



# Аналитика угроз и противодействие вредоносному программному коду

Павел Родионов  
Cisco CSE Security

18 мая 2016

# Как хакеры зарабатывают деньги?

**Глобальный рынок кибер-преступности: \$450B-\$1T**

SSN \$1



Данные кредиток \$0.25-\$60



Мобильное ВПО \$150



Эксплойты \$100k-\$300K



Медицинские записи >\$50



Спам \$50/500K emails



Аккаунт Facebook \$1 за аккаунт с 15 друзьями



DDoS as a Service ~\$7/час



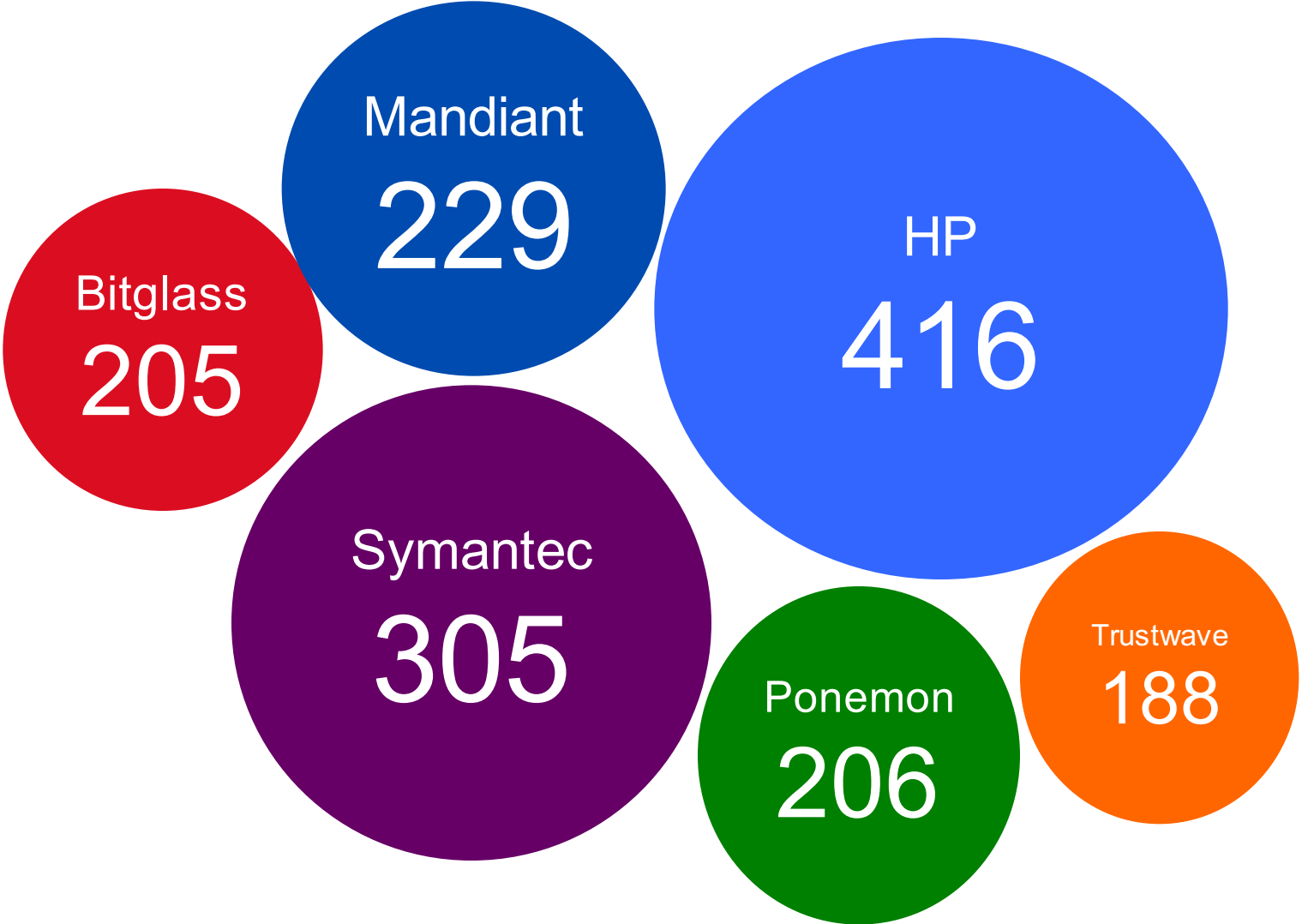
Банковский аккаунт >\$1000 зависит от типа и баланса



Обработка ВПО \$2500 (коммерческое ВПО)



# Время обнаружения вторжений очень велико



# Один пример: эксплойт-кит Angler



Постоянные обновления увеличили уровень проникновения Angler до 40%  
**В два раза эффективнее, чем другие exploit kits в 2014**

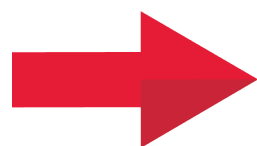
# Теневая инфраструктура устойчива и скрытна

## Базовая инфраструктура Angler



15000

Уникальных сайтов,  
перенаправляющих на Angler



99,8%

из них использовались менее 10 раз

# Rombertik

Вредоносное ПО эволюционирует не только в сторону кражи данных — если его обнаруживают и пытаются воздействовать на него, он может уничтожить зараженную систему.



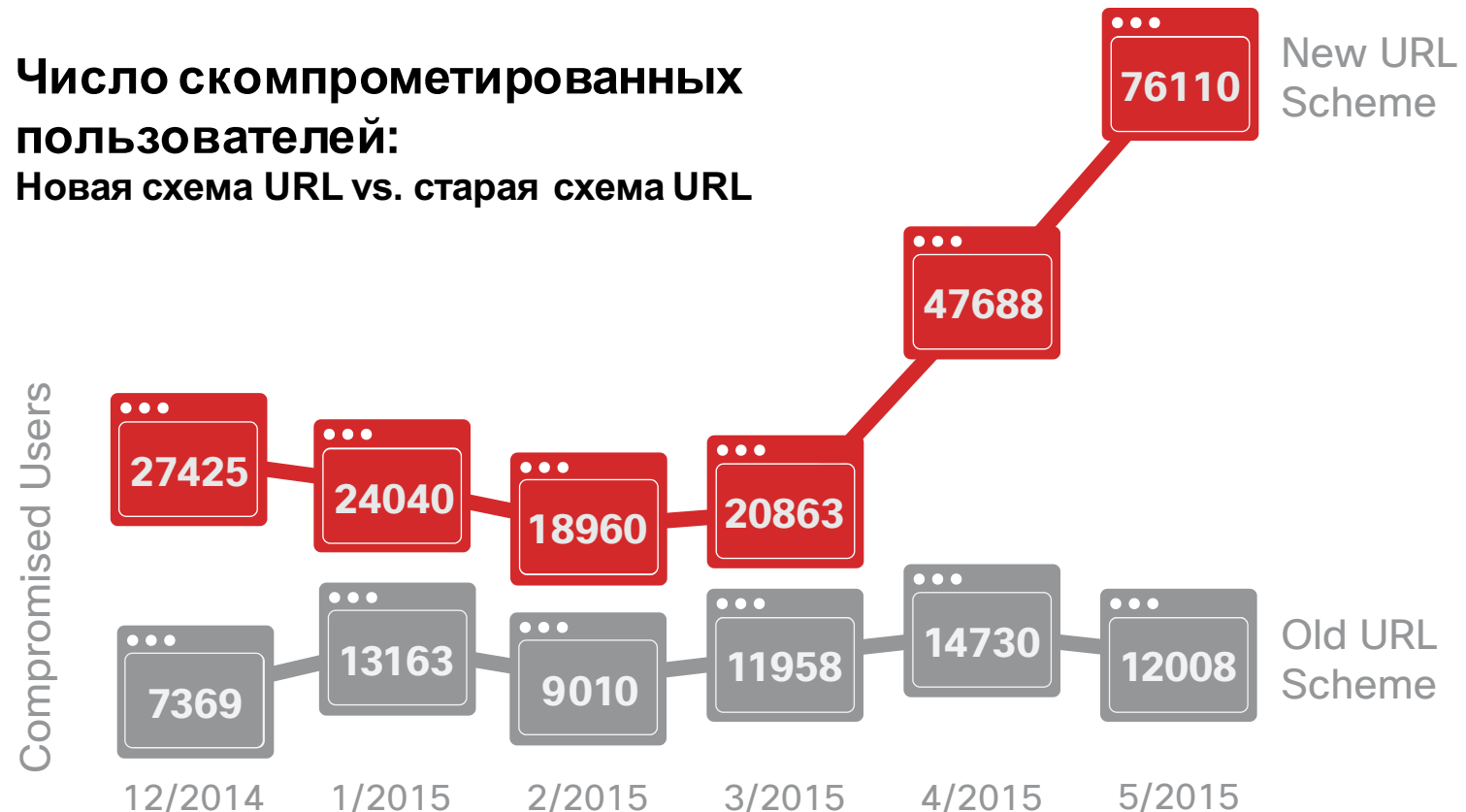
# Обход «песочниц»

Вредоносное ПО эволюционирует в сторону защиты от исследования в песочницах, где вредоносный код запускается и анализируется. Данные методы не новы, но в 2015-м году они стали применяться все чаще.



# Постоянная модификация вредоносного кода

Adware MultiPlug использует собственную схему кодирования URL для обхода обнаружения, тем самым увеличивая «эффективность» по отношению к скомпрометированным пользователям



Изменение домена – раз в 3 месяца (уже 500 доменов)

Непрерывное изменение имен Add-On для браузера (уже 4000 имен)

# Эволюция вымогателей: Цель – данные, а не системы

Фокусировка вымогателей – редкие языки (например, исландский) или группы пользователей (например, онлайн-геймеры)



Личные файлы



Финансовые данные



TOR

Вымогатели теперь полностью автоматизированы и работают через анонимные сети



Фото

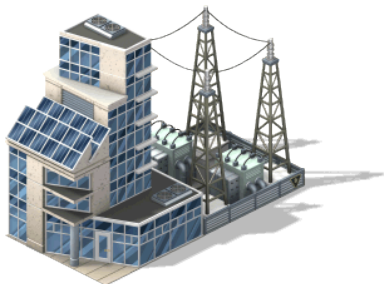


Email

\$300-\$500

Злоумышленники провели собственное исследование идеальной точки цены. Сумма выкупа не чрезмерна

# Наша реальность! Кибератаки в Украине



**Май 2014**

Атака на  
предприятия  
Укрзалізниці

**Август 2014**

Blackenergy 0-Day  
атака на широкий  
спектр органов  
госвласти в  
Украине

**Октябрь 2015**

Blackenergy атака  
на медиакомпани.  
Уничтожение  
видеоматериалов,  
вывод из строя  
рабочих мест  
операторов

**Декабрь 2015**

Blackenergy атака на  
ряд облэнерго. Вывод  
из строя АСУТП  
электростанций,  
обесточена  
значительная  
территория на  
несколько часов

**Декабрь 2015**

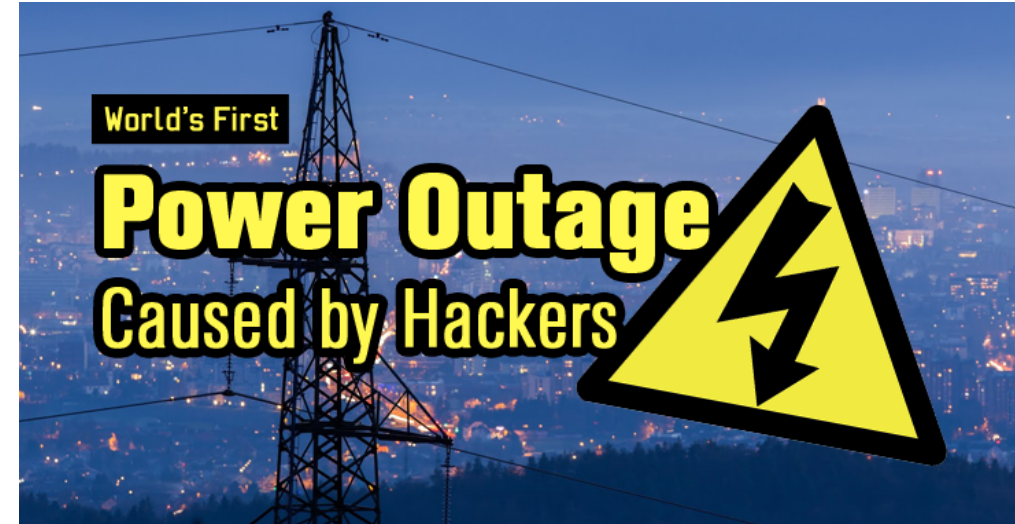
Атака на АП  
Борисполь при помощи  
BlackEnergy



