



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

SECURITY
REIMAGINED

Сколько вендоров предлагают защиту от APT?



200+

Что все продают?



Что в итоге?

Банк J.P.Morgan после взлома

Dear Fellow Shareholders,



Jamie Dimon,
Chairman and
Chief Executive Officer

What a year. Despite tremendous challenges, your company earned \$179 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

*«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

1

100% защиты не бывает

Недостатки традиционного подхода

146 ДНЕЙ

СРЕДНЕЕ ВРЕМЯ ОБНАРУЖЕНИЯ УСПЕШНОГО ВЗЛОМА

32 ДНЯ

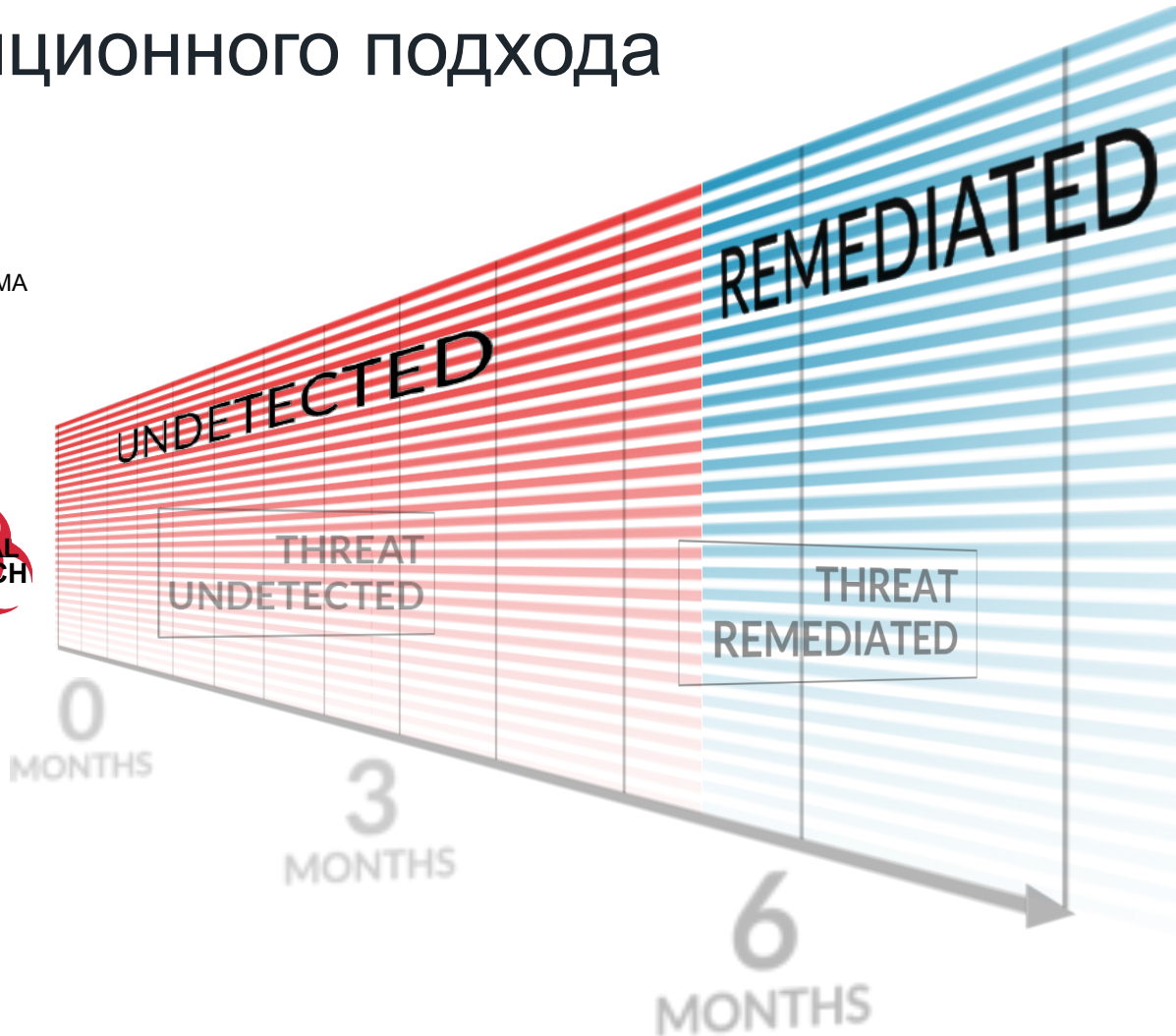
НА УСТРАНЕНИЕ ПОСЛЕДСТВИЙ

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

Еще одна простая истина

2

*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

3

*В слове APT ключевое слово –
persistent*

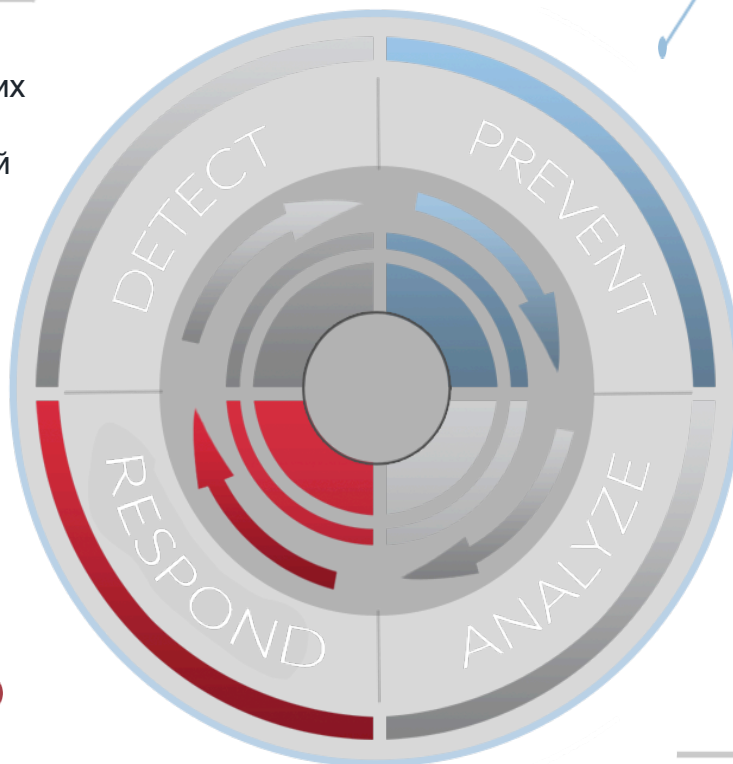
Непрерывный цикл защиты от АРТ

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 заблокировать 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



Как строится современная составная атака (Multi-Flow Attack)



SECURITY
REIMAGINED

Этапы составной атаки (Kill-Chain)



Вредоносный /
взломанный веб-сайт



Серверы с
дополнительным
контентом



Вредоносный код
зашифрован в
легитимном
контенте



Внешний сервер
управления



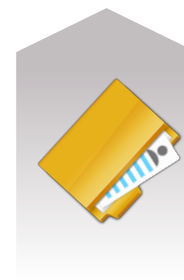
Эксплойт
«нулевого» дня /
JavaScript



Запрос контента
2-й, 3-й и т.д.
фазы



Расшифрование,
сборка и запуск



Обратный канал,
удаленное
управление /
доступ, кража
данных

Пример 2: HAMMERTOSS (2015)

