Защита от целенаправленных атак

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

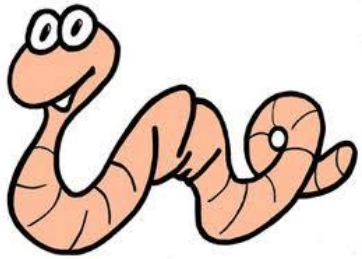
- Китай посредством успешной атаки похищает техническую документацию на новые истребители F-35 и F-22

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

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

Особенности APT

ДиалогНаука

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

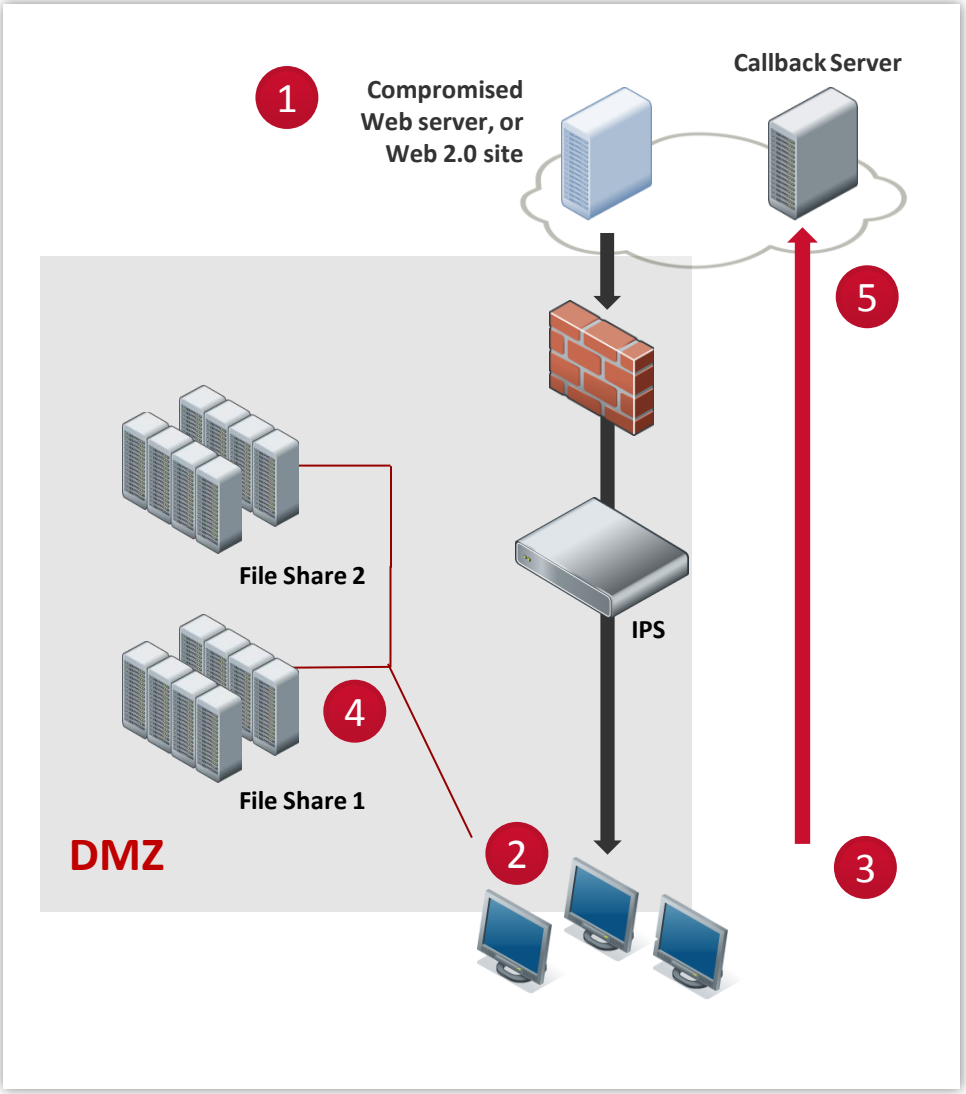
APT

- считается наиболее опасным типом атак
- не вредоносное ПО
- спланированная атака, мотивированная деньгами, политикой/национальными интересами и направленная для достижения определенной цели (как получение доступа в проектах тестов на проникновение)

