FireEye – эффективное решение для защиты от APT-угроз

ДиалогНаука

Обо мне

Николай Петров, CISSP

Заместитель генерального директора, ДиалогНаука

Первым в России был удостоен звания CISSP

На протяжении многих лет являюсь единственным сертифицированным инструктором (ISC)2 в России

Работал в компаниях Philip Morris, Kerberus,

MIS Training Institute, (ISC)2, Ernst & Young

План презентации

1. Атаки в 2009-2014
2. Особенности APT
3. Решение FireEye

Продолжительность 30 мин

Известные атаки

- Operation Aurora
- F-35 и F-22
- Stuxnet
- RSA
- Citigroup
- Globalpayments
- NY Times
- Red October
- NetTraveler

Известные атаки

2009

Operation Aurora

- август- декабрь Китай взламывает Google для доступа к почтовым ящикам китайских правозащитников.
- уязвимость 0-дня в Microsoft IE & SSL соединение с серверами управления в Иллинойсе, Техасе и Тайване.
- Yahoo, Symantec, Northrop Grumman, Morgan Stanley, и Dow Chemical так же пострадали от этой атаки

F-35 и F-22

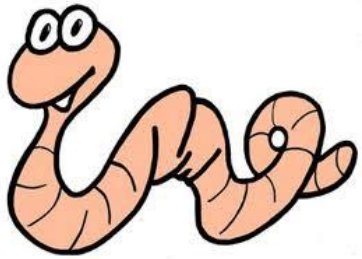
- Китай посредством успешной атаки похищает техническую документацию на новые истребители F-35 и F-22

Известные атаки

2010

Stuxnet

- В июле обнаружен компанией ВирусБлокАда
- Предполагается, что кроссплатформенный червь был разработан США и Израилем для атаки на Иранский ядерный проект
- Атака продолжалась 9 месяцев и за это время отмечены 3 модификации червя
- Уязвимости 0-дня и Rootkits для Windows и Siemens PLC (programmable logic controller)
- Ни одна из Иранских систем не имела прямого соединения с Интернет
- После инсталляции с USB флеш 3 раза, червь себя удалял
- Атака началась с 3 USB флеш дисков и инфицировала 12 000 компьютеров в 5-ти Иранских организациях
- Первая широко известная и успешная атака систем АСУТП



Известные атаки

2011

RSA

- RSA SecurID используется большинством компаний Fortune 500 для обеспечения безопасности удаленного доступа
- RSA подтвердила, что 17 марта 2011 она подверглась атаке, известной как APT
- Был украден алгоритм связывающий серийные номера карт и криптографические ключи внутри SecurID карт
- В отчетности по форме 10-Q EMC указан ущерб $81.3 млн

Citigroup

- В результате атаки обнаруженной в июне 2011 украдены 360,000 идентификаторов кредитных карт, из которых 3,400 были использованы для кражи более $2.7 млн долларов США

citigroup
HACKED

Известные атаки

2012

Global Payments

- В результате атаки обнаруженной в марте 2012 украдены 7,000,000 идентификаторов кредитных карт
- Visa и MasterCard временно приостановили обслуживание Global Payments
- Ущерб $85 млн

Flame (Skywiper)

- Обнаружен в мае «ЛК»
- Предполагается, что это ПО разработано США и Израилем для замедления Иранской ядерной программы
- Распространяется через LAN и USB, записывает экраны, нажатия клавиатуры, сетевой трафик, включая Skype
- В апреле Flame вынудил Иран изолировать свои нефтяные терминалы от Интернет
- Flame поддерживал команду самоуничтожения «kill», и после обнаружения и публикаций в прессе, эта команда была активирована

Известные атаки

2013

NY Times

- Атака началась на следующий день после публикации статьи о причастности к коррупции премьер министра Китая Вэнь Цзябао – 24 октября 2012
- Была обнаружена в январе 2013
- Расследование показало, что были установлены 45 вариантов вредоносного ПО. Только один из них был обнаружен Symantec и помещен в карантин
- Атакующие получили доступ к файлам и электронной почте сотрудников NY Times, включая редакторов Шанхайского бюро

Red October

- Обнаружен в январе «ЛК»
- Действовал на протяжении последних 5 лет
- собиралась информация с мобильных устройств, компьютеров и сетевого оборудования
- Хакеры создали более 60 доменов, находившихся преимущественно в России и Германии, откуда контролировалось заражение

Известные атаки

2013

NetTraveler

- Обнаружен в июне «ЛК»
- Компьютеры в 40 странах мира
- NetTraveler отслеживает нажатия клавиш, получает список доступных файлов и автоматически копирует документы Microsoft Office, PDF, а также файлы систем автоматизированного проектирования
- Специалисты «ЛК» смогли получить доступ к некоторым командным серверам NetTraveler и обнаружили на них 22 Гб похищенных данных

NetFile-801.exe

Известные атаки

2014

Careto

- Обнаружен в феврале «ЛК»
- Сеть троянов для различных платформ, Windows, Mac OS X, Linux, Android
- Цель атаки – государственные организации, дипломатические офисы и посольства, энергетические и нефтегазовые компании, исследовательские организации
- Атаке подверглись 380 целей в 31 стране мира
- Разработка началась в 2007 г., большинство модулей созданы в 2012 г
- Заражение происходит с помощью рассылок по электронной почте писем, содержащих ссылки на поддельные сайты
- Использует уязвимости в продуктах «ЛК», чтобы оставаться невидимым в системе
- Careto похищает документы, ключи шифрования, настройки VPN и другие данные