Русскоязычная хакерская группа (APT29)

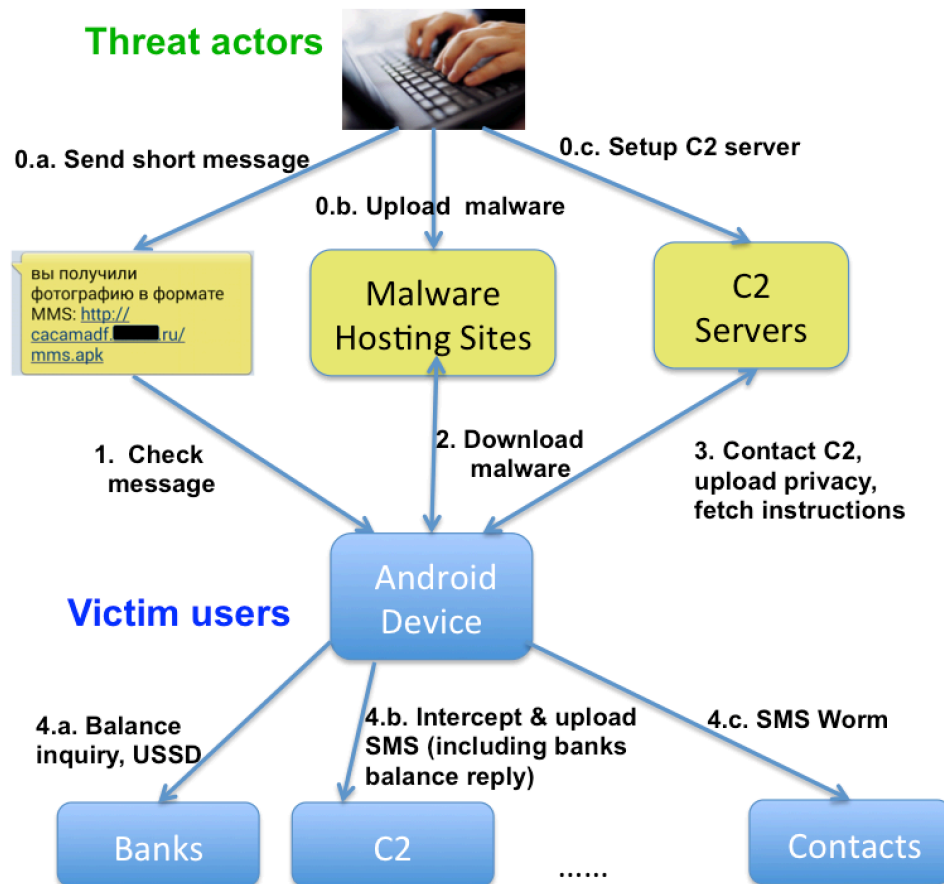
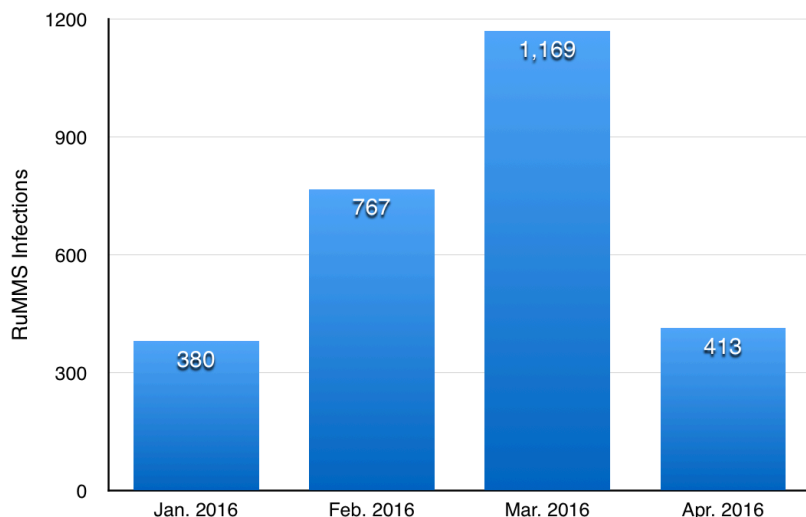


Пример 3: Android malware – RuMMS (2016)

СМС фишинг с российским хостингом

[http://yyyyyyyyy\[.\]XXXX.ru/mms.apk](http://yyyyyyyyy[.]XXXX.ru/mms.apk)