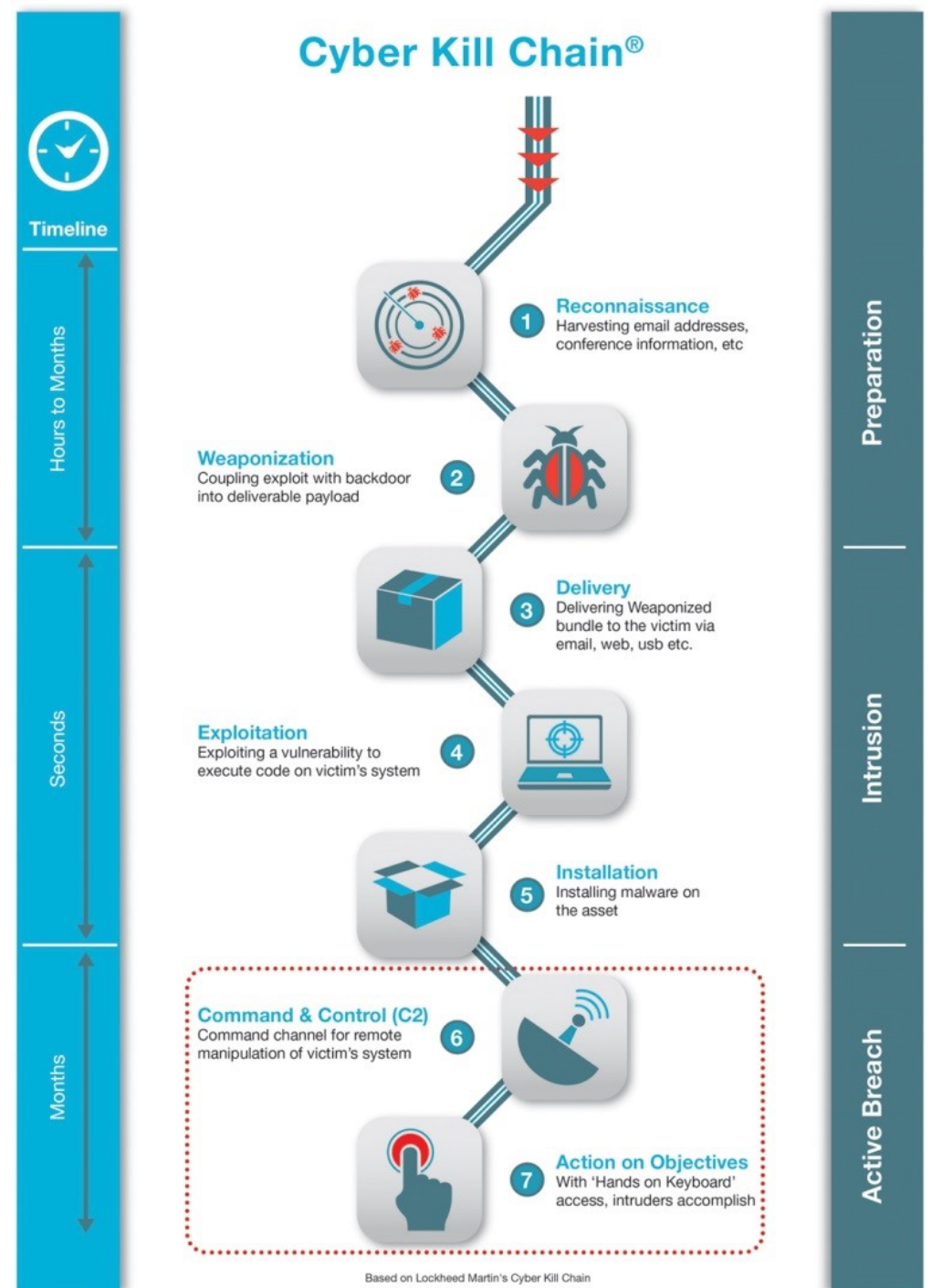
Time

# Кибератаки в Украине

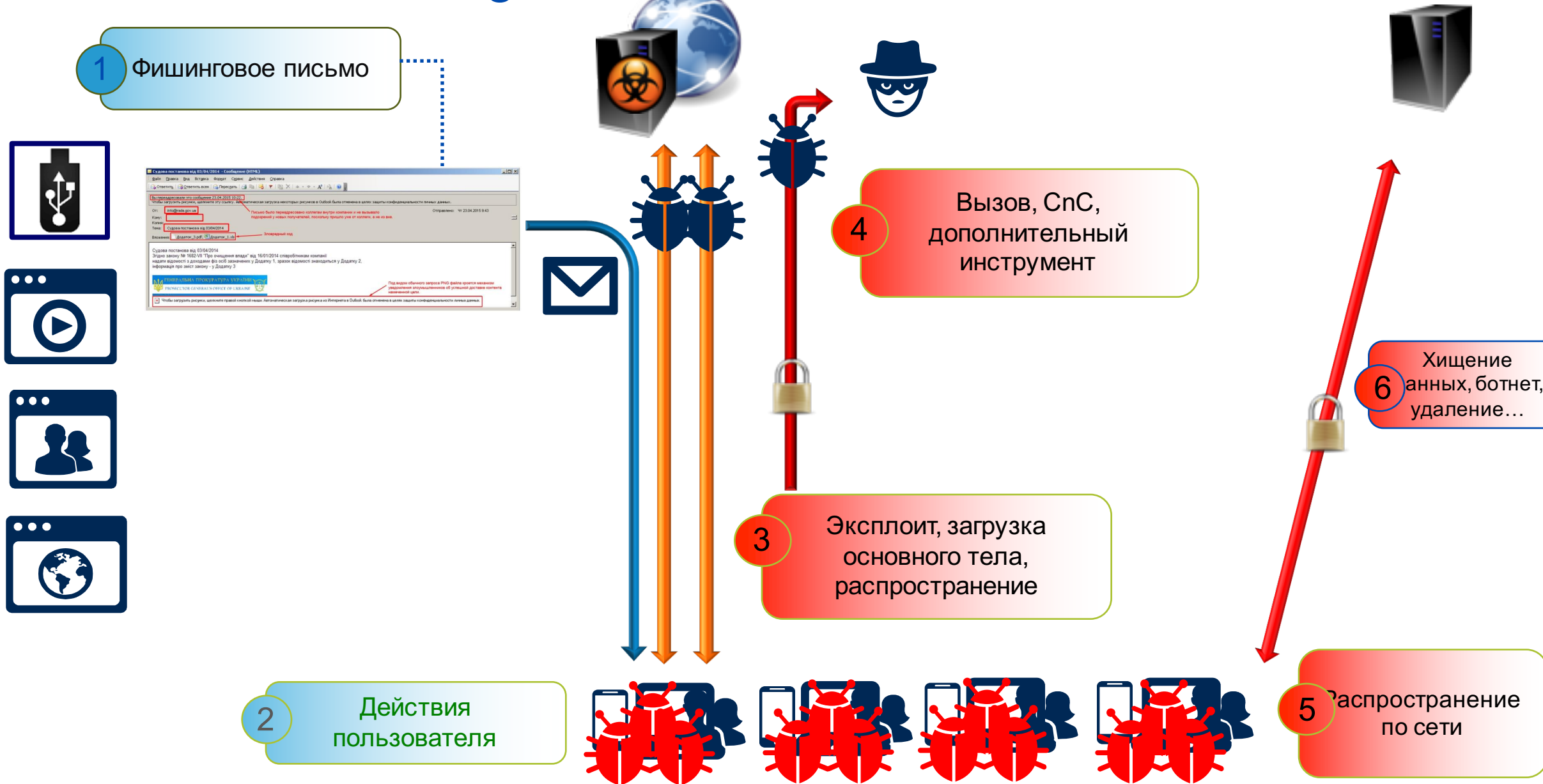
- Перед атакой следует стадия рекогносцировки  
производится анализ email адресов компании,  
формирование соответствующих образцов созданных писем,  
чтобы пользователь их открыл
- Атака включает рассылку электронных писем с  
вредоносным содержанием, который не  
обнаруживается традиционными средствами  
защиты
- Для включения базовых механизмов  
безопасности часто даже не надо менять  
оборудование  
SPF, DKIM, DMARC, NIST 800-177 (общее описание)



# Cyber KillChain



# Типичная атака. Starlight Media



# То самое письмо!

**Судова постанова від 03/04/2014 - Сообщение (HTML)**

Файл Правка Вид Вставка Формат Сервис Действия Справка

Ответить Ответить всем Переслать

Вы переадресовали это сообщение 23.04.2015 10:22.  
Чтобы загрузить рисунки, щелкните эту ссылку. Автоматическая загрузка некоторых рисунков в Outlook была отменена в целях защиты конфиденциальности личных данных.

От: info@rada.gov.ua  
Кому: [Redacted]  
Копия: [Redacted]  
Тема: Судова постанова від 03/04/2014  
Вложения: Додаток\_3.pdf; Додаток\_1.xls

Отправлено: Чт 23.04.2015 9:43

Письмо было переадресовано коллегам внутри компании и не вызвало подозрений у новых получателей, поскольку пришло уже от коллеги, а не из вне.

Зловредный код

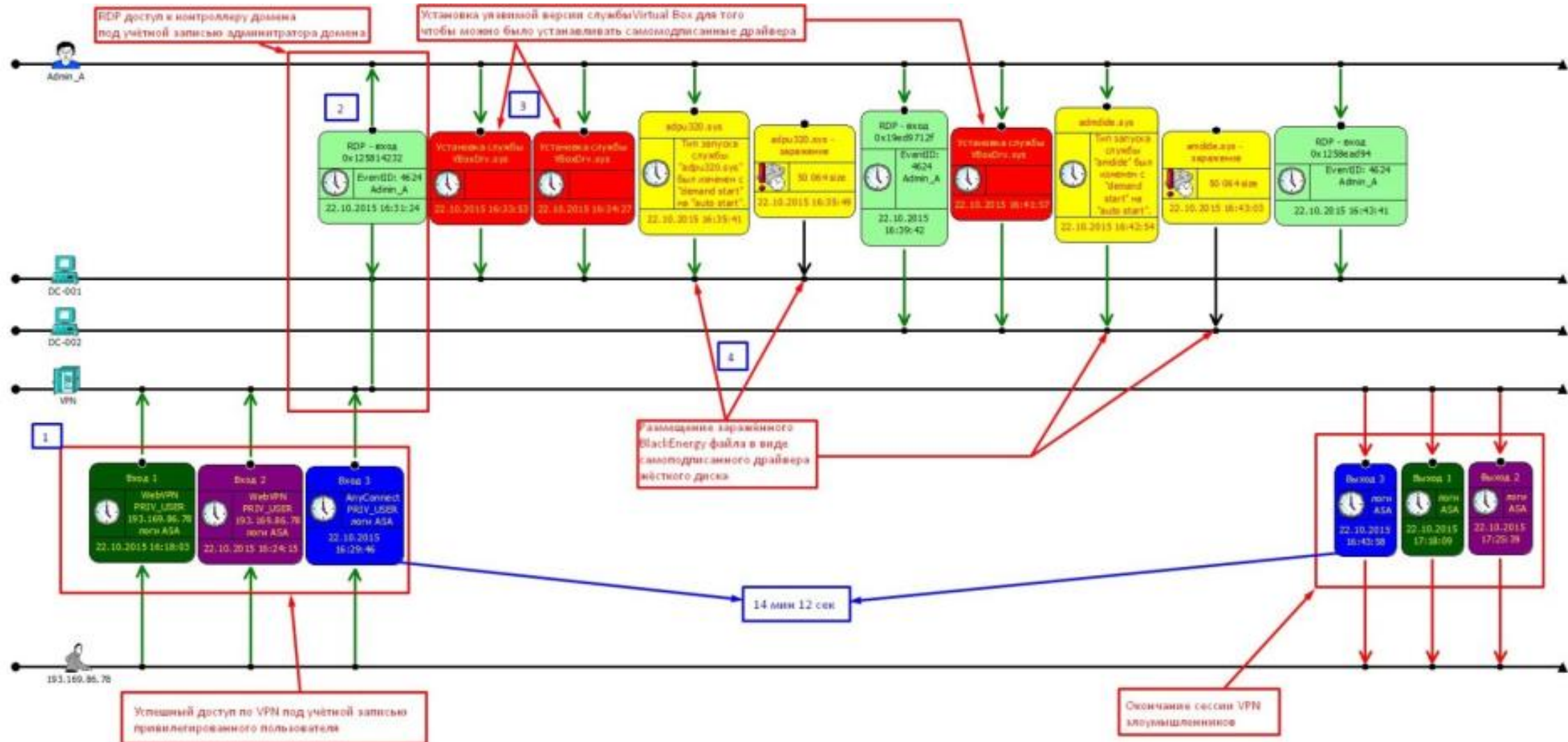
Судова постанова від 03/04/2014  
Згідно закону № 1682-VII "Про очищення влади" від 16/01/2014 співробітникам компанії надати відомості з доходами фіз осіб зазначених у Додатку 1, зразок відомості знаходиться у Додатку 2, інформація про зміст закону - у Додатку 3

ГЕНЕРАЛЬНА ПРОКУРАТУРА УКРАЇНИ  
PROSECUTOR GENERAL'S OFFICE OF UKRAINE

Под видом обычного запроса PNG файла кроется механизм уведомления злоумышленников об успешной доставке контента намеченной цели.

Чтобы загрузить рисунки, щелкните правой кнопкой мыши. Автоматическая загрузка рисунка из Интернета в Outlook была отменена в целях защиты конфиденциальности личных данных.

# 14 минут на установку инструментов



# Продолжительность атаки и этапы её расследования

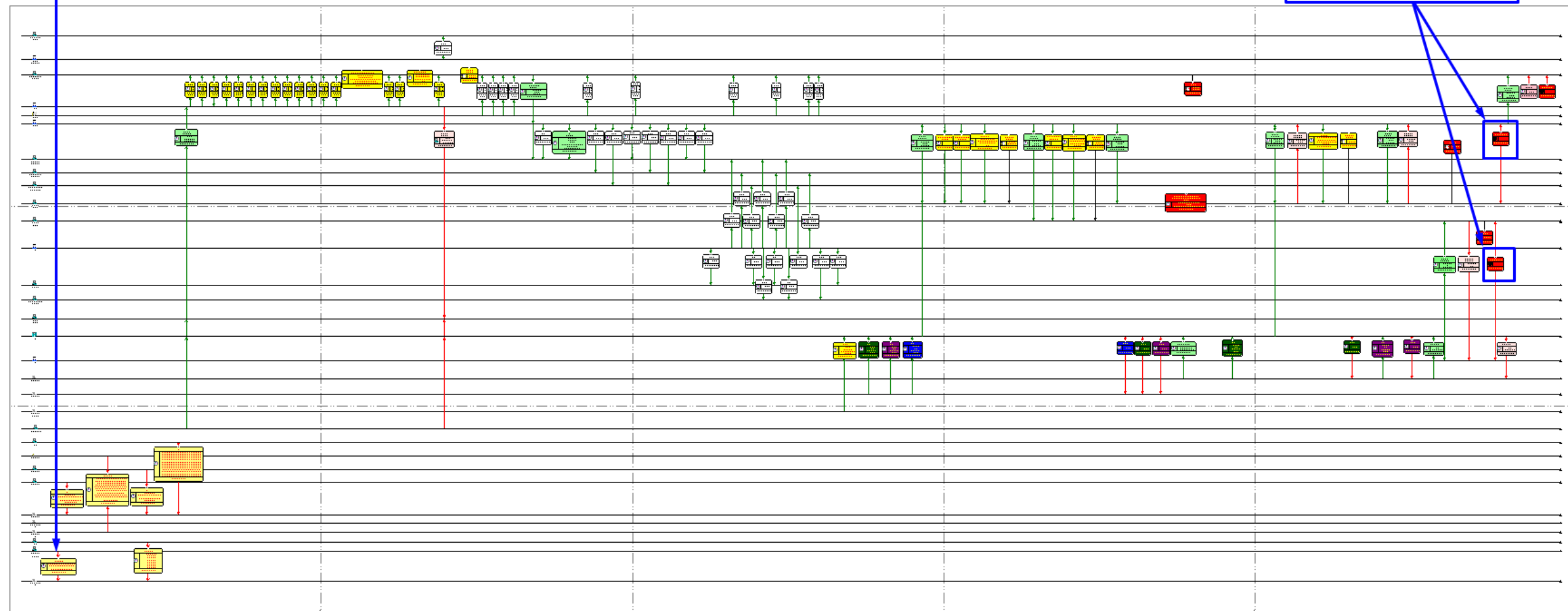
Initial malware delivery attempt

23.04.2015

By continuously collecting and analyzing evidence we reconstructed attack timeline and traced it back to April 2015

Data was destroyed by KILLDISK

24.10.2015 Day of the attack start and beginning of the investigation



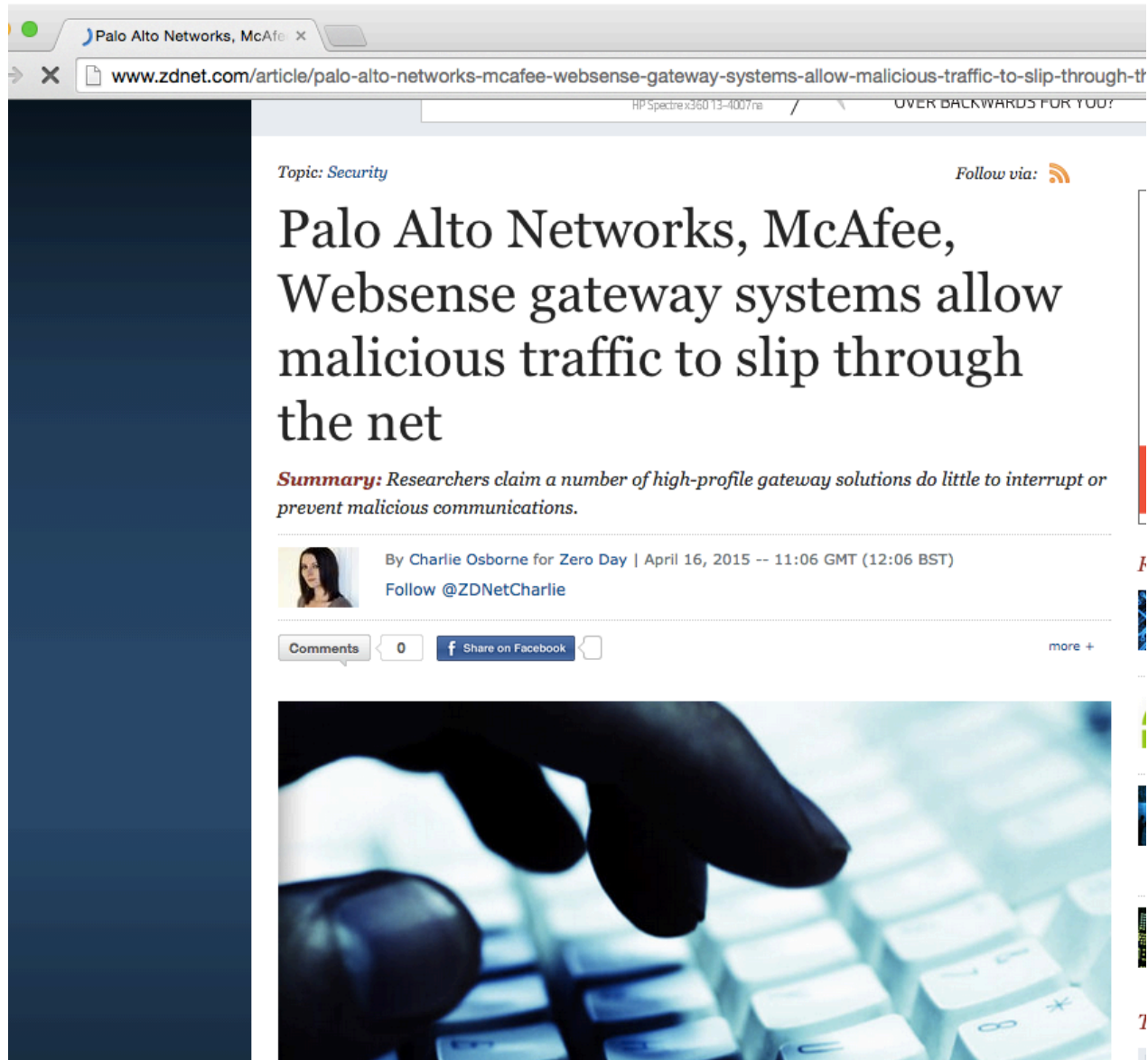


В центре внимания Cisco – анализ угроз

# Почему традиционный периметр не защищает?



# А это подтверждение статистики



The screenshot shows a web browser window with the URL [www.zdnet.com/article/palo-alto-networks-mcafee-websense-gateway-systems-allow-malicious-traffic-to-slip-through-the-net/](http://www.zdnet.com/article/palo-alto-networks-mcafee-websense-gateway-systems-allow-malicious-traffic-to-slip-through-the-net/). The article title is "Palo Alto Networks, McAfee, Websense gateway systems allow malicious traffic to slip through the net". The author is Charlie Osborne for Zero Day, dated April 16, 2015. The article includes a summary: "Researchers claim a number of high-profile gateway solutions do little to interrupt or prevent malicious communications." Below the text is a photograph of a hand typing on a computer keyboard.