Известные атаки

2014

SearchInform

- Обнаружен в марте
- Поставщик DLP решений для Газпрома, Русала, ВТБ, ВТБ 24, Газпромнефть, Лукойл-Информ, МТТ, Промсвязьбанк, Главгосэкспертиза России
- Утекли конфиденциальные данные о сделках, клиентах, особенностях работы DLP-системы
- Злоумышленники утверждают, что взлом был осуществлен в 2012-м году и с тех пор компания-жертва даже не догадывалась, что у нее утекают данные

SearchInform
Information Security

Особенности APT

Особенности APT

APT - целенаправленная сетевая атака, при которой атакующий получает неавторизованный доступ в сеть и остается необнаруженным в течении длительного времени

Термин APT введен U.S. Air Force в 2006

- **Advanced:** Атакующий является экспертом и использует свои собственные, неизвестные другим инструменты для эксплуатации уязвимостей
- **Persistent:** Атакующий не ограничен во времени, т е он будет тратить столько времени, сколько нужно, чтобы получить доступ и остаться незамеченным
- **Threat:** Атакующий организован, мотивирован, обладает необходимыми финансовыми ресурсами

APT

- считается наиболее опасным типом атак
- не вредоносное ПО
- спланированная атака, мотивированная деньгами, политикой/национальными интересами и направленная для достижения определенной цели

Особенности APT

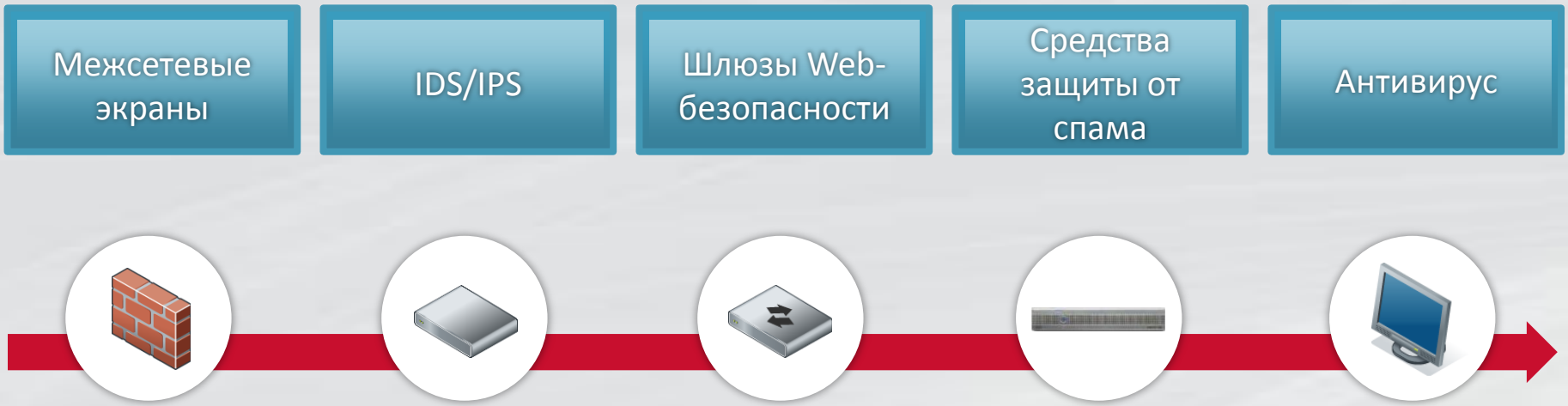
Обход защиты основанной на анализе сигнатур

- Традиционные продукты, такие как IDS/IPS, межсетевые экраны следующего поколения (NGFW), шлюзы Web-безопасности (secure Web gateways), антивирусное ПО— анализируют сигнатуры для обнаружения известным им атак, и в некоторых случаях, неизвестных атак, которые используют известные им уязвимости

