# Методы современных киберпреступников

## И защита от них

Pavel Rodionov

CSE Security, Cisco EMEAR

*30 сентября 2016*

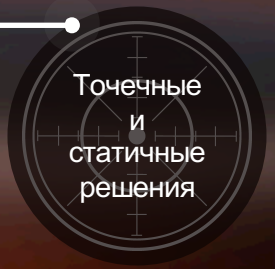
# Думать как хакер

- Высокая мотивация киберкриминала
- Изменение бизнес-моделей
- Динамичность ландшафта угроз

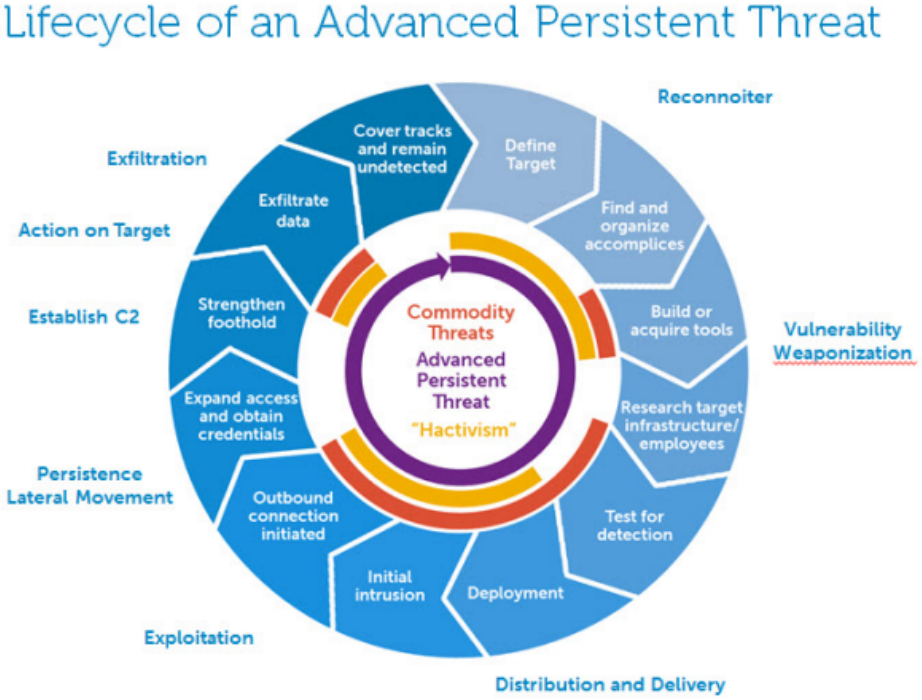
Фрагментация

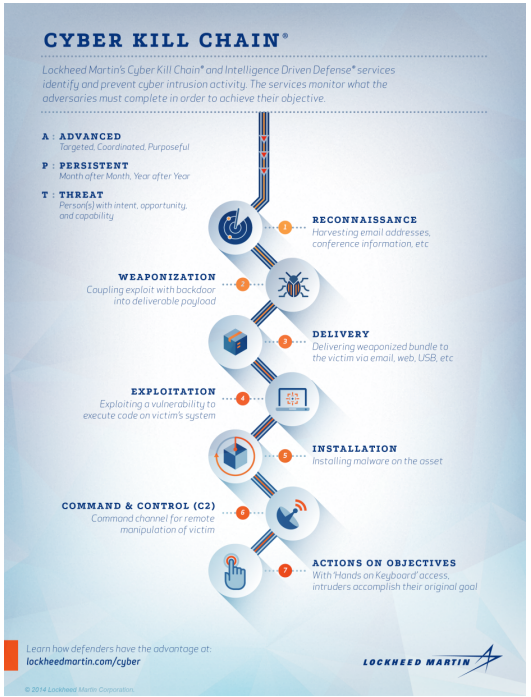
Сложность

Требуют лишнего управления



# Что такое убийственная цепочка?



# Из чего состоит убийственная цепочка?

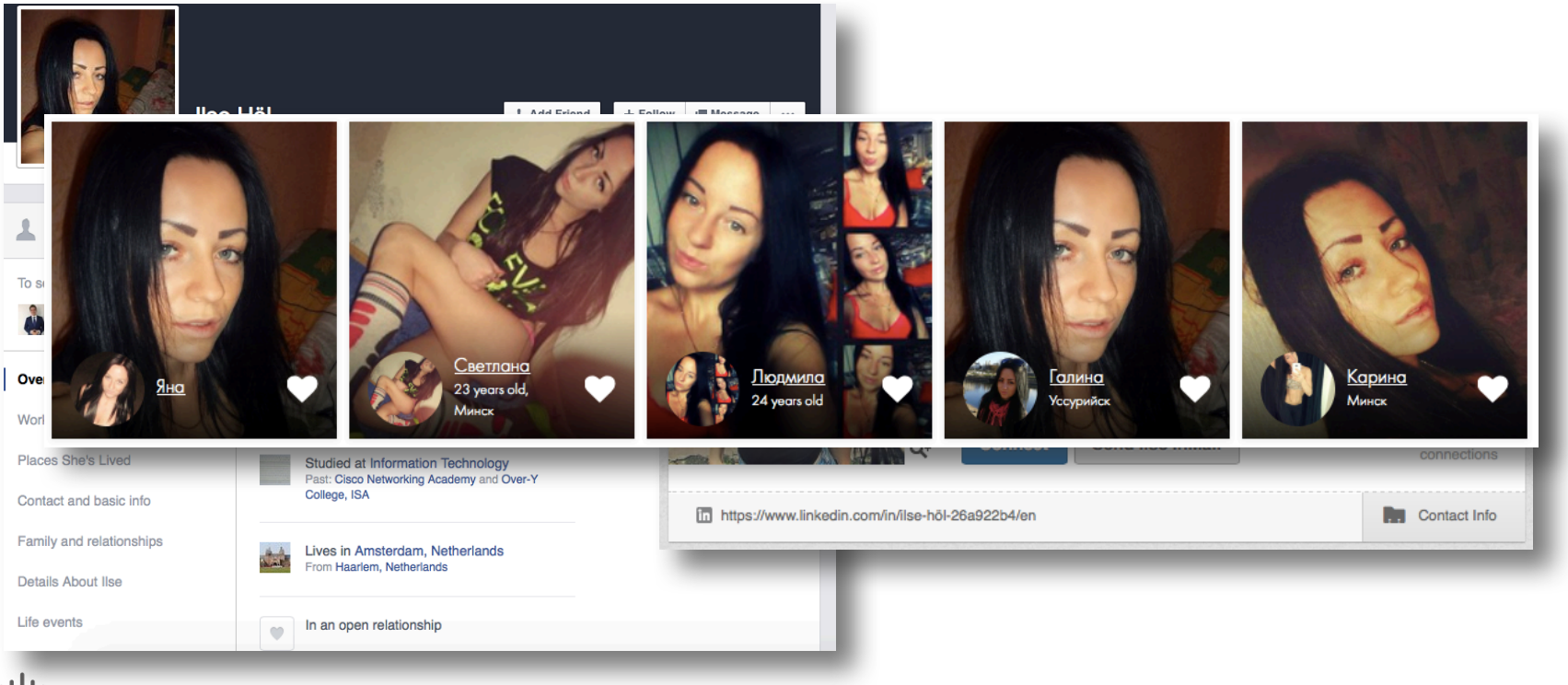
# Как хакер проводит разведку вашей сети?



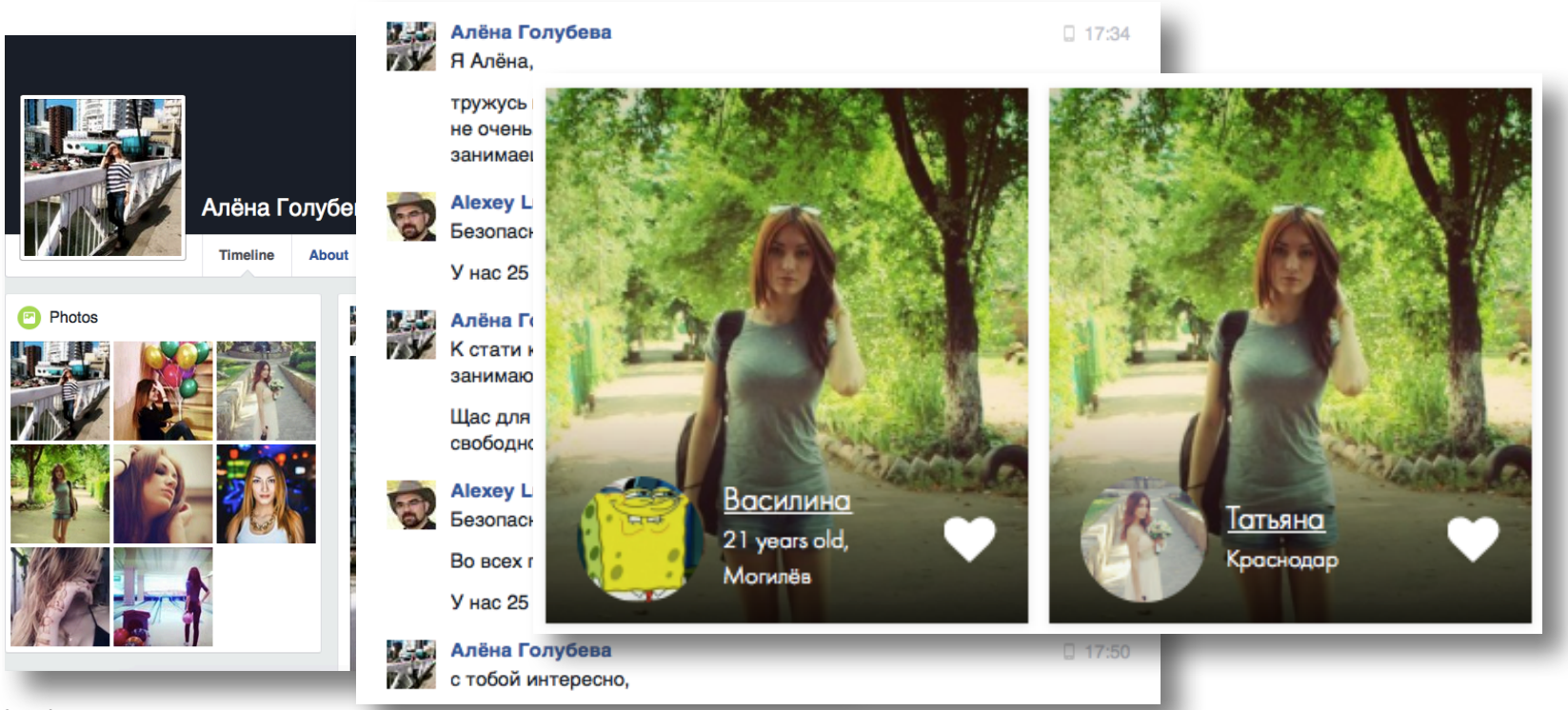




# Красивая приманка



# Не только через почту, но и через соцсети



# Взлом любой компании за час

## Security Day компании CTI

Руководитель направления ИБ CTI начал выступление с того, что что предложил любому участнику семинара "взломать" его компанию за время проведения мероприятия. Тому, кто не побоится назвать имя своей компании для проведения теста на проникновения, был предложен приз в виде бутылки хорошего виски. Что характерно, нашлась только одна компания, представитель которой не побоялся предложить себя в качестве подопытного кролика. Для чистоты эксперимента было названо только имя компании (по понятным причинам я его называть не буду) и специалисты CTI приступили к работе.

# Взлом любой компании за час

## Security Day компании CTI

- Спустя всего час с небольшим они вышли с участниками на связь по Cisco Webex и продемонстрировали первые результаты:
  - в Интернет была найдена информация о компании и отдельных ее сотрудниках
  - сотрудники CTI связались с сотрудницей компании, представившись потенциальным клиентом
  - сотруднице прислали запароленный архив с документами якобы для анализа и последующего заключения договора
  - в архиве находились не самые свежие (4-5-тидневной выдержки) malware, на которые ругнулся антивирус ESET Nod32
  - "клиент" пообещал прислать новый "небитый" файл, что и сделал спустя несколько минут, запаковав за это время malware так, чтобы Nod32 ее не распознал
  - сотрудница компании-жертвы запустила файл, который и заразил ее компьютер
  - часть случайно собранных на жестком диске файлов была слита на Яндекс.Диск в качестве демонстрации.

# Примеры последних атак

25 апреля в 18:45

## Разное → Киберпреступники пытались совершить крупнейшее ограбление банка

Блог компании ESET NOD32

Известная оборонная компания Великобритании BAE Systems, которая занимается перспективным военными разработками, аэрокосмической индустрией, а также информационной безопасностью, обнародовало результаты анализа крупной кибератаки на банк в Бангладеш, в результате которой злоумышленникам удалось скомпрометировать известную международную банковскую платформу SWIFT и похитить $81 млн.

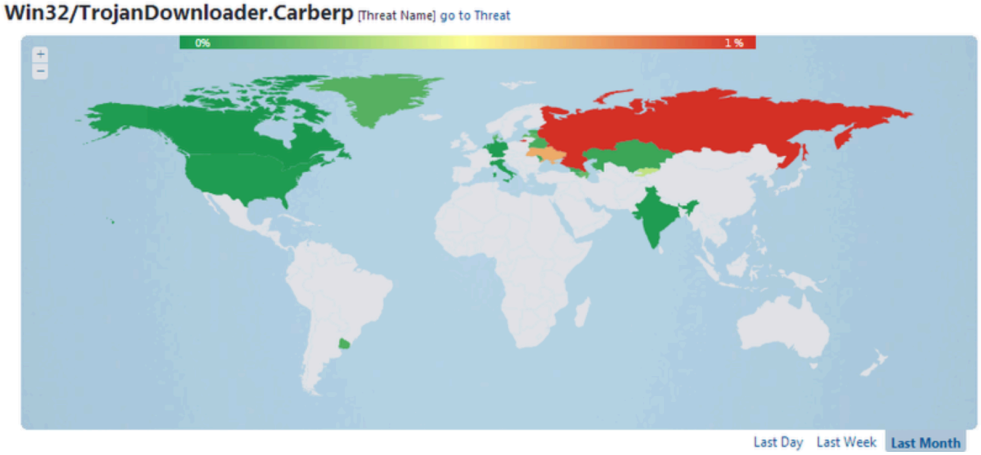

(*картинка Reuters*)

## Carberp: бесконечная история

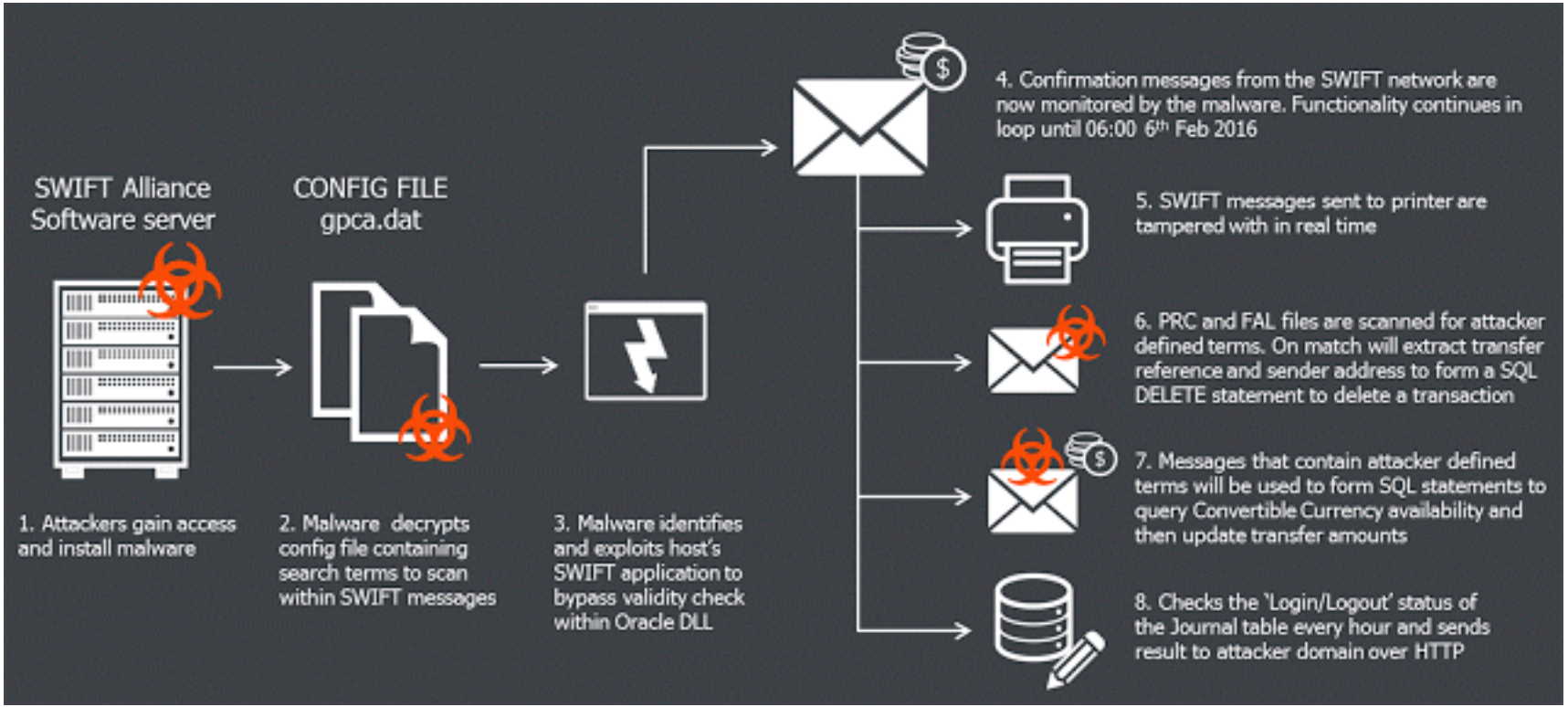
Информационная безопасность*, Блог компании ESET NOD32

Киберпреступная группа Carberp была одной из первых групп, которые массивно использовали семейство вредоносных программ, нацеленных на компрометацию систем удаленного банковского обслуживания и проведение мошеннических операций против крупнейших банков России. Многие члены основной группы Carberp уже были арестованы, но это семейство вредоносных программ по-прежнему активно и продолжает развиваться. Наш коллега Александр Матросов произвел анализ последней модификации банковского троя Carberp, который мы хотим представить ниже.

На скриншоте представлена статистика ESET Virus Radar, которая показывает регионы, наиболее пострадавшие от инфекции Carberp в течение последнего месяца.



# Атака на SWIFT

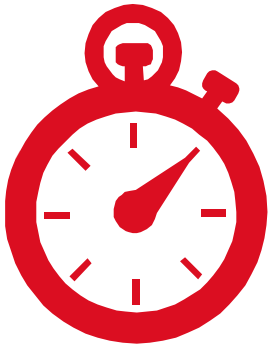



http://baesystemsai.blogspot.ru/2016/04/two-bytes-to-951m.html

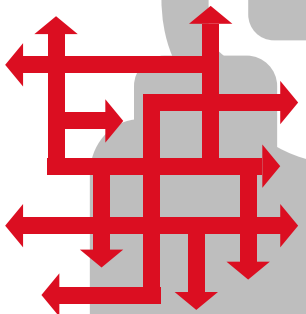
# Транспортная система Сан-Франциско

# Изменение в поведении атак

**Скорость**

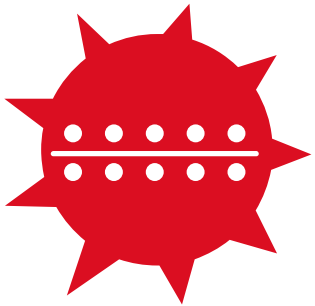


**Ловкость**



**Адаптация**

**Уничтожение**



Инновации, использование старых приемов на новый лад
и обход защитных механизмов

# Теневая инфраструктура устойчива и скрытна

Разработаны для уклонения, восстановления и контроля работоспособности


**15000**

Уникальных сайтов, перенаправляющих на Angler

**99,8%**

из них использовались менее 10 раз

Document1 [Compatibility Mode] - Word

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW

Sign in

Paste Cut Copy Format Painter

Clipboard

Calibri (Body) 11

Font

Paragraph

Normal No Spac... Heading 1 Title Subtitle Subtle Em... Emphasis Intense E... Strong

Styles

Find Replace Select

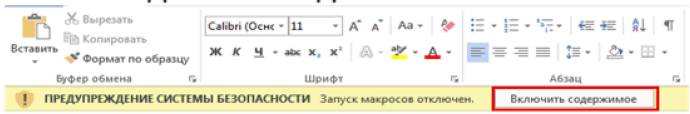
Editing

MISSING PROOFING TOOLS This document contains text in Polish which isn't being proofed. You may be able to get proofing tools for this language. Download Never Show Again

Microsoft® Office™

ДОКУМЕНТ СОЗДАН В НОВОЙ ВЕРСИИ MICROSOFT OFFICE

ВКЛЮЧИТЕ СОДЕРЖИМОЕ ДЛЯ ОТОБРАЖЕНИЯ КОНТЕНТА



# Rombertik

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

## Анти-анализ

### Получение доступа

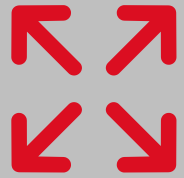
- Спам
- Фишинг
- Социальный инжиниринг

## Стойкость

### Уход от обнаружения

- Записать случайные данные в память 960 миллионов раз
- Засорение памяти в песочнице

## Вредоносное поведение



### Украсть данные пользователя

- Доставка данных пользователя обратно злоумышленникам
- Кража любых данных, а не только банковских

### Уничтожение если обнаружено

- Уничтожение MBR
- После перезагрузки компьютер перестает работать

# 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.

# Эволюция вариантов вымогателей

Стечение обстоятельств – легкое и эффективное шифрование, популярность эксплойт-китов и фишинга, а также готовность жертв платить выкуп шантажистам

# Инновации программ-вымогателей

Индивидуальное шифрование для каждой цели

Использование биткойнов для анонимных платежей

Маркировка уже зашифрованных систем

Установка крайних сроков:
1. Для увеличения выкупа
2. Для удаления ключа шифрования

# Программы-вымогатели второго поколения

## Самораспространение

- Использование уязвимостей в широко распространенных продуктах
- Репликация на все доступные накопители
- Заражение файлов
- Базовые функции для атак методом подбора
- Устойчивость управления и контроля, в т.ч. полное отсутствие инфраструктуры контроля и управления
- Использование уже имеющегося в системе ВПО

## Модульность

- Распространение через файлы автозапуска и USB-накопители большой емкости
- Эксплойты в инфраструктуре аутентификации
- Сложные системы управления, контроля и отчетности
- Ограничители потребления системных ресурсов
- Фильтрация целевых адресов для заражения (RFC 1918)

# Прямые атаки формируют большие доходы

## Более эффективны и более прибыльны

**147** серверов в месяц, перенаправляющих трафик

**90K** целей на сервер в день

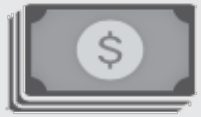
**10%** обслуженных запросов от эксплойтов

**40%** скомпрометировано

**62%** доставленных программ-вымогателей

**2,9%** уплаченных выкупов

X



**$300** средняя сумма выкупа

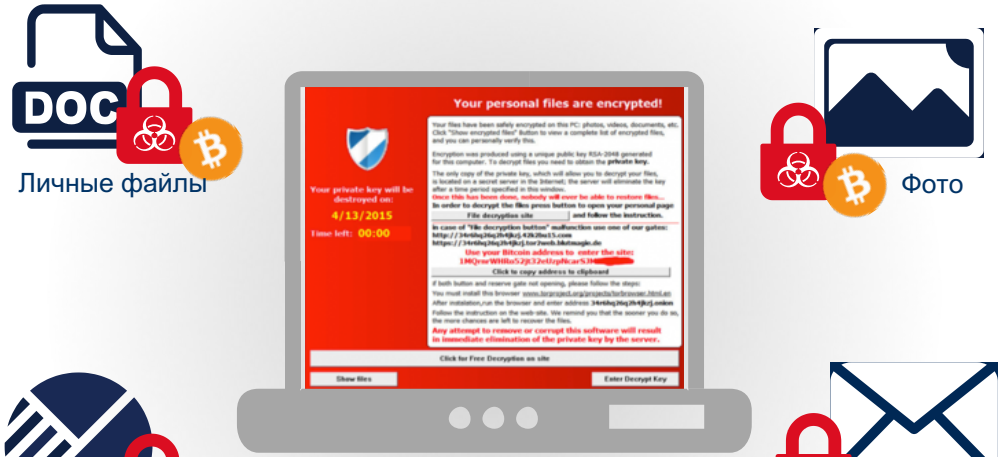
=

**$34M** годовой валовой доход от программ-вымогателей на кампанию

Выкуп платят 9515 пользователей в месяц

# Эволюция вымогателей: Цель – данные, а не системы

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




TOR

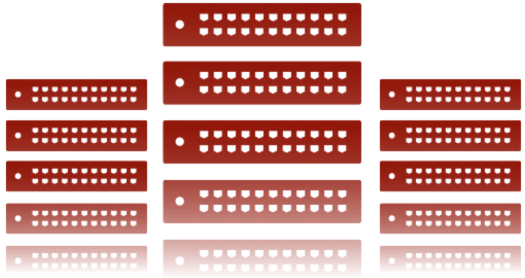
Вымогатели теперь полностью автоматизированы и работают через анонимные сети

$300-$500

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

# Инфраструктура: создание цифровой экономики на базе уязвимой инфраструктуры

Слабая, уязвимая инфраструктура не сможет стать надежной опорой для экономики следующего поколения.



Устройства работают
с известными уязвимостями
в среднем

**5 лет**

И эта проблема носит системный характер

Cisco

**5,64**

лет

Apache/
OpenSSH

**5,05**

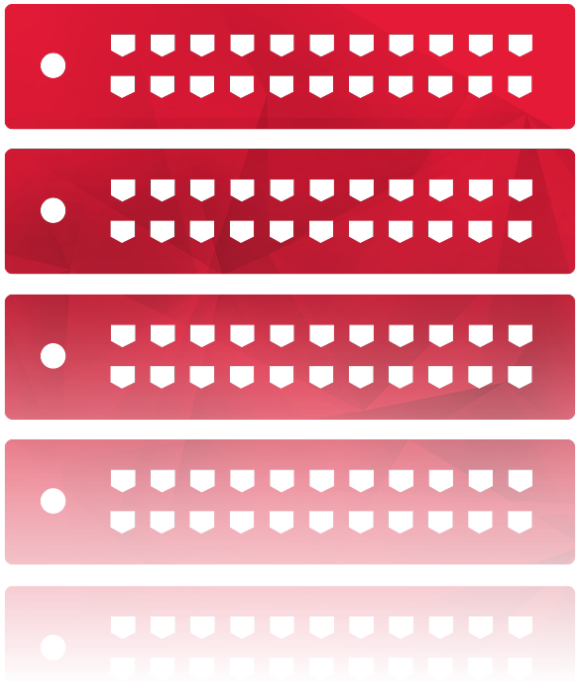
лет

# Надежность порождает самоуверенность

**92%** устройств, доступных через Интернет, содержали известные уязвимости (в среднем 26 на устройство)

**31%** устройств, доступных через Интернет, были сняты с поддержки

**5%** устройств, доступных через Интернет, находились за пределами своего жизненного цикла



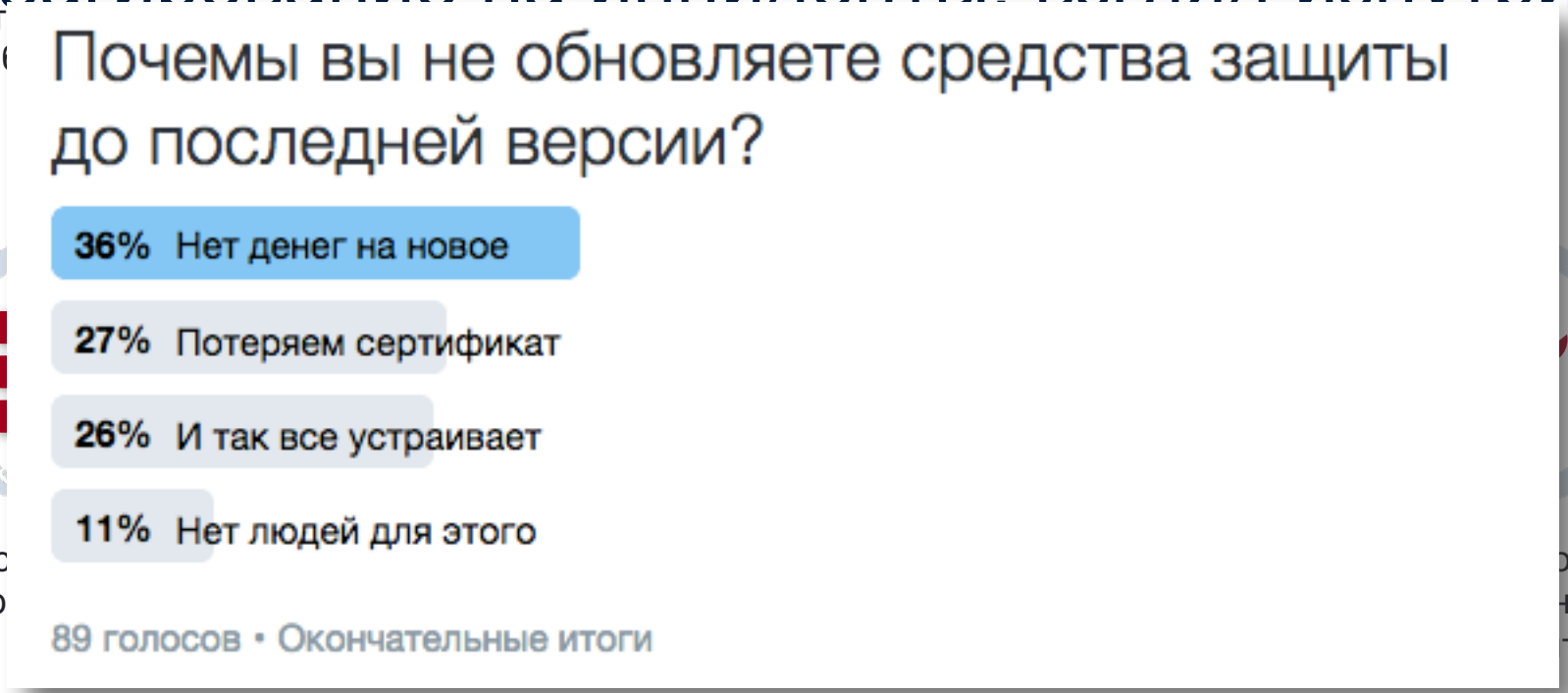
# Кто забывает обновлять инфраструктуру?

# Реагирование на инциденты: взгляд изнутри

Уст
по

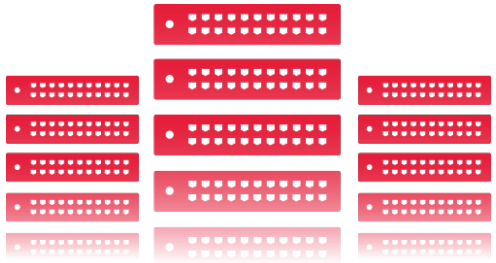
Ус
инф

ован
ных
тов



# DNS: слепая зона для безопасности

Популярный протокол, который используют злоумышленники для управления, утечки данных и перенаправления трафика



91,3%

Вредоносного ПО использует DNS

68%

Организаций **не** мониторят его

# Что еще было выявлено?

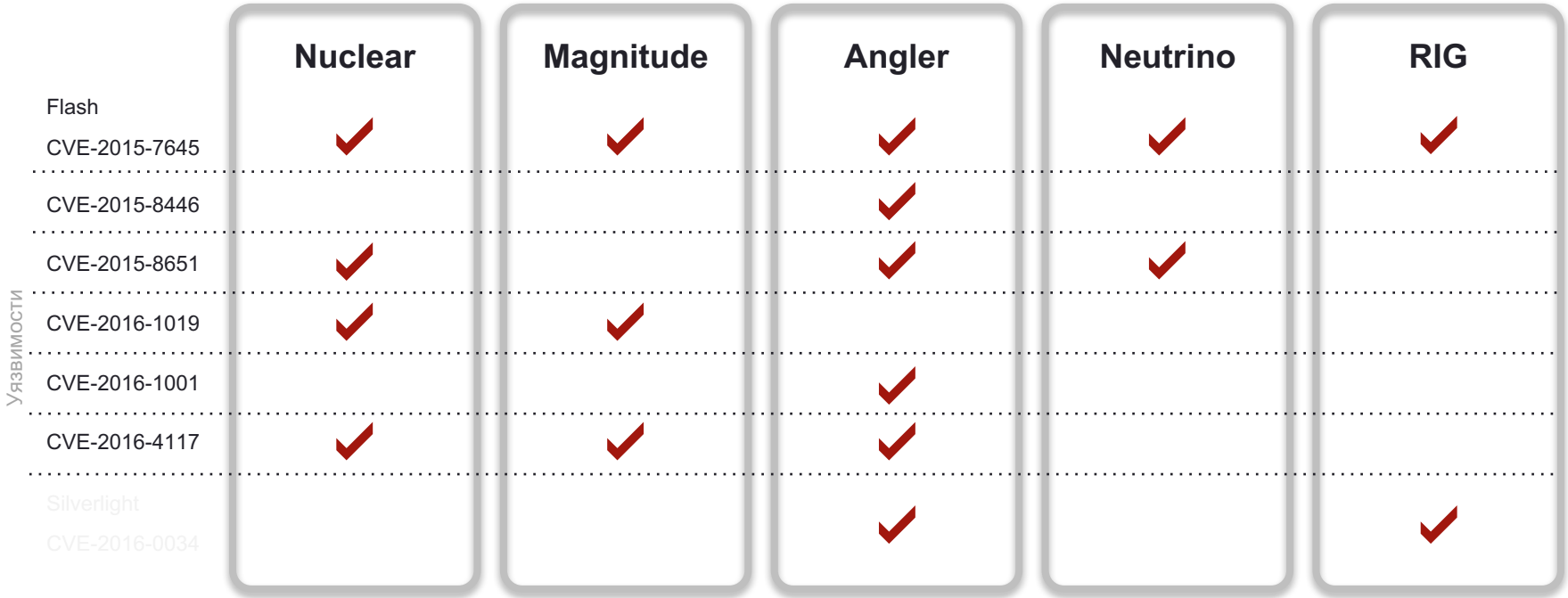
- Адресное пространство заказчика входит в блок-списки третьих сторон по спаму и вредоносному ПО
- Адресное пространство заказчиков маркировано для известных серверов внешнего управления Zeus и Palevo
- Активные кампании вредоносного ПО, в том числе CTB-Locker, Angler и DarkHotel
- Подозрительные действия, включая использование сети Tor, автоматическое перенаправление электронной почты и онлайн-преобразование документов
- Повсеместное туннелирование DNS на домены, зарегистрированные в Китае
- «Тайпсквоттинг» DNS
- Внутренние клиенты, обходящие доверенную инфраструктуру DNS клиента

# Какие протоколы используют вымогатели?

| | Шифрование C&C | | | | Шантаж |
|---|---|---|---|---|---|
| ИМЯ | DNS | IP | NO C&C | TOR | ОПЛАТА |
| Locky | ● | ● | | | DNS |
| SamSam | | | ● | | DNS (TOR) |
| TeslaCrypt | ● | | | | DNS |
| CryptoWall | ● | | | | DNS |
| TorrentLocker | ● | | | | DNS |
| PadCrypt | ● | | | | DNS (TOR) |
| CTB-Locker | ● | | | ● | DNS |
| FAKBEN | ● | | | | DNS (TOR) |
| PayCrypt | ● | | | | DNS |
| KeyRanger | ● | | | ● | DNS |

# Комплекты эксплойтов: Adobe Flash и вредоносная реклама

Большинство наборов эксплойтов используют уязвимости Adobe Flash и Microsoft Silverlight



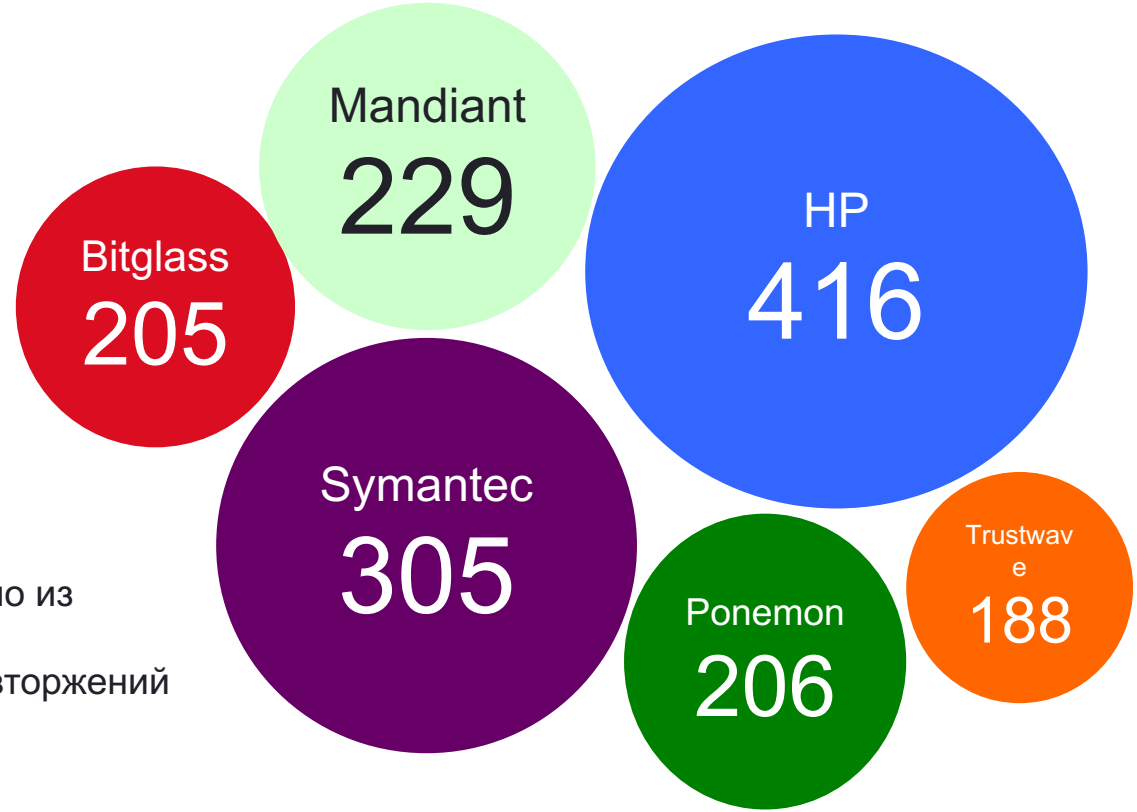
# Заражения браузера: чума, которая не проходит

Более чем

**85%**

опрошенных компаний
страдают каждый месяц

# К чему это все приводит?

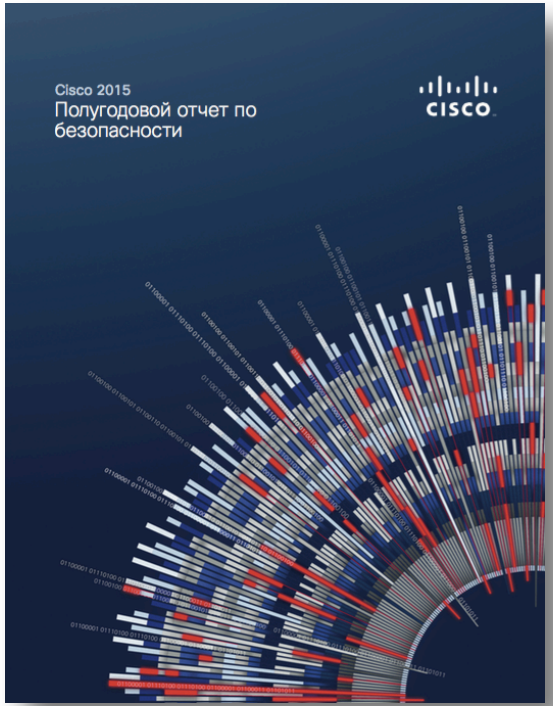



2287 дней – одно из самых длинных незамеченных вторжений

# 6 принципов комплексной защиты от угроз

1. Требуется архитектура безопасности и сети
2. Даже лучшие в своем классе технологии в одиночку не способны справляться с современным ландшафтом угроз
3. Интегрированная безопасность поможет бороться с зашифрованной вредоносной активностью
4. Открытые API имеют критическое значение
5. Требуется меньше компонентов для установки и управления
6. Автоматизация и координация помогают снизить время на обнаружение, локализацию и устранение последствий от атак

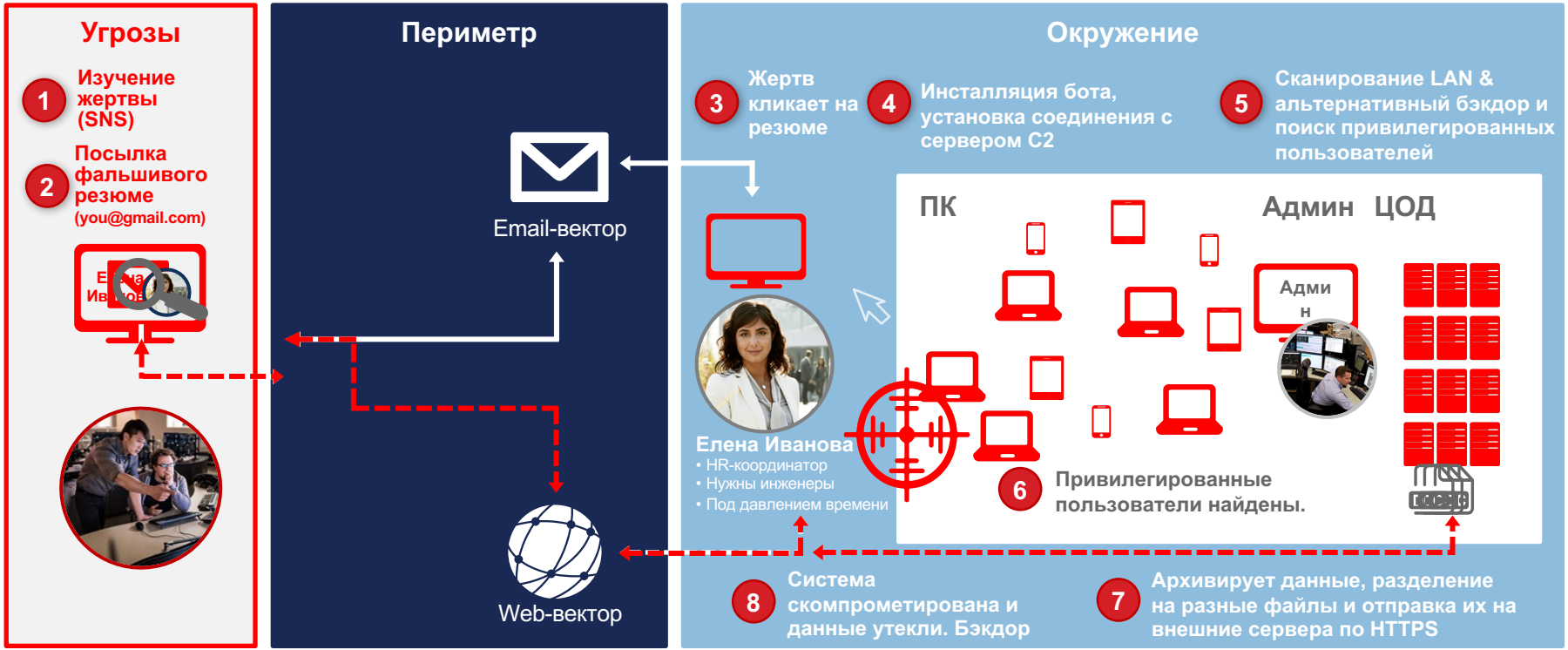
# Дополнительная информация про угрозы

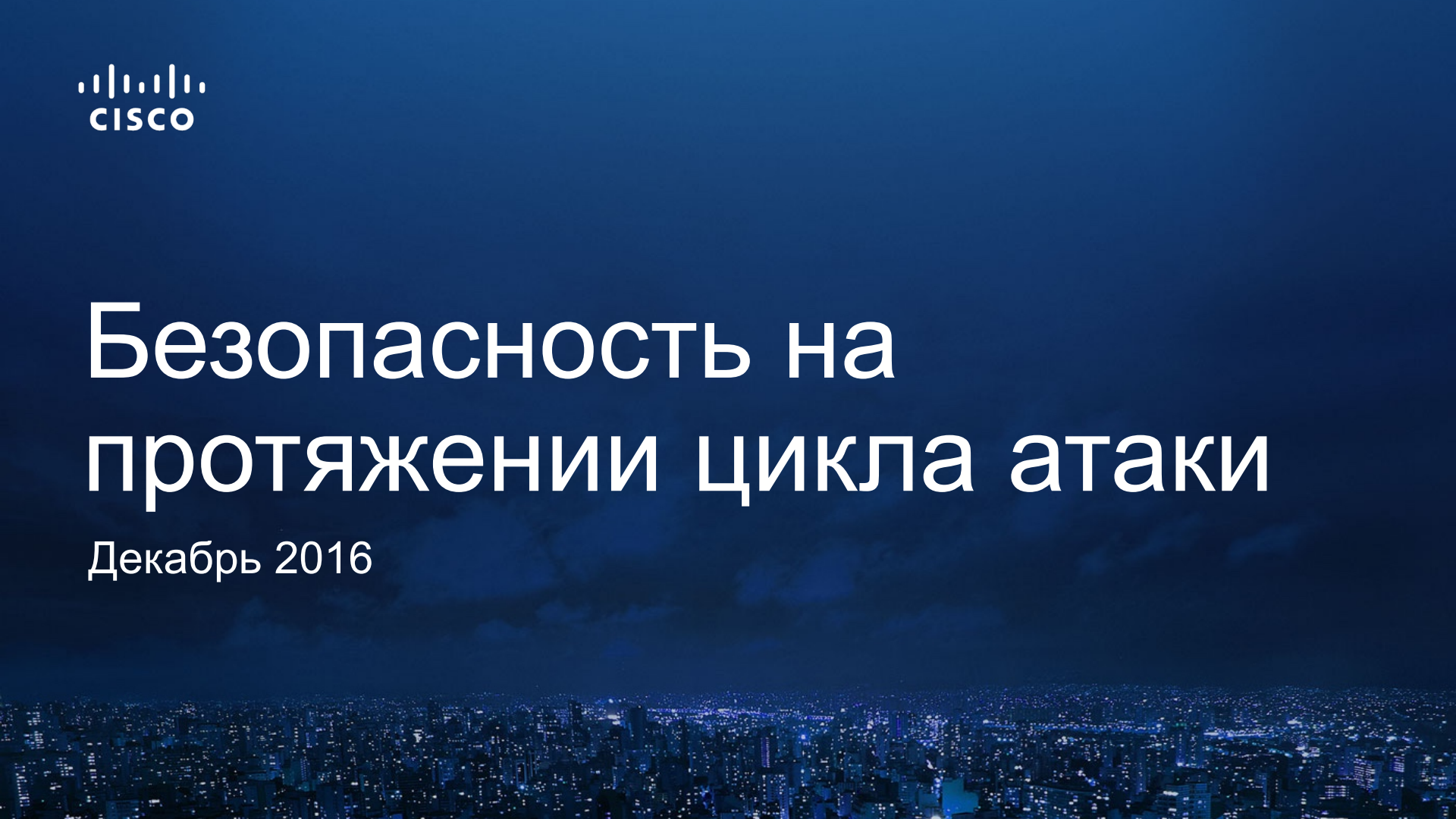





cisco

# Анатомия современной атаки






# Безопасность на протяжении цикла атаки

Декабрь 2016

# Новая модель безопасности

| Подготовка | Вторжение | Активная брешь |
|---|---|---|

**1. Рекогносцировка**
Сбор информации для создания стратегии атаки и инструментов для атаки

**2. Вооружение**
Объединение эксплоита с уязвимостью в запускаемый код

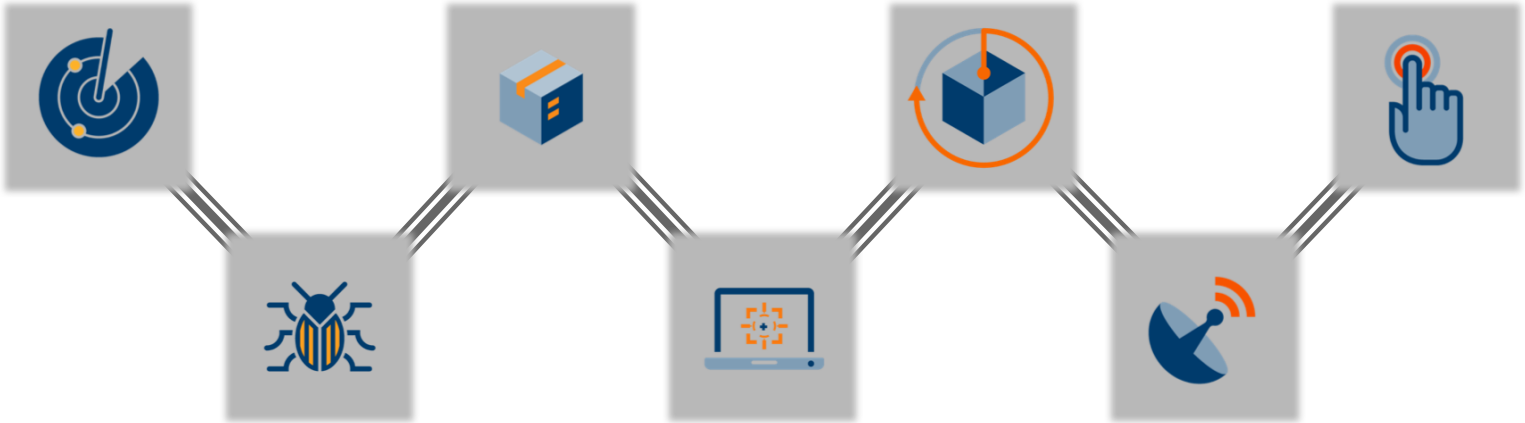
**3. Доставка**
Доставка бандла жертве через email, web, USB и т.д.

**4. Эксплуатация**
Эксплуатация уязвимости для выполнения кода на системе жертвы

**5. Инсталляция**
Установка malware на компьютере жертвы

**6. Command & Control**
Командный канал для удаленной манипуляции системой жертвы

**7. Действия по цели**
С полным доступом к системе нарушитель достигает своей цели



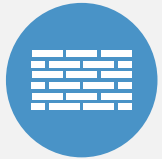
Основано на «убийственной цепочке» от Lockheed Martin

# 1. Рекогносцировка

Сбор информации для создания стратегии атаки и соответствующих инструментов

- OS
- AV
- Приложения
- Порты
- Персональная информация

# Уменьшите свою экспозицию для угроз



**Межсетевые экраны**

Блокируйте неавторизованный доступ и активность с помощью контроля потоков трафика

**Обнаружение и контроль приложений (AVC)**

Контролируйте поведение приложений для уменьшения плоскости атаки и снижения риска утери данных

**URL фильтрация**

Запрещайте доступ к специфическим сайтам или же категориям сайтов


**Возможности VPN**

Защищайте как подключения site-to-site, так и удаленные подключения с помощью шифрованных каналов связи

**Системы предотвращения вторжений нового поколения (NGIPS)**

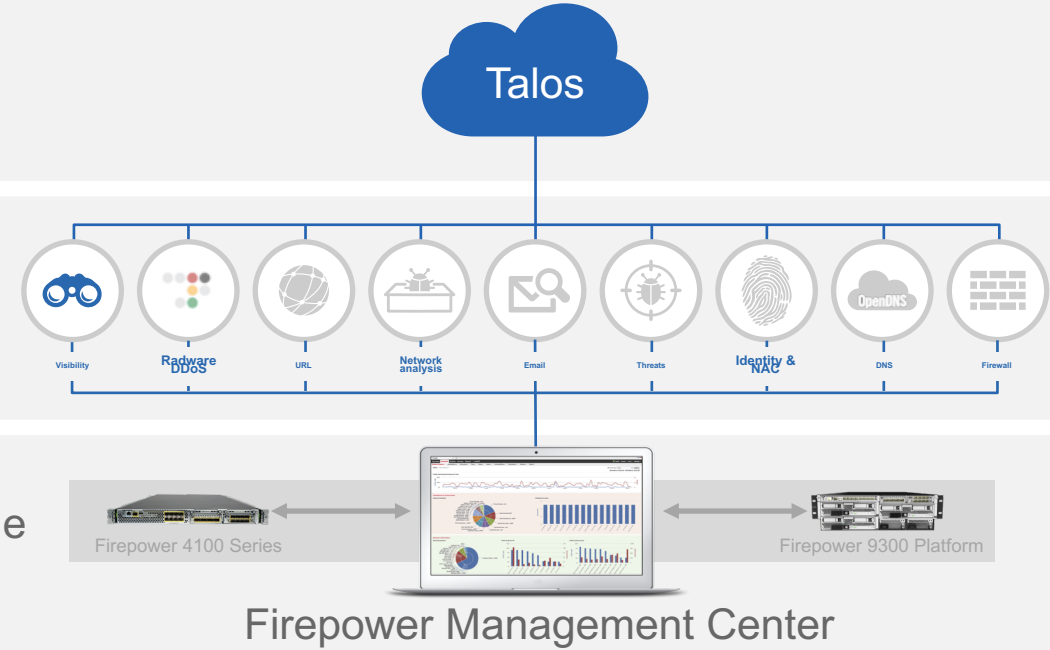
Обнаруживайте и предотвращайте угрозы до их входа в сеть

# Получите больше с расширенной аналитикой и интегрированной безопасностью

Общая информация

Общий контекст

Постоянное применение политик



# Cisco StealthWatch. Сеть как сенсор

Пример: NetFlow уведомления в StealthWatch

**Сканирование сети**

**TCP, UDP, Port Scanning Across Multiple Hosts**

**Нарушения политик**

**Hosts that are baselined, exceeding predetermined thresholds.**

# РЕШЕНИЯ БЕЗОПАСНОСТИ НАЧИНАЮТСЯ С CISCO ASA

ASA

## ВИРТУАЛЬНЫЙ

vmware KVM Xen Microsoft Hyper-V

**ASAv**

- Полный функционал ASA
- Независимость от гипервизора
- Независимость от virtual switch
- Динамическая масштабируемость

Unified Policy

Common 64 bit OS

ACI Integrated

## ФИЗИЧЕСКИЙ

**ASA 5585-X**

Кластеризация до 16 устройств с производительностью до 640Gbps

ASAv доступна на VMWare, KVM и Hyper-V

# Платформы Cisco NGFW

Новые устройства

Firepower 4100
и Firepower 9300 с Firepower Threat Defence и ASA

Fireport Threat Defence на ASA 5500-X

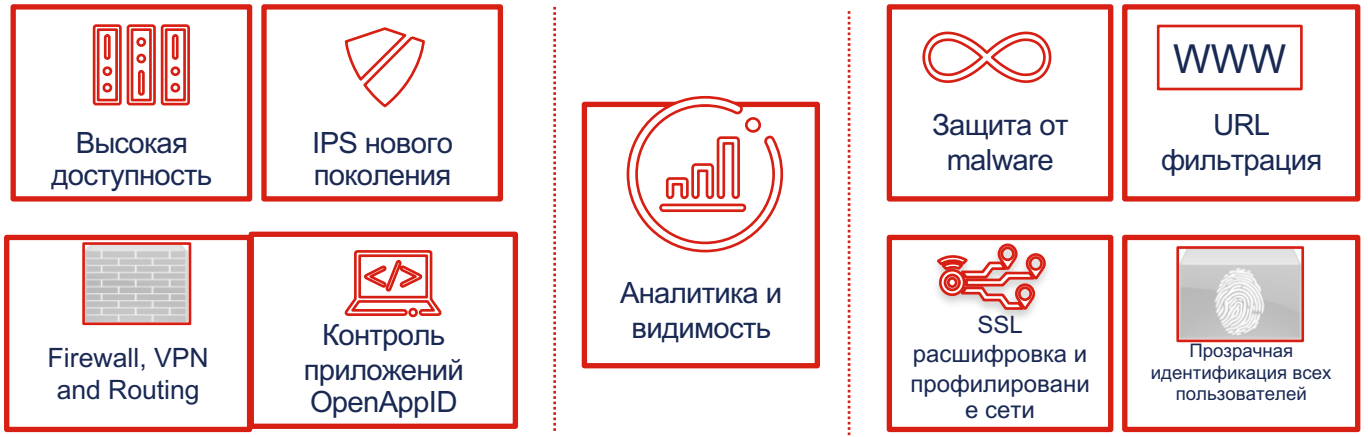
Firepower сервисы
На ASA 5585-X и 5500-X

Все управляются с помощью Firepower Management Center

# Cisco Firepower NGFW

Best of Breed

## Межсетевой экран ориентированный на защиту от угроз




Одна ОС + простое управление

**Простой, Октрытый, автоматизированный и эффективный**

# Передовая автоматизация Cisco NGFW

*Он совсем не похож на то, что используют другие!*

**Использование контекста**
Создание профилей узлов, ISE pxgrid, интеграция со сканерами уязвимостей

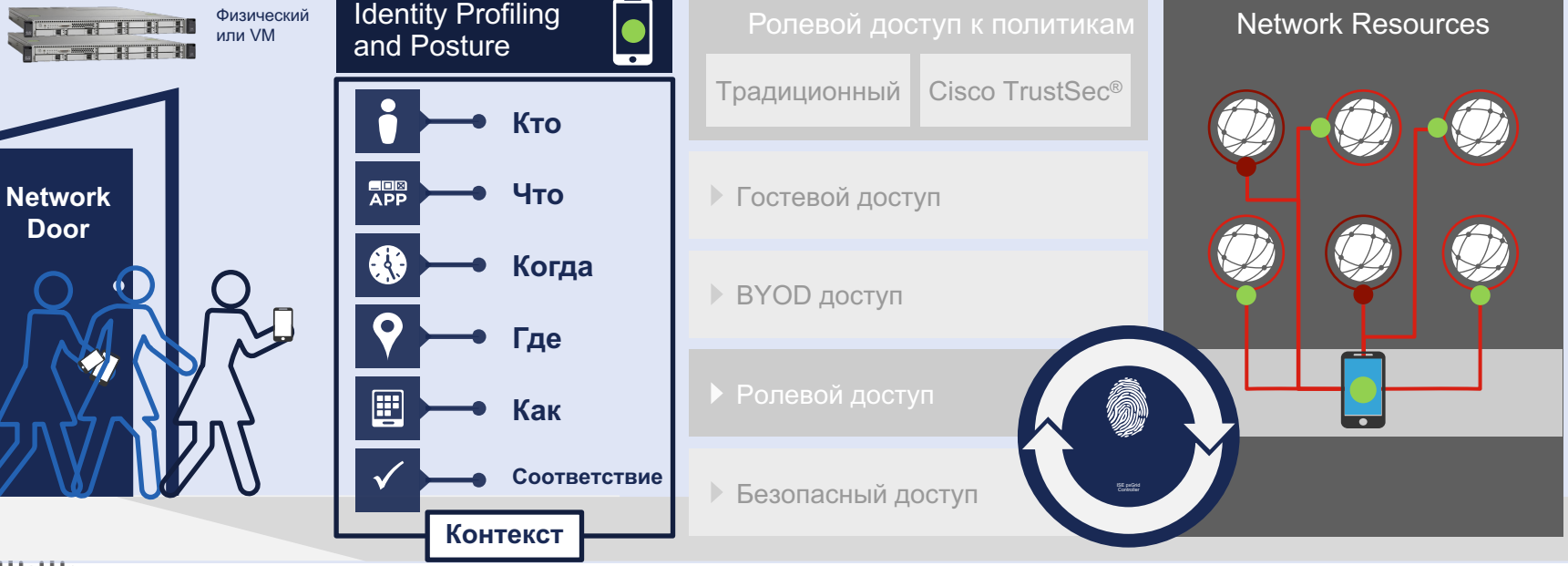
**Автоматизированная настройка**
Автоматическое создание политик безопасности на основании профиля сети


**Оценка уровня влияния и IoC**
Корреляция угроз уменьшает количество событий, которые требуют реакции на 99%

**Идентификация приложений, которой вы можете доверять**
OpenAppID

# Представляем Cisco Identity Services Engine

Централизованное решение безопасности, которое автоматизирует доступ к сетевым ресурсам на основании контекста и разделяет контекстные данные.



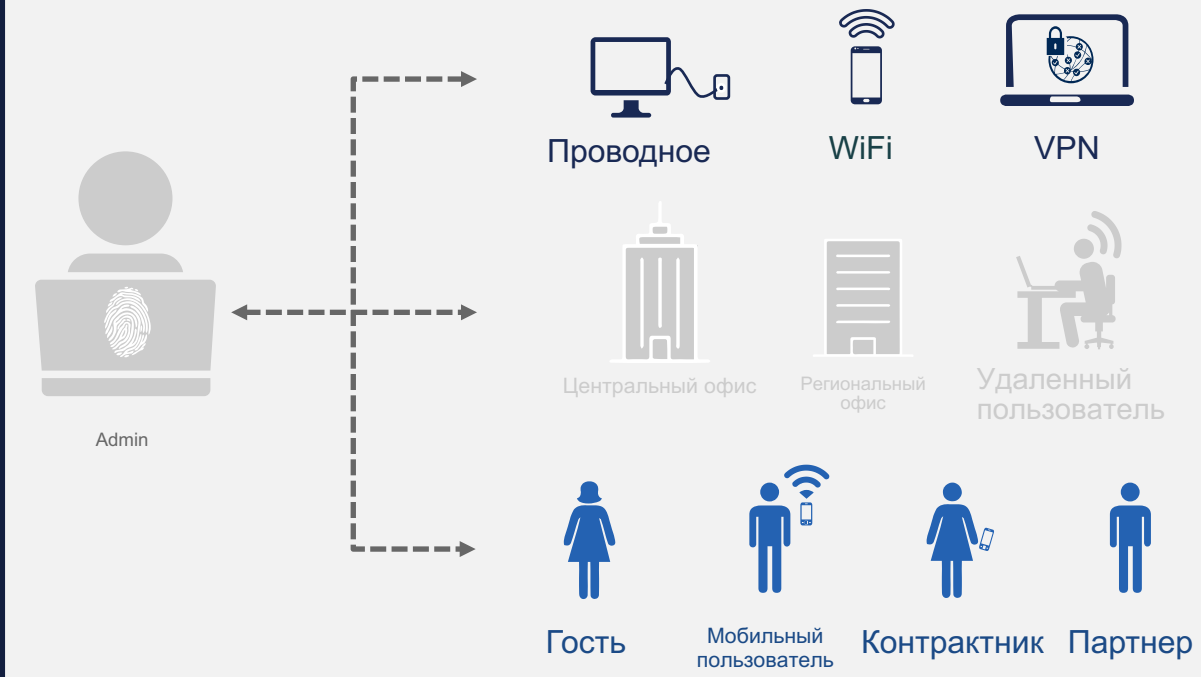
# Cisco ISE

## Контролируйте все из одной точки. Сеть, данные, приложения

Безопасный доступ из любой точки, вне зависимости от типа подключения

Применяйте политики доступа и использования по всей сети

Мониторинг доступа, активности и соответствия некорпоративных активов, действия по ограничению, если требуется



# Расширяйте контроль с авторизацией по местоположению

## Интеграция с Cisco Mobility Services Engine (MSE)

**Что новго для Cisco ISE 2.0?**

Интеграцияс Cisco® Mobility Services Engine (MSE) добавляет физическое расположение пользователя в контекст и определяет, какой доступ назначить

**Выгоды**

- **Детальный контроль** Сетевого доступа с авторизацией по местоположению для индивидуальных пользователей
- **Расширенное применение политик** с автоматической проверкой местоположения и реавторизацией
- **Упрощенное управление** с помощью настройки авторизации со средствами управления Cisco ISE

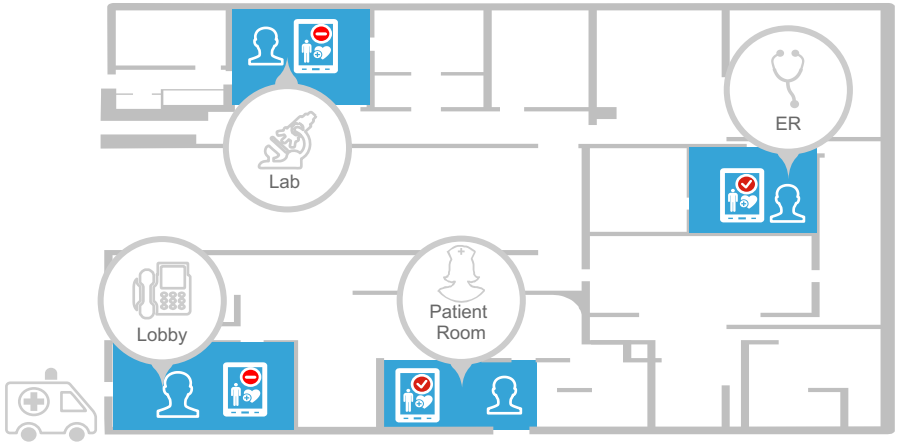
### Авторизация по местоположению

Админ определяет иерархию мест и назначает пользователю специфические права доступу на основании места

Данные пациентов

### Доступ к данным пациентов

| | Лобби | Палата | Лаборатория | ER |
|---|---|---|---|---|
| Врач | Нет доступа | Есть доступ | Нет доступа | Есть доступ |




**Возможности**

- Настройки иерархии мест по всем возможным объектам. Применяет атрибуты места Cisco MSE в запрос доступа для использования в политике авторизации
- Периодическая проверка Cisco MSE на предмет изменения местоположения
- Реавторизация доступа для нового местоположения

# 2. Вооружение

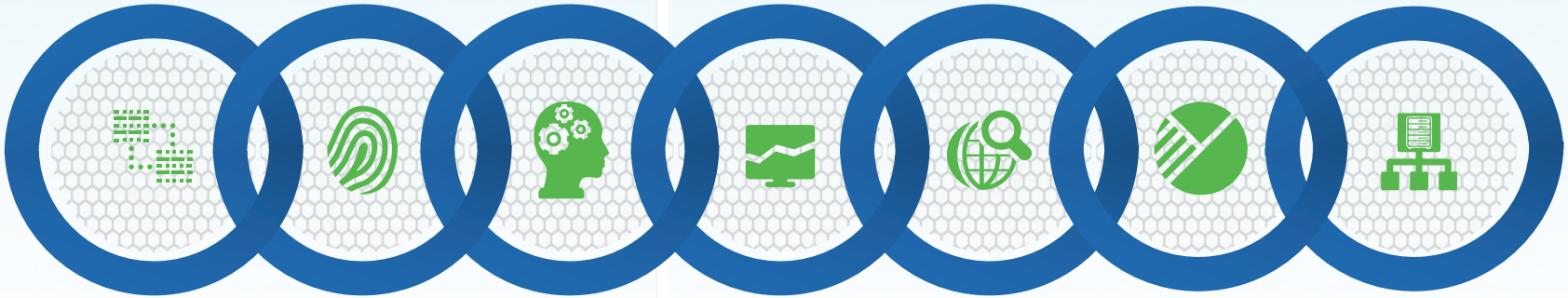
Объединение эксплоита с уязвимостью в запускаемый код

- Exploit Kits
- Противодействие AV
- Обфускация
- Руткит

# Cisco Advanced Malware Protection

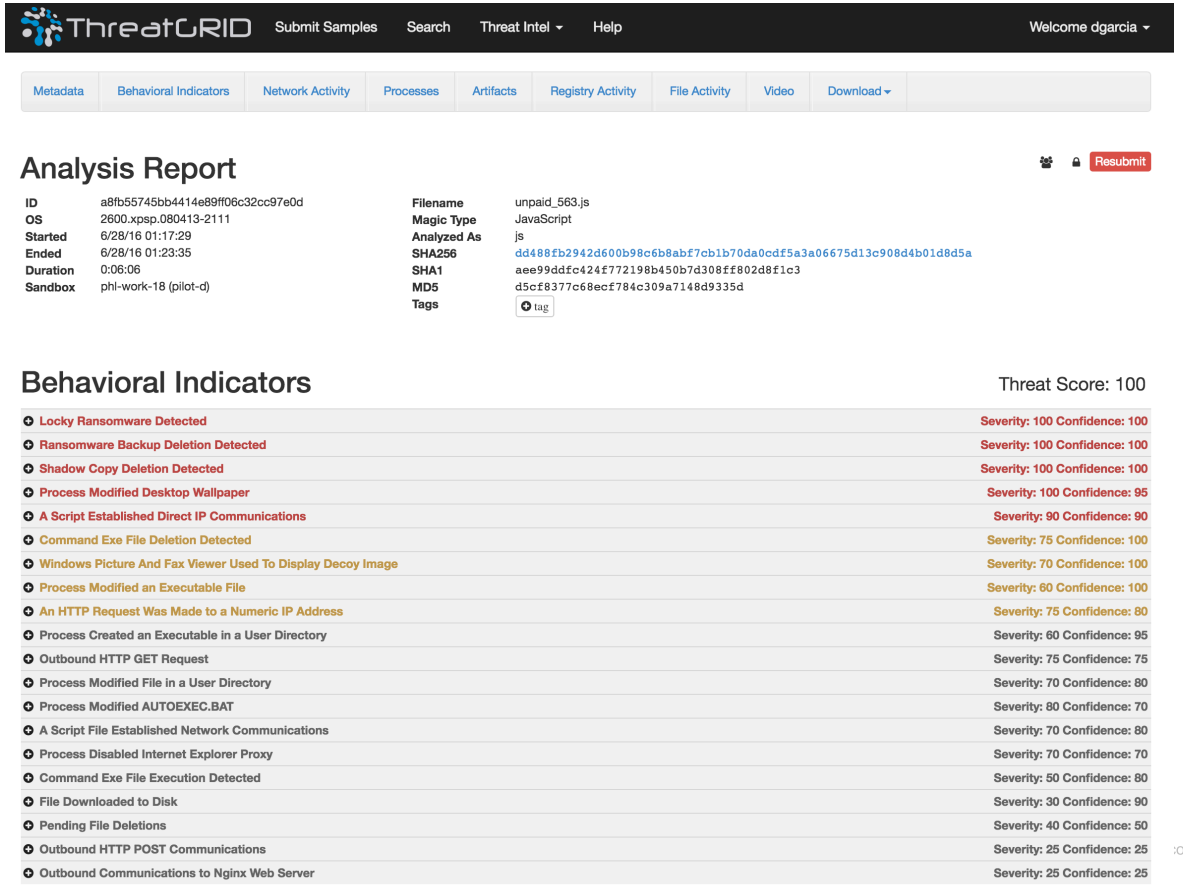
## Репутационная фильтрация и поведенческий анализ

| Репутационная фильтрация | | | Поведенческий анализ | | | |
|---|---|---|---|---|---|---|



Сигнатуры | Нечеткие отпечатки | Машинное обучение | Индикаторы компрометации | Динамический анализ | Расширенная аналитика | Корреляция потоков

# Cisco AMP ThreatGrid



# 3. Доставка

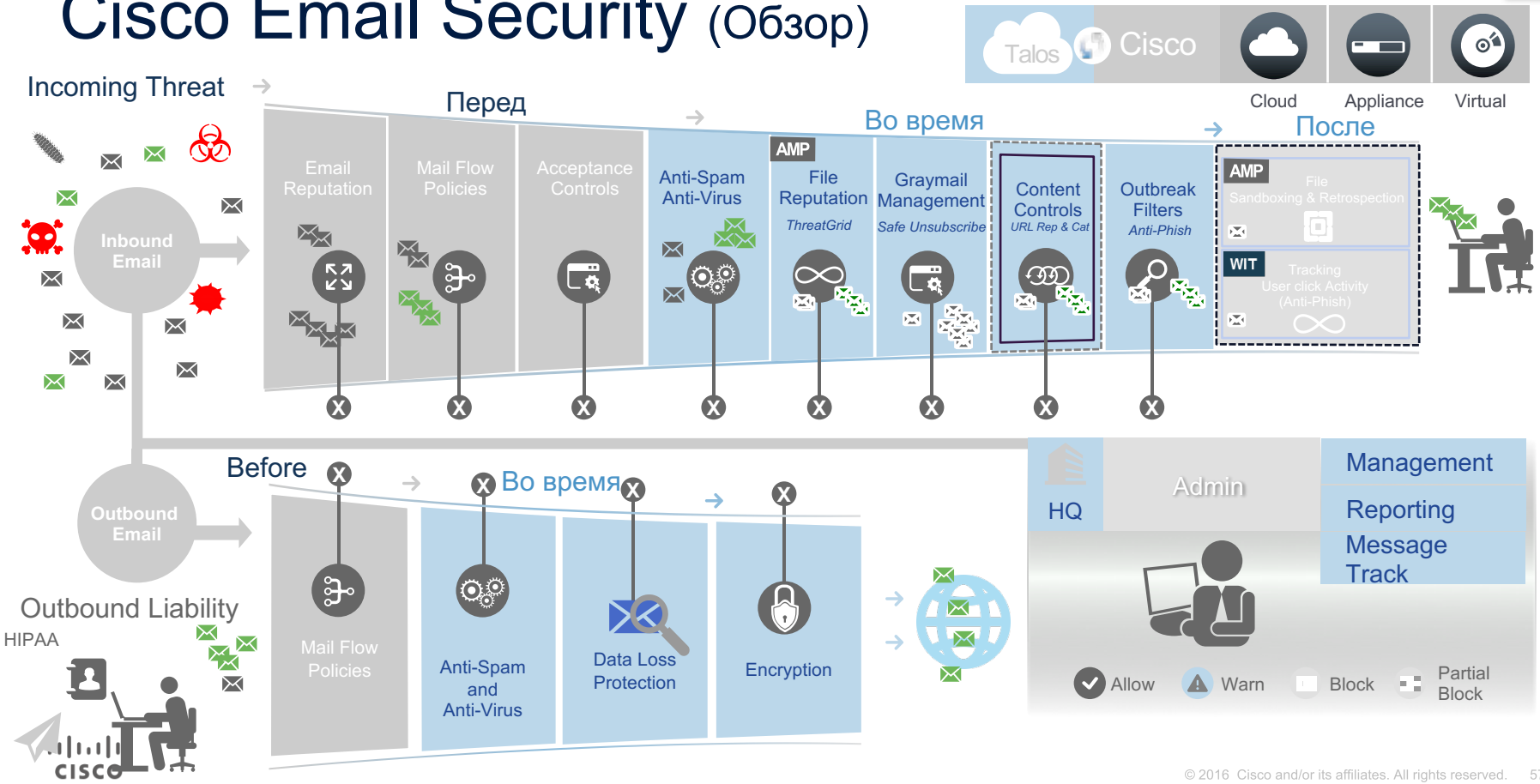
Доставка бандла жертве через email, web, USB и т.д..

- Фишинг
- Watering hole
- Вредоносная реклама

# Наиболее опасные угрозы

| | Watering hole | Целевой фишинг | Dropper |
|---|---|---|---|
| |  |  |  |
| Подход | Инфекция или инъекция в доверенный сайт | Атака пользователей с скомпрометированными ссылками | Доставка malware со скрытыми и самоудаляющимися программами. |
| Тактика | Рекогнисцировка на цели | Использование социальной инженерии | Получение доступа (DLL Injection, Remote Access etc) Контроль МЭ, антивирусов и т.д. |
| Влияние | Доставка атакующего эксплоита | Доставка атакующего эксплоита | Компрометация системы, личных данных, систем авторизации. |
| Вектор | | | |

# Cisco Email Security (Обзор)



# Интеграция Cisco Email Security Integration с информационными системами Threat Intelligence

## Непревзойденная коллективная аналитика безопасности

Информация Threat

Cisco® Talos

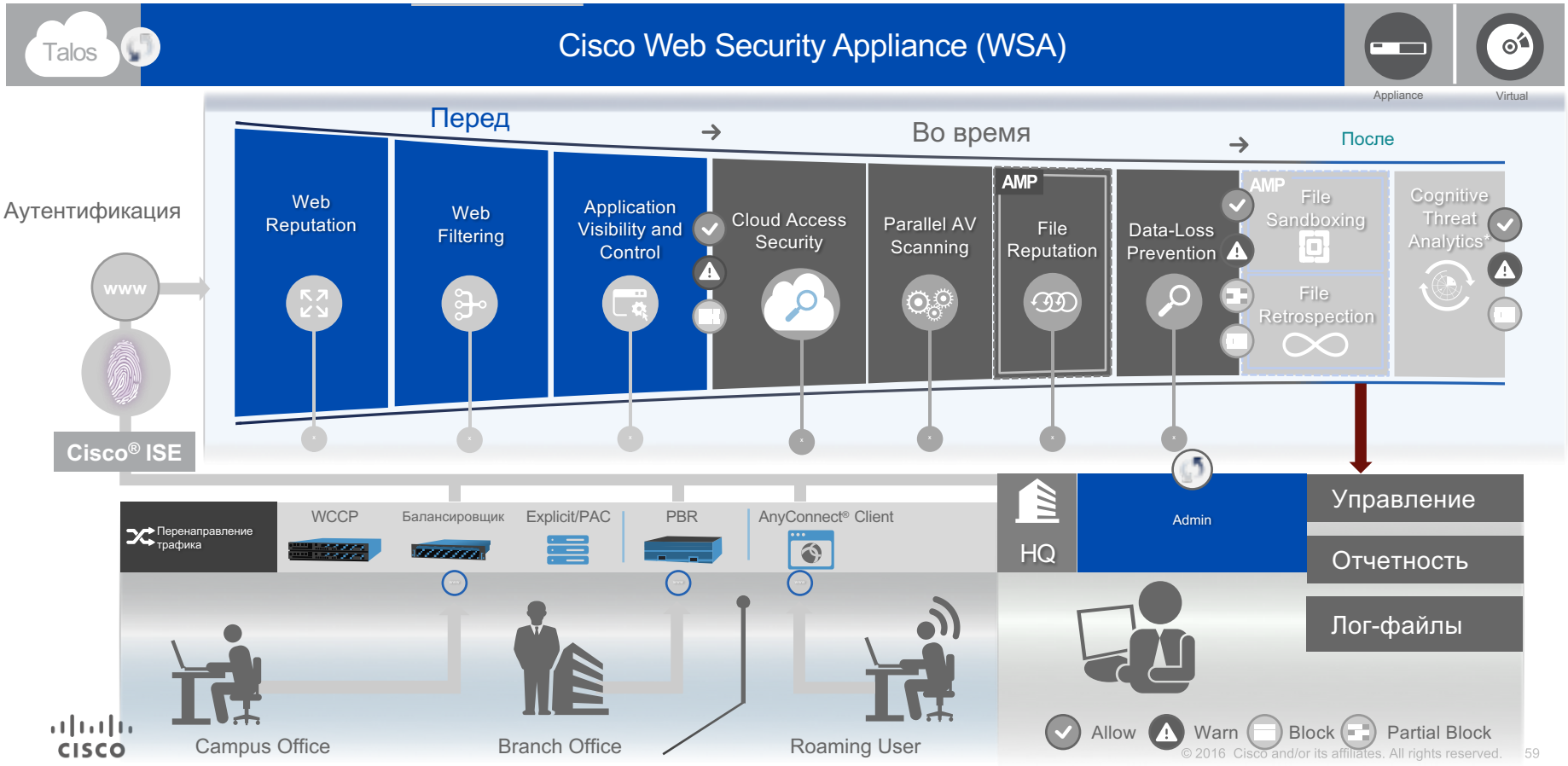
Research Response

Email | Endpoints | Web | Networks | IPS | Devices

| | |
|---|---|
| 1.6 млн сенсоров | 35% мирового трафика email |
| 100 TB данных в день | 13 млрд веб запросов |
| 150 million+ хостов | 24x7x365 работа |
| 600+ инженеров, исследователей | 40+ языков |

ESA + AMP Advanced Malware Protection

- 180,000+ новых семплов в день
- FireAMP™ сообщество
- Информация об уязвимостях Microsoft и других
- OpenSource сообщества Snort и ClamAV
- Honeypots
- Программа Sourcefire AEGIS™
- Частные и публичные данные об угрозах
- Динамический анализ



# Где вы применяете правила безопасности?


## ВЫГОДЫ

Снижение количества предупреждений вдвое

Трафик не достигает цели

Интернет-доступ быстрее, не медленнее

Глобальная настройка менее чем за 10 минут

# Использование Domain Name Services как инструмента безопасности

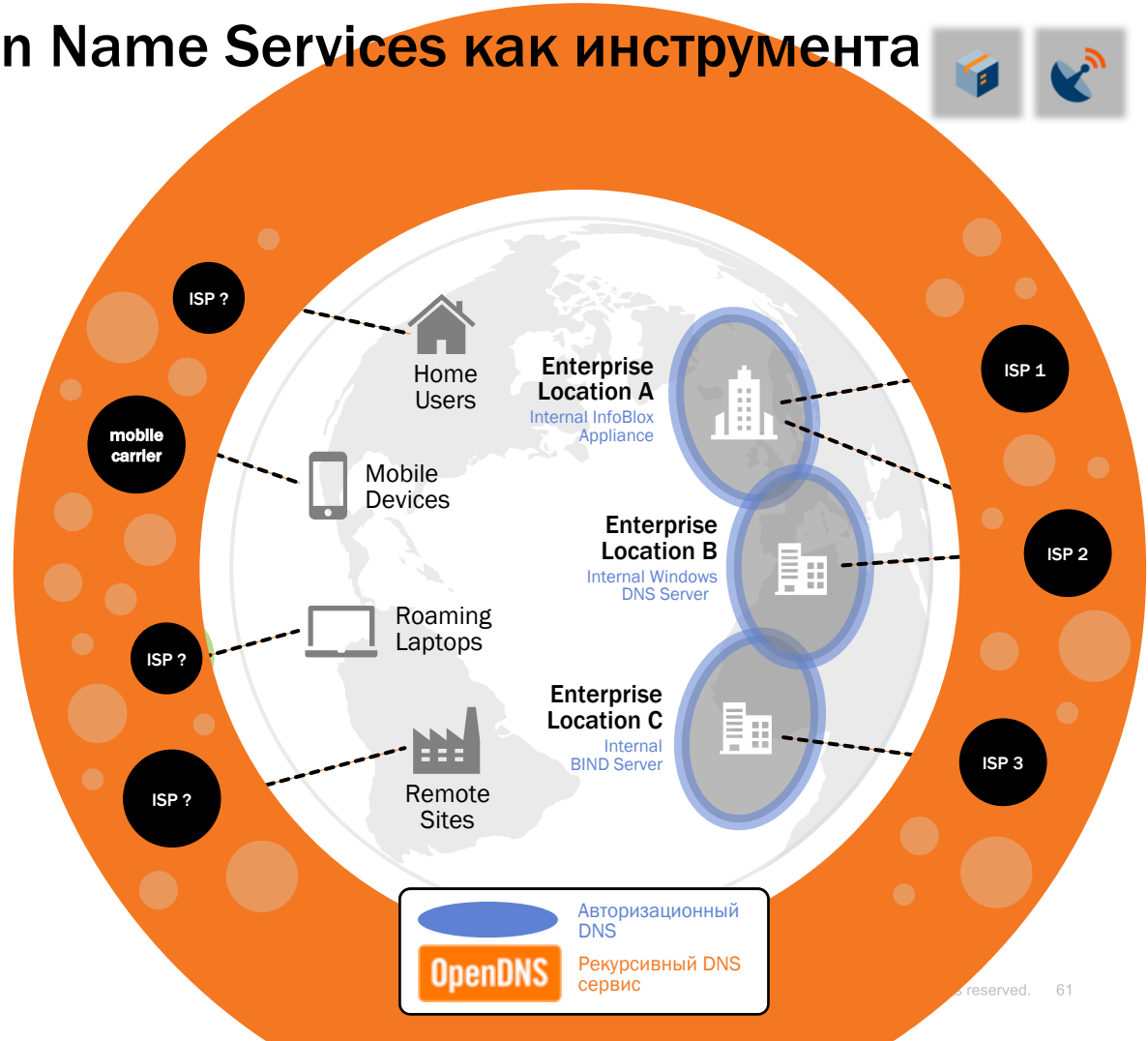
## ВЫГОДЫ

Видимость глобальной интернет-активности

Сетевая безопасность без задержек

Постоянное применение политик

Хорошая видимость облаков



# В чем уникальность Cisco Umbrella


## Защита любых устройств, в любой точке

## Постоянное применение & и видимость

Запросы перенаправляются автоматически из любой точки

## Расширение защиты за пределы периметра

Блокирование всей интернет-активности, которая направлена на домены, обнаруженные вашими устройствами безопасности или источниками threat intelligence

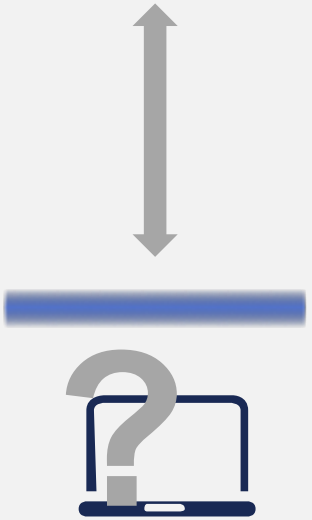
# 4. Эксплуатация

Эксплуатация уязвимости для исполнения кода в системе жертвы

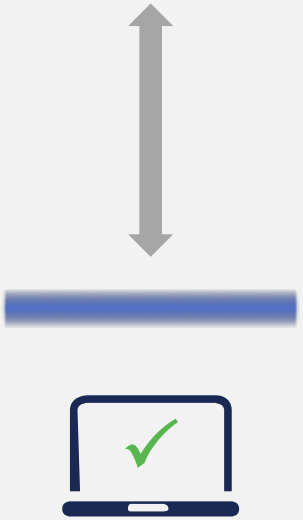
- День 0
- Нет патчей
- Социальная инженерия

# Удостоверьтесь, что Cisco ISE включен и работает

**Идентификация устройств**



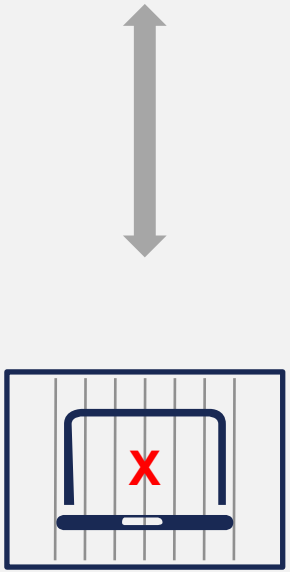
**Проверка состояние**



**Соответсвие политикам**

- AV installed? ✓
- Registered? ✓
- OS Patches? x
- Custom Criteria? ✓
- Vulnerable? x

**Карантин несоответствующих устройств**