300+ вариантов вредоносных
Android APK



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



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

Более 200 различных окружений

2

Мульти-версионная виртуальная эмуляция

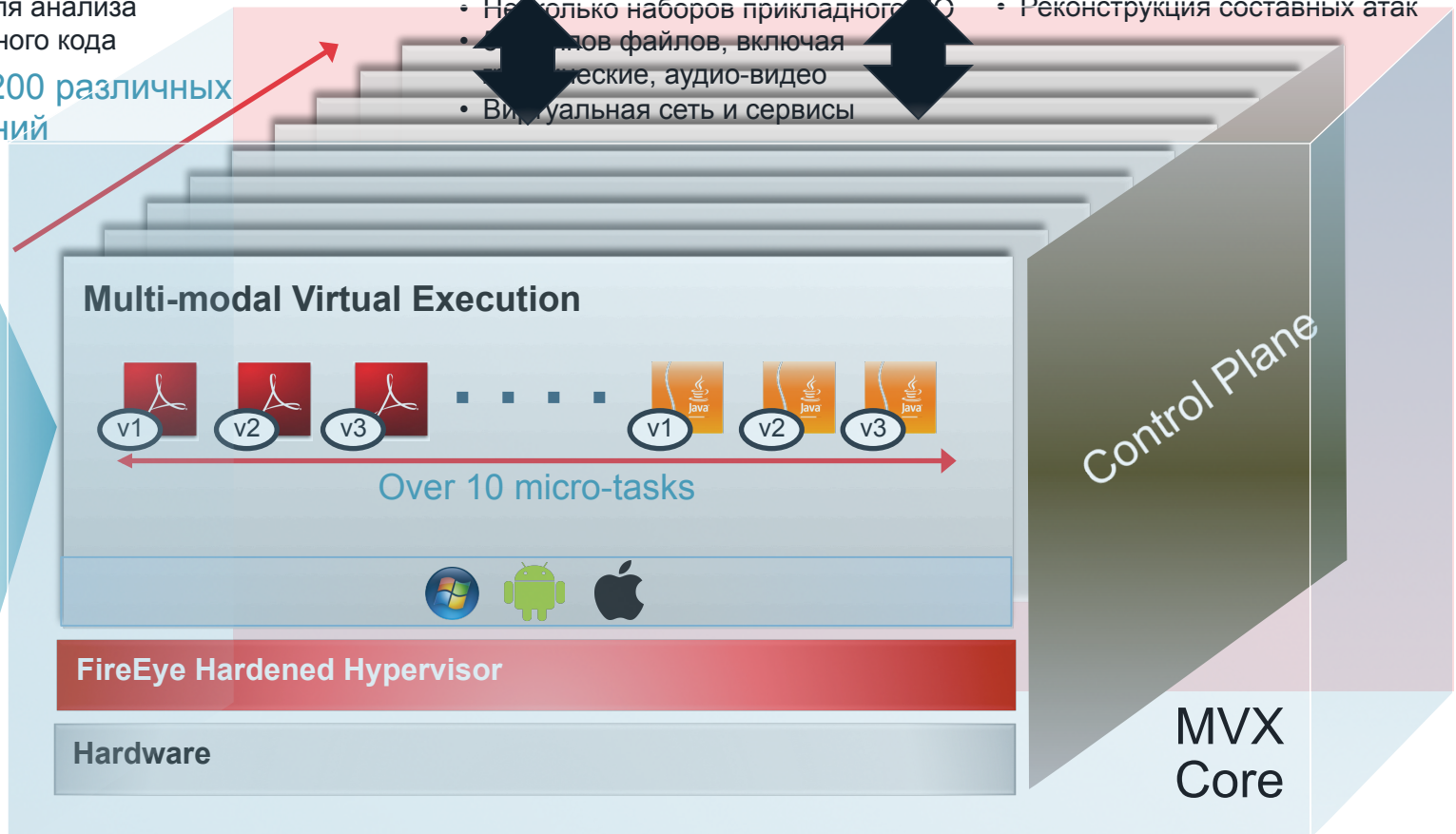
Локальная база DTT Облако DTT

- Несколько ОС (Windows, Mac)
- Несколько Service Pack
- Несколько наборов прикладного ПО
- Тысячи файлов, включая документы, аудио-видео
- Виртуальная сеть и сервисы

3

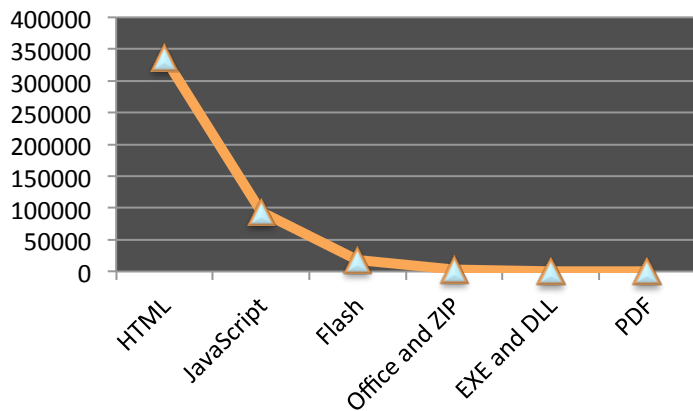
Масштабирование защиты

- Более 2000 одновременных эмуляций
- Реконструкция составных атак



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**

Фаза 1
Уменьшить False
Negatives

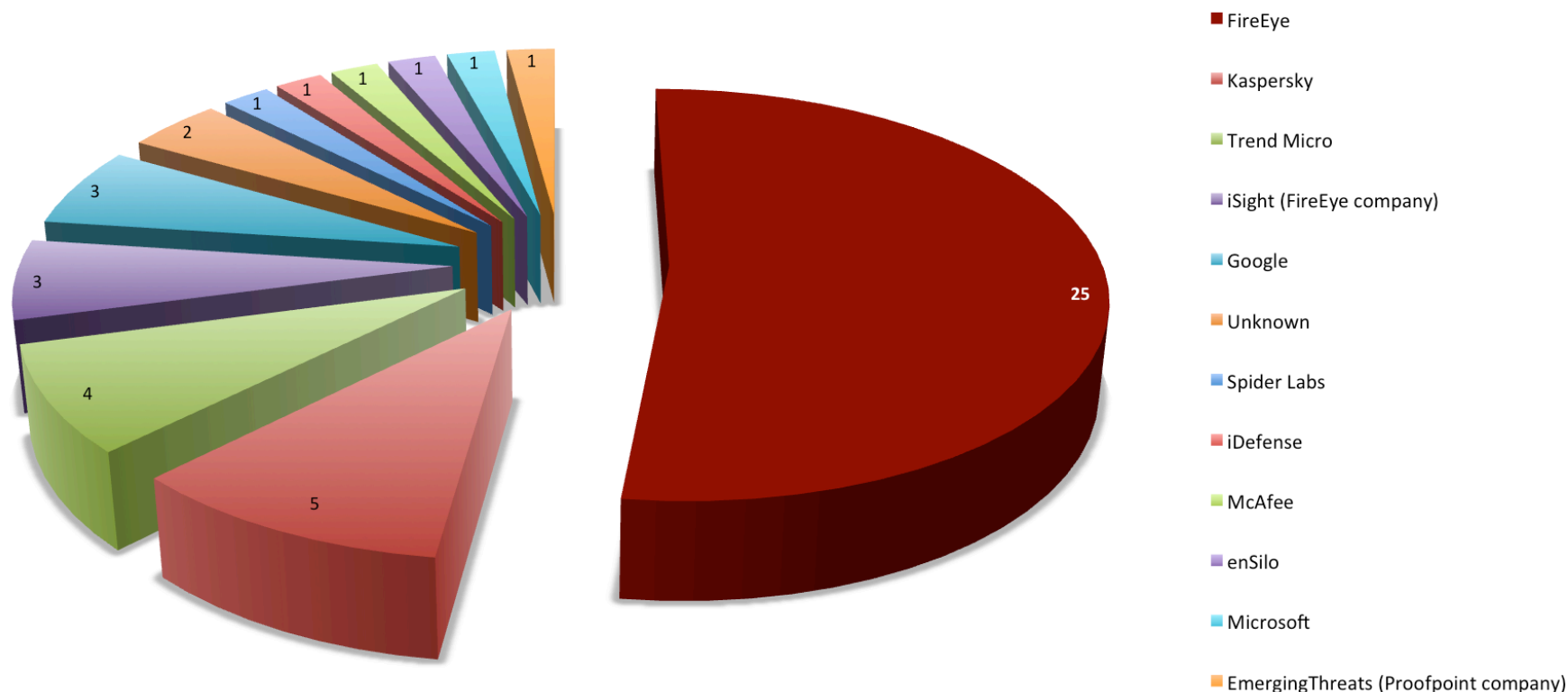
**Динамический
анализ в
виртуальных
машинах
(ядро MVX)**