Обход защиты основанной на анализе аномалий

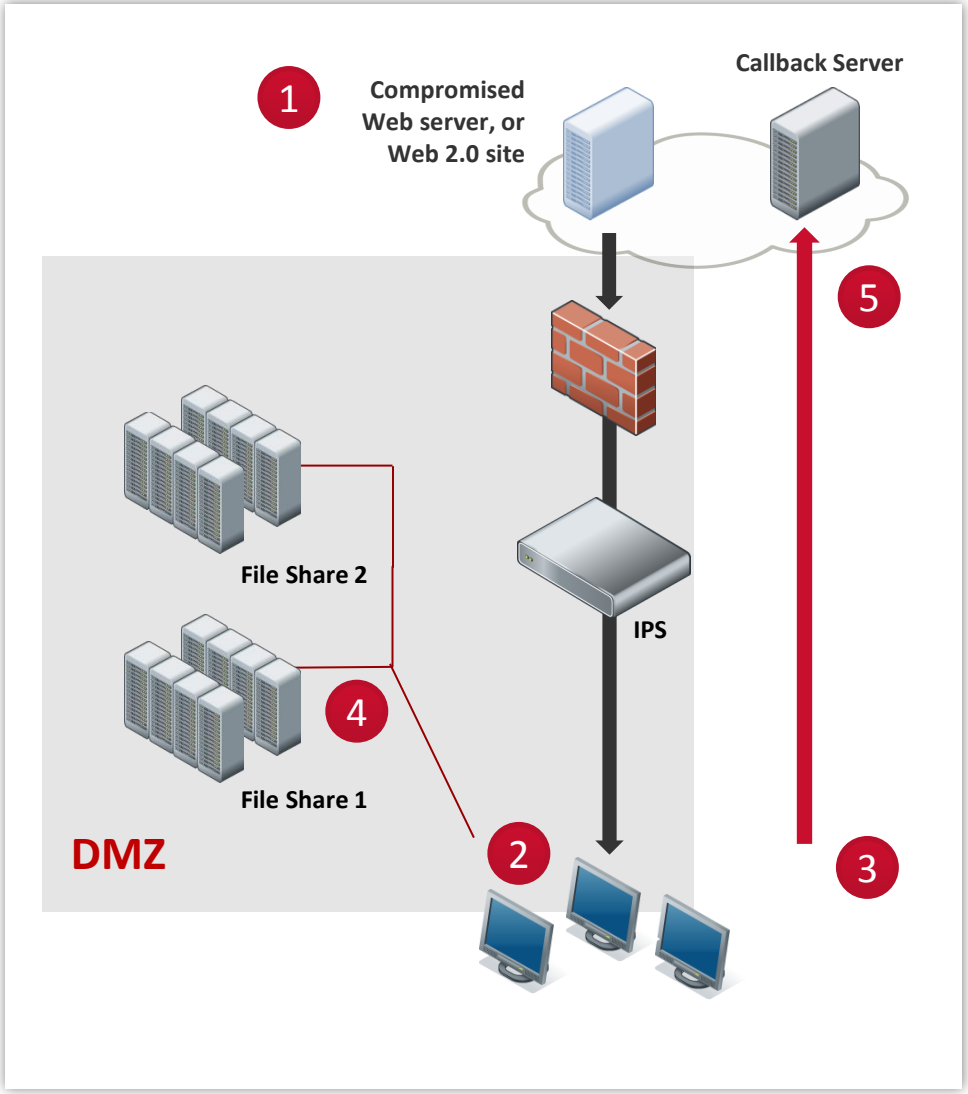
- Продвинутые IDS/IPS и решения анализирующие сетевые аномалии могут обнаруживать APT. Они собирают траффик (e.g., NetFlow, sFlow, cFlow) с сетевых устройств и сравнивают его с “обычным” сетевым трафиком в имевшем место в течении дня, недели, месяца
- Однако такие решения подвержены ошибкам 1-го и 2-го рода. False positives – когда нормальный трафик принимается за атаку, и наоборот, false negatives – когда атака воспринимается как нормальный трафик

Особенности APT



Традиционные технологии не могут остановить APT

Особенности APT



1. Эксплуатация уязвимости
2. Загрузка вредоносного кода
3. Связь с сервером управления
4. Дальнейшее распространение атаки
5. Передача конфиденциальной информации

Особенности APT

Стадия 1

- Эксплуатация уязвимости обычно происходит через Web (JavaScript, JPG) или email (вложение XLS, PDF)
- Достаточно кликнуть мышью на гиперссылке
- Открывается Web броузер (или другое приложение Adobe Reader, Microsoft Word, or Microsoft Excel)
- Гиперссылка использует скрытый адрес закодированный с помощью base64. После его раскодирования, компьютер жертвы устанавливает соединение с сервером атакующего, откуда загружается вредоносное ПО

Стадия 2

- Устанавливается соединение с сервером управления и загрузка дополнительного вредоносного кода

Стадия 3

- Вредоносное ПО устанавливает шифрованное соединение с сервером управления (например, SSL)
- Обходит традиционную защиту предлагаемую межсетевыми экранами и системами обнаружения вторжений

Особенности APT

Стадия 4

- Обычно зараженный компьютер не содержит данные, необходимые атакующему
- Атака распространяется на компьютеры ИТ администраторов, файловые сервера и сервера БД

Стадия 5

- Передача большого объема данных или данных в открытом виде обнаруживается системами IDS/IPS и DLP
- Данные передаются порциями по 50-100 МБ в зашифрованном виде

Решение FireEye

ДиалогНаука

Решение FireEye

- Компания FireEye с 2004 г в США
- Поставляет продукты с 2006 г
- Мировой лидер – FireEye используют 40% компаний Fortune 100

Отчет Gartner

“Все согласны с тем, что целенаправленные атаки обходят традиционные средства защиты и остаются необнаруженными в течение длительного времени. Угроза реальна. Ваши сети скомпрометированы независимо от того, знаете Вы об этом или нет.”

Отчет Gartner 2012

Как вы думаете, в сети вашей организации есть вредоносное ПО?

