульти-версионная виртуальная эмуляция

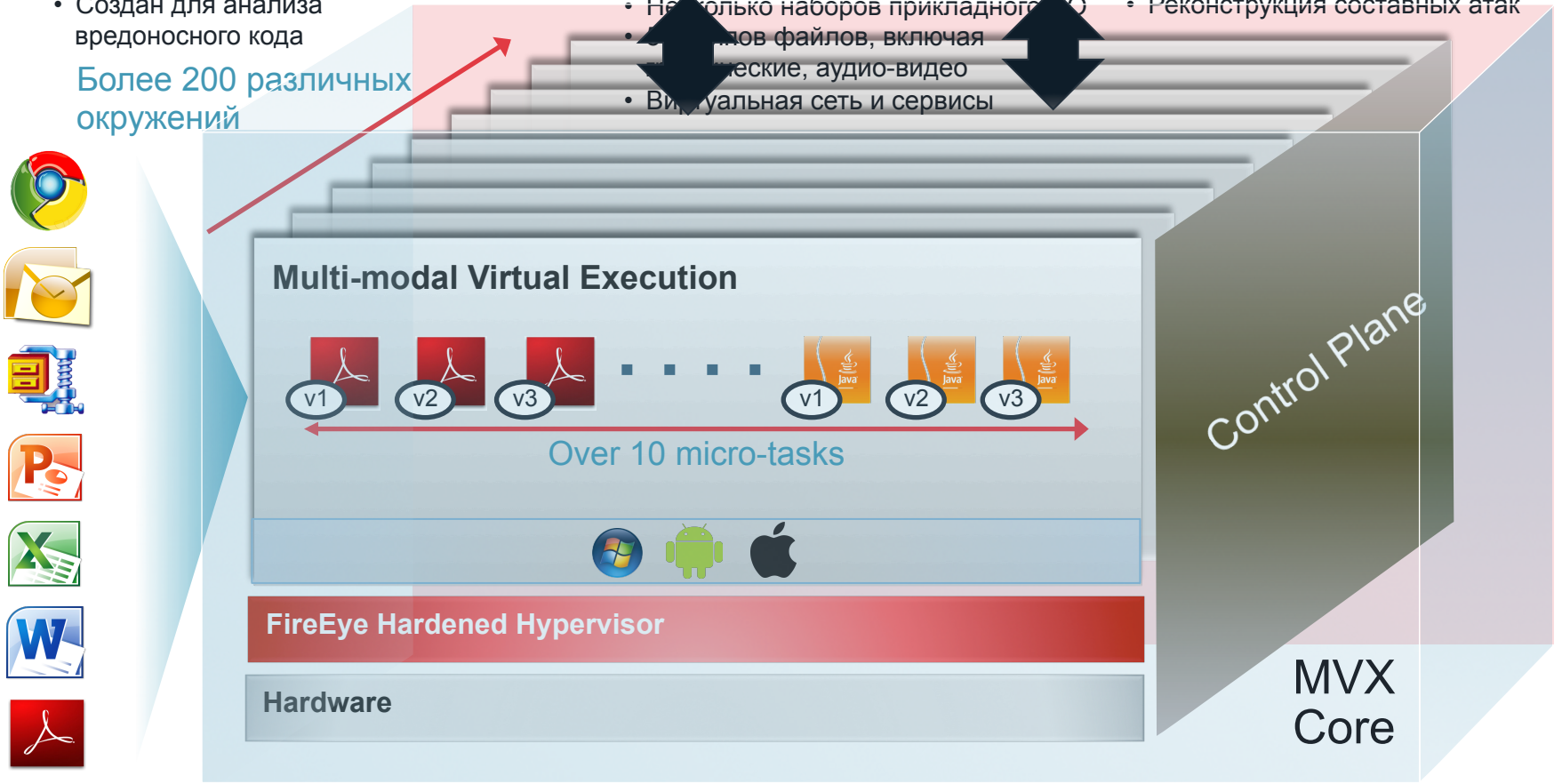
- Несколько ОС (Windows, Mac)
- Несколько Service Pack
- Несколько наборов прикладного ПО
- [illegible] файлов, включая [illegible]ческие, аудио-видео
- Виртуальная сеть и сервисы

3 Масштабирование защиты

- Более 2000 одновременных эмуляций
- Реконструкция составных атак

Локальная база DTI Облако DTI

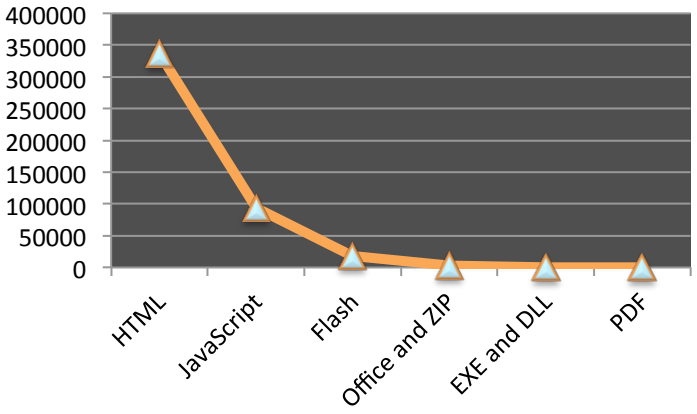
Более 200 различных окружений



FireEye

Как мы обнаруживаем 0-day веб-эксплойты и составные атаки?

Кол-во объектов в час (в сред.)



HTML и Javascript – это 95% анализируемых объектов

YARA, SNORT

MD5 (VirusTotal)

Intrinsic Analysis

Riskware (PUP)

Статический анализ, фильтрация, **кеширование трафика**

Динамический анализ в виртуальных машинах

(ядро MVX)

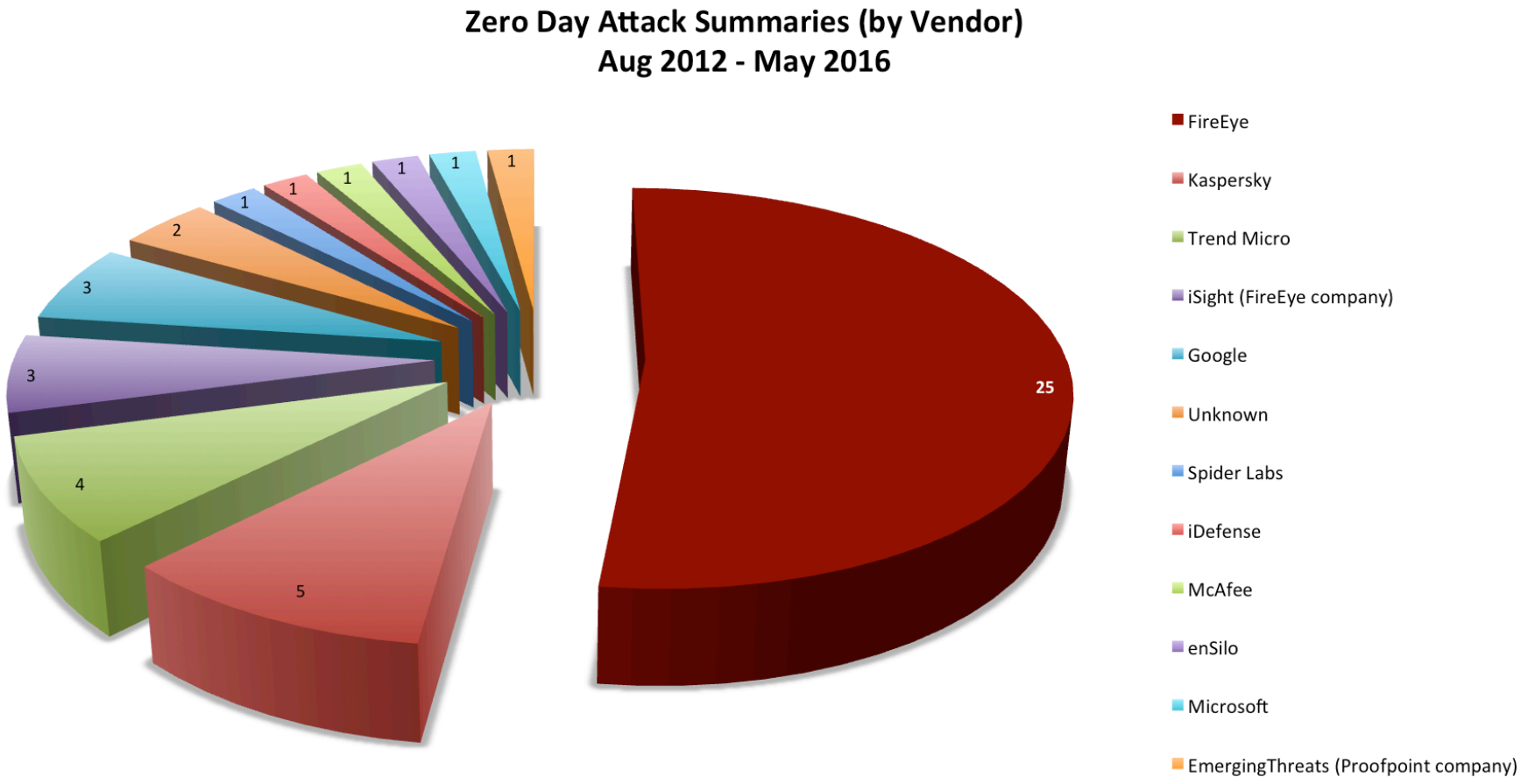
Фаза 1
Уменьшить False Negatives

Фаза 2
Уменьшить False Positives

MVX

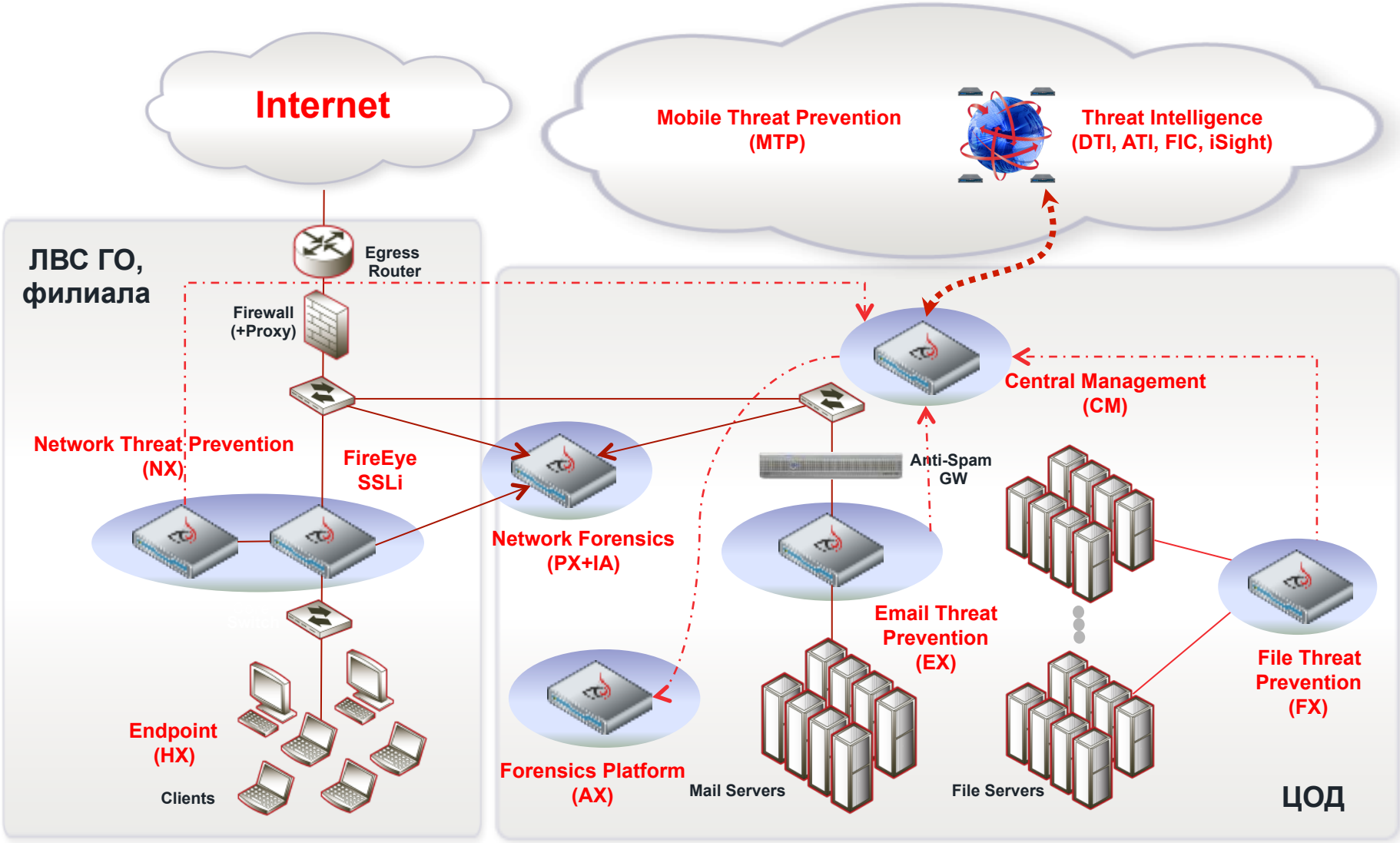
FireEye

Обнаруженные уязвимости «нулевого» дня, использованные в атаках за последние 3 года (согласно данным на сайте CVE*)



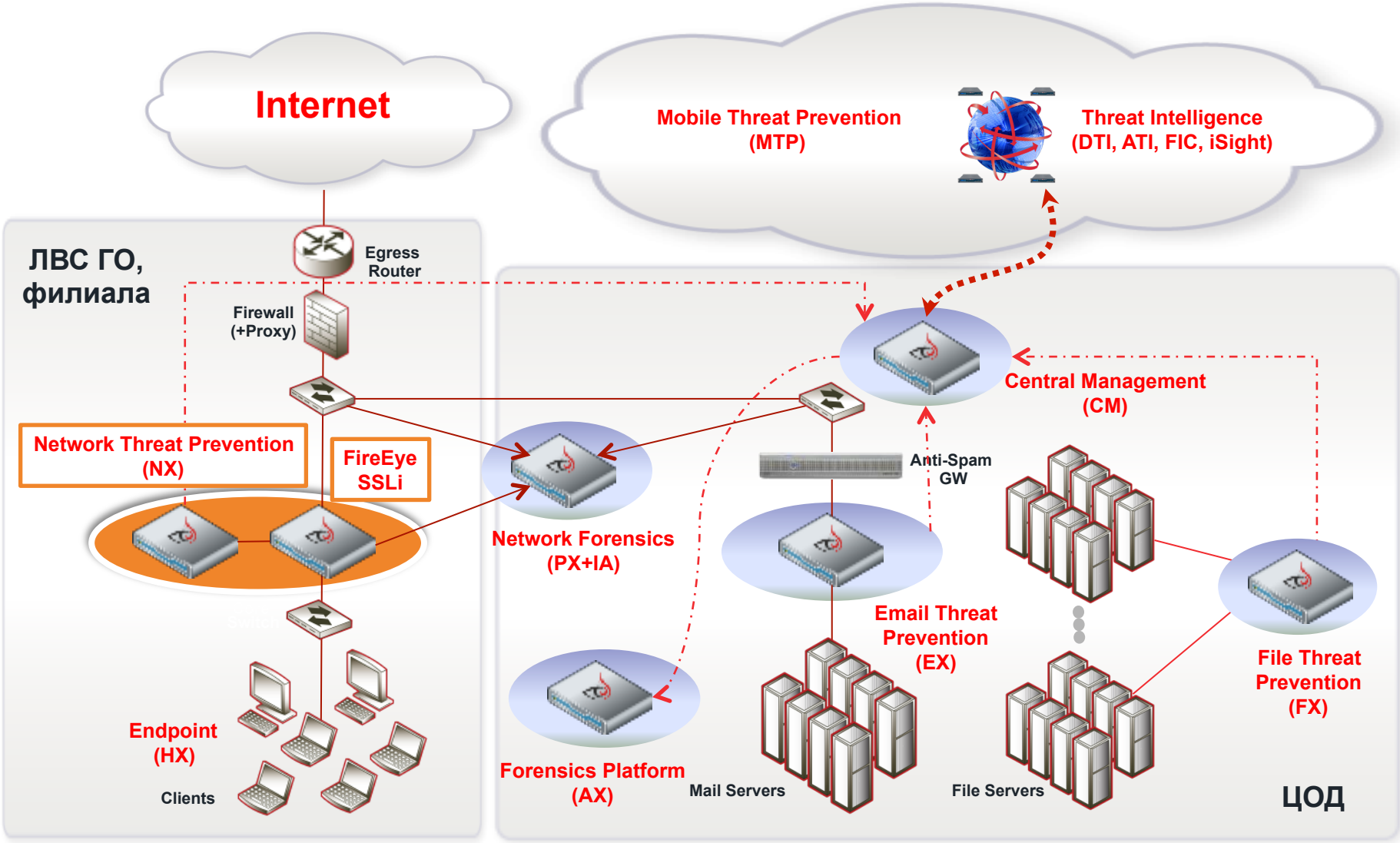
*Детальный список со ссылками на описание уязвимостей и атак доступен по запросу

Компоненты платформы FireEye



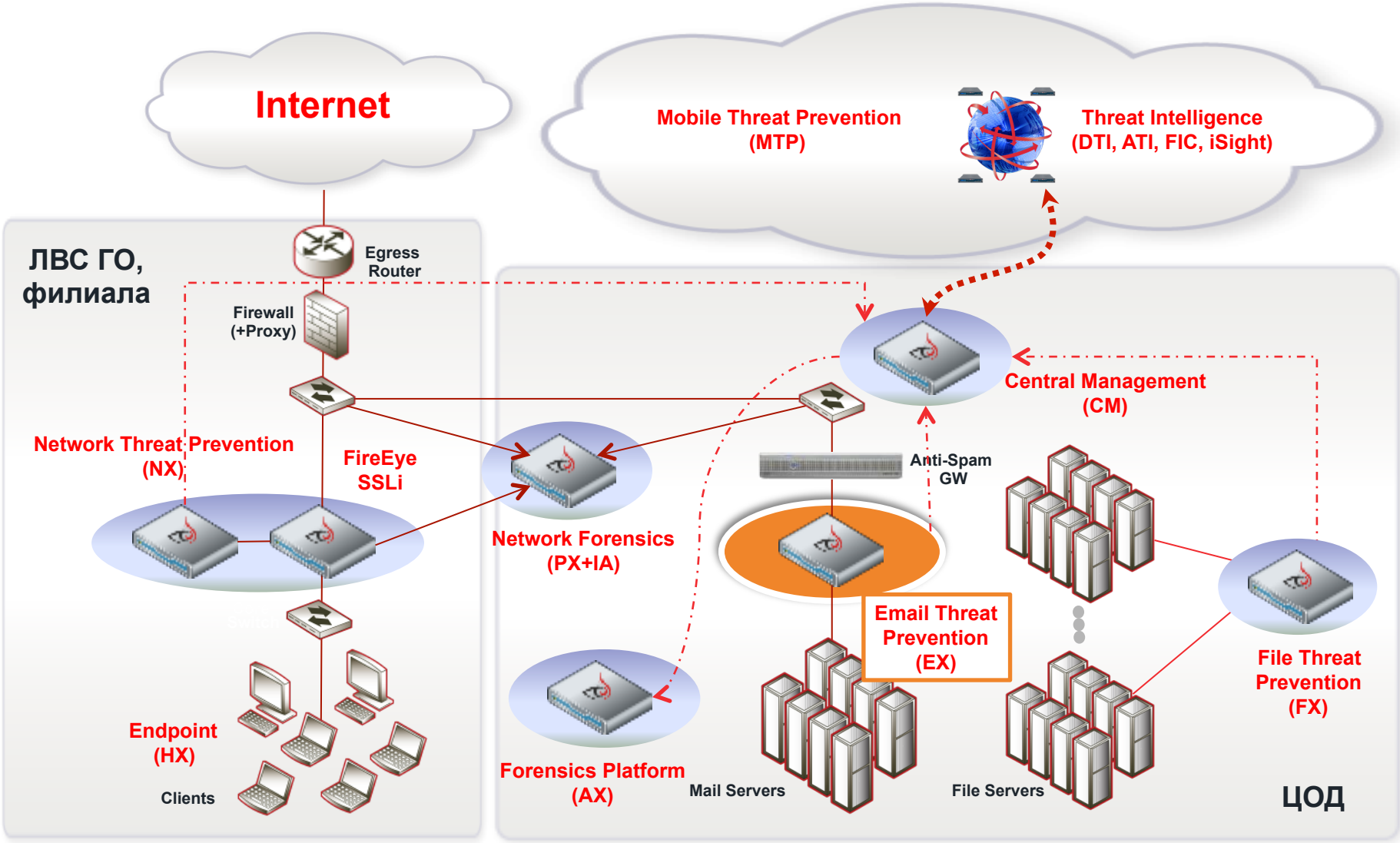
FireEye

Компоненты платформы FireEye: NX
Защита на уровне веб-трафика пользователей



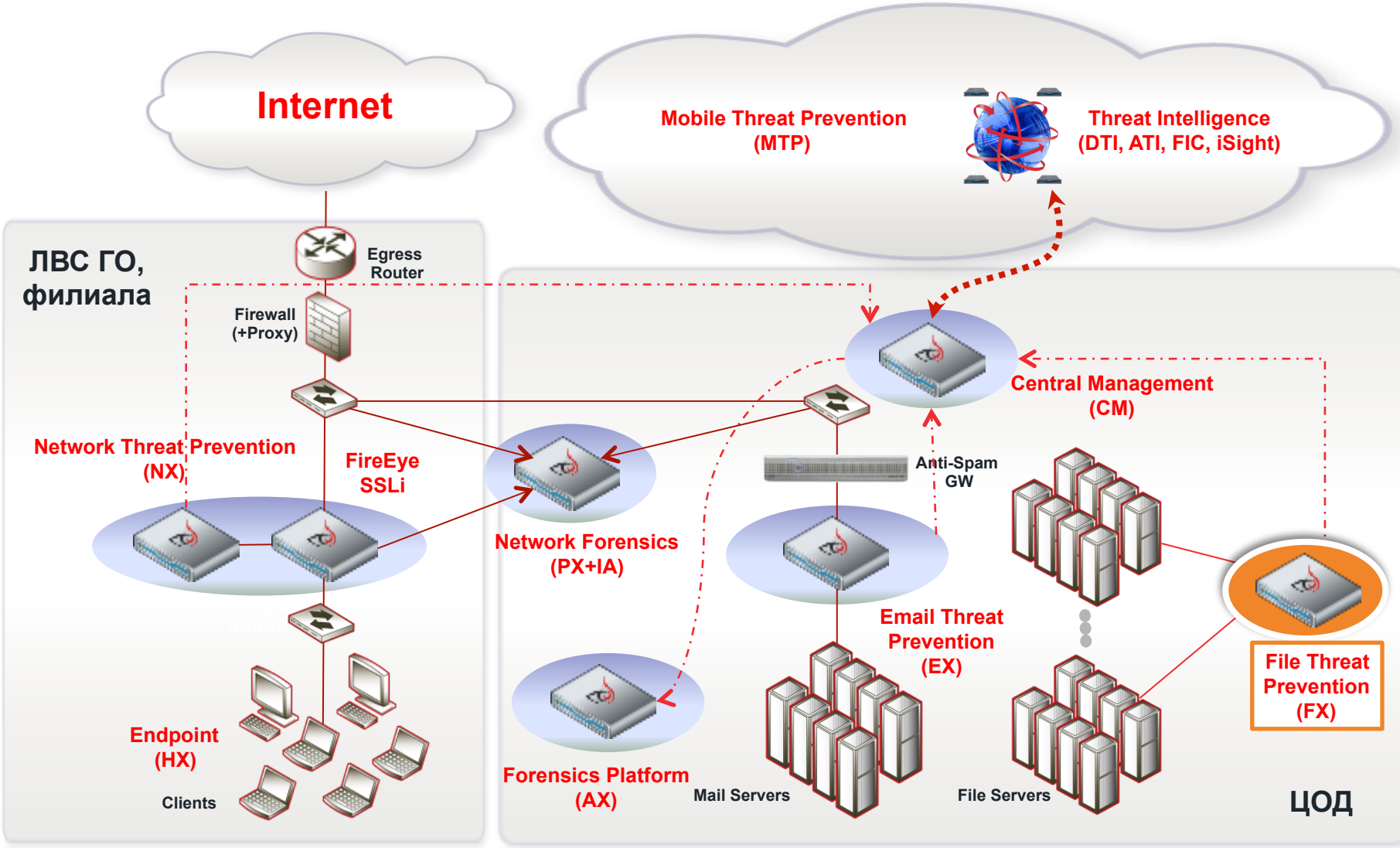
FireEye

Компоненты платформы FireEye: EX
Защита на уровне почтового-трафика



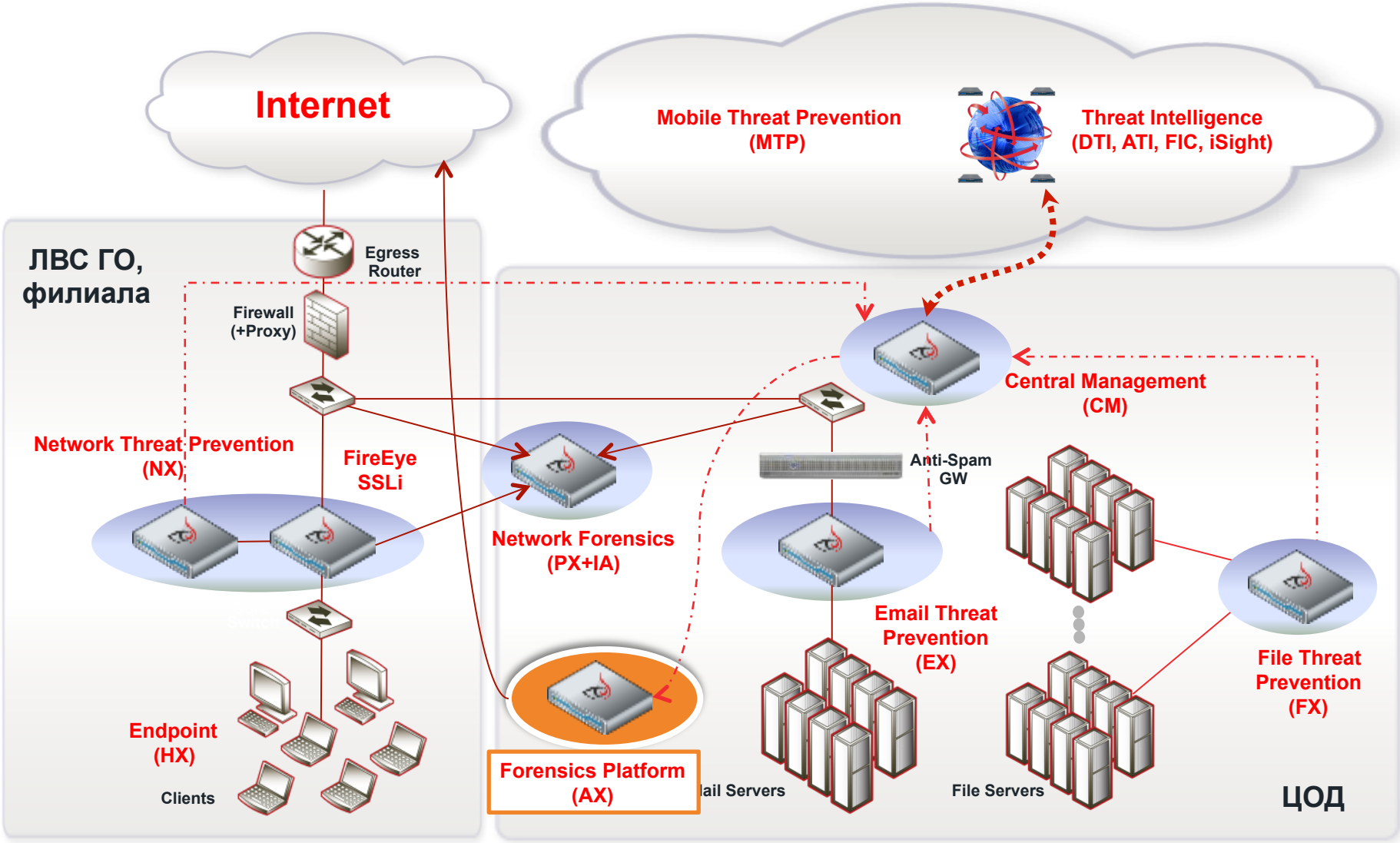
FireEye

Компоненты платформы FireEye: FX
Защита на уровне корпоративных файловых сервисов



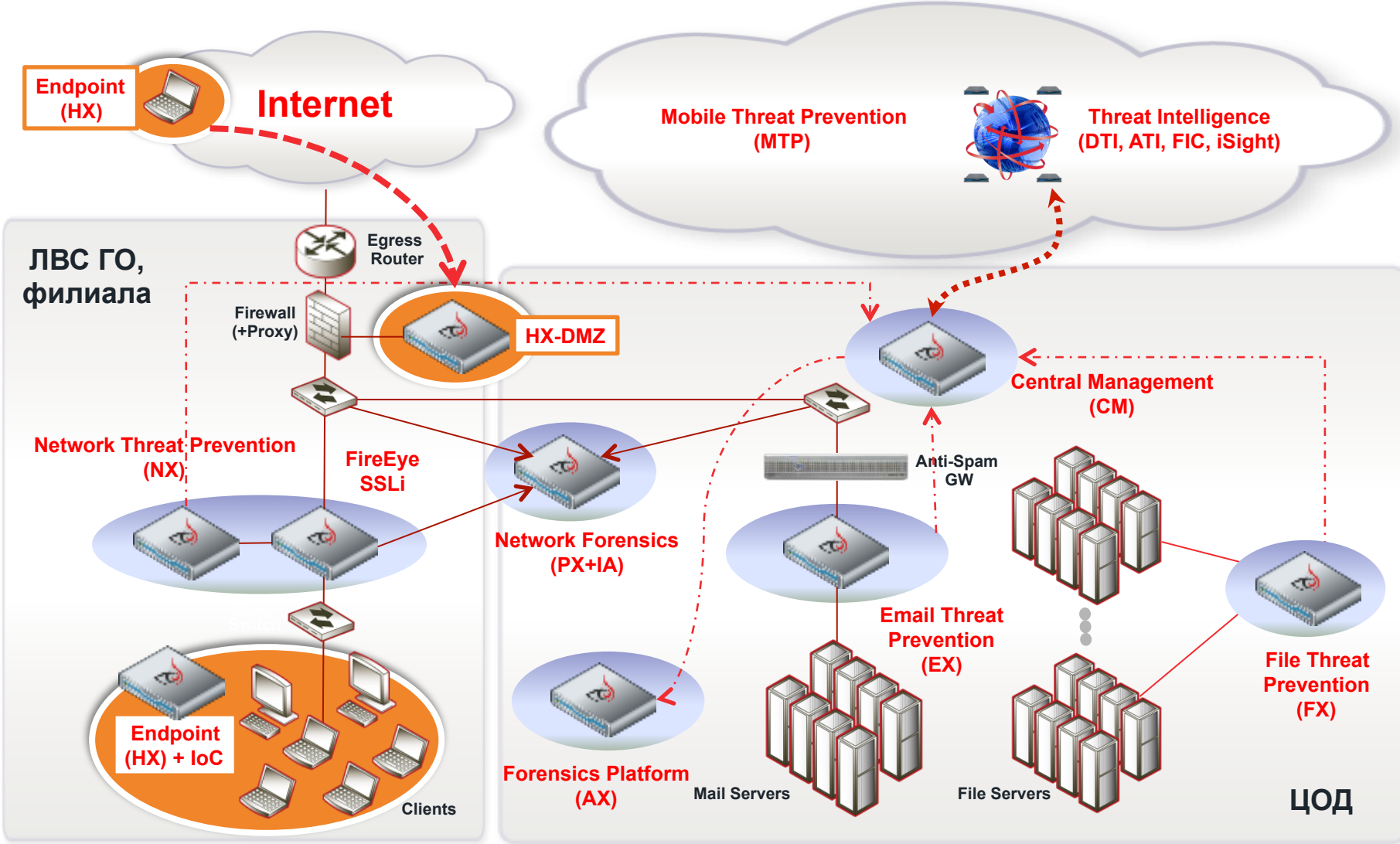
FireEye

Компоненты платформы FireEye: AX
Детальный анализ с доступом в Интернет из MVX + API



FireEye

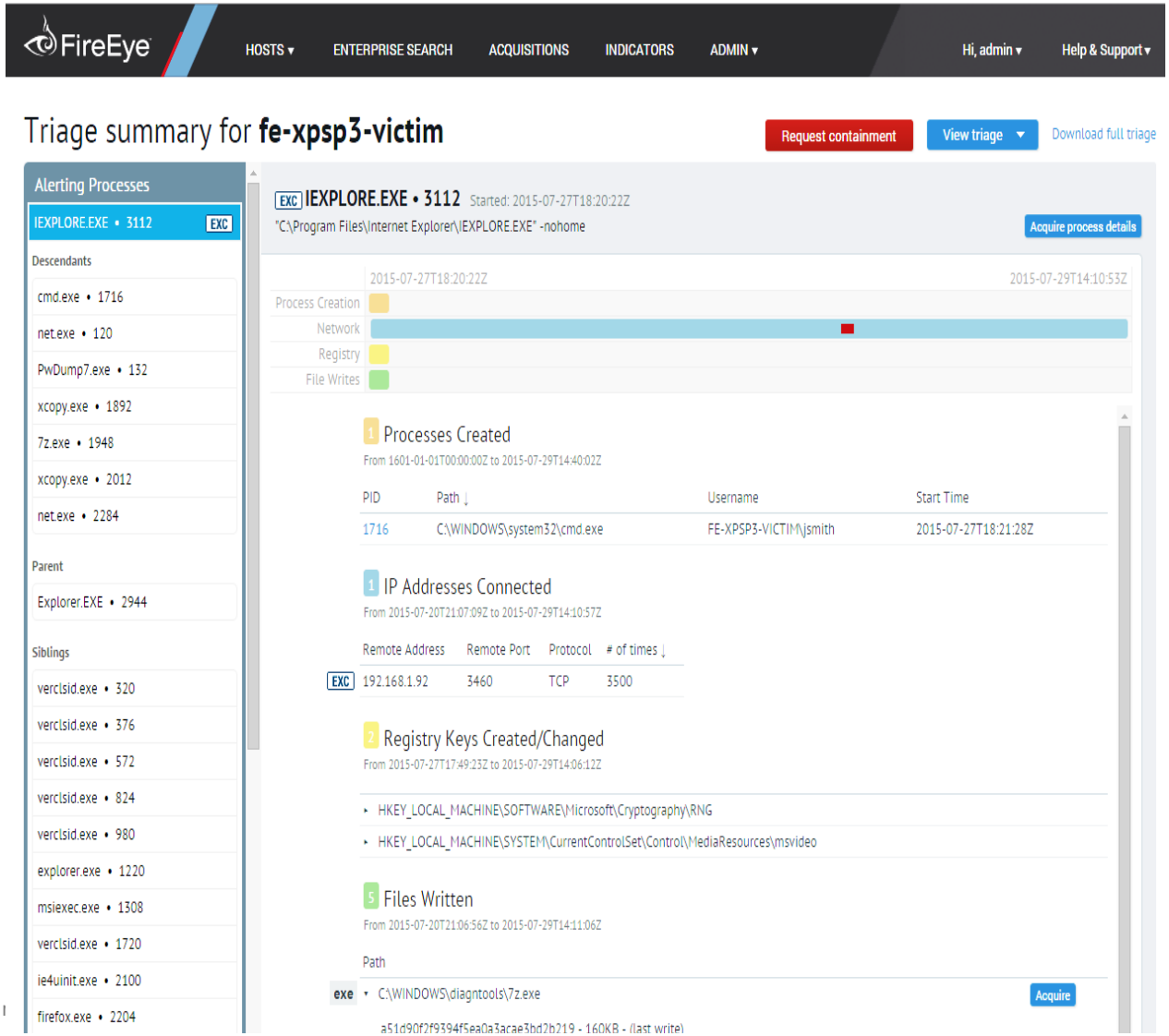
Компоненты платформы FireEye: HX
Расследование инцидентов на уровне конечных точек



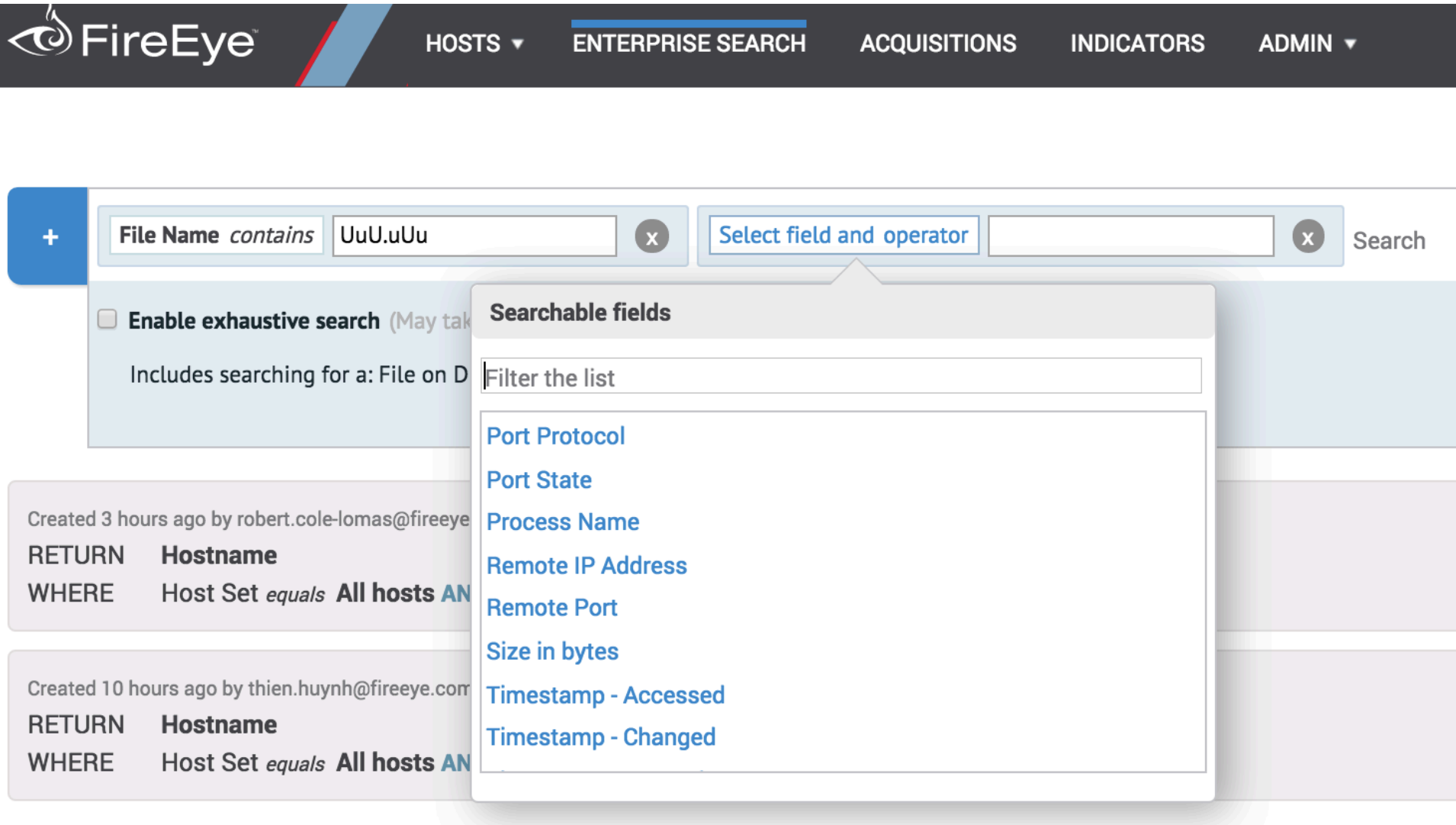
FireEye

HX: Triage Viewer – визуализация и простой анализ поведения ВПО на любой станции

- Позволяет увидеть все взаимосвязанные события, которые произошли до и после срабатывания **IoC**
- Повышение эффективности работы аналитика (снижаются требования к его квалификации и опыту)
- Возможность использования внешней аналитики для получения сведений о контексте угрозы (iSight Partners)



HX: быстрый корпоративный поиск по 70+ параметрам на всех конечных точках



HX: обнаружение 0-day эксплойтов **непосредственно** на рабочих станциях

Обнаружение новых эксплойтов (ExD) без сигнатур аналогично «песочнице»:

- Memory corruption
- Heapspray
- Office macros
- Drive by download
- Java sandbox bypass
- Kernel exploit

Взвешенная система оценки по совокупности обнаруженных техник
Предотвращение (ExP) – вторая половина 2016

Hosts with Alerts (30)

1-30 of 30

Actions Go 0 hosts selected

Hostname	IP Address	Newest Alert	Alerts	Alert Types	Acquisitions
victim-PC	10.100.9.26	33 hours ago	8	PRE EXC XPL	3
victim-PC	10.100.9.21	3 days ago	8	PRE EXC XPL	9
victim-PC	10.100.9.20	3 days ago	5	PRE EXC XPL	3
victim-PC	10.100.8.229	6 days ago	6	PRE EXC XPL	9
victim-PC	10.100.8.217	7 days ago	5	PRE EXC XPL	3
victim-AT	10.100.8.213	7 days ago	5	PRE EXC XPL	5
victim-PC	10.100.8.179	7 days ago	3	PRE XPL	1
victim-PC	10.100.8.166	8 days ago	5	PRE EXC XPL	4
victim-PC	10.100.8.164	8 days ago	8	PRE EXC XPL	5
victim-PC	10.100.8.157	8 days ago	6	PRE EXC XPL	4
victim-PC	10.100.8.156	8 days ago	7	PRE EXC XPL	2

Detail for victim-PC

Alerts (8) | Host Details

Latest triage (download)

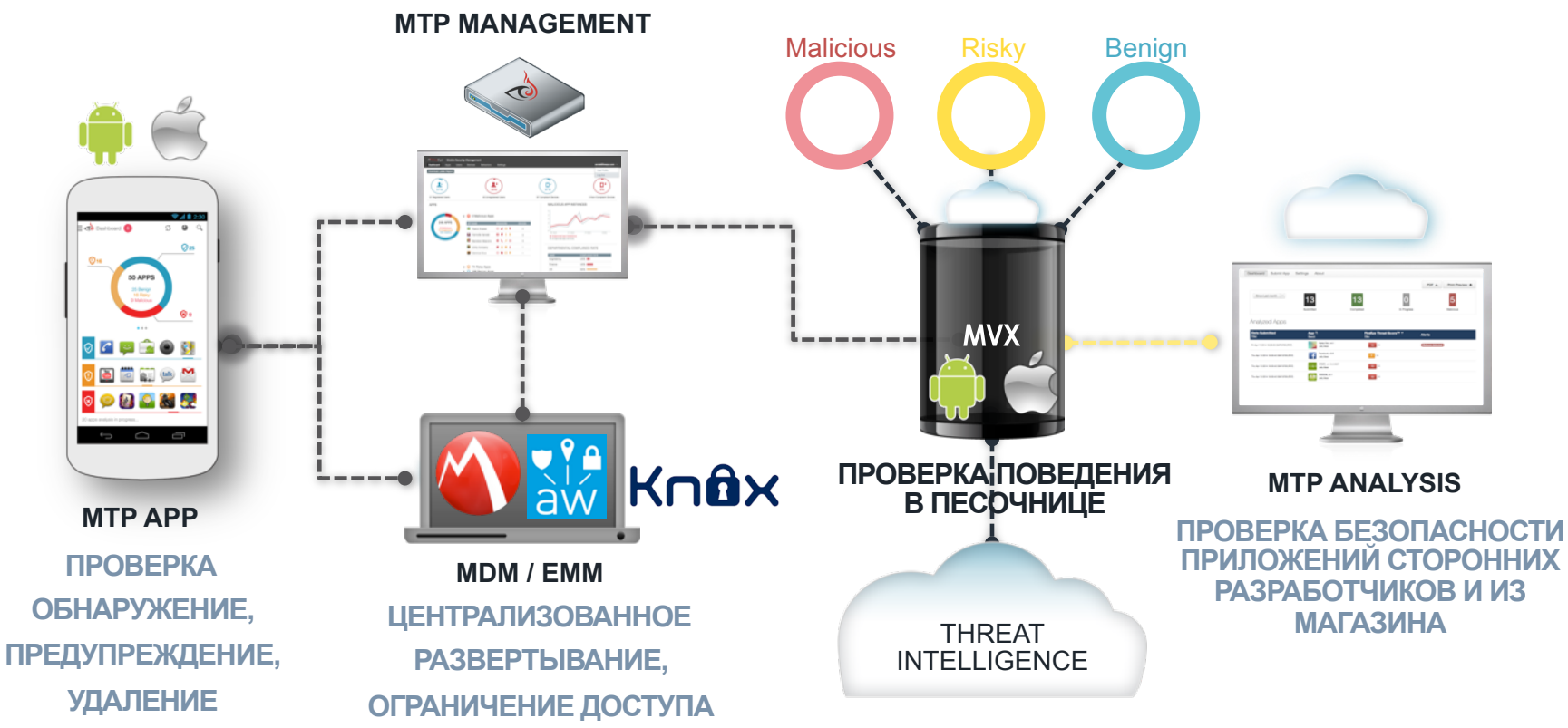
XPL **Exploit** detected in **iexplore.exe**

Alerted 3 days ago

Events

ROP Shellcode Activity
Thread created in remote process using ROP
Exploit Shellcode accessing internet
Exploit Shellcode requesting http content
Exploit Shellcode is creating a file
Exploit Shellcode writing to a file
Process hiding file/folder
Exploit Shellcode launching a process
Drive By Download detected
Executable file created in temp folder

Компоненты платформы FireEye: MX/MTP
Защита на уровне мобильных устройств



- **Динамический анализ приложений для Android (в т.ч. сторонних) и iOS**
- Оповещение пользователей и/или администраторов ИБ об обнаруженных угрозах
- Применение политик в зависимости от состояния устройства

FireEye

Непрерывный цикл защиты: Обнаружить, Предотвратить, Расследовать, Отреагировать, Автоматизировать

SECURITY REIMAGINED

ЦИКЛ ЗАЩИТЫ ОТ APT

1 Обнаружить

+

2 Предотвратить

- Без сигнатур
- Угрозы «нулевого» дня и целенаправленные атаки
- Составные и мульти-векторные атаки
- Детальные отчеты и IoC
- Защита в реальном времени
- Масштабирование и производительность

ЦИКЛ ЗАЩИТЫ ОТ APT

3 Расследовать инцидент

на уровне рабочих станций

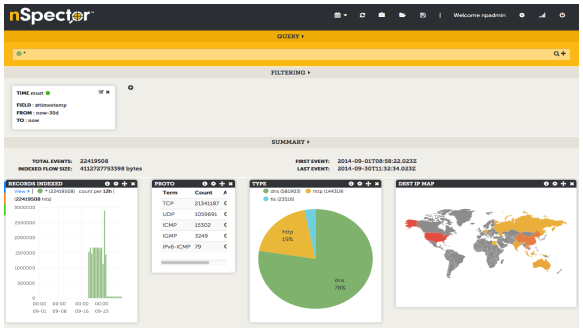
- Автоматическое подтверждение компрометации по IoC
- Анализ истории событий в момент инцидента и в прошлом
- Изоляция станции
- Независимо от физического местоположения

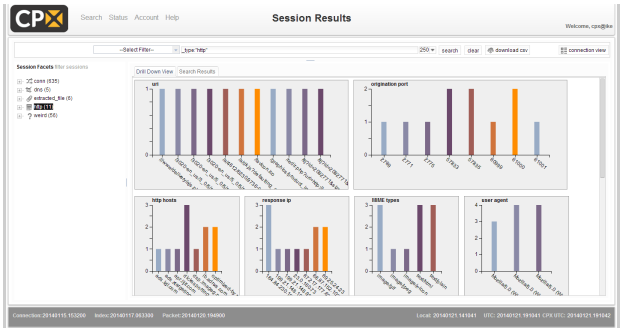
ЦИКЛ ЗАЩИТЫ ОТ APT

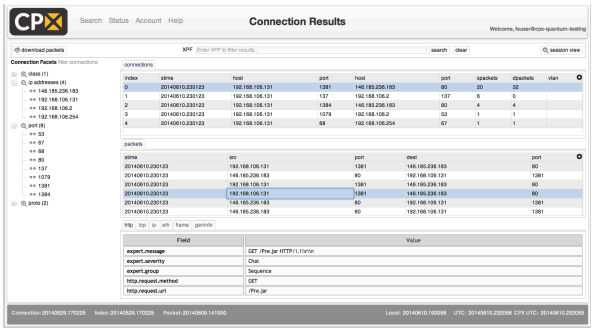
3 Расследовать инцидент на уровне сети

Как протекала атака от начала до конца? Какие данные были украдены?

От лога к PCAP





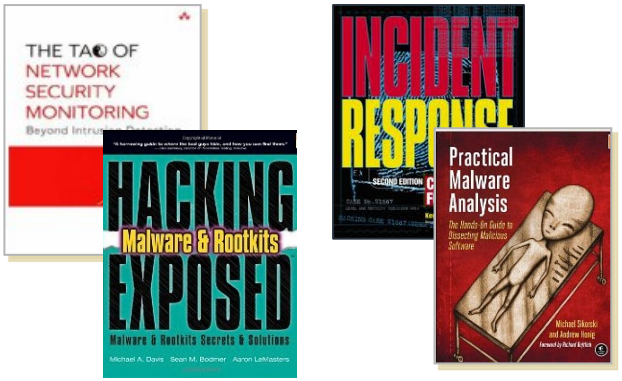


FireEye

ЦИКЛ ЗАЩИТЫ ОТ APT

4 Отреагировать

Intelligence & Attribution:
Знать своего врага, его цели и методы и адекватно строить защиту



ЦИКЛ ЗАЩИТЫ ОТ APT

5 Автоматизировать процессы реагирования

Снизить время на рутинные проверки в нескольких системах, департаментах и внешних сервисах, сократить трудозатраты и стоимость, повысить эффективность SOC, IR, CERT

FireEye Security Orchestrator

FireEye

Вопросы?

Вы можете в любое время пересылать фишинговые письма, и направлять тестовые файлы и ссылки на следующие ящики (на оба сразу):

aleksey.beloglazov@ork.selabs.fireeye.com

aleksey.beloglazov@dxb.selabs.fireeye.com

При этом необходимо направлять мне уведомление:

Aleksey.Beloglazov@FireEye.com