Фаза 2
Уменьшить False
Positives

MVX

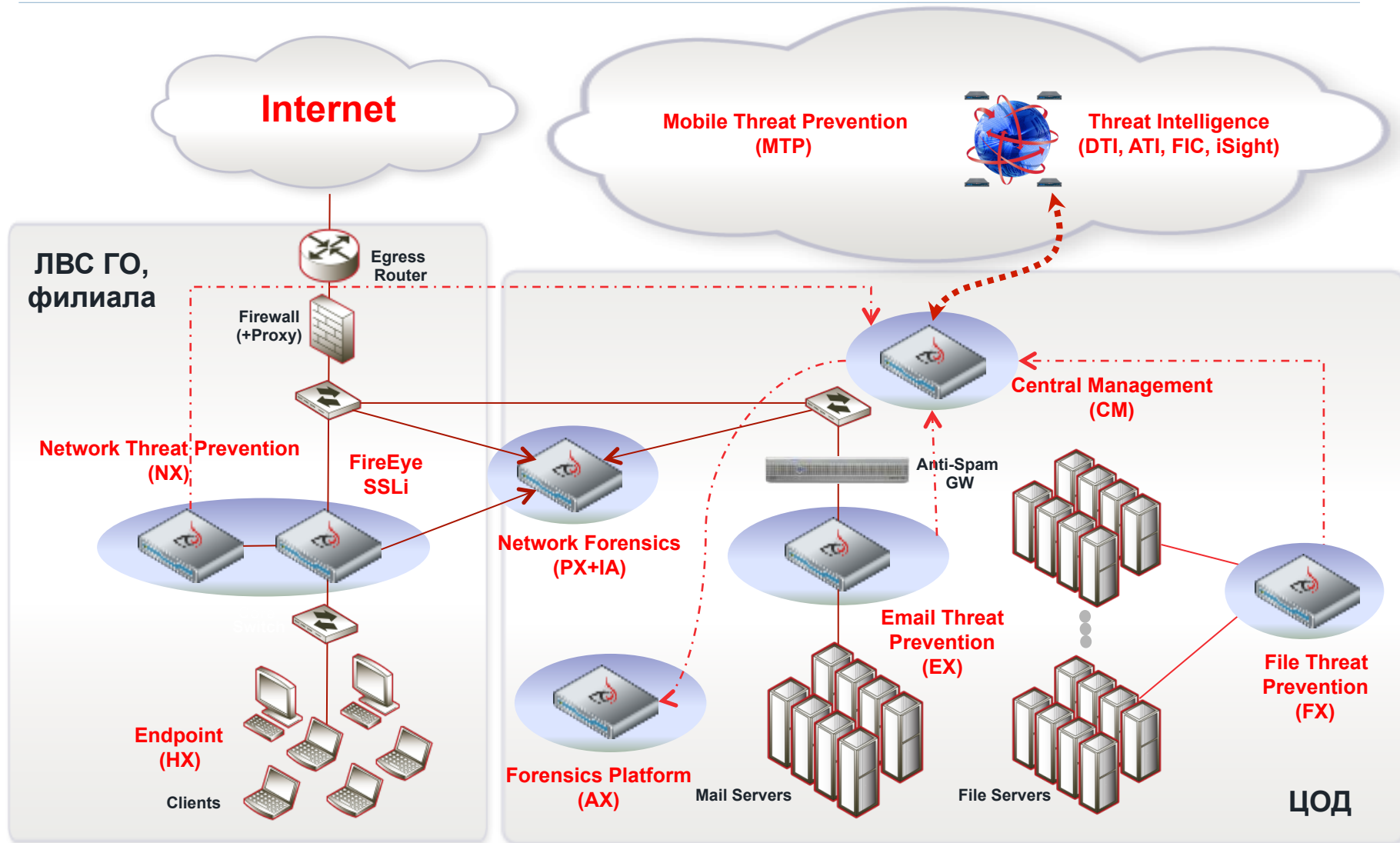
Обнаруженные уязвимости «нулевого» дня, использованные в атаках за последние 3 года (согласно данным на сайте CVE*)

Zero Day Attack Summaries (by Vendor)
Aug 2012 - May 2016



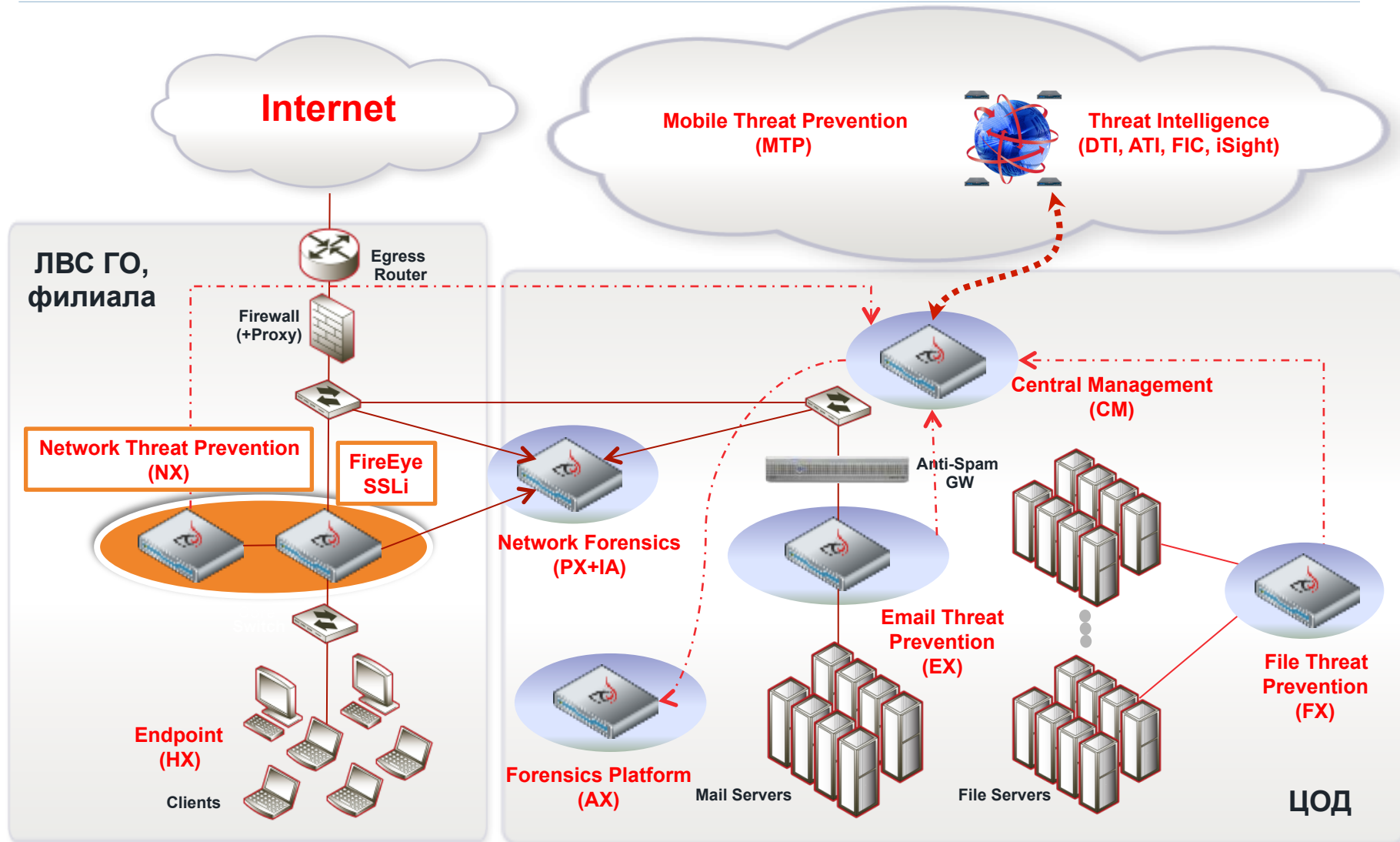
*Детальный список со ссылками на описание уязвимостей и атак доступен по запросу