Результаты тестирования

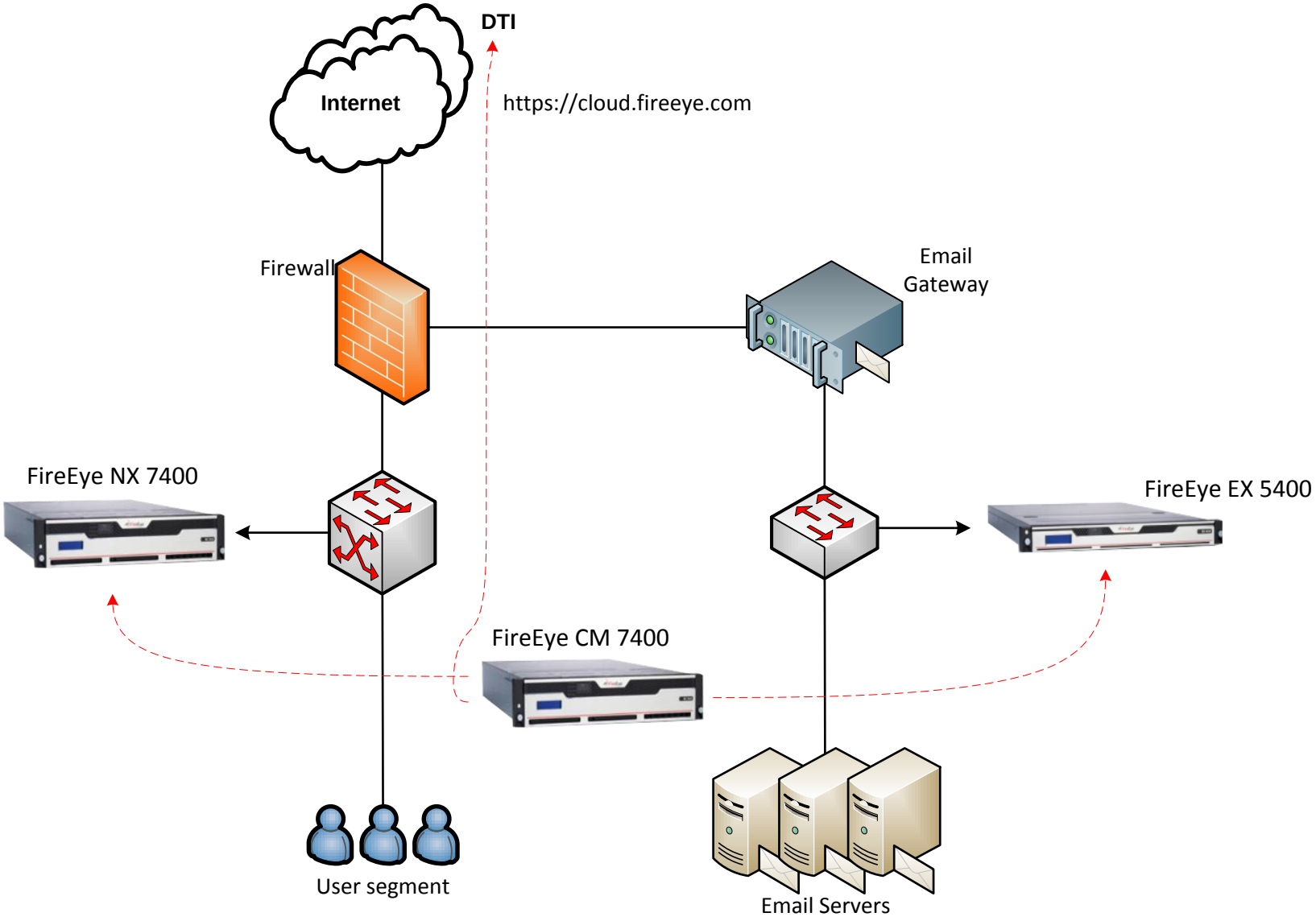
Мы провели более 10 пилотных проектов в Москве

В результате пилотного тестирования, FireEye обнаружил:

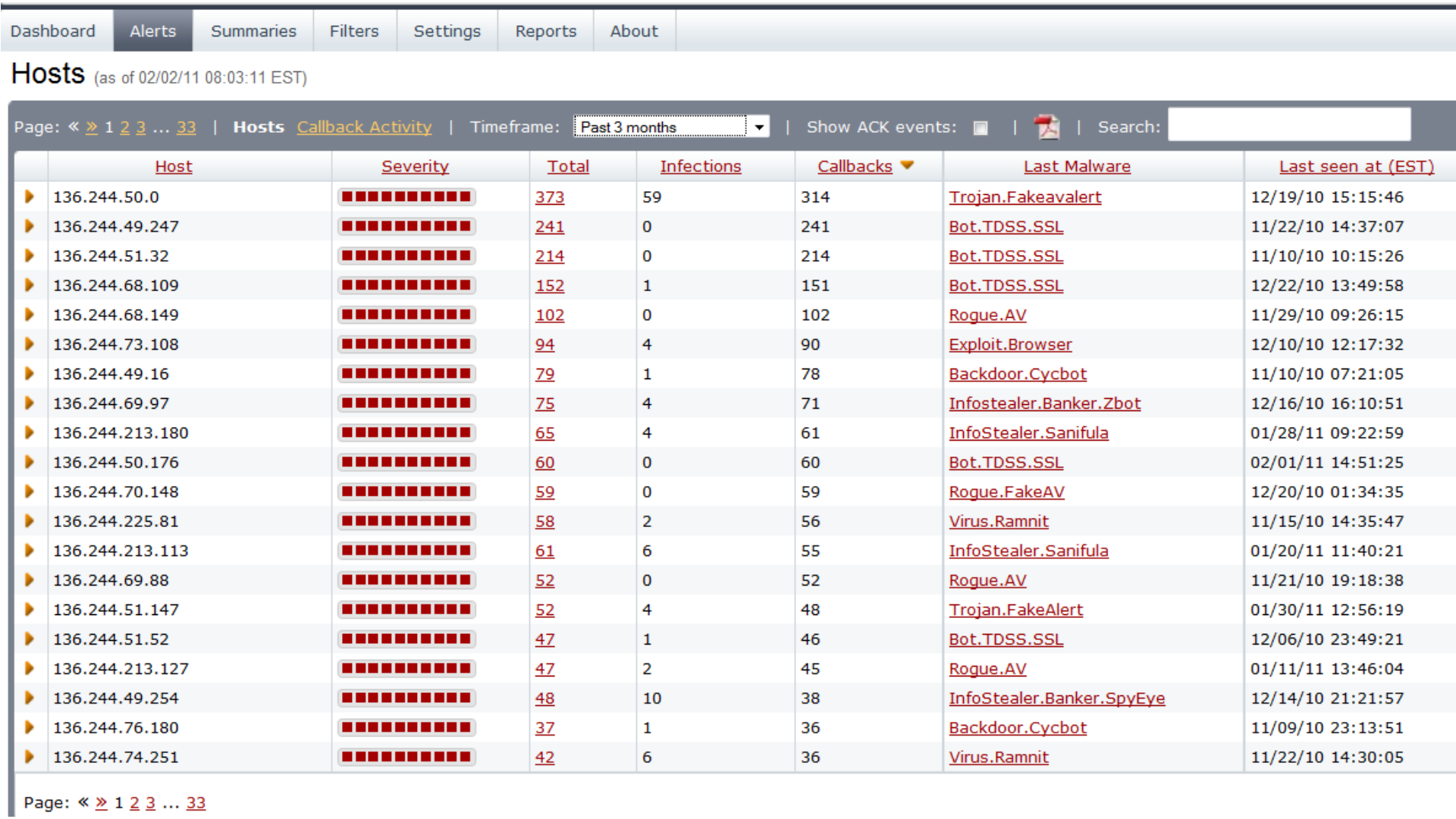
- Не менее 8 рабочих станций контролируются злоумышленниками извне Компании
- Не менее 24 рабочих станций потенциально заражены троянскими программами и могут контролироваться злоумышленниками извне Компании
- Основные каналы распространения WEB и электронная почта

Количество рабочих станций у клиента - 2000

Схема тестирования



Экран системы



Dashboard | Alerts | Summaries | Filters | Settings | Reports | About

Hosts (as of 02/02/11 08:03:11 EST)

Page: « » 1 2 3 ... 33 | **Hosts** Callback Activity | Timeframe: Past 3 months | Show ACK events: | Search:

Host	Severity	Total	Infections	Callbacks	Last Malware	Last seen at (EST)
136.244.50.0		373	59	314	Trojan.Fakeavalert	12/19/10 15:15:46
136.244.49.247		241	0	241	Bot.TDSS.SSL	11/22/10 14:37:07
136.244.51.32		214	0	214	Bot.TDSS.SSL	11/10/10 10:15:26
136.244.68.109		152	1	151	Bot.TDSS.SSL	12/22/10 13:49:58
136.244.68.149		102	0	102	Rogue.AV	11/29/10 09:26:15
136.244.73.108		94	4	90	Exploit.Browser	12/10/10 12:17:32
136.244.49.16		79	1	78	Backdoor.Cycbot	11/10/10 07:21:05
136.244.69.97		75	4	71	Infostealer.Banker.Zbot	12/16/10 16:10:51
136.244.213.180		65	4	61	InfoStealer.Sanifula	01/28/11 09:22:59
136.244.50.176		60	0	60	Bot.TDSS.SSL	02/01/11 14:51:25
136.244.70.148		59	0	59	Rogue.FakeAV	12/20/10 01:34:35
136.244.225.81		58	2	56	Virus.Ramnit	11/15/10 14:35:47
136.244.213.113		61	6	55	InfoStealer.Sanifula	01/20/11 11:40:21
136.244.69.88		52	0	52	Rogue.AV	11/21/10 19:18:38
136.244.51.147		52	4	48	Trojan.FakeAlert	01/30/11 12:56:19
136.244.51.52		47	1	46	Bot.TDSS.SSL	12/06/10 23:49:21
136.244.213.127		47	2	45	Rogue.AV	01/11/11 13:46:04
136.244.49.254		48	10	38	InfoStealer.Banker.SpyEye	12/14/10 21:21:57
136.244.76.180		37	1	36	Backdoor.Cycbot	11/09/10 23:13:51
136.244.74.251		42	6	36	Virus.Ramnit	11/22/10 14:30:05