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

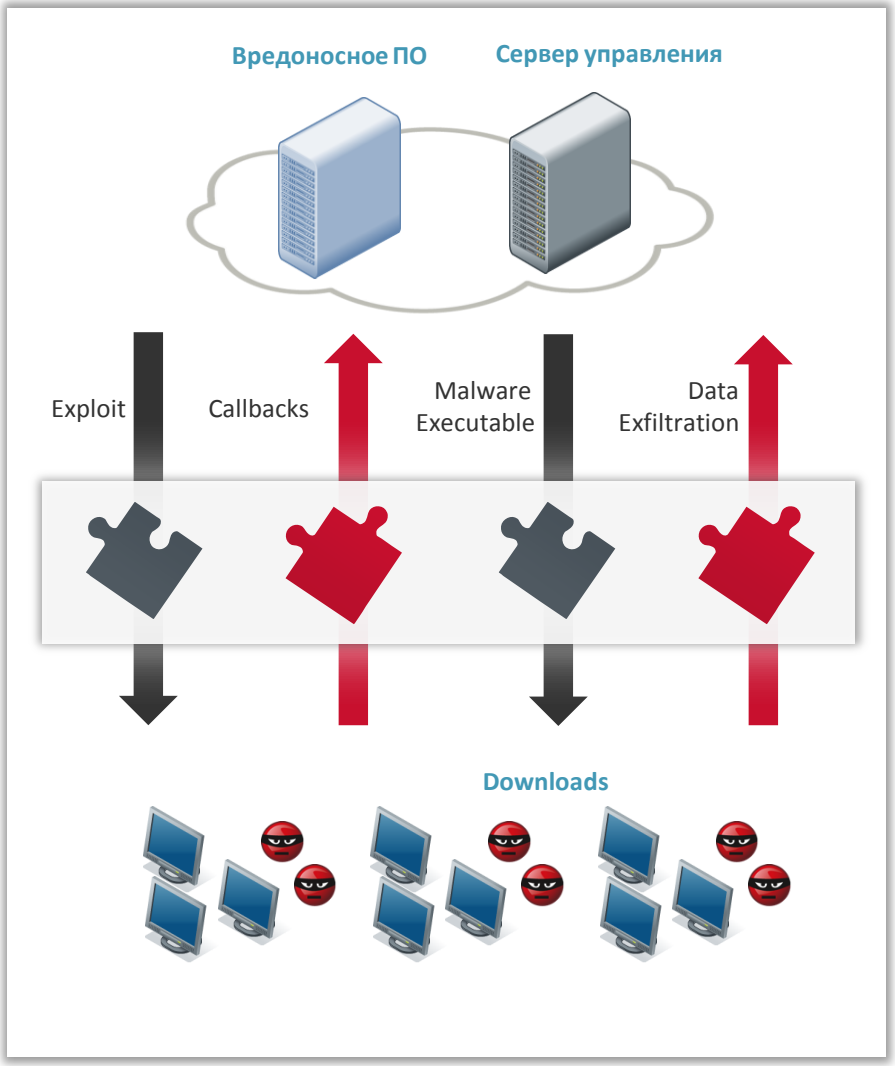
Решение FireEye

ДиалогНаука

Решение FireEye

- Компания FireEye с 2004 г в США
- Поставляет продукты с 2006 г
- Мировой лидер

Решение FireEye

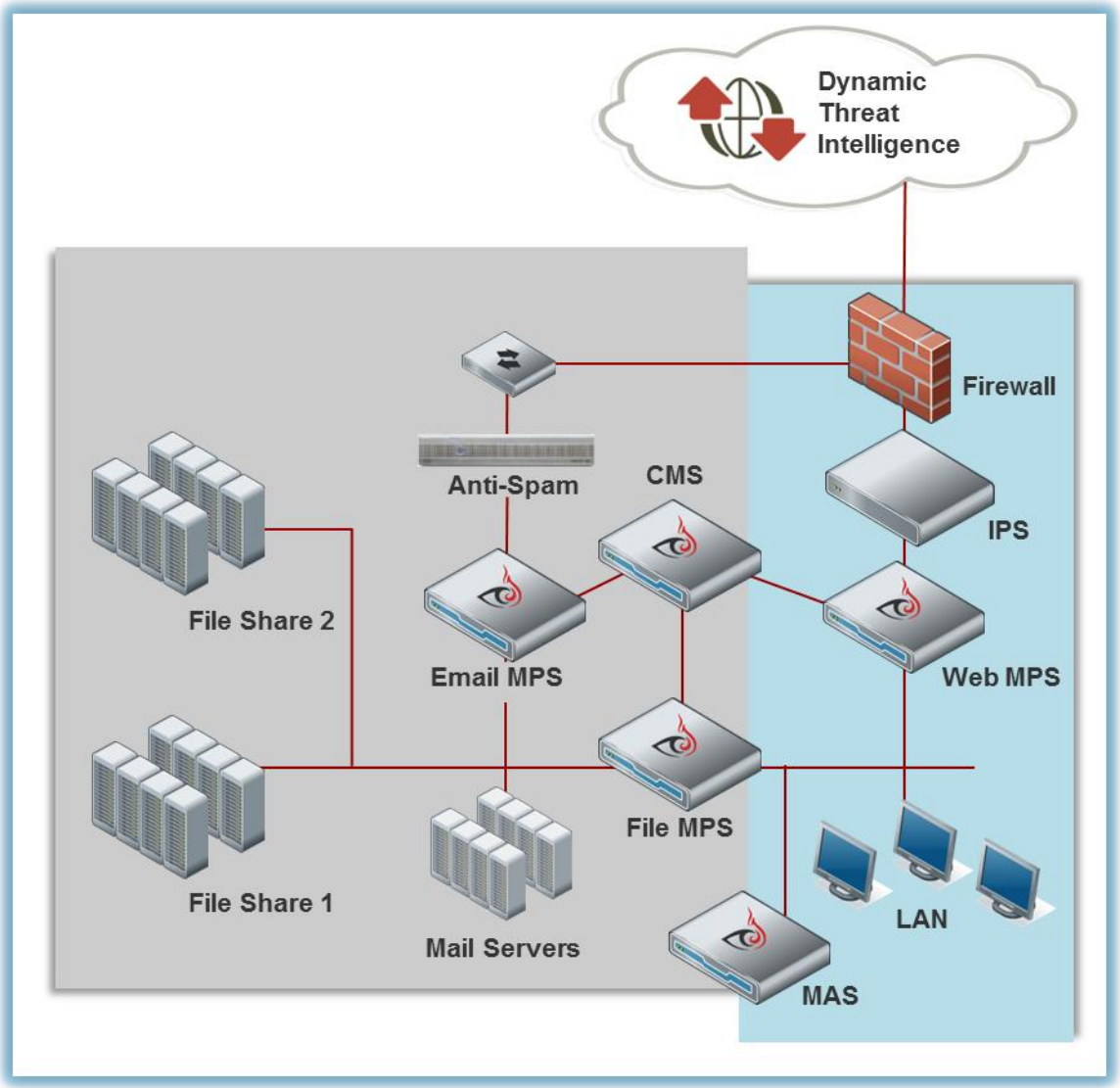


- FireEye контролирует все этапы атаки
- Блокирует активность на любом этапе
- В отличии от других (.exe и .dll), анализирует asf, com, doc, docx, dll, exe, gif, ico, jpeg, jpg, mov, mp3, mp4, pdf, png, ppsx, ppt, pptx, qt, rtf, swf, tiff, unk, vcf, xls, xlsx, zip… и т. д.