Компоненты платформы FireEye



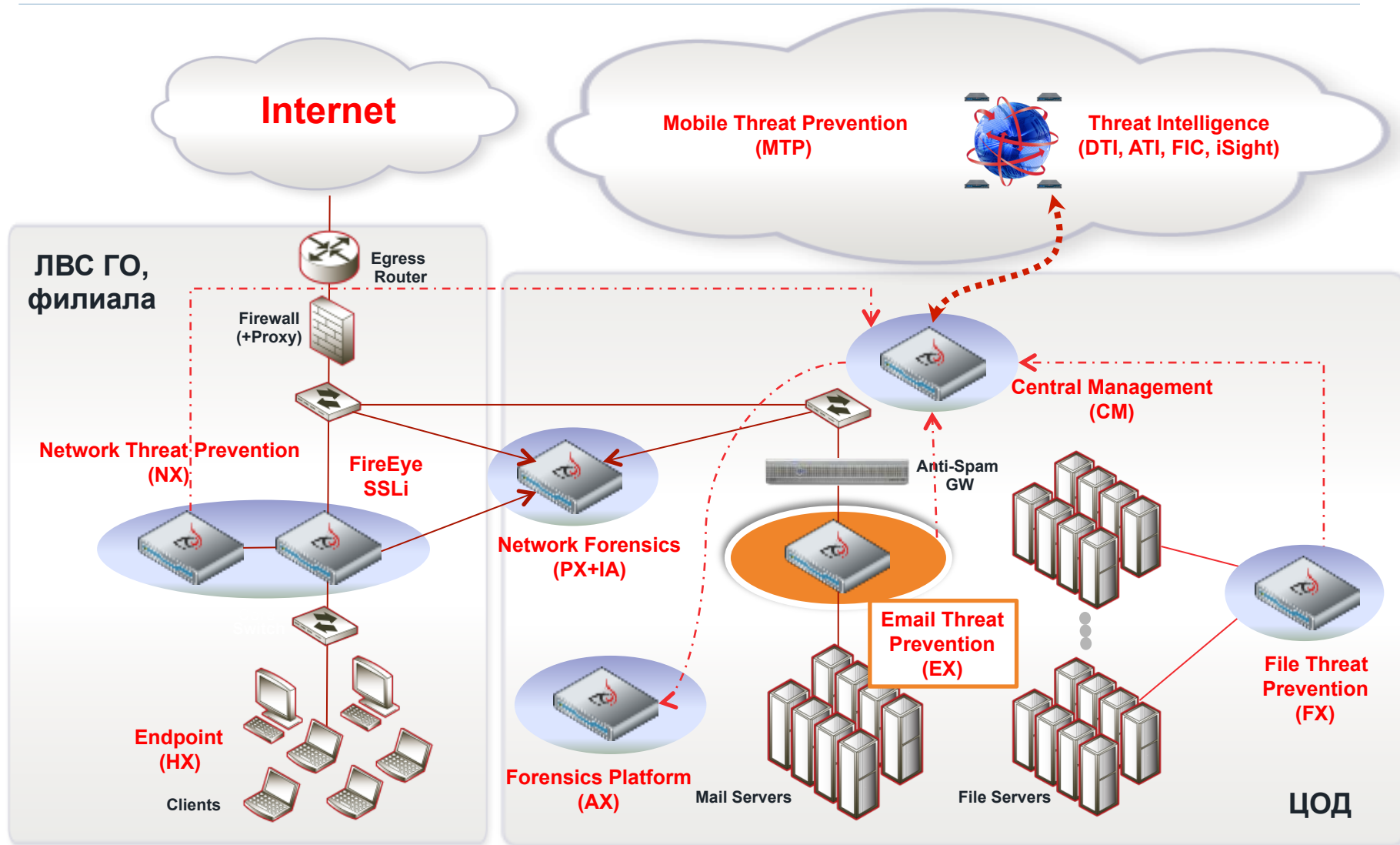
Компоненты платформы FireEye: NX

Защита на уровне веб-трафика пользователей



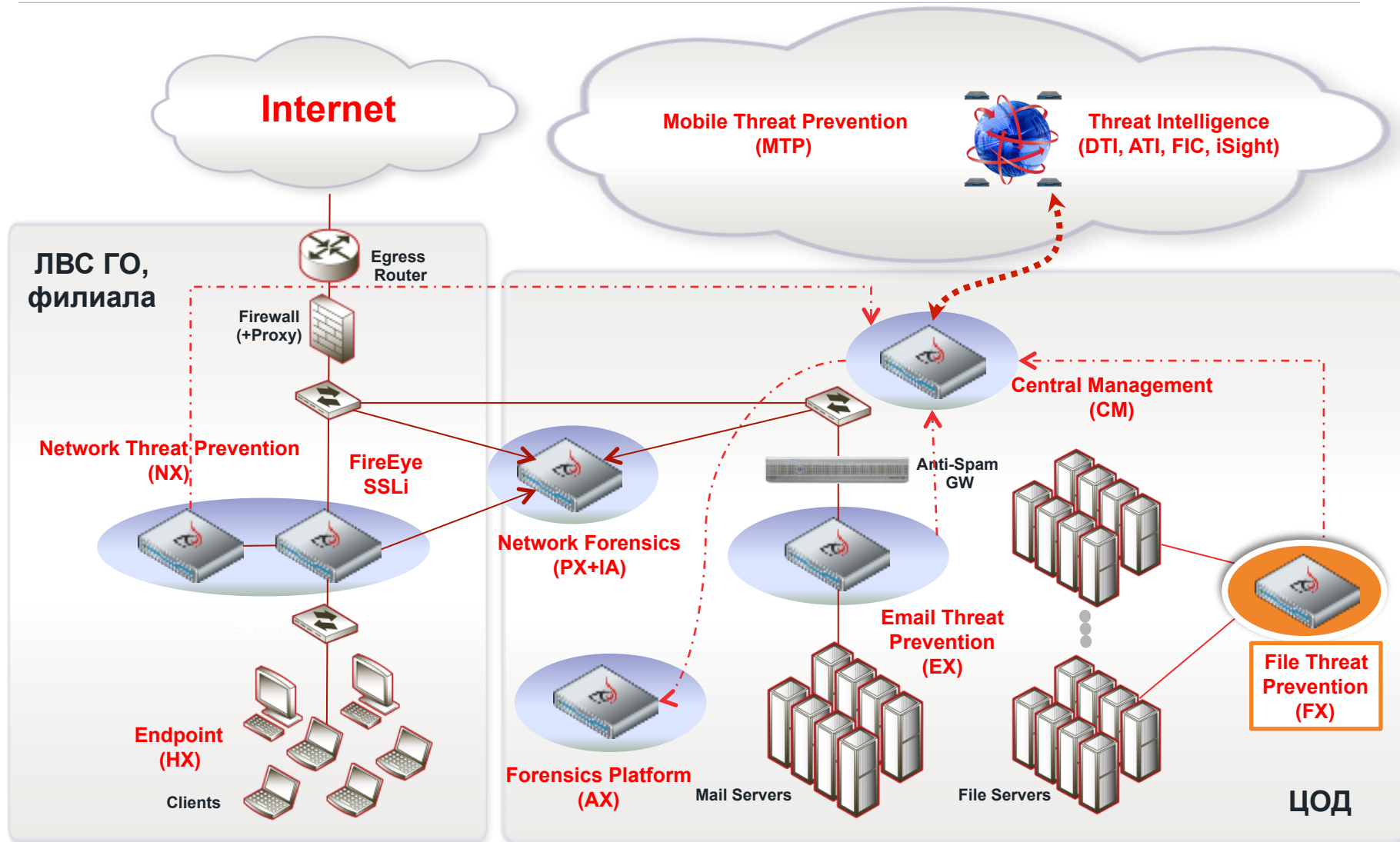
Компоненты платформы FireEye: EX

Защита на уровне почтового-трафика



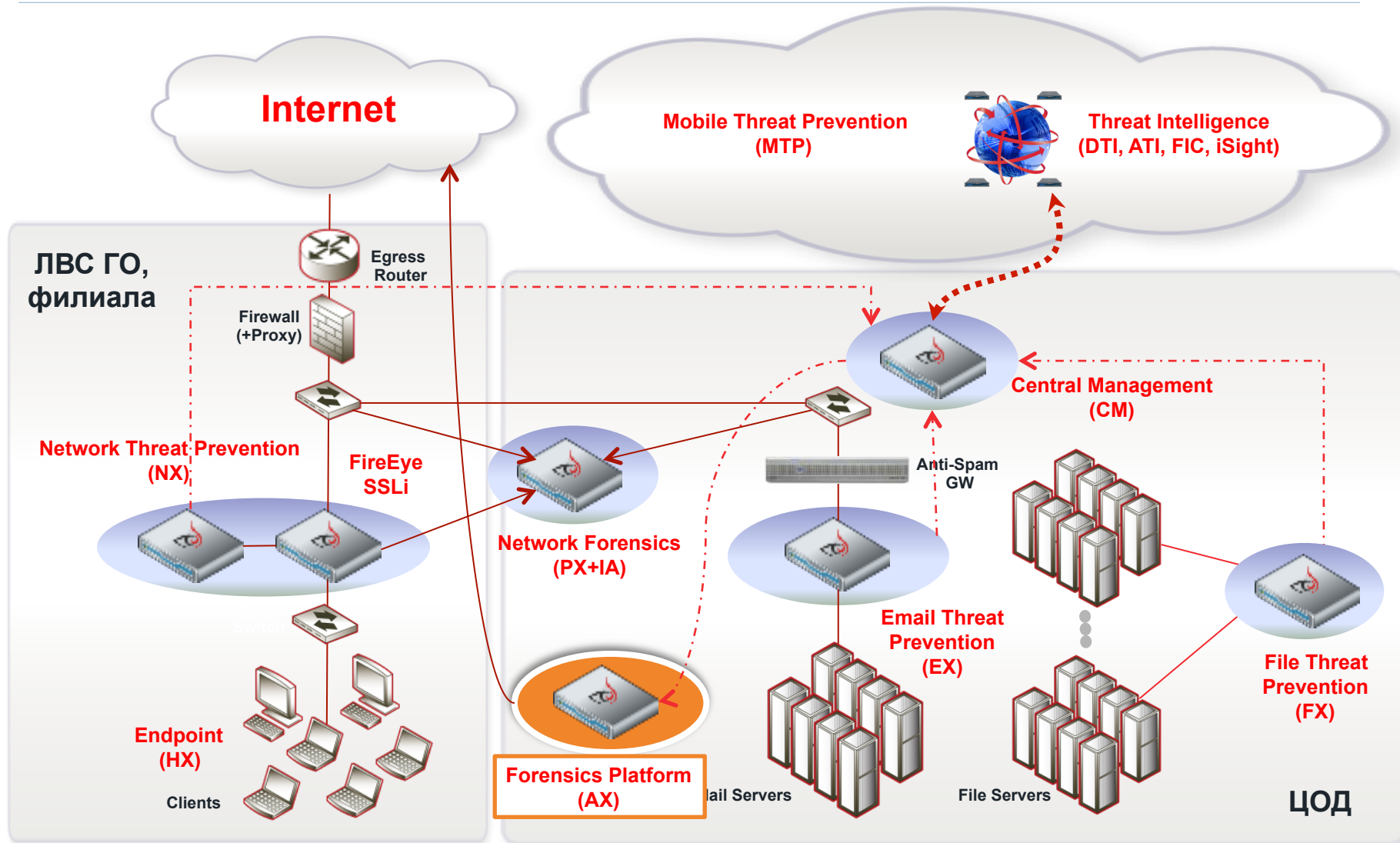
Компоненты платформы FireEye: FX

Защита на уровне корпоративных файловых сервисов



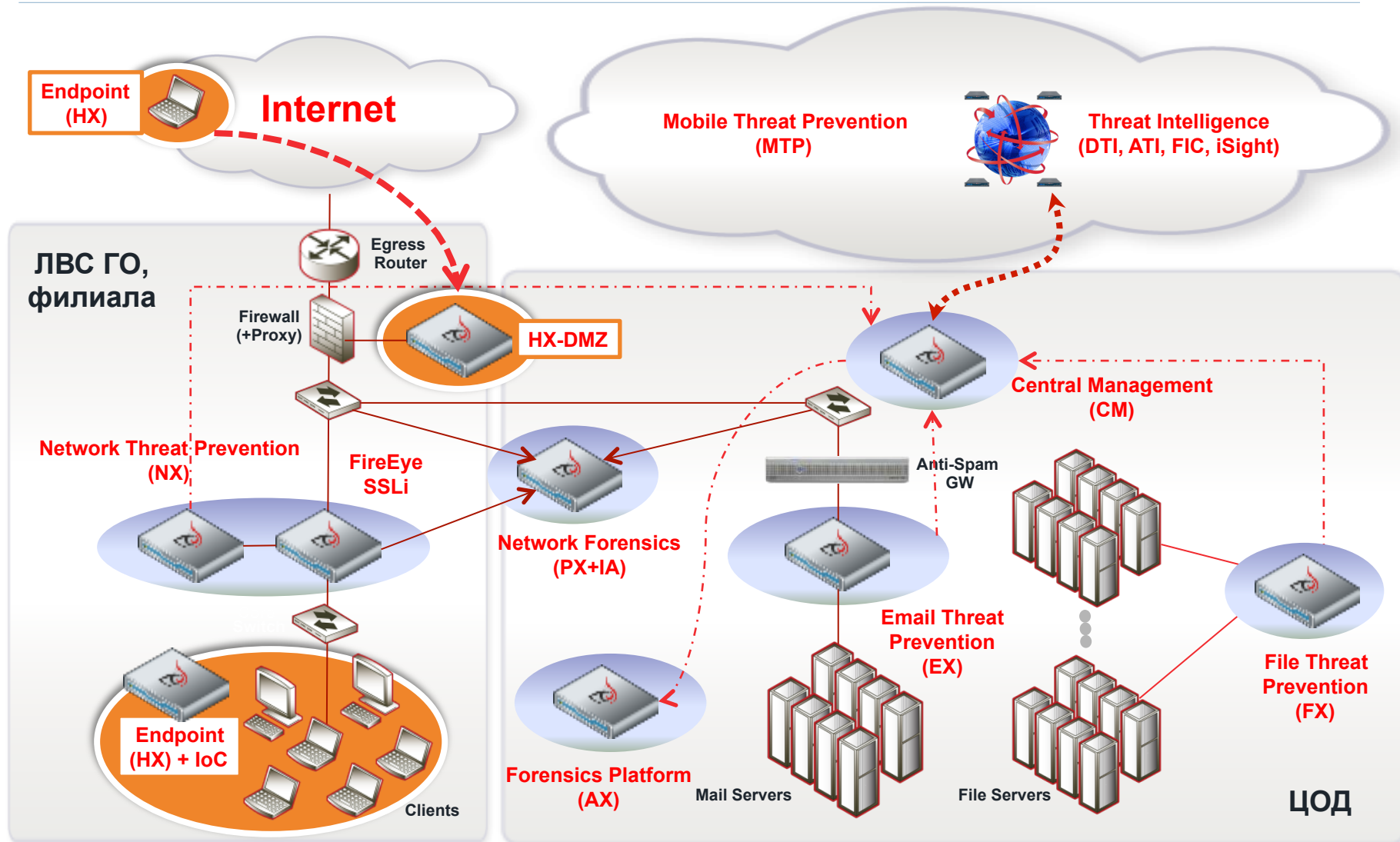
Компоненты платформы FireEye: AX

Детальный анализ с доступом в Интернет из MVX + API



Компоненты платформы FireEye: HX

Расследование инцидентов на уровне конечных точек



НХ: 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)

The screenshot displays the FireEye Triage Viewer interface. The top navigation bar includes the FireEye logo and links for HOSTS, ENTERPRISE SEARCH, ACQUISITIONS, INDICATORS, ADMIN, and user information (Hi, admin | Help & Support). The main title is "Triage summary for **fe-xpsp3-victim**". On the right, there are buttons for "Request containment", "View triage", and "Download full triage".

The left sidebar, titled "Alerting Processes", lists several processes with their PIDs and EXC status:

- cmd.exe • 1716
- net.exe • 120
- PwDump7.exe • 132
- xcopy.exe • 1892
- 7z.exe • 1948
- xcopy.exe • 2012
- net.exe • 2284
- Parent: Explorer.EXE • 2944
- Siblings: verclsid.exe • 320, verclsid.exe • 376, verclsid.exe • 572, verclsid.exe • 824, verclsid.exe • 980, explorer.exe • 1220, msisexec.exe • 1308, verclsid.exe • 1720, ie4uinit.exe • 2100, firefox.exe • 2204

The main content area shows details for **EXC IEXPLORE.EXE • 3112**, started on 2015-07-27T18:20:22Z. The command line is "C:\Program Files\Internet Explorer\IEXPLORE.EXE" -nohome. A timeline bar shows activity from 2015-07-27T18:20:22Z to 2015-07-29T14:10:53Z. Below the timeline, several sections are visible:

- Processes Created**: From 1601-01-01T00:00:00Z to 2015-07-29T14:40:02Z. A table shows a process created with PID 1716, Path C:\WINDOWS\system32\cmd.exe, Username FE-XPSP3-VICTIM\jsmith, and Start Time 2015-07-27T18:21:28Z.
- IP Addresses Connected**: From 2015-07-20T21:07:09Z to 2015-07-29T14:10:57Z. A table shows a connection to 192.168.1.92 on port 3460 using TCP, with 3500 attempts.
- Registry Keys Created/Changed**: From 2015-07-27T17:49:23Z to 2015-07-29T14:06:12Z. Two keys are listed: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\ RNG and HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MediaResources\msmvideo.
- Files Written**: From 2015-07-20T21:06:56Z to 2015-07-29T14:11:06Z. A file is listed: C:\WINDOWS\diagntools\7z.exe with a size of 160KB and a last write time of 2015-07-29T14:11:06Z.

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

The screenshot displays the FireEye HX interface. At the top, the navigation bar includes the FireEye logo and tabs for HOSTS, ENTERPRISE SEARCH (which is active), ACQUISITIONS, INDICATORS, and ADMIN. Below the navigation bar, a search query is entered: "File Name contains UuU.uUu". To the right of the query is a dropdown menu labeled "Select field and operator" with a search button. A dropdown menu is open, showing a list of "Searchable fields" including: Port Protocol, Port State, Process Name, Remote IP Address, Remote Port, Size in bytes, Timestamp - Accessed, and Timestamp - Changed. Below the search bar, there are two search results. The first result is titled "Created 3 hours ago by robert.cole-lomas@fireeye.com" and shows a query: "RETURN Hostname WHERE Host Set equals All hosts AND". The second result is titled "Created 10 hours ago by thien.huynh@fireeye.com" and shows a query: "RETURN Hostname WHERE Host Set equals All hosts AND".