Page: « » 1 2 3 ... 33

Решение FireEye

1

Аппаратный гипервизор FireEye

- Специализированный гипервизор
- Разработан для анализа угроз

2

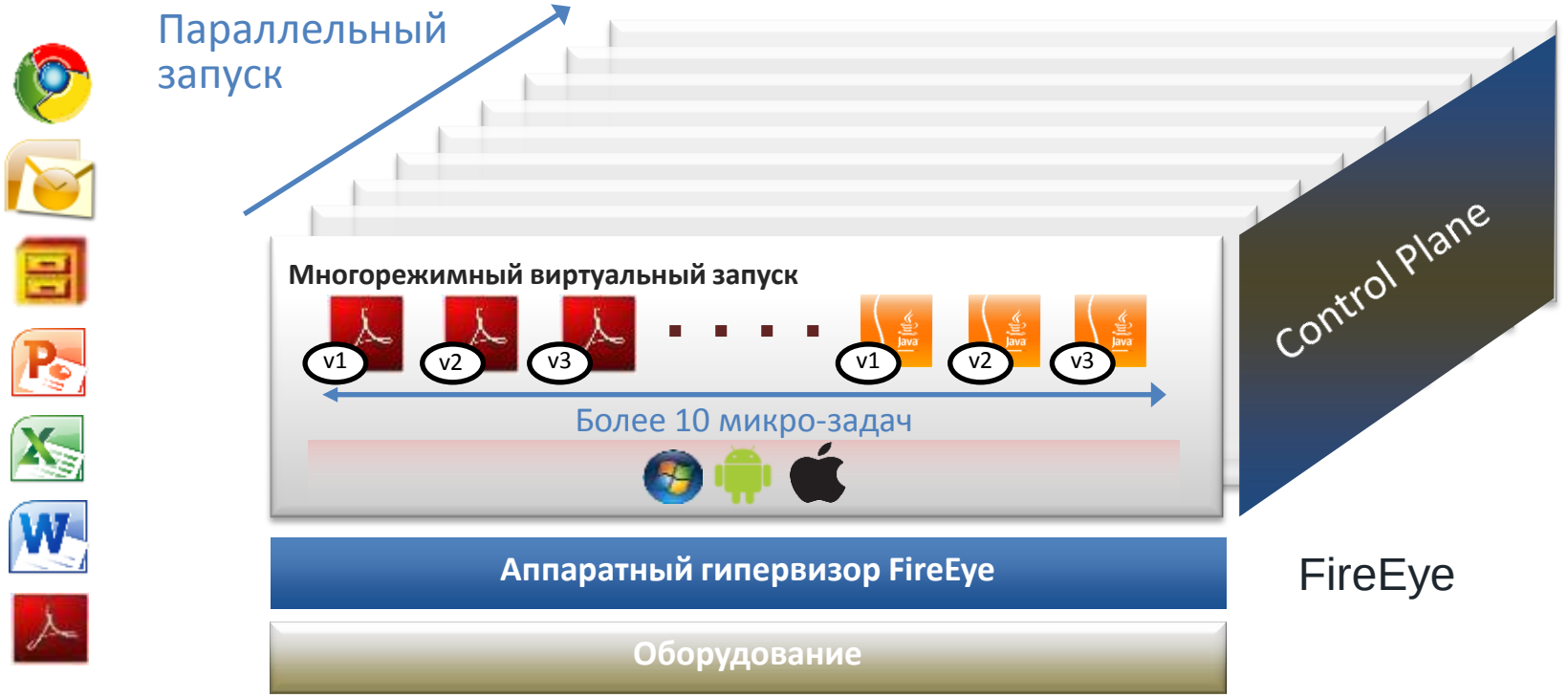
Многопоточный виртуальный запуск

- Разные ОС
- Разные сервис-паки
- Разные приложения
- Разные типы файлов

3

Защита от угроз в масштабе

- Параллельный запуск
- Многоуровневый анализ

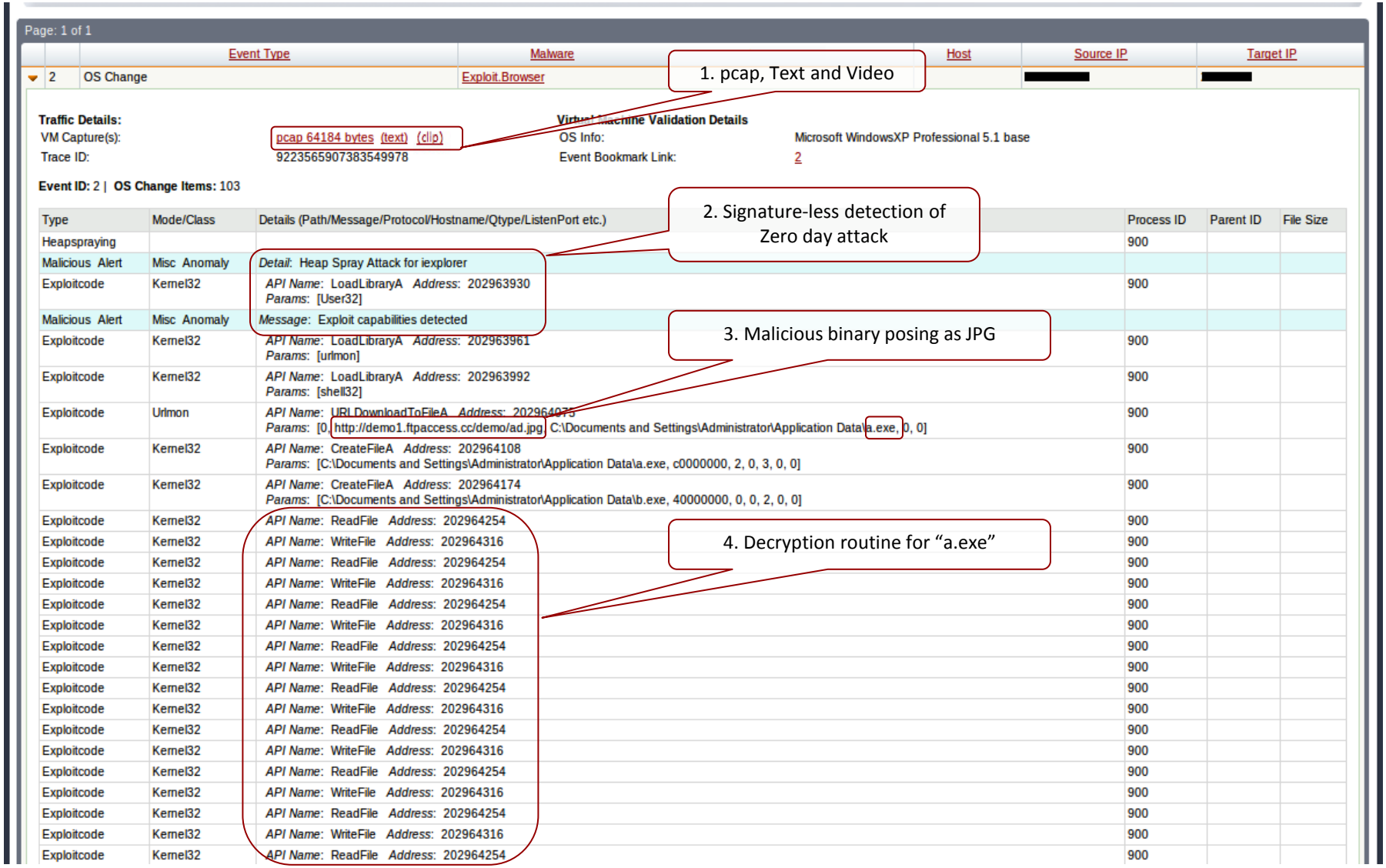


Передача информации об атаках

Передача информации об атаках

- Файлы из вашей сети не передаются в Облако (Персональные данные, конфиденциальная информация)
- Идентификаторы вредоносного ПО со всего мира
- Возможность выбрать вариант обмена информацией

Операция Аврора



Операция Аврора

Exploitcode	Kernel32	*API Name*: WriteFile *Address*: 202964316	900		
Exploitcode	Kernel32	*API Name*: ReadFile *Address*: 202964254	900		
Exploitcode	Kernel32	*API Name*: WriteFile *Address*: 202964316	900		
Exploitcode	Kernel32	*API Name*: VirtualProtect *Address*: 202964803	900		
Exploitcode	Kernel32	*API Name*: LoadLibraryA *Address*: 202964499 *Params*: [shdocvw]	900		
File	Created	C:\Documents and Settings\Administrator\Application Data\a.exe	900		
File	Created	C:\Documents and Settings\Administrator\Application Data\b.exe	900		
File	Delete	C:\Documents and Settings\Administrator\Application Data\a.exe	900		
Process	Started	C:\Documents and Settings\Administrator\Application Data\b.exe *Packed*: yes *GUI*: no MD5: 9f880ac607cbd7cdfffa609c5883c708 SHA1: 08b33a64a85b93530d07ec3ea611e4875ee6c169	1304	900	34816
Malicious Alert	Misc Anomaly	*Detail*: Process started from a packed binary			
Malicious Alert	Anomaly Tag	*Message*: Startup behavior anomalies observed *Detail*: Browser started an unknown process			
File	Date Change	C:\WINDOWS\system32\Rasmon.dll MD5: 0f9c5408335833e72fe73e6166b5a01b SHA1: cfa826c339898e882a1276b694fc935d56b83093	1304		90112
Regkey	Added	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\UpsXZE	544		
Malicious Alert	Misc Anomaly	*Message*: System services modified *Detail*: service loaded through windows			
Regkey	Deleted	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\UpsXZE	1320		
Regkey	Added	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\RaSXkNk	1320		
Network	Dns Query	*Protocol Type*: udp *Qtype*: Host Address *Hostname*: 360.homeunix.com	1320		
Network	Connected	*Protocol Type*: tcp *IP Address*: [redacted] *Destination Port*: 443	1320		
Malicious Alert	Misc Anomaly	*Message*: Malware communication observed			
File	Created	C:\WINDOWS\DFS.bat	1304		
Process	Started	C:\WINDOWS\system32\cmd.exe /c "C:\WINDOWS\DFS.bat" *Packed*: no *GUI*: no MD5: 84ddf54db542b2eb9ef08144fb6e3645 SHA1: 43c3eeadfd2c3aadd32f9a7c750e4b1465d3bc9a	1280	1304	375808
Process	Terminated	C:\Documents and Settings\Administrator\Application Data\b.exe	1304	900	
File	Delete	C:\Documents and Settings\Administrator\Application Data\b.exe	1280		
File	Delete	C:\WINDOWS\DFS.bat	1280		
Appexception		*Exception Faulting Address*: 0x65 *Exception Code*: 0xC0000005 *Exception Level*: SECOND_CHANCE *Exception Type*: STATUS_ACCESS_VIOLATION *Instruction Address*: 0x00000000781444dc *Description*: Data from Faulting Address controls Branch Selection *Classification*: UNKNOWN	900		
Malicious Alert	Misc Anomaly	*Detail*: Crash detected due to second chance			
File	Created	C:\Program Files\Debugging Tools for Windows (x86)\DBG0.tmp	1312		
Uac	Service	UpsXZE			
Malicious Alert	Misc Anomaly	*Detail*: System service running/stopped			

1	VM-verified Outbound Comm.	Exploit.Browser		[redacted]	[redacted]

5. Decrypted Trojan
(Later named the Hydraq.Trojan)

6. Registry Keys Modified

7. Hydraq callback
New Binary DFS.bat

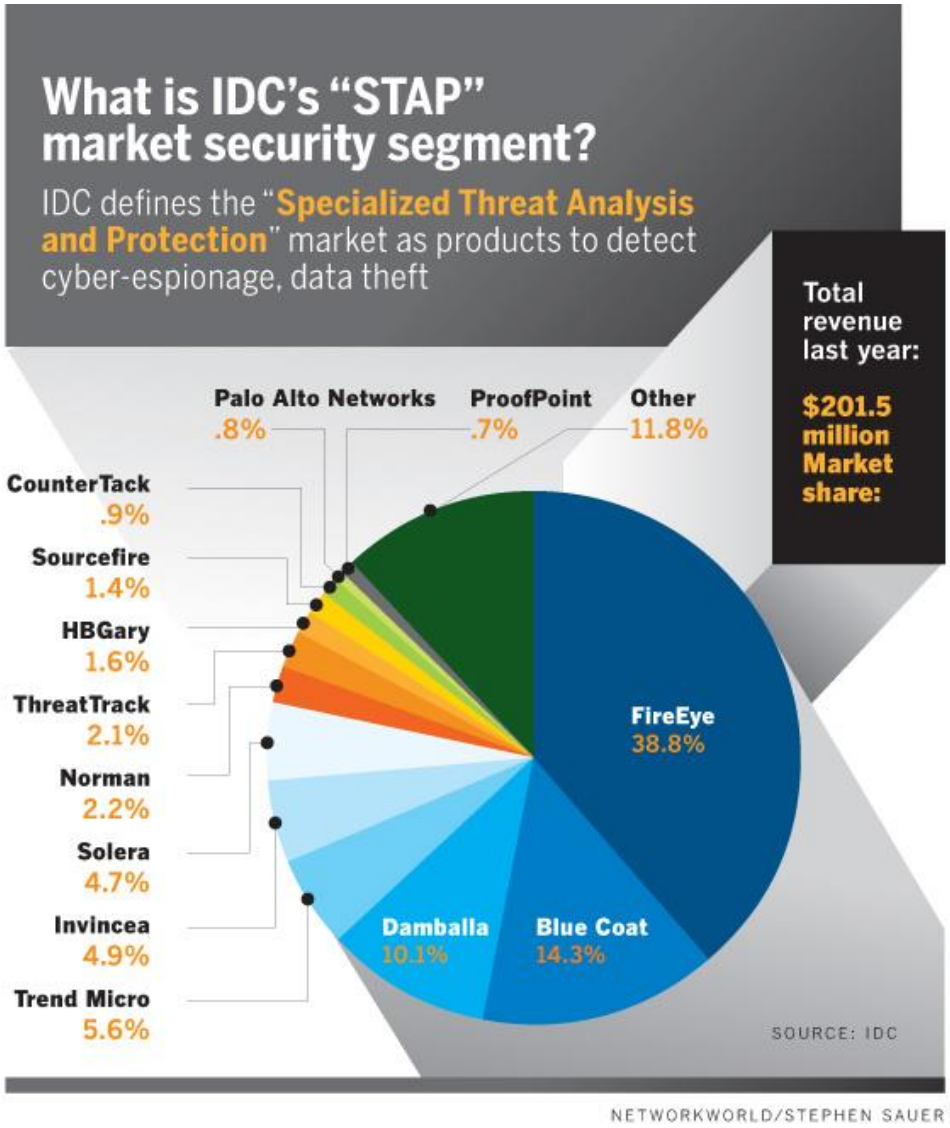
8. Unpacked and hidden from system processes

9. Install files deleted once infection complete

Почему FireEye?

- **16 из 22** уязвимостей нулевого дня (Zero Day) в 2013-2014 году были обнаружены FireEye
- Выполняет анализ не только исполняемых файлов и MS Office, но и других (более 30 типов файлов, включая графические, аудио, видео)
- Выполняется анализ веб-сессии целиком, а не отдельного файла
- Обладает специализированым гипервизором для анализа угроз и позволяет обнаруживать неизвестные угрозы
- Обеспечивает **близкое к реальному времени** скорость анализа (не более 5 мин)
- Позволяет блокировать вредоносную активность на каждой стадии атаки
- Отсутствуют ложные срабатывания

Доля рынка


What is IDC's "STAP" market security segment?
IDC defines the "Specialized Threat Analysis and Protection" market as products to detect cyber-espionage, data theft
Total revenue last year:
$201.5 million
Market share:
Palo Alto Networks .8%
ProofPoint .7%
Other 11.8%
CounterTack .9%
Sourcefire 1.4%
HBGary 1.6%
ThreatTrack 2.1%
Norman 2.2%
Solera 4.7%
Invincea 4.9%
Trend Micro 5.6%
FireEye 38.8%
Damballa 10.1%
Blue Coat 14.3%
SOURCE: IDC
NETWORKWORLD/STEPHEN SAUER

Дополнительная информация – мои статьи за 2014 г

«Защищаемся от целенаправленных атак»

Национальный Банковский Журнал, №2 февраль 2014

«Целенаправленные атаки – обнаружение и защита»

Информационная безопасность, №2 май 2014

«Расследование целевых атак»

Безопасность Деловой Информации, №06 II квартал 2014

Вопросы?

ДиалОгНаука