Решение FireEye

Компоненты системы

- Web MPS
- Email MPS
- File MPS
- MAS
- CMS



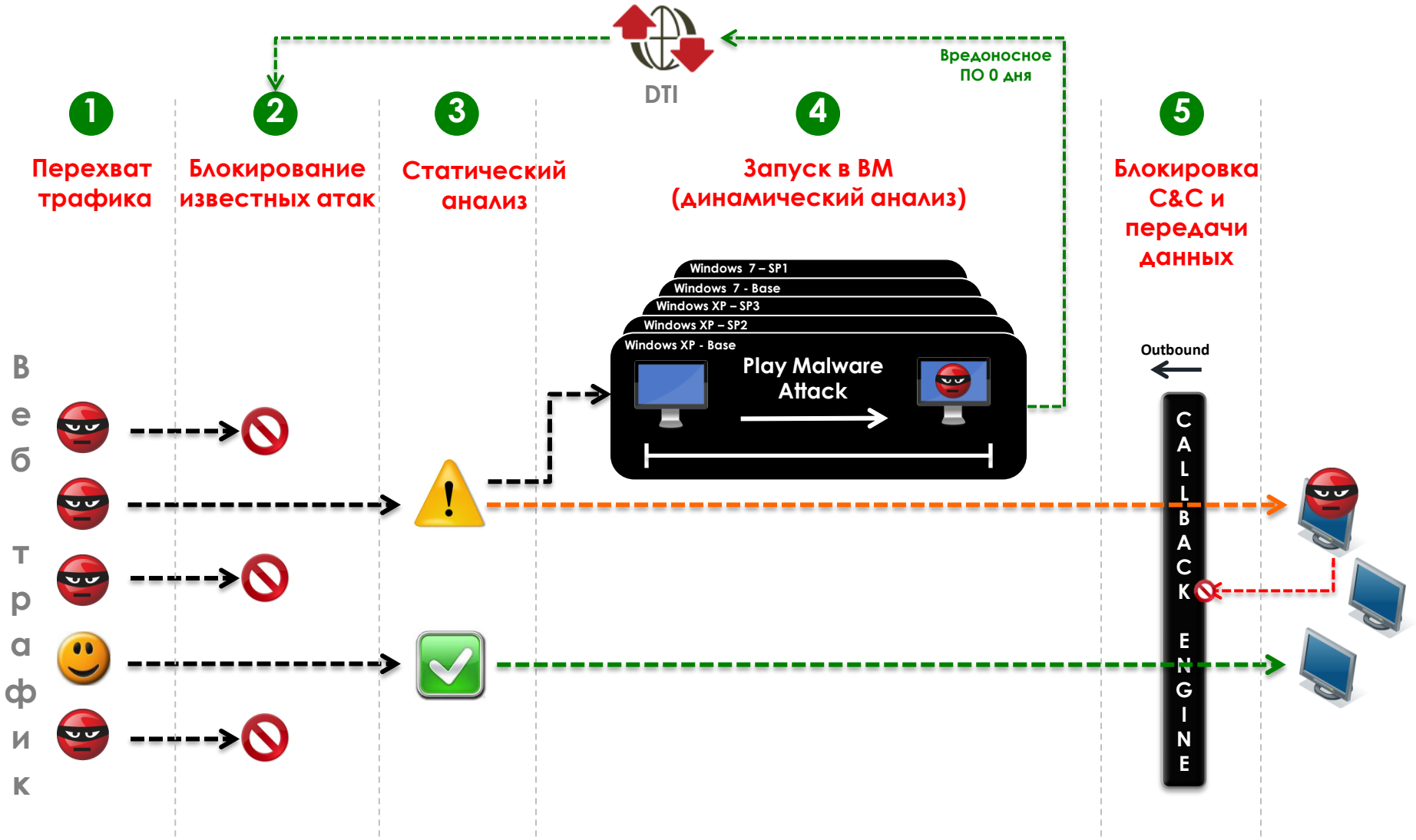
Web MPS

- Отсутствие ложных срабатываний
- Анализ web-объектов (страницы, флеш, PDF, документы и исполняемые файлы)
- Блокирование соединений
- Интеграция с Email MPS, File MPS and MAS
- Передача информации об атаках в облако (Dynamic Threat Intelligence)

ОСОБЕННОСТИ

- Блокирование входящих и исходящих соединений
- Анализ большинства web-объектов (PDF, JavaScript, URLs)
- Поддержка 1 Gbps

Web MPS


DTI
Вредоносное ПО 0 дня
1
Перехват трафика
2
Блокирование известных атак
3
Статический анализ
4
Запуск в ВМ (динамический анализ)
5
Блокировка C&C и передачи данных
Windows 7 – SP1
Windows 7 - Base
Windows XP – SP3
Windows XP – SP2
Windows XP - Base
Play Malware Attack
Outbound
CALLBACK ENGINE
Веб трафик

Защита от «составных» атак

Атаки, использующие URLs в Email

- Анализ URL в Web MPS
- Интеграция Web MPS для корреляции URL при атаках spear phishing
- Интеграция с Web MPS для блокирования новых каналов управления вредоносным ПО