16 апреля 2015 года  
<http://www.zdnet.com/article/palo-alto-networks-mcafee-websense-gateway-systems-allow-malicious-traffic-to-slip-through-the-net/>

Дело **СОВСЕМ** не в названиях компаний, проблема в **МЕТОДОЛОГИИ**

# В центре внимания Cisco — анализ угроз!



## Приобретение компании Sourcefire Security

- Ведущие в отрасли СОПВ нового поколения
- Мониторинг сетевой активности
- Advanced Malware Protection
- Разработки отдела по исследованию уязвимостей (VRT)
- Инновации в ПО с открытым исходным кодом (технология OpenAppID)

## Коллективные исследования Cisco – подразделение Talos по исследованию и анализу угроз

- Подразделение Sourcefire по исследованию уязвимостей — VRT
- Подразделене Cisco по исследованию и информированию об угрозах — TRAC
- Подразделение Cisco по безопасности приложений — SecApps

## Приобретение компании Lancope

- Исследования угроз



AMP + FirePOWER  
AMP > управляемая защита от угроз

Cognitive + AMP

Коллективный анализ вредоносного кода  
> Система коллективной информационной безопасности



## Приобретение компании Cognitive Security

- Передовая служба исследований
- Улучшенные технологии поведенческого анализа в режиме реального времени

## Приобретение компании ThreatGRID



- Коллективный анализ вредоносного кода
- Анализ угроз
- «Песочница»

## Приобретение компании OpenDNS

- Анализ DNS/IP-трафика
- Анализ угроз



# Гипотезы безопасности Cisco



Цифровая эволюция

+



Операционный фокус

+



Нехватка людей

Требуются изменения в ИБ



Видимость



Знание угроз



Платформы



Консалтинг



Интеграция



Управление



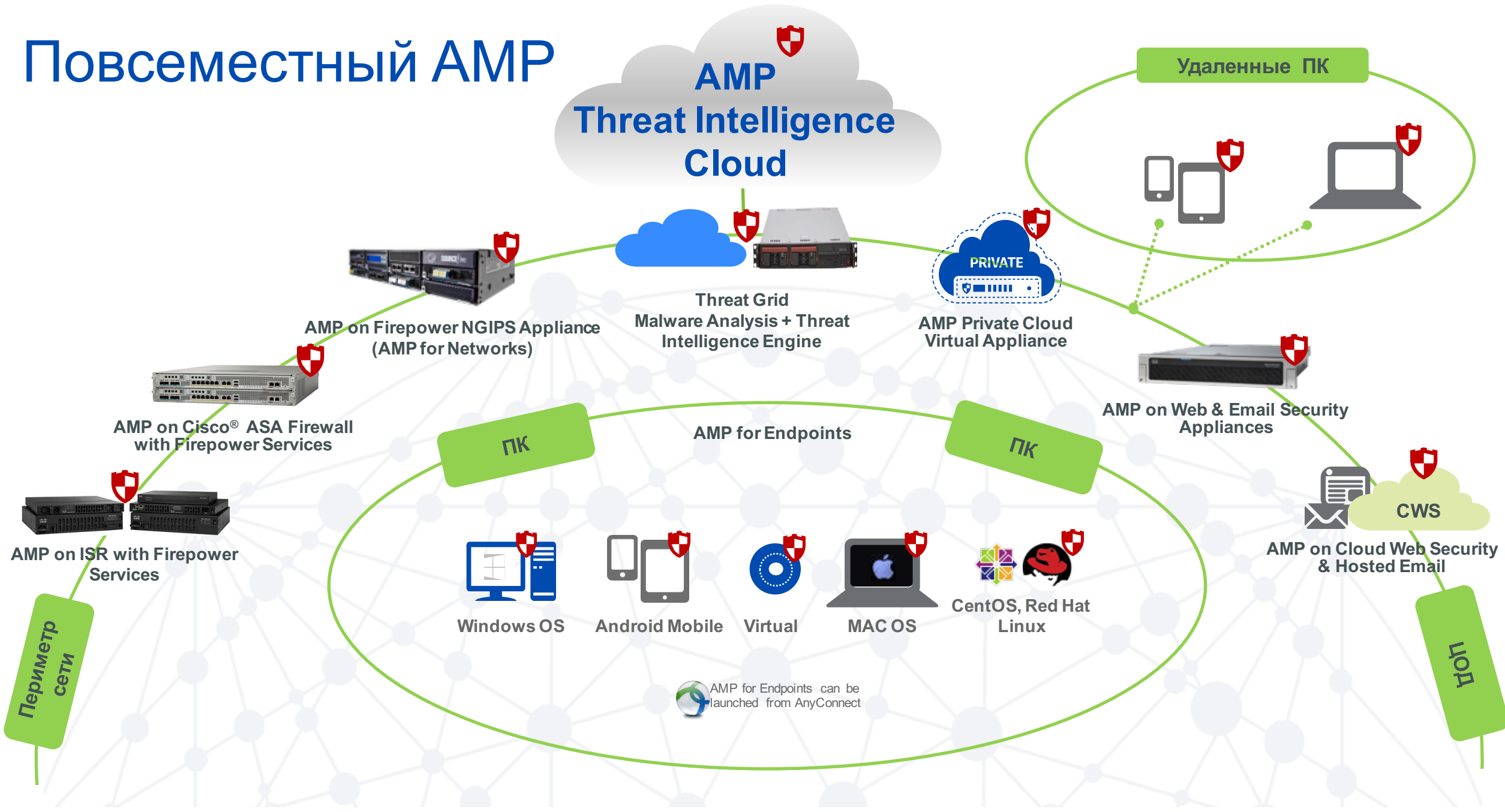
# Cisco Advanced Malware Protection

# Что мы знаем о современном вредоносном ПО?

- Сложные программные продукты, созданные квалифицированными программистами и архитекторами (НЕ ОДИН .EXE файл, НЕ ОДИН вектор атаки)
- Высокий уровень доработки продуктов для очередной кампании
- Дропперы и даунлоудеры и иже с ними: внедрение одного модуля на 99% приведёт к внедрению следующих уникальных модулей
- Известно, что вредоносное ПО будут искать
- Известно про запуск в песочницах
- Развитая индустрия создания специфического ПО с неплохими бюджетами и высоким уровнем заинтересованности
- Все лучшие методологии разработки и отладки

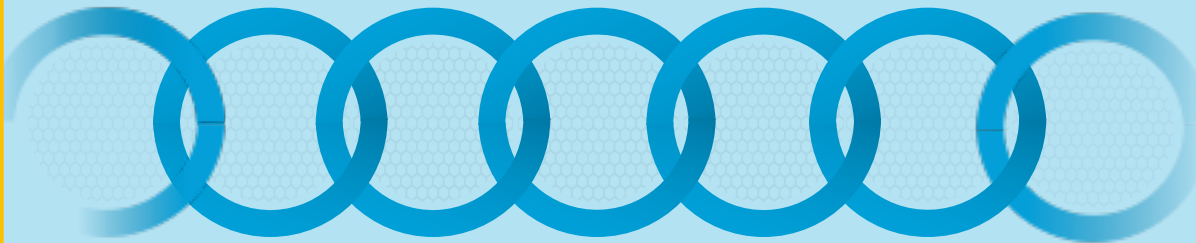


# Повсеместный AMP



# Cisco AMP расширяет защиту NGFW и NGIPS

Точечное обнаружение



Репутация файла и анализ его поведения

Ретроспективная безопасность



Непрерывная и постоянная защита

# Cisco AMP защищает с помощью репутационной фильтрации и поведенческого анализа файлов

## Фильтрация по репутации

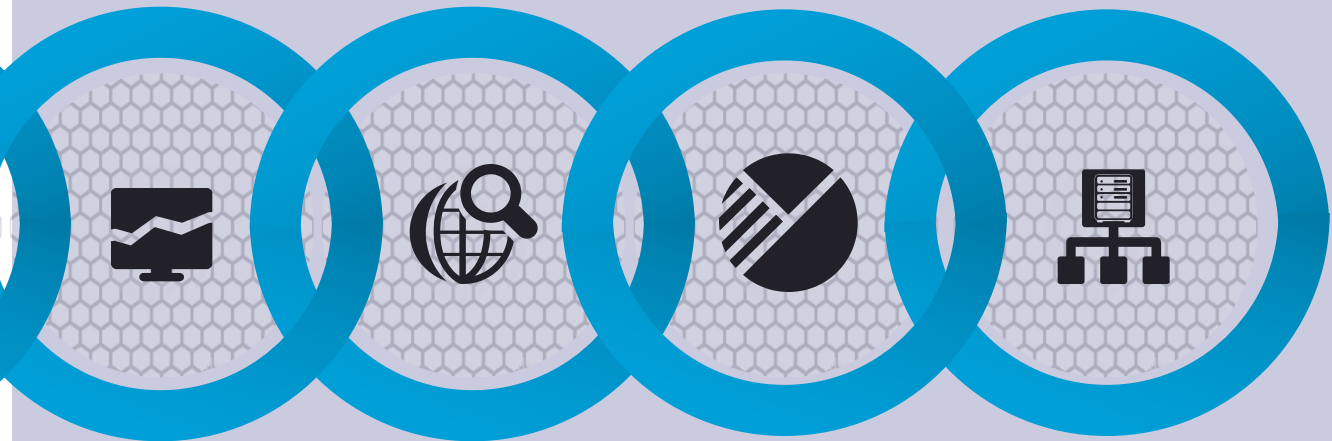


Идентичная  
сигнатура

Нечеткие  
идентифицирующие  
метки

Машинное  
обучение

## Поведенческое обнаружение



Признаки  
компрометации

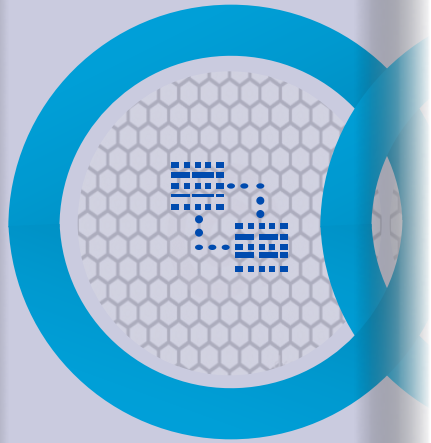
Динамический  
анализ

Расширенная  
аналитика

Сопоставление  
потоков устройств

# Фильтрация по репутации основывается на трех функциях

## Фильтрация



Идентичная  
сигнатура иде

- 1 Сигнатура неизвестного файла анализируется и отправляется в облако
- 2 Сигнатура файла признана не вредоносной и принята
- 3 Сигнатура неизвестного файла анализируется и отправляется в облако
- 4 Известно, что сигнатура файла является вредоносной; ей запрещается доступ в систему



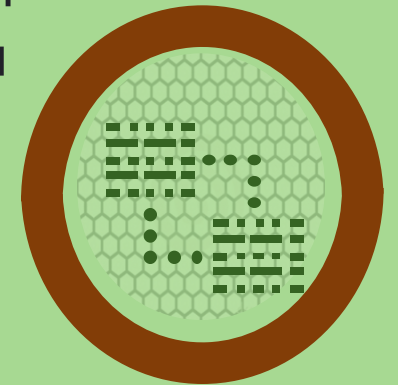
# Техника: точные сигнатуры

- Так действуют традиционные антивирусы
- Отпечаток файла снимается с помощью SHA256 и отправляется в облако для сравнения с базой сигнатур
- **Сам файл не отправляется в облако**
- Быстро и аккуратно обнаруживается угроза
- Снижение нагрузки на другие механизмы обнаружения

**Сигнатуры («точные»):**  
Очень простой подход, который наверняка реализован в любом решении любого поставщика

Точное соответствие файлу

Очень легко обходится простыми модификациями с файлом ☹️



# Возможность создания собственных сигнатур

- Создание собственных сигнатур, например, для контроля перемещения файлов с конфиденциальной информацией или полученных из внешних источников семплов вредоносного кода или даже приложений (для NGFW/NGIPS)

**Simple Custom Detections** + Create

**Quick SCD** Save

**Add SHA-256**  
Add a file by entering the SHA-256 of that file.

**Upload File**  
Upload File To List

**Upload Set of SHA-256's**  
Upload a file containing a set of SHA-256's.

**Files included:**  
09c46e36...82d11cd2  
0723932d...1fbfe85f

**Simple Custom Detections** + Create

**Simple Threat Conviction**  
4 files added Created by Patrick Billings on 2013-11-17 10:46  
Used in policies: 1AUDIT PB, 1st Alpha Audit only Policy  
Used on groups: 1 BLI Test Systems

**Alex test report.pdf**  
1 file added Created by Alex Tatistcheff on 2013-11-15 18:39  
Used in policies: Alex Windows  
Used on groups: Alex's Systems

**1ed**  
0 files added Created by Ed Mendez on 2013-11-10 18:23  
Not associated with any policy or group.

**ed**  
1 file added Created by Ed Mendez on 2013-11-10 18:18  
Used in policies: PolicyTest, Eds Mac test policy  
Used on groups: MyTestGroup, MyTestGroup

**Bill-SAFE List**  
4 files added Created by Patrick Billings on 2013-10-29 03:41  
Used in policies: 1 Protect, 1 Triage  
Used on groups: 1st Alpha Audit Group

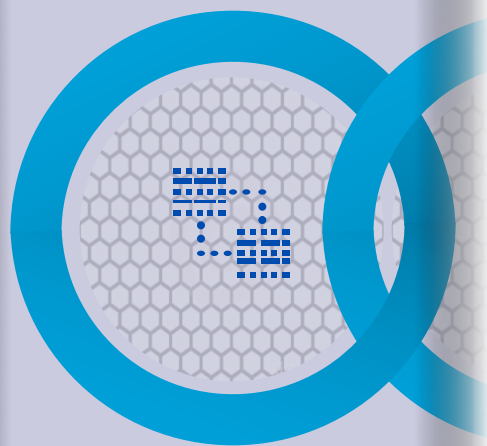
**Simple Custom Detections** are a powerful tool that allow you to perform a series of different actions to exert more granular control over your environment. Simple Custom Detection lists can be assigned to unique groups in your organization and need not apply to your whole environment.

**Outbreak Control**  
Use this feature to stop malware that is spreading through your environment but is not being detected by your antivirus solution. Detected files will be removed and quarantined.

**Application Control**  
Adding key files from software packages to a Simple Custom Detection list will prevent them from being installed in your environment. This will also remove and quarantine the same files if they are already present in your environment.

**Intellectual Property Control**  
Files included in Simple Custom Detections will not be allowed on endpoints that have a policy that references the list. These files will be removed and quarantined.  
Please see the help documentation for further information on these topics.

# Фильтрация по репутации основывается на трех функциях



Идентичная  
сигнатура

Идентичная  
сигнатура

- 1 Сигнатура файла анализируется и определяется как вредоносная
- 2 Доступ вредоносному файлу запрещен
- 3 Полиморфная модификация того же файла пытается получить доступ в систему
- 4 Сигнатуры двух файлов сравниваются и оказываются аналогичными
- 5 Доступ полиморфной модификации запрещен на основании его сходства с известным вредоносным ПО



# Техника: ядро Ethos

- ETHOS - ядро формирования нечетких отпечатков с помощью статической/пассивной эвристики
- Полиморфные варианты угрозы часто имеют **общие структурные** свойства
- Не всегда нужно анализировать все содержимое бинарного файла
- Повышение масштабируемости - обнаруживается и оригинал и модификации
- Традиционно создаются вручную
  - Лучшие аналитики = несколько общих сигнатур в день
- У нас полная автоматизация = **МАСШТАБИРОВАНИЕ**

**Ethos:** создание обобщенных сигнатур, что опять же достаточно традиционно для отрасли

Адресуются семейства вредоносного кода

Потенциальное увеличение числа ложных срабатываний



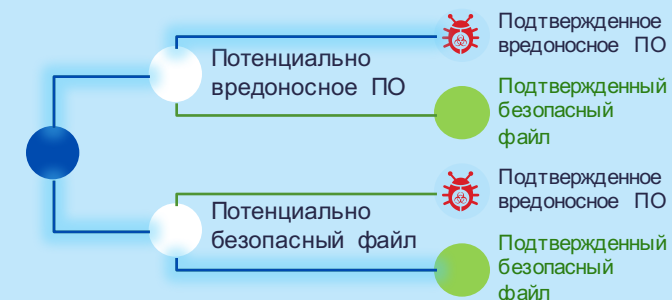
# Фильтрация по репутации основывается на трех функциях



- 1 Метаданные неизвестного файла отправляются в облако для анализа
- 2 Метаданные признаются потенциально вредоносными
- 3 Файл сравнивается с известным вредоносным ПО и подтверждается как вредоносный
- 4 Метаданные второго неизвестного файла отправляются в облако для анализа
- 5 Метаданные аналогичны известному безопасному файлу, потенциально безопасны
- 6 Файл подтверждается как безопасный после сравнения с аналогичным безопасным файлом

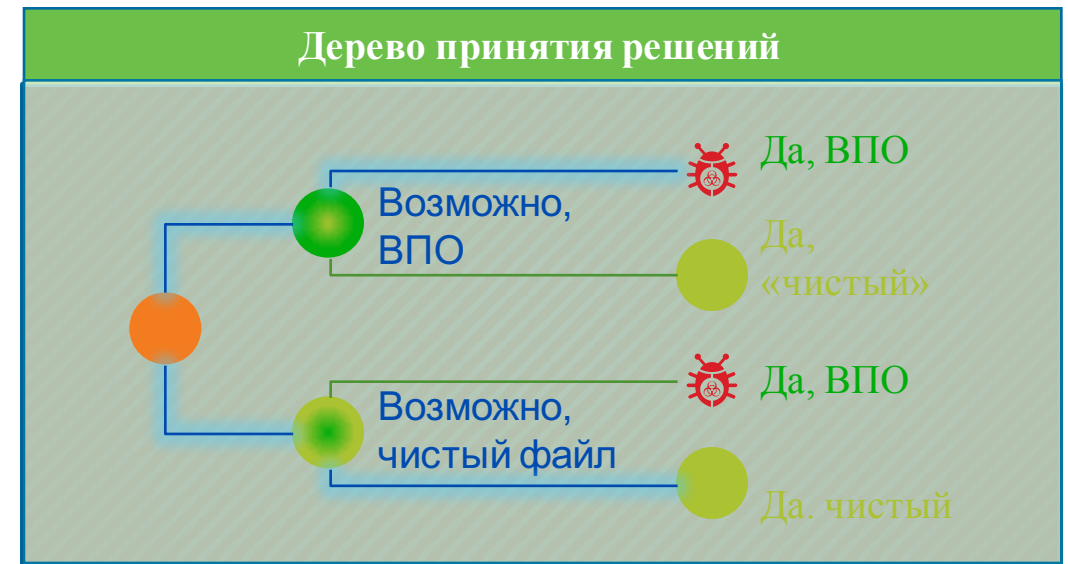


## Дерево решений машинного обучения



# Техника: ядро Spero

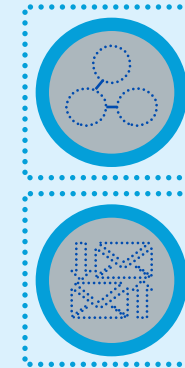
- Метки AMP = более 400 атрибутов, полученных в процессе выполнения
  - Сетевые подключения?
  - Нестандартные протоколы?
  - Использование интерфейсов API (каких)?
  - Изменения в файловой системе?
    - Самокопирование
    - Самоперенос
  - Запуск других процессов?
- Автоматизирует классификацию файлов на основе общих схожих признаков
- Машинное обучение позволяет находить и классифицировать то, что не под силу человеку – из-за возможности анализа больших объемов данных



# Поведенческое обнаружение основывается на четырех функциях



1. Неизвестный файл проанализирован, обнаружены признаки саморазмножения
2. Эти признаки саморазмножения передаются в облако
3. Неизвестный файл также производит независимые внешние передачи
4. Это поведение также отправляется в облако
5. Об этих действиях сообщается пользователю для идентификации файла как потенциально вредоносного



# Техника: анализ вредоносных признаков

- Анализ поведения файла — большое количество анализируемых параметров
- Требуется больше времени на анализ, чем сигнатуры
- Потенциально ложные срабатывания
- Подробная информация о причинах принятия того или иного решения
- Выдача финального Threat Score

**File Analysis Detail > 53de8225fc823c...0**

General Information	
Analysis	
Start time	
Start date	
Number of analysed new started processes	
Score	
Status	

**Warnings:**

- Too many NtReadFile calls (excessive behavior)
- Too many NtUserPostMessage calls (excessive behavior)
- Too many NtProtectVirtualMemory calls (excessive behavior)
- Too many NtAllocateVirtualMemory calls (excessive behavior)
- Too many NtUserMessageCall calls (excessive behavior)
- Too many NtReadVirtualMemory calls (excessive behavior)
- Too many NtSetInformationFile calls (excessive behavior)
- Too many NtWriteFile calls (excessive behavior)

**Classification / Threat Score**

Persistence, Installation, Boot Survival :	
Hiding, Stealthiness, Detection and Removal Protection :	
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection :	
Spreading :	
Exploiting :	
Networking :	
Data spying, Sniffing, Keylogging, Ebanking Fraud :	

**Classification / Threat Score**

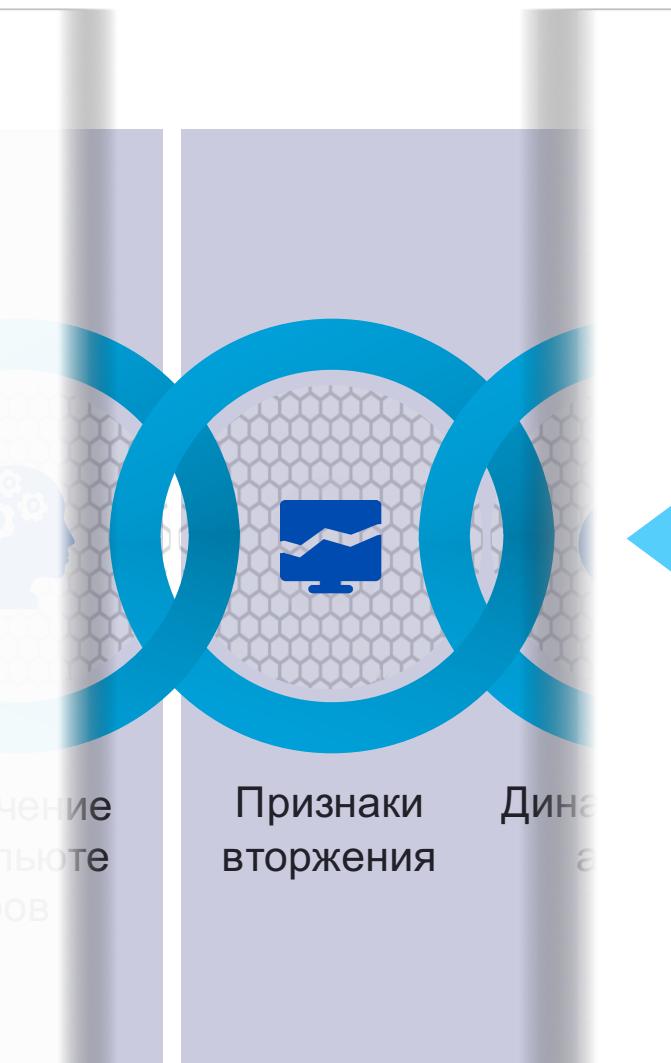
Factor	Score	Threat Level
AV Detection	1	Low
Networking	1	Low
Persistence and Installation Behavior	100	Very High
PE File Obfuscation	6	Low
System Summary	39	Medium
HIPS / PFW / Operating System Protection Evasion	95	Very High
Anti Debugging	63	High
Virtual Machine Detection	14	Low
Language and Operating System Detection	1	Low

# Уровень угрозы может быть настроен

<input checked="" type="checkbox"/> Enable File Reputation Filtering	
<input checked="" type="checkbox"/> Enable File Analysis <i>When File Analysis is enabled, files may be automatically sent to the cloud for further analysis. This provides the highest level of protection against known and targeted threats. File Analysis is only available when file reputation filtering is enabled.</i>	
Cloud Domain:	<input type="text" value="a.immunet.com"/>
Cloud Server Pool:	<input type="text" value="cloud-sa.amp.sourcefire.com"/>
Heartbeat Interval:	<input type="text" value="15"/> seconds
Reputation Threshold:	<input type="text" value="60"/> <i>valid range 1 through 100, recommended value 60</i>
Query Timeout:	<input type="text" value="2"/> seconds
File Analysis Server URL:	<input type="text" value="https://intel.api.sourcefire.com"/>
Client ID (Reference Only):	File Reputation: f6eb4487-9abc-4c75-b937-fab3c6f32c78 File Analysis: 02564c4e575341313438323837230000000000

На примере Cisco AMP for Content Security (WSA)

# Поведенческое обнаружение основывается на четырех функциях



1. Известные файлы загружаются в облако, где механизм динамического анализа запускает их в изолированной среде
2. Два файла определяются как вредоносные, один подтвержден как безопасный
3. Сигнатуры вредоносных файлов обновляются в облаке информации и добавляются в пользовательскую базу



# Техника: динамический анализ

- Файлы для динамического анализа (песочница) могут быть загружены автоматически или в ручном режиме
- Загрузка файла осуществляется только в случае его неизвестности (неизвестен статус и Threat Score)
  - «Чистые», уже проверенные ранее файлы или вредоносное ПО с вычисленным Threat Score в песочницу не загружаются, чтобы не снижать производительность решения
- Файлы можно загружать через прокси-сервера
- Результат представляется в виде обзора и детального анализа

# Анализ в облаке может занимать время

## File Analysis

Printable (PDF)

### Search for File Analysis Data

Enter any SHA256 to search for file analysis results from the Cisco cloud.

Search by SHA256:

Time Range:

15 Feb 2014 00:00 to 17 Mar 2014 13:07 (GMT -08:00)

Data in time range: 100.0 % complete

### Completed Analysis Requests from This Appliance

Displaying 1 - 10 of 20 items.

File SHA256	Time of Analysis Request	Time Analysis Completed
05efa119...58c9aaf5	17 Mar 2014 07:48:30	17 Mar 2014 07:53:22
a0d7ed88...fb6e3228	17 Mar 2014 07:45:03	17 Mar 2014 07:48:56
ccd00f2f...47f8a370	17 Mar 2014 07:31:21	17 Mar 2014 07:34:59
eec23d66...985dbd50	13 Mar 2014 13:12:36	13 Mar 2014 13:16:18
7fb078f3...fc7ea522	24 Feb 2014 17:49:46	24 Feb 2014 17:53:22
4c9e7d1e...36338ec2	24 Feb 2014 17:49:44	24 Feb 2014 17:53:20
75e23b4f...b42a0723	24 Feb 2014 16:57:00	24 Feb 2014 17:00:43
175fce5f...8fd0aa29	24 Feb 2014 16:57:02	24 Feb 2014 17:00:36
ec6ed12d...15da3295	24 Feb 2014 16:56:28	24 Feb 2014 17:00:06
879f08a4...e80cb4ef	24 Feb 2014 15:54:47	24 Feb 2014 15:58:25

Displaying 1 - 10 of 20 items.

07 Jan 2014 00:00 to 07 Apr 2014 23:55 (GMT -05:00)

Data in time range: 99.7 % complete

### Completed Analysis Requests from This Appliance

Items Displayed

Displaying 1 - 10 of 11 items.

« Previous | 1 | 2 | Next »

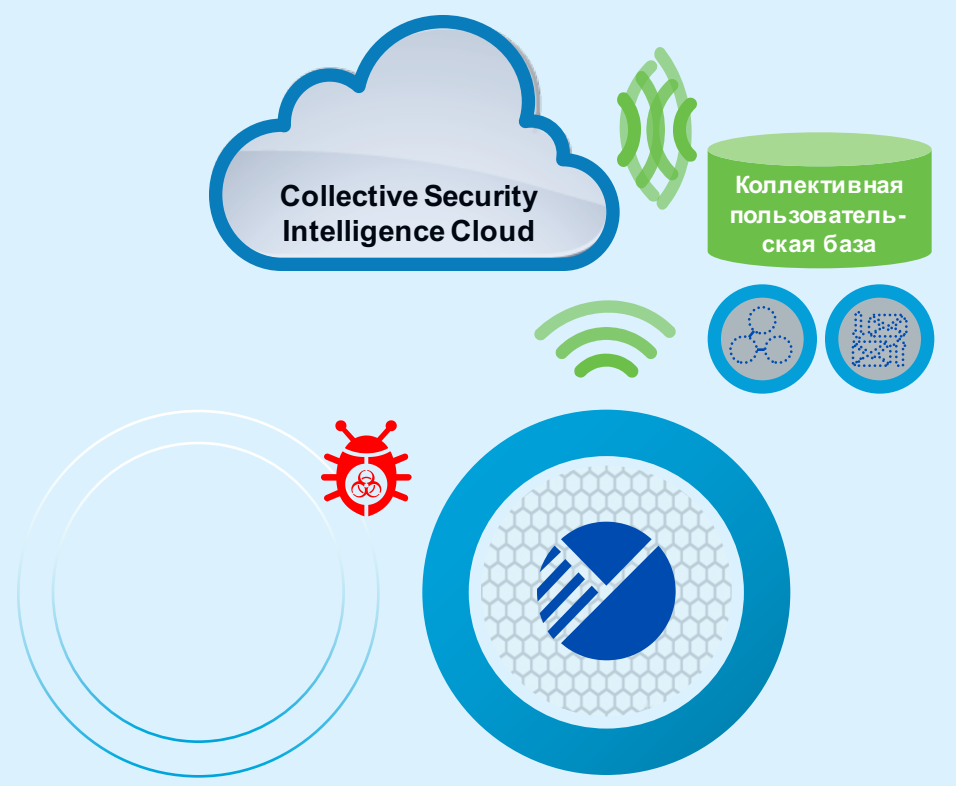
File SHA256	Time of Analysis Request	Time Analysis Completed	Disposition
9862e8ae...50c6ee70	03 Apr 2014 11:29:18	03 Apr 2014 12:46:39	Malicious
5b4edb7a...e55619e0	03 Apr 2014 09:39:48	03 Apr 2014 11:04:05	Malicious
5e1acca7...dd9539dd	03 Apr 2014 09:39:45	03 Apr 2014 11:02:05	Malicious
9cca49ee...8b8416f0	03 Apr 2014 06:24:15	03 Apr 2014 08:01:43	Malicious
ec53e7ec...3bab3237	03 Apr 2014 06:24:25	03 Apr 2014 07:50:08	Malicious
8aef1e1a...10f3c943	03 Apr 2014 06:25:30	03 Apr 2014 07:48:14	Malicious
e81896b1...683667ab	03 Apr 2014 06:25:31	03 Apr 2014 07:43:13	Malicious
3c194ac1...4f42d460	03 Apr 2014 06:24:23	03 Apr 2014 07:42:21	Malicious
d39df27e...e2dc9e65	03 Apr 2014 06:24:34	03 Apr 2014 07:42:15	Malicious

На примере Cisco AMP for Content Security (ESA)

# Поведенческое обнаружение основывается на четырех функциях



- 1 Получает информацию о неопознанном ПО от устройств фильтрации по репутации
- 2 Получает контекст для неизвестного ПО от коллективной пользовательской базы
- 3 Анализирует файл в свете полученной информации и контекста
- 4 Идентифицирует вредоносное ПО и добавляет новую сигнатуру в пользовательскую базу



# Индикаторы компрометации

- Индикатор компрометации – объединение нескольких связанных событий безопасности в единое мета-событие

- ИОС “CNC Connected” (узел вероятно находится под чужим управлением)

Узел подключился к серверу C&C

Сработала система обнаружения вторжений по сигнатуре “Malware-CNC”

На узле запущено приложение, которое установило соединение с сервером C&C

- Встроенные и загружаемые индикаторы компрометации

The screenshot shows the 'Host Profile' for IP 10.5.61.104. It lists various identifiers like NetBIOS Name, Device (Hops), and MAC Addresses. Below this, the 'Indications of Compromise' section is highlighted, showing three events:

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

Below the table, the 'Systems' section shows the host's OS details:

Hardware	OS Vendor	OS Product	OS Version	Source
	Google	Chromium	3701.81.2	FireSIGHT

На примере Cisco AMP for Networks

The screenshot shows the 'Endpoint IOC - Installed Endpoint IOCs' page in Cisco AMP for Endpoint. It displays a list of installed indicators of compromise:

Indicator Name	Uploaded	Status	Actions
PoSeidon registry text contains winhost or pes13 PoSeidon_Registry.ioc	2015-03-22 21:44:27 UTC	Active	View Edit
PoSeidon process name contains winhost PoSeidon_Process.ioc	2015-03-22 21:44:09 UTC	Active	View Edit
PoSeidon filename contains winhost, pes13, or u... PoSeidon_Filename.ioc	2015-03-22 21:43:50 UTC	Active	View Edit
Check for SHA256 from ThreatGrid artifacts doc.ioc	2015-02-04 22:19:01 UTC	Active	View Edit

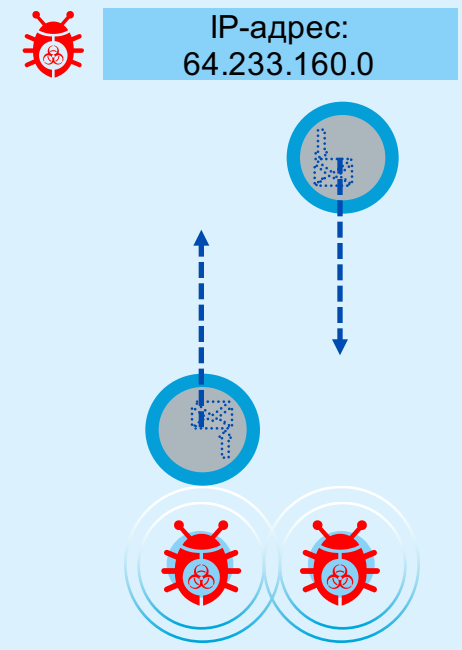
На примере Cisco AMP for Endpoint

# Поведенческое обнаружение основывается на четырех функциях



Статистический анализ    Расширенная аналитика потоков

- 1 Сопоставление потоков устройств производит мониторинг источника и приемника входящего/исходящего трафика в сети
- 2 Обнаруживаются два неизвестных файла, связывающихся с определенным IP-адресом
- 3 Один передает информацию за пределы сети, другой получает команды с этого IP-адреса
- 4 Collective Security Intelligence Cloud распознает внешний IP-адрес как подтвержденный вредоносный сайт
- 5 Из-за этого неизвестные файлы идентифицируются как вредоносные



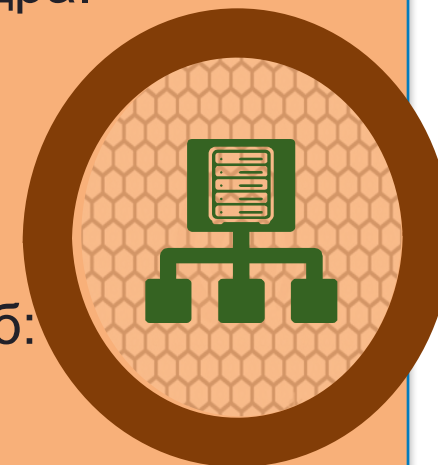
# Техника: Анализ потоков данных с устройств

- Мониторятся внутренние и внешние сети
- Данные по репутации IP-адресов
- Регистрация URL / доменов
- Временные метки
- Передаваемые файлы

**Корреляция потоков устройств:** Анализ сетевых потоков на уровне ядра. Позволяет блокировать или предупреждать о любых сетевых действиях

В облаке есть информация об: известных серверах CnC, фишинговых сайтах, серверах ZeroAccess CnC, и т.д.

Пользовательские списки



# Сила в комбинации методов обнаружения

- На конечных узлах не хватает ресурсов для анализа все усложняющегося вредоносного кода
- Не существует универсального метода обнаружения вредоносного кода – у каждого метода есть своя область применения, свои достоинства и недостатки
- Каждый метод может быть обойден вредоносным кодом; особенно специально подготовленным

**7 методов обнаружения в Cisco AMP повышают эффективность защиты!!!**

# Почему необходима непрерывная защита?

Объем и контрольные  
ТОЧКИ



Эл. почта



Оконечные устройства



Интернет



Сеть



Система  
предотвращения  
вторжений IPS



Устройства

Поток  
телеметрических  
данных



Идентифицирующие метки  
и метаданные файла



Файловый и сетевой  
ввод/вывод



Информация о процессе

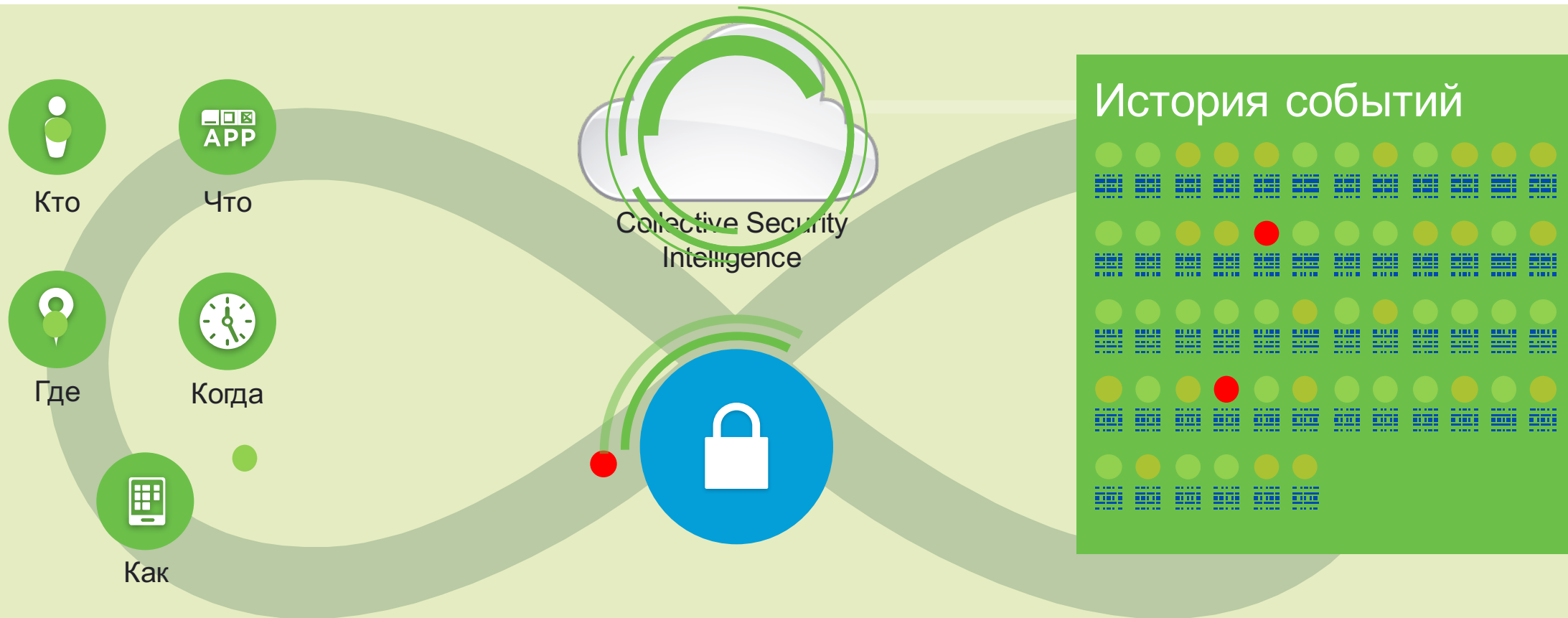
Непрерывная подача

1111010011101 1100001110001110 1001 1101 1110011 0110011  
1110 1001 1101 1110011 0110011 101000 0110 00 011100  
100001 1100 0111010011101 1100001110001110 1001 1101



Непрерывный анализ

# Почему необходима непрерывная защита?

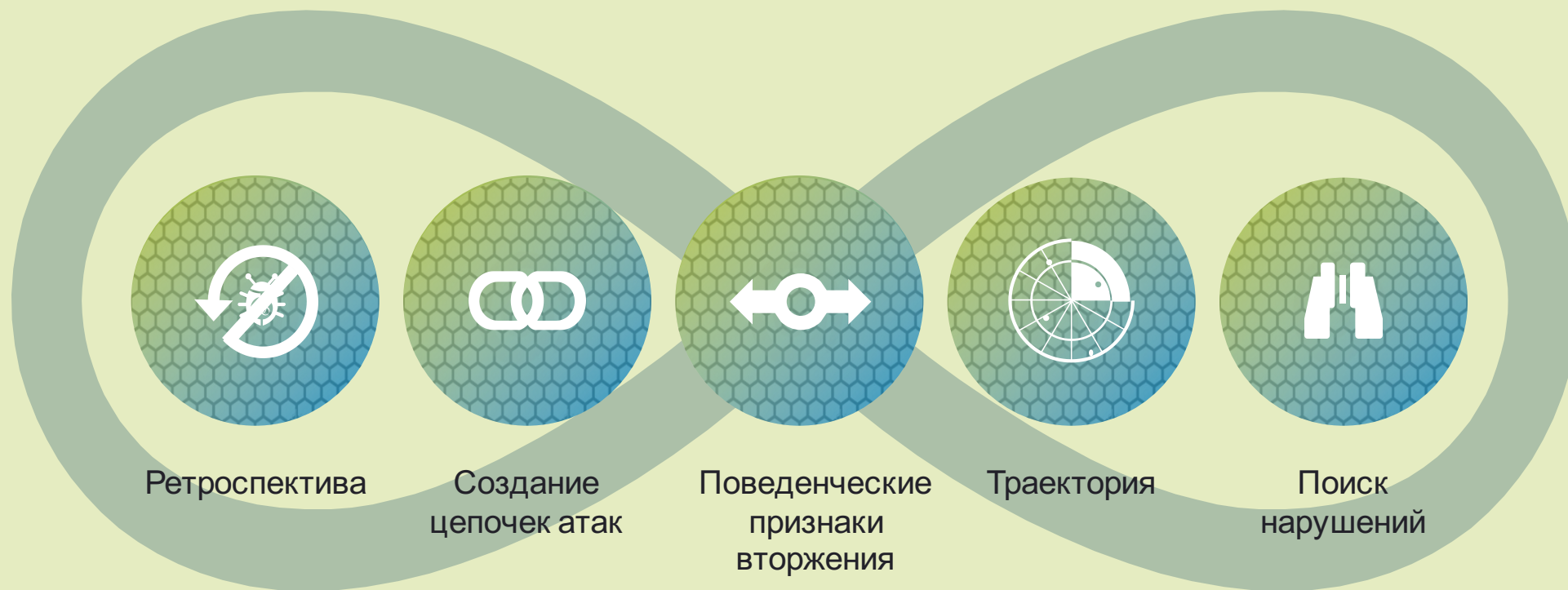


Контекст

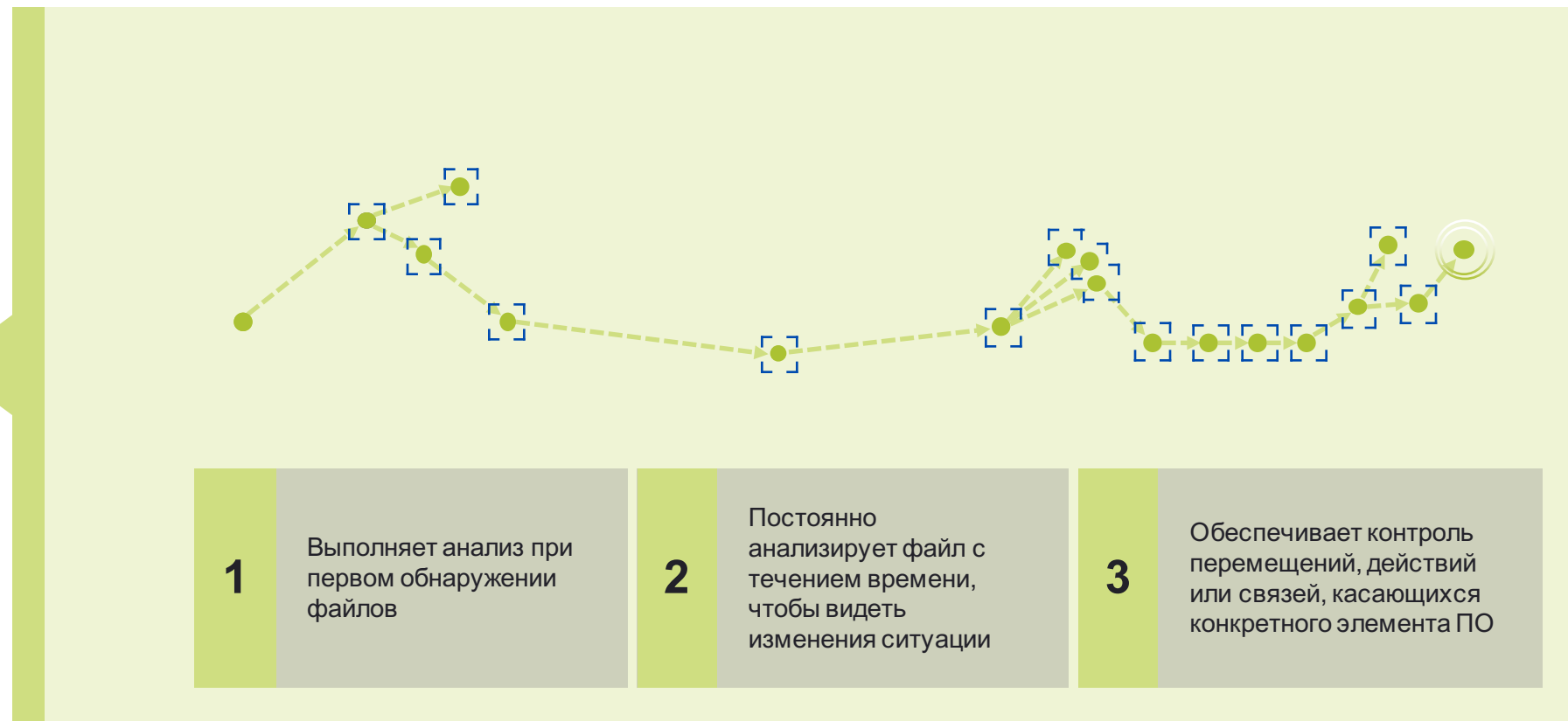
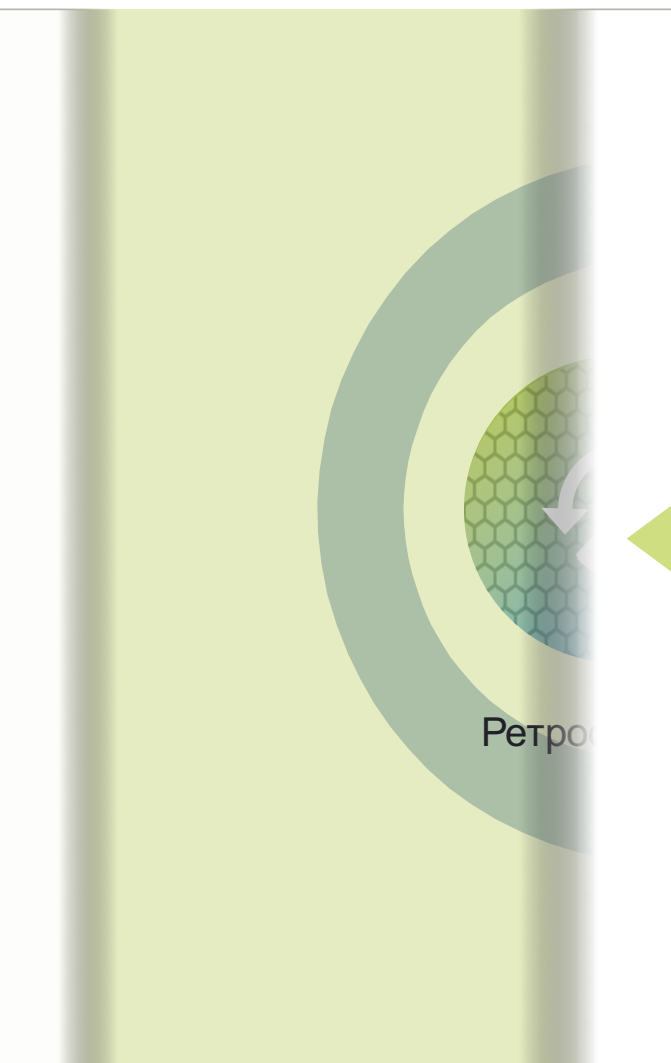
Применение

Непрерывный анализ

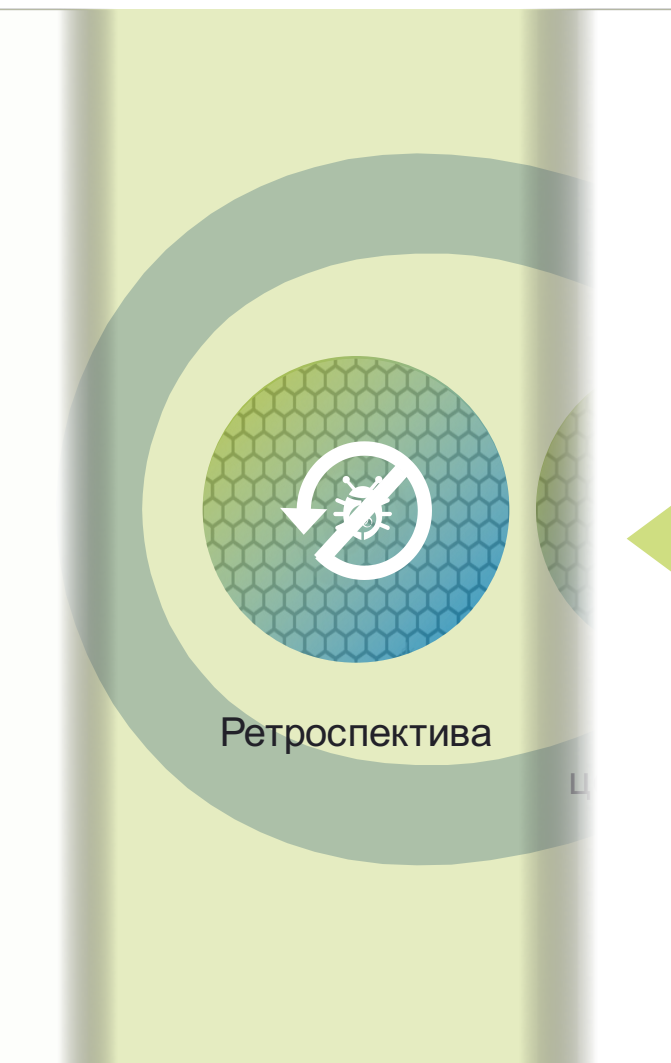
# Cisco AMP обеспечивает ретроспективную защиту



# Ретроспективная безопасность основана на...



# Ретроспективная безопасность основана на...

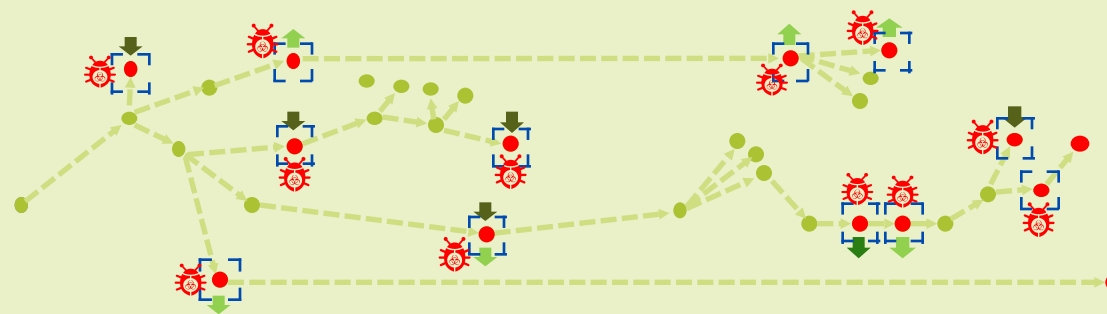


Использует ретроспективные возможности тремя способами:

- 1 Ретроспективный анализ файлов
- 2 Ретроспектива процесса
- 3 Ретроспектива связи



**Создание цепочки атак**  
Анализирует данные, собранные ретроспекцией файлов, процессов и связи для обеспечения нового уровня интеллектуальных средств мониторинга угроз



## Ретроспектива связей

Производит мониторинг, какие приложения выполняют действия

# Пример ретроспективы файла и связей

**Network File Trajectory for 0517f034...588e1374**

**File SHA-256** 0517f034...588e1374  
**File Name** WindowsMediaInstaller.exe  
**File Type** MSEXE  
**File Category** Executables  
**Current Disposition** Malware  
**Threat Score** High

**First Seen** 2013-12-06 10:57:13 on 10.4.10.183  
**Last Seen** 2013-12-06 18:17:27 on 10.4.10.183  
**Event Count** 7  
**Seen On** 4 hosts  
**Seen On Breakdown** 2 senders → 3 receivers

**Trajectory**

Dec 06, 2013

10.4.10.183  
10.5.11.8  
10.3.4.51  
10.5.60.66

10:57 17:40 18:06 18:10 18:14 18:17

**Events** Transfer Block Create Move Execute Scan Retrospective Quarantine  
**Dispositions** Unknown Malware Clean Custom Unavailable

На примере Cisco AMP for Networks

## Advanced Malware Protection Verdict Updates

Printable (PDF)

**Time Range:** 30 days

15 Feb 2014 00:00 to 17 Mar 2014 13:11 (GMT -08:00) Data in time range: 100.0 % complete

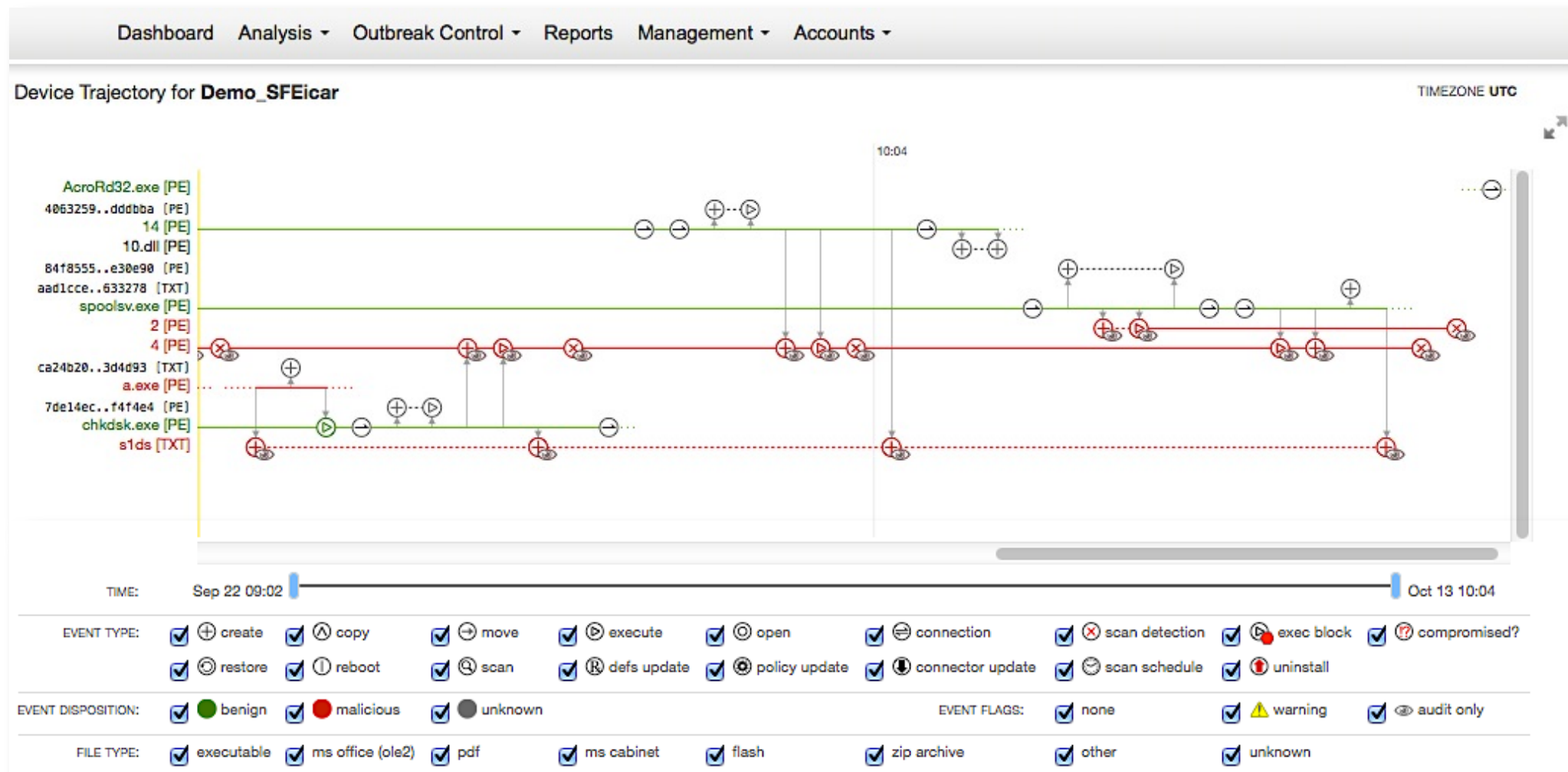
**Files with Retrospective Verdict Changes**

File SHA256	Time of Retrospective Verdict Change	Current Disposition
b6b60eab07393ca00ad10a9180f1...	19 Feb 2014 16:44:39	malicious

Columns... | Export...

На примере Cisco AMP for Content Security (ESA)

# Пример ретроспективы процессов

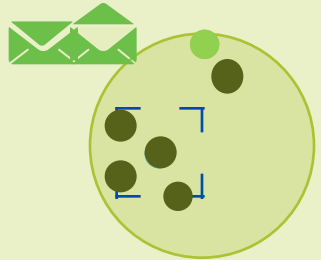


На примере Cisco AMP for Endpoints

# Ретроспективная безопасность основана на...



Поведенческие признаки вторжения используют ретроспективу для мониторинга систем на наличие подозрительной и неожиданной активности



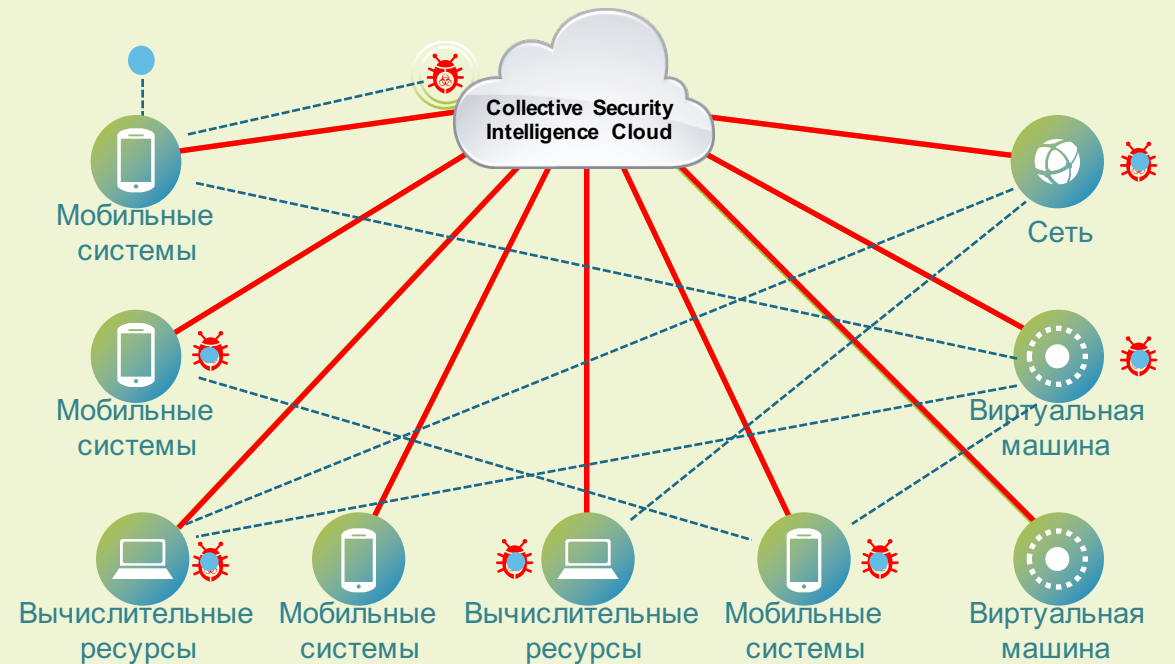
- 1** Известный файл допущен в сеть
- 2** Известный файл копирует себя на несколько машин
- 3** Копирует содержимое с жесткого диска
- 4** Отправляет скопированное содержимое на неизвестный IP-адрес

С помощью связывания в цепочки действий при атаке, Cisco® AMP способен распознать характерные шаблоны поведения для указанного файла и идентифицировать его, не производя поиск по меткам или сигнатурам файлов

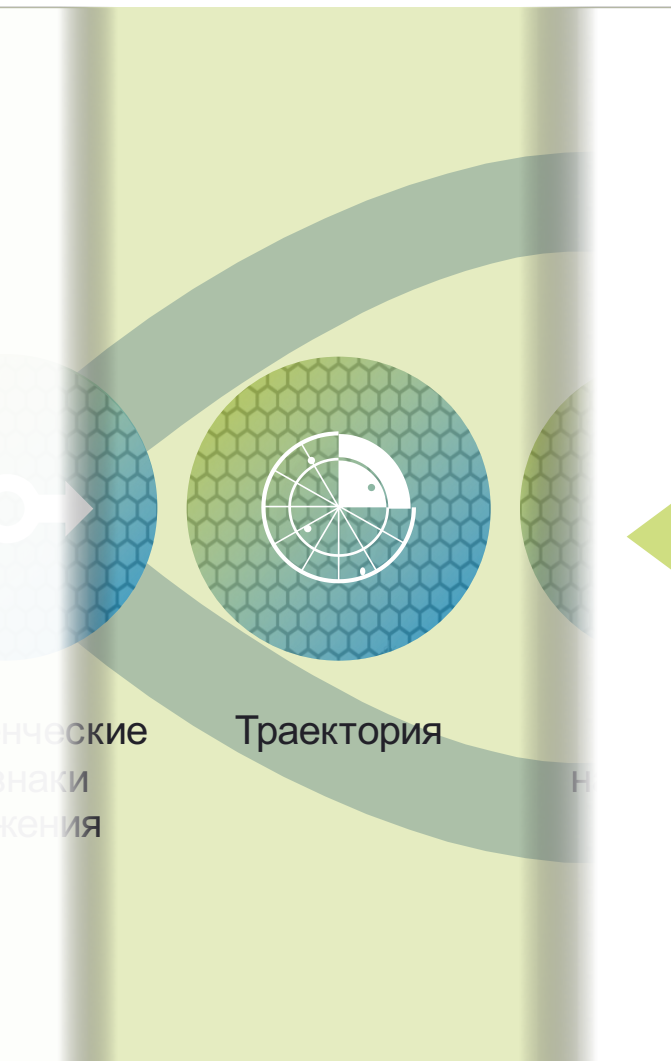
# Ретроспективная безопасность основана на...



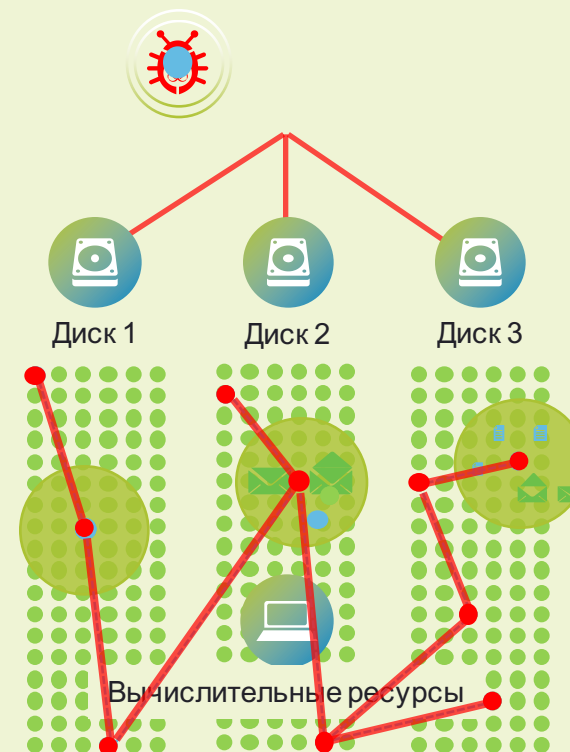
1. Неизвестный файл загружается на устройство
2. Сигнатура записывается и отправляется в облако для анализа
3. Неизвестный файл перемещается по сети на разные устройства  
Траектория файла автоматически записывает время, способ, входную точку, затронутые системы и распространение файла
4. Аналитики в изолированной зоне определяют, что файл вредоносный, и уведомляют все устройства
5. Траектория файла обеспечивает улучшенную наглядность масштаба заражения



# Ретроспективная безопасность основана на...



1. Неизвестный файл загружается на конкретное устройство
2. Файл перемещается на устройстве, выполняя различные операции
3. При этом траектория устройства записывает основную причину, происхождение и действия файлов на машине
4. Эти данные указывают точную причину и масштаб вторжения на устройство



# Что делать в случае обнаружения вредоносного кода?

- Вариант реагирования на обнаруженный вредоносный код зависит от варианта реализации AMP
- AMP for Endpoints
  - Режим аудита – разрешить запускать вредоносный код
  - Пассивный режим – не ждать ответа из облака и запустить вредоносный код (блокировать после)
  - Активный режим – ждать ответа из облака, не запуская файл
- AMP for Content Security
  - Пропустить, заблокировать или поместить в карантин (для ESA)
- AMP for Networks
  - Пропустить, заблокировать или сохранить вредоносный код

# Какие файлы можно анализировать?

- Файлы, передаваемые по сети (HTTP, SMTP, POP3, IMAP, SMB, FTP), можно захватывать и сохранять для дальнейшего анализа

**Edit File Rule** [?] [X]

Application Protocol:  [v]  
Direction of Transfer:  [v]

Action:  [v]  
 Spero Analysis for MSEXE  
 Dynamic Analysis

**Store Files**  
 Malware  
 Unknown  
 Clean  
 Custom

**File Type Categories**

<input type="checkbox"/> Office Documents	15
<input type="checkbox"/> Archive	17
<input type="checkbox"/> Multimedia	2
<input type="checkbox"/> Executables	5
<input type="checkbox"/> PDF files	1
<input type="checkbox"/> Encoded	0
<input type="checkbox"/> Graphics	0
<input type="checkbox"/> System files	0
<input type="checkbox"/> Dynamic Analysis Capable	1

**File Types**

- 7Z (7-Zip compressed file)
- ACCDB (Microsoft Access 2007 file)
- ARJ (Compressed archive file)
- BINARY\_DATA (Universal Binary/Ja
- BINHEX (Macintosh BinHex 4 Comp
- BZ (bzip2 compressed archive)
- CPIO\_CRC (Archive created with th
- CPIO\_NEWC (Archive created with
- CPIO\_ODC (Archive created with th

**Selected File Categories and Types**

# Обнаружение известного вредоносного кода

Context Explorer	Connections	Intrusions	Files ▶ Malware Events	Hosts	Users	Vulnerabilities	Correlation	Custom
↓			Bocinex.exe	4c136a95...271b4828		MSEXE	2	
↓			W32.Trojan.Breach.VRT skunk-straddling.pdf	f02e1bb1...3b483a04		PDF	1	
↓			W32.Trojan.Breach.VRT repair-cadets.pdf	f02e1bb1...3b483a04		PDF	1	
↓			W32.Trojan.Breach.VRT ankles-bushiest.pdf	f02e1bb1...3b483a04		PDF	1	
↓			W32.Spy:Malwaregen.17db.1201 Weelsof.exe	e32ecc71...881078ce		MSEXE	1	
↓			W32.Spy:Malwaregen.17db.1201 IRCBot.exe	e32ecc71...881078ce		MSEXE	1	
↓			W32.Spy:Malwaregen.17db.1201 InternetAntivirus.exe	e32ecc71...881078ce		MSEXE	1	
↓			W32.Spy:Malwaregen.17db.1201 Dofail.exe	e32ecc71...881078ce		MSEXE	1	
↓			W32.Banker:Spy.16hi.1201 Korgo.exe	b73b0e49...b67c4049		MSEXE	1	
↓			W32.Banker:Spy.16hi.1201 Hacker_Defender.exe	b73b0e49...b67c4049		MSEXE	1	
↓			W32.8BBFF65DB8-100.SBX.VIOC Helompy.exe	8bbff65d...75dc60d6		MSEXE	1	
↓			W32.8BBFF65DB8-100.SBX.VIOC Bofra.exe	8bbff65d...75dc60d6		MSEXE	1	
↓			W32.7FF810938B-100.SBX.VIOC Pramro.exe	7ff81093...293edc5c		MSEXE	1	
↓			W32.7FF810938B-100.SBX.VIOC Oficla.exe	7ff81093...293edc5c		MSEXE	1	
↓			W32.7FF810938B-100.SBX.VIOC Dishiqy.exe	7ff81093...293edc5c		MSEXE	1	
↓			W32.7FF810938B-100.SBX.VIOC Conhook.exe	7ff81093...293edc5c		MSEXE	1	
↓			W32.7AF5A19B73-100.SBX.VIOC Sefnit.exe	7af5a19b...5b44869b		MSEXE	1	
↓			W32.7AF5A19B73-100.SBX.VIOC Sefnit.exe	7af5a19b...5b44869b		MSEXE	1	

# Полная информация о вредоносном коде



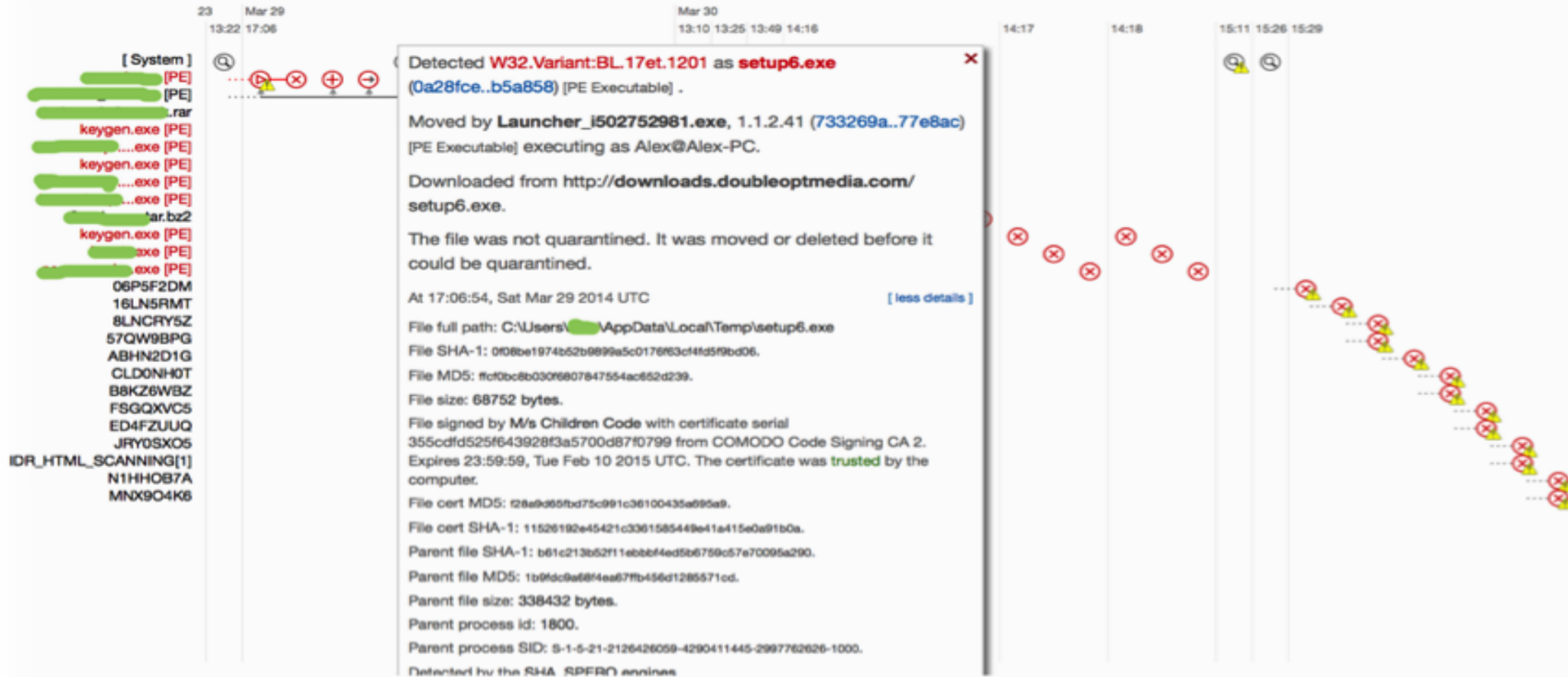
10 installs  
0 detections (7 days)

Support Help Logout

Dashboard Analysis Outbreak Control Reports Management Accounts

## Device Trajectory for Alex-PC

TIMEZONE UTC



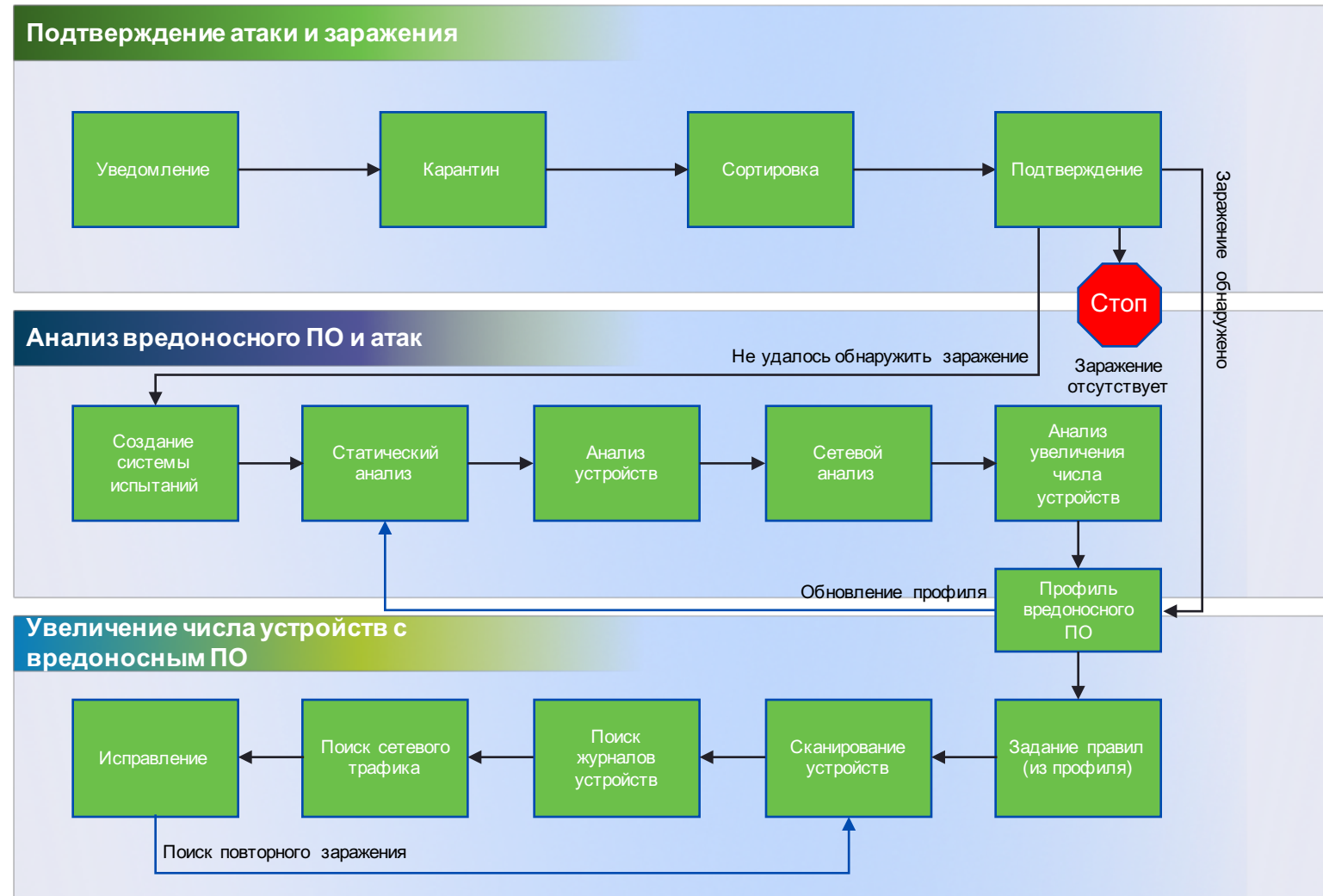
TIME: Feb 23 13:30

May 16 12:15

- EVENT TYPE:  create  copy  move  execute  open  connection  scan detection  exec block  compromised?  
 restore  reboot  scan  defs update  policy update  connector update  scan schedule  uninstall

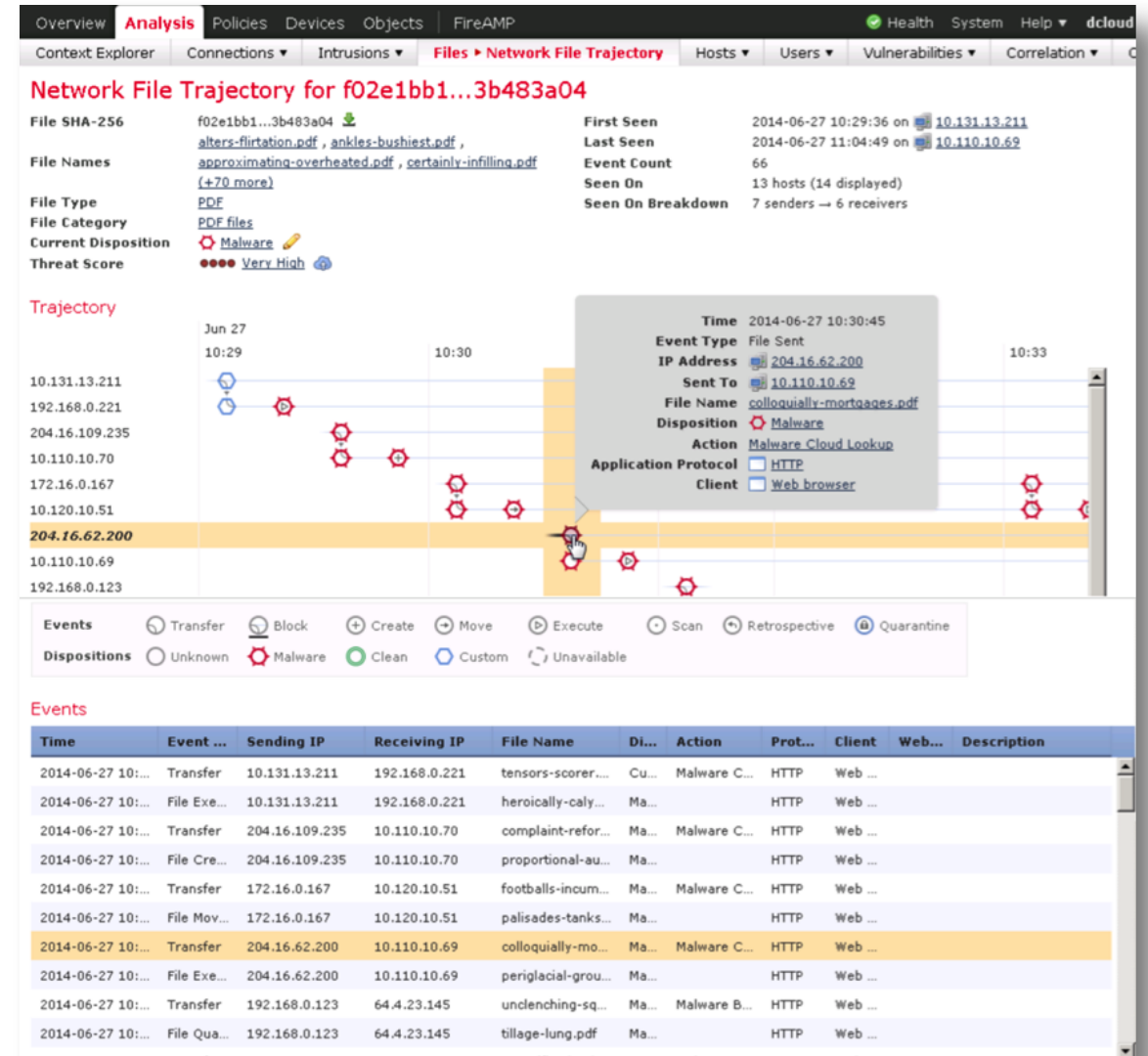
# Вопрос не в том, произойдет ли заражение, а как скоро мы его обнаружим, устраним и поймем причины?

- С чего начать?
- Насколько тяжела ситуация?
- Какие системы были затронуты?
- Что сделала угроза?
- Как можно восстановить?
- Как можно предотвратить ее повторение?



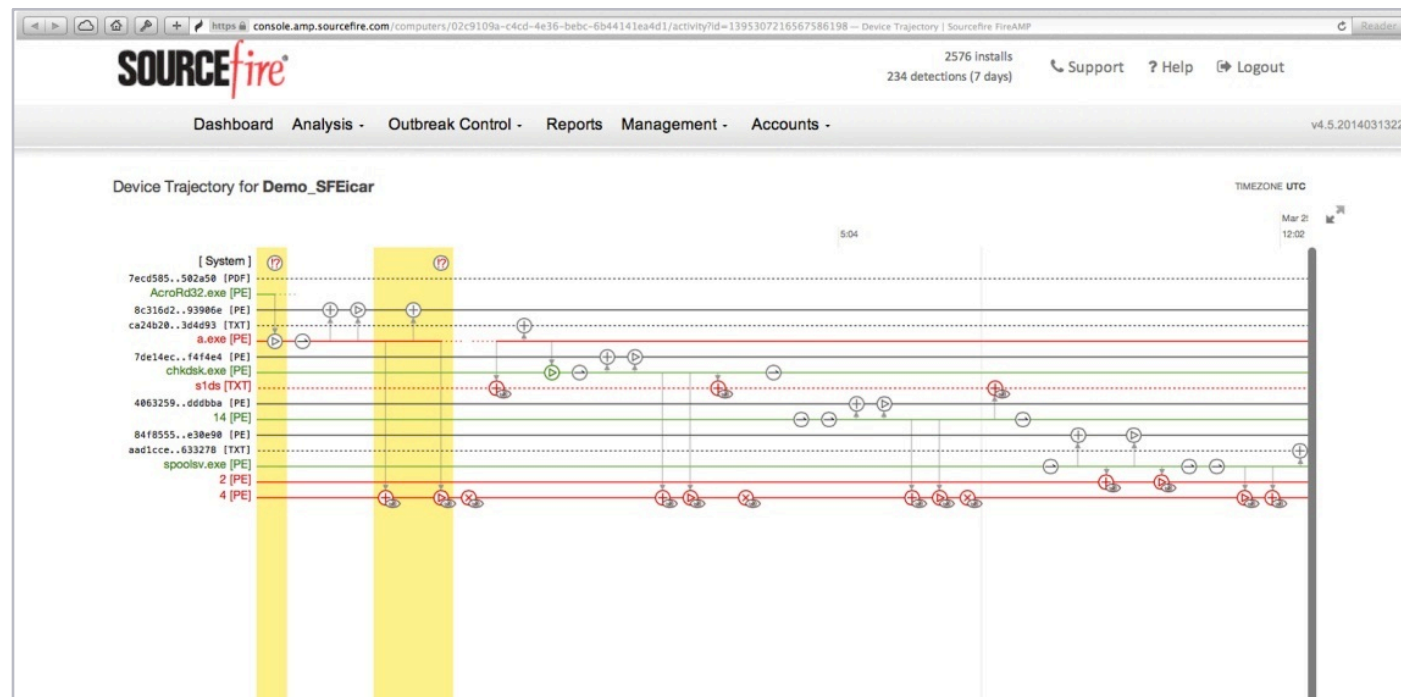
# Ретроспективный анализ файлов позволяет определить

- Какие системы были инфицированы?
- Кто был инфицирован?
- Когда это произошло?
- Какой процесс был отправной точкой?
- Почему это произошло?
- Что еще произошло?



# Ретроспективный анализ процессов позволяет определить

- Как угроза попала на узел?
- Что плохого происходит на моем узле?
- Как угроза взаимодействует с внешними узлами?
- Чего я не знаю на своем узле?
- Какова последовательность событий?



# Трекинг каждого вредоносного файла

## Web Tracking

**Search**

**Proxy Services** | **L4 Traffic Monitor** | **SOCKS Proxy**

Available: 22 Oct 2013 13:44 to 13 Feb 2014 15:10 (GMT +01:00)

Time Range:

User/Client IPv4 or IPv6:  (e.g. jdoe, DO, 10.1.1.0, or 2001:420:80:1::5)

Website:  (e.g. google.com)

Transaction Type:

▶ **Advanced** *Current Criteria: File SHA256: 53de8225fc823c6efc8ad33a3a741fbe4c56b041ef51e4d70605d8e3143d024d.*

**Clear**

SHA-256

Пользователи и IP, которые загрузили вредоносный файл к себе

Generated: 18 Feb 2014 11:02 (GMT +01:00)

**Results**

Displaying 1 - 3 of 3 items.

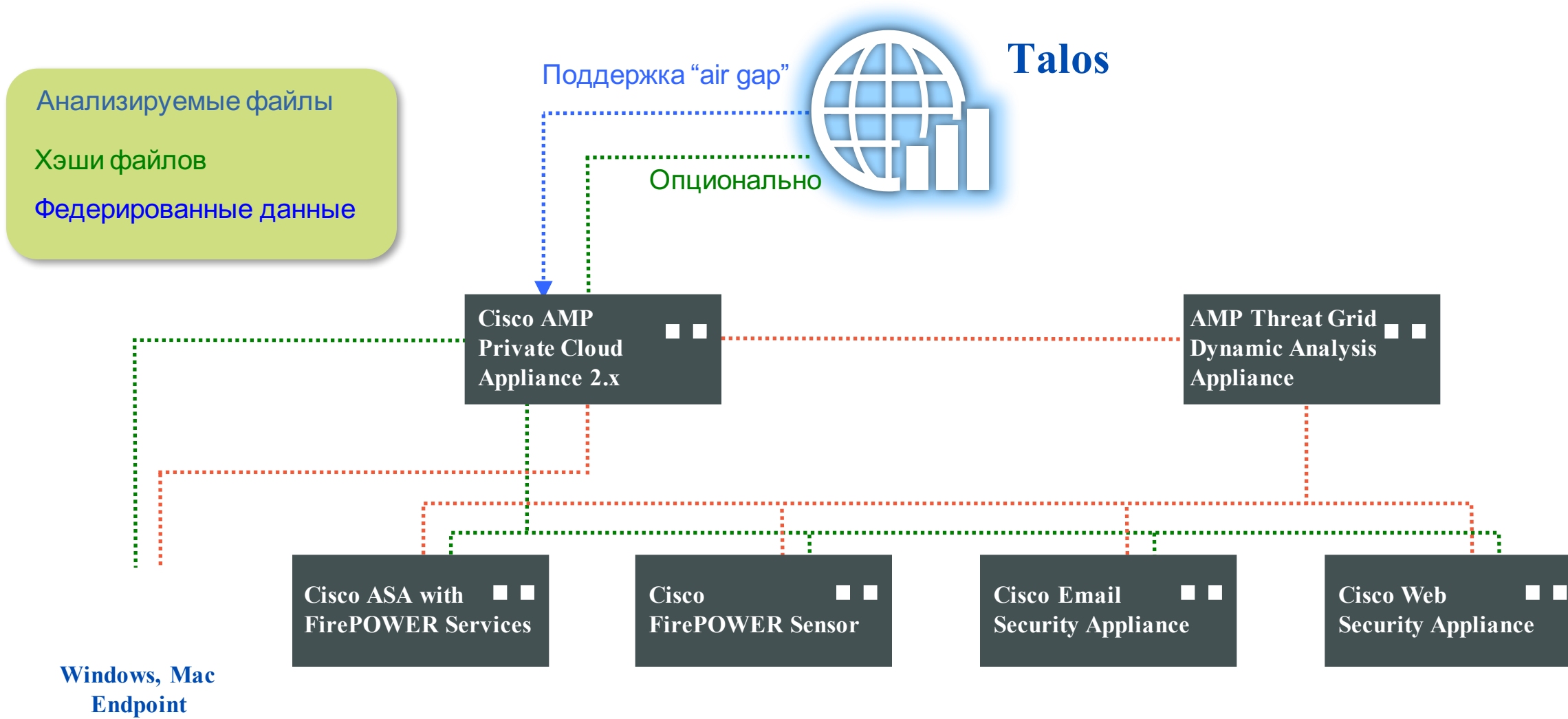
Time (GMT +01:00) ▼	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
11 Feb 2014 14:49:59	<a href="http://batcoroadlinescorporation.com">http://batcoroadlinescorporation.com</a>		Allow	116.7KB	sales fd00:1:2:3::1
11 Feb 2014 14:32:44	<a href="http://batcoroadlinescorporation.com">http://batcoroadlinescorporation.com</a>		Allow	116.7KB	sales fd00:1:2:3::1
11 Feb 2014 14:25:41	<a href="http://vistatech.us">http://vistatech.us</a>		Allow	116.5KB	sales fd00:1:2:3::1

Displaying 1 - 3 of 3 items.



# Вопросы конфиденциальности

# AMP Private Cloud 2.0



# А можно анализировать вручную?

- Нередко бывает необходимость анализировать файлы, попавшие в службу безопасности на USB-носителях или иных носителях, а также проводить более глубокий анализ обнаруженных с помощью Cisco AMP вредоносных программ
- Не у всех бывает реализована автоматическая защита с помощью Cisco AMP
- Организация может захотеть создать собственную службу Threat Intelligence или Security Operations Center

**ThreatGRID** Submit Samples Search Threat Intel Help Welcome pwood

Metadata Behavioral Indicators Network Activity Processes Artifacts Registry Activity File Activity Video Download

### Analysis Report

<b>ID</b>	c1005e42bc57bbe2f590a0028bbd9f40	<b>Filename</b>	LATEST_ZeuS.exe
<b>OS</b>	2600.xpsp.080413-2111	<b>Magic Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>Started</b>	10/3/14 01:56:13	<b>Analyzed As</b>	exe
<b>Ended</b>	10/3/14 02:02:25	<b>SHA256</b>	f1b14e419865272b35a573921cbbd4d646a47b89b439170bac4881f9266ab71
<b>Duration</b>	0:06:12	<b>SHA1</b>	9ad141de379e20072d6f81eb7e49f2de0bd0f69a
<b>Sandbox</b>	ulcer (pilot-d)	<b>MD5</b>	f4c827a3f9c5dfc8492db47122668f66
		<b>Tags</b>	

**Warnings**

- Executable Failed Integrity Check

### Behavioral Indicators

Threat Score: 100

Possible ZeuS Variant Detected	Severity: 100 Confidence: 100
Process Modified an Executable File	Severity: 95 Confidence: 95
Process Modified Autorun Registry Key Value	Severity: 80 Confidence: 60
Outbound HTTP GET Request	Severity: 75 Confidence: 75
Process Modified File in a User Directory	Severity: 70 Confidence: 80
Potential Sandbox Detection - Enumeration of ProductID	Severity: 60 Confidence: 70
Process Created an Executable in a User Directory	Severity: 60 Confidence: 95
Command Exe File Execution Detected	Severity: 50 Confidence: 80
Potential Code Injection Detected	Severity: 50 Confidence: 50
Possible Fast Flux Domain Detected [Beta]	Severity: 35 Confidence: 20
Executable with Encrypted Sections	Severity: 30 Confidence: 90

# Cisco AMP Threat Grid

- Платформа для глубокого анализа вредоносного кода
  - Доступ через портал, выделенное устройство или с помощью API
- Может применяться при построении собственных систем Threat Intelligence или SOC
- Уже используется многими компаниями при проведении расследований – EnCase, Maltego и т.п.



# Детальный анализ вредоносного ПО в AMP Threat Grid

## Behavioral Indicators

- Process Modified an Executable File
  - Process Created a File in the Windows Startup Folder
- A new file was added to the Windows StartUp folder to ensure that Please review the 'Disk Artifacts' section in order to view additional

Process ID	Process Name
1100 (15e65a21af32dd3b5fe65da4807be21e.exe)	15e65a21

- Process Modified File in a User Directory
- Process Disabled Internet Explorer Proxy
- Process Created an Executable in a User Directory
- Potential Code Injection Detected
- Dynamic DNS Domain Detected
- PE Has Sections Marked Executable and Writable
- Possible Fast Flux Domain Detected [Beta]
- Outbound HTTP
- PE COFF Header
- PE Optional Header
- PE DOS Header
- PE COFF Header

## DNS Traffic

Query Type: A, Query Data: alexrpi.tk  
 TTL: -  
 Query ID: 28943  
 Timestamp: +101.195

### Answers

Query ID
28943
28943

### Nameserver Records

Data  
 b  
 c  
 a.ns  
 d

## HTTP Traffic

- POST http://alexrpi.tk:80/solar/ Server IP: 195.20.34.1 Server Port
- POST http://alexrpi.tk:80/solar/ Server IP: 195.20.34.1 Server Port
- POST http://alexrpi.tk:80/solar/ Server IP: 195.20.34.1 Server Port
- POST http://alexrpi.tk:80/solar/ Server IP: 195.20.34.1 Server Port

## TCP/IP S

## Registry Activity

### Created Keys

Created Key	PID	Access List	Option List
USER\S-1-5-21-1202660629-583907252-1801674531-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\IP3P\History	1148 (Explorer.EXE)	ENUMERATE_SUB_KEYS, CREATE_SUB_KEY	REG_OPTION_NON_VOLATILE

### Modified Keys

### Deleted Key Values

## Filesystem Activity

Files Created: 3 Files Read: 17 Files Modified: 5 Files Deleted: 0

Path	PID	Action
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\8HMRBCBR\solar[1].htm	1148 (Explorer.EXE)	Created
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\MRMBYDAX\solar[1].htm	1148 (Explorer.EXE)	Created
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\lsass.exe	1100 (15e65a21af32dd3b5fe65da4807be21e.exe)	Created
VAUTOEXEC.BAT	1148 (Explorer.EXE)	Read
I\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\8HMRBCBR	1148 (Explorer.EXE)	Modified

## Processes

- Name: 15e65a21af32dd3b5fe65da4807be21e.exe  
 PID: 1100 Children: 1 File Actions: 3 Registry Actions: 2 Analysis Reason: Is target sample.
- Name: lsass.exe  
 PID: 1600 Children: 0 File Actions: 3 Registry Actions: 0 Analysis Reason: Parent is being analyzed  
 Process Name: lsass.exe  
 Image Filename: C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\lsass.exe  
 Analysis Reason: Parent is being analyzed  
 Command Line: "C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\lsass.exe"  
 Children New: true  
 Started At: Tue Sep 30 2014 13:41:00 UTC  
 Current Directory: C:\temp\  
 Image Base Address: C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\lsass.exe  
 Window Title: WinSta0\Default  
 Shell Info: WinSta0\Default  
 Desktop Info: WinSta0\Default

### Artifacts

ID	Relation to Process	Path
...	Created from process	C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\lsass.exe

Process Graph

# Типовые сценарии использования AMP Threat Grid

- Доступ к порталу
  - Зависит от числа аналитиков и ежедневно загружаемых образцов вредоносного кода
  - Приватная маркировка загружаемых семплов (опционально)
  - Устройство Threat Grid (опционально) позволяет загружать образцы на него, без загрузки в облако
- Интеграция с решениями Cisco
  - AMP for Endpoints
  - AMP for Networks (FP / ASA)
  - AMP for WSA / CWS
  - AMP for ESA / CES
- API для автоматизации передачи образцов в Threat Grid включен во все лицензии с подпиской

# Вариант развёртывания внутри сети, без прямого доступа в Интернет

- Локальный анализ вредоносного ПО с полной поддержкой облака Cisco® AMP Threat Grid
- В целях соблюдения нормативных требований все данные остаются на территории заказчика
- Непрерывный однонаправленный поток данных из облака Cisco AMP Threat Grid для актуализации контекста
- Ощущения пользователя не меняются при переходе от облака к устройству (UI, API, ....)
- TG5000:
  - Анализ до 1500 образцов в день
  - Cisco UCS C220 M3 Chasis (1U)
  - 6 x 1TB SAS HDD (аппаратный RAID)
- TG5500:
  - Анализ до 5000 образцов в день
  - Cisco UCS C220 M3 Chasis (1U)
  - 6 x 1TB SAS HDD (аппаратный RAID)



# Отличия портала от локального устройства AMP Threat Grid

- Масштабируемость
  - Отсутствуют ограничения на число загружаемых для анализа образцов (в устройстве – до 5000 в день)
- Скорость обработки образцов
  - Обработка 1000 образцов занимает около 30 минут. На устройстве такое же количество обрабатывается за 4 часа
- Стоимость
  - Устройство стоит дороже доступа к portalу
- Анализ угроз
  - Сопоставление угроз в облаке осуществляется со всеми образцами, загруженными в него и помеченными как публичные. На устройстве сопоставление осуществляется только с локальными образцами
- Обновления для поведенческих индикаторов
  - Обновления для устройства выпускаются каждый квартал, а для портала – каждые 2 недели

# Преимущества и недостатки локального устройства

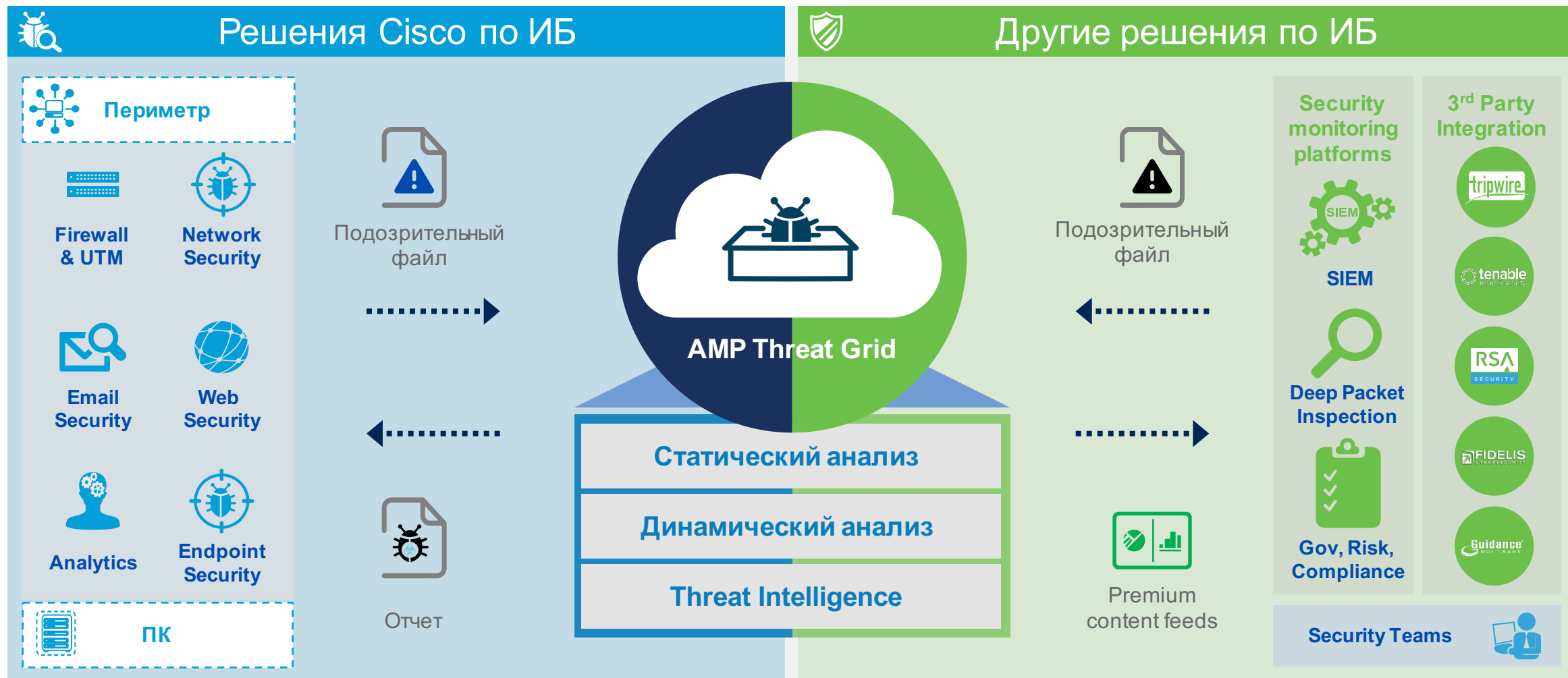
## Преимущества

- Конфиденциальность данных
- Возможность работы в изолированной сети
- Независимость от наличия Интернет-канала

## Недостатки

- Обновления поведенческих индикаторов приходят с задержкой
- Невозможность полного анализа Интернет-активности вредоносного ПО
- Невозможность сопоставления данных с другими публичными семплами

# Повсеместный AMP Threat Grid



# Cisco Advanced Malware Protection

## Gartner Endpoint Detection and Response (EDR)

- Обнаружение инцидентов безопасности.  
С помощью мониторинга активности хостов и объектов, нарушения политик или же с помощью набора внешних индикаторов компрометации
- Сдерживание инцидента на хосте  
Блокирование сетевого трафика или же выполнения файла. Удаленно контролируется
- Расследование инцидентов безопасности  
Функция расследования должна включать исторические данные всех основных событий на хосте для того, чтобы определить как технические изменения (активности файлов, реестра, сети, драйверов) и их влияние на бизнес (обход, эскалация привилегий, распространение, эксфильтрация, геолокация, подключение к СпС и подозрительное авторство)
- Восстановление узла до первоначального состояния  
В идеале решение должно удалять вредоносные файлы, делать откат к предыдущему состоянию и восстанавливать другие изменения. Решение должно создавать инструкции по предотвращению, должно быть доступно для других инструментов, особенно для организаций, которые имеют разделение обязанностей и жесткие процедуры контроля изменений  
В реальности проще всего восстановить систему из предыдущего snapshot, или же полностью реинициализировать систему и восстановить данные из резервной копии. Это может оказаться менее затратно по времени по сравнению с детальным анализом состояния и восстановлением изменений

Thank you.