FireEye

HOSTS ▾ ENTERPRISE SEARCH ACQUISITIONS INDICATORS ADMIN ▾

+ File Name *contains* UuU.uUu x Select field and operator x Search

☐ Enable exhaustive search (May take a while)
Includes searching for a: File on Disk

Created 3 hours ago by robert.cole-lomas@fireeye.com
RETURN Hostname
WHERE Host Set *equals* All hosts AND

Created 10 hours ago by thien.huynh@fireeye.com
RETURN Hostname
WHERE Host Set *equals* All hosts AND

Searchable fields

Filter the list

- Port Protocol
- Port State
- Process Name
- Remote IP Address
- Remote Port
- Size in bytes
- Timestamp - Accessed
- Timestamp - Changed

НХ: 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 0 hosts selected

	Hostname	IP Address	Newest Alert	↑ Alerts	Alert Types	Acquisitions
<input type="checkbox"/>	victim-PC	10.100.9.26	33 hours ago	8	PRE EXC XPL	3
<input type="checkbox"/>	victim-PC	10.100.9.21	3 days ago	8	PRE EXC XPL	9
<input type="checkbox"/>	victim-PC	10.100.9.20	3 days ago	5	PRE EXC XPL	3
<input type="checkbox"/>	victim-PC	10.100.8.229	6 days ago	6	PRE EXC XPL	9
<input type="checkbox"/>	victim-PC	10.100.8.217	7 days ago	5	PRE EXC XPL	3
<input type="checkbox"/>	victim-AT	10.100.8.213	7 days ago	5	PRE EXC XPL	5
<input type="checkbox"/>	victim-PC	10.100.8.179	7 days ago	3	PRE XPL	1
<input type="checkbox"/>	victim-PC	10.100.8.166	8 days ago	5	PRE EXC XPL	4
<input type="checkbox"/>	victim-PC	10.100.8.164	8 days ago	8	PRE EXC XPL	5
<input type="checkbox"/>	victim-PC	10.100.8.157	8 days ago	6	PRE EXC XPL	4
<input type="checkbox"/>	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**