Central Management System

Web MPS

Email MPS

Передача информации об атаках

Локально

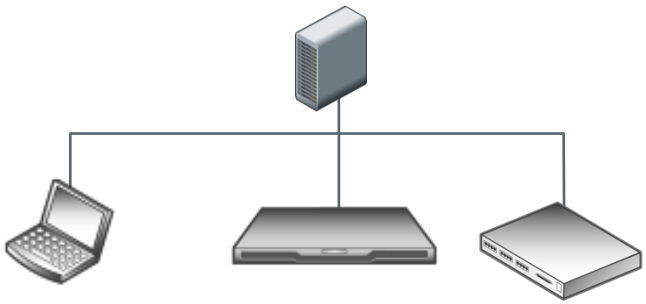
Уровень компании

Глобально

Web MPS

Seconds

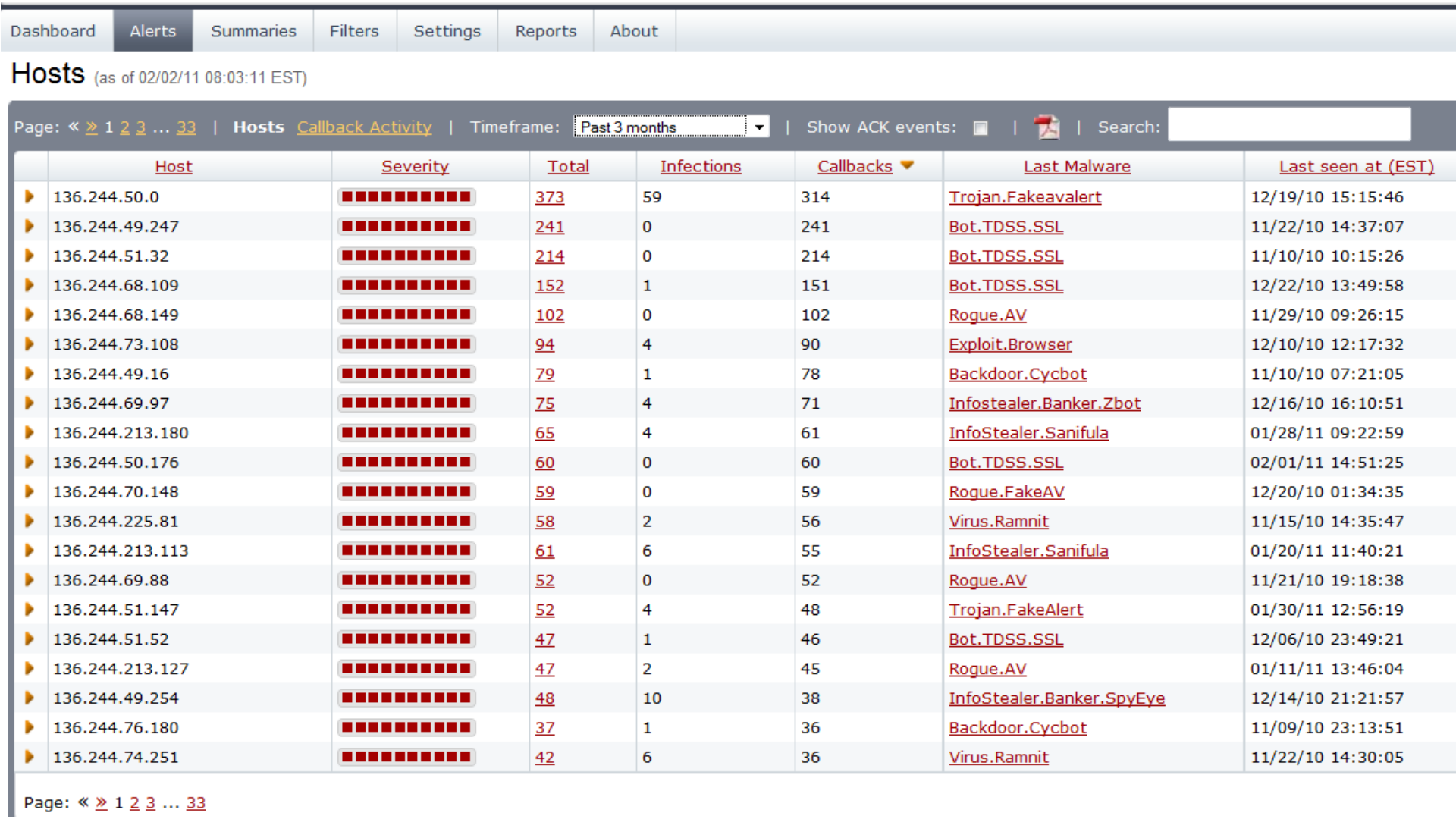
Central Management System



Качество обнаружения угроз 0-дня

Date	CVE ID	App	Details
Aug 2012	CVE-2012-4681	Java	http://www.fireeye.com/blog/technical/cyber-exploits/2012/08/java-zero-day-first-outbreak.html
Dec 2012	CVE-2012-4792	IE	http://www.fireeye.com/blog/technical/targeted-attack/2012/12/council-foreign-relations-water-hole-attack-details.html
Jan 2013	CVE-2013-0422	Java	http://www.fireeye.com/blog/technical/malware-research/2013/01/happy-new-year-from-new-java-zero-day.html
Feb 2013	CVE-2013-0634	Flash	http://www.fireeye.com/blog/technical/cyber-exploits/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html
Feb 2013	CVE-2013-0640 CVE-2013-0641	PDF	http://www.fireeye.com/blog/technical/cyber-exploits/2013/02/in-turn-its-pdf-time.html
Feb 2013	CVE-2013-1493	Java	http://www.fireeye.com/blog/technical/cyber-exploits/2013/02/yaj0-yet-another-java-zero-day-2.html
May 2013	CVE-2013-1347	IE	http://www.fireeye.com/blog/technical/cyber-exploits/2013/05/ie-zero-day-is-used-in-dol-watering-hole-attack.html

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

Вопросы?