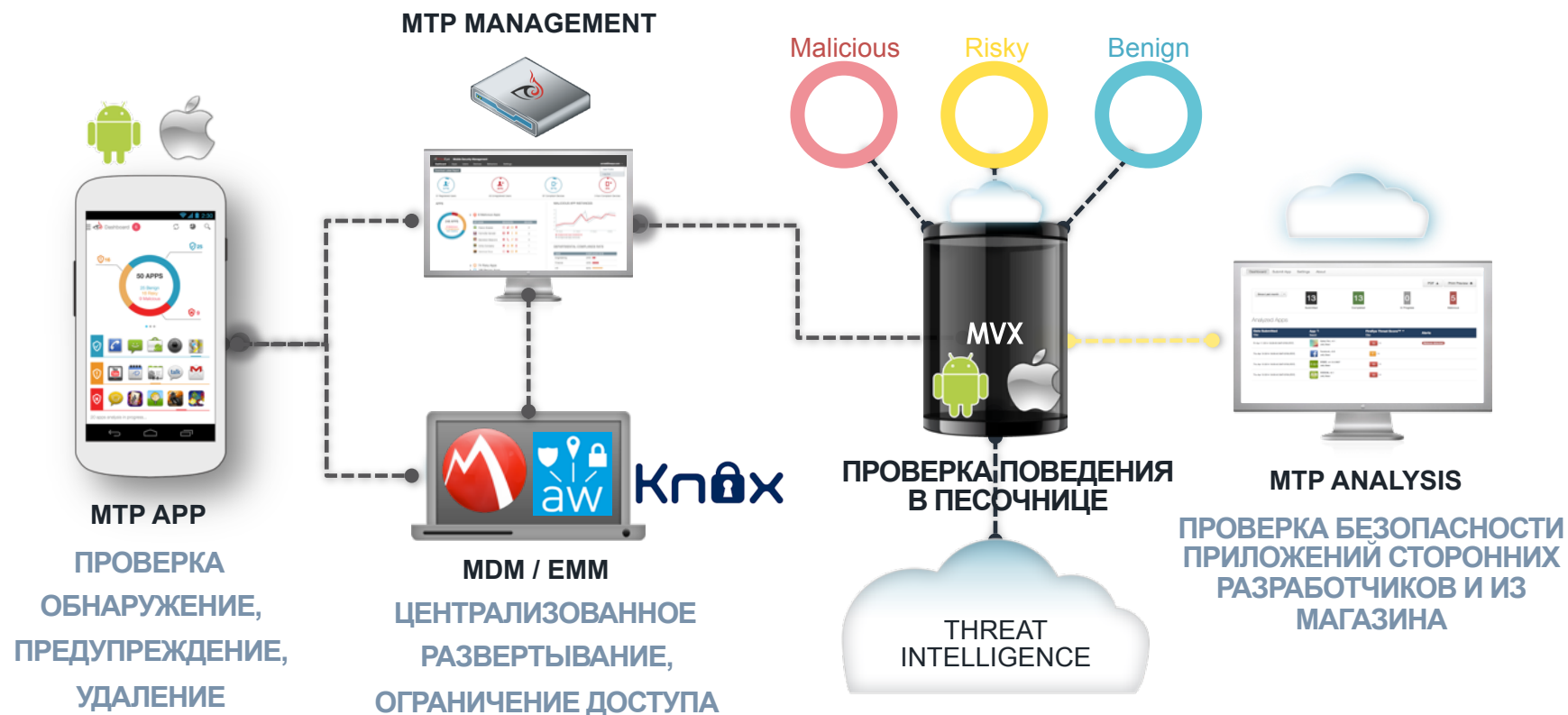
Alerted 3 days ago

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



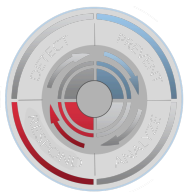
- **Динамический анализ приложений для Android (в т.ч. сторонних) и iOS**
- Оповещение пользователей и/или администраторов ИБ об обнаруженных угрозах
- Применение политик в зависимости от состояния устройства



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



SECURITY
REIMAGINED



ЦИКЛ ЗАЩИТЫ ОТ АРТ

1

Обнаружить

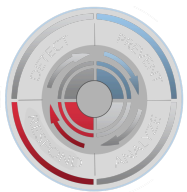
+

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 АРТ

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



Airplane



Hotel



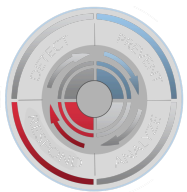
Corporate Headquarters



Home Office



Coffee Shop



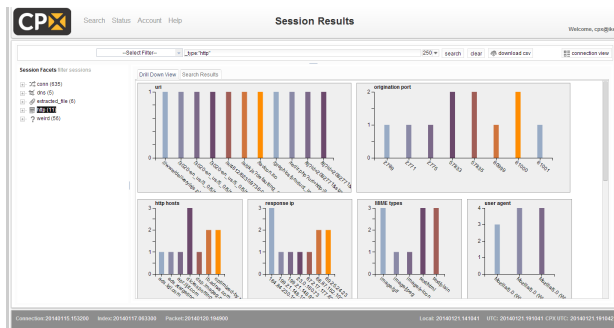
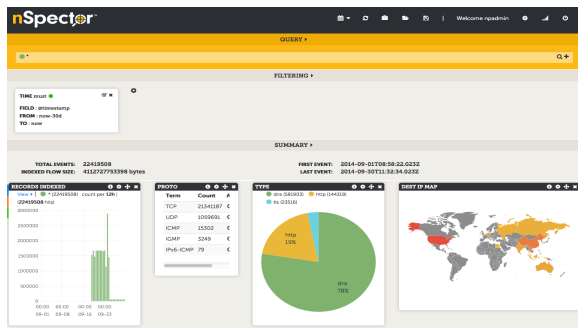
ЦИКЛ ЗАЩИТЫ ОТ АРТ

3 Расследовать инцидент на уровне сети

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

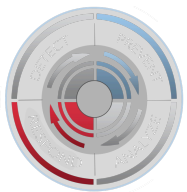


От лога к PCAP



CPX Connection Results interface. It displays a table of network connections with columns for 'Index', 'Source', 'Destination', 'Port', 'Protocol', 'Status', and 'Size'. The table includes a search bar and a 'Download' button.

Index	Source	Destination	Port	Protocol	Status	Size
0	201.40.10.230:23	192.168.108.131	80	TCP	EST	0
1	201.40.10.230:23	192.168.108.131	137	TCP	EST	0
2	201.40.10.230:23	192.168.108.131	137	TCP	EST	0
3	201.40.10.230:23	192.168.108.131	137	TCP	EST	0
4	201.40.10.230:23	192.168.108.131	80	TCP	EST	0



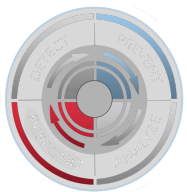
ЦИКЛ ЗАЩИТЫ ОТ АРТ

4

Отреагировать

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





ЦИКЛ ЗАЩИТЫ ОТ АРТ

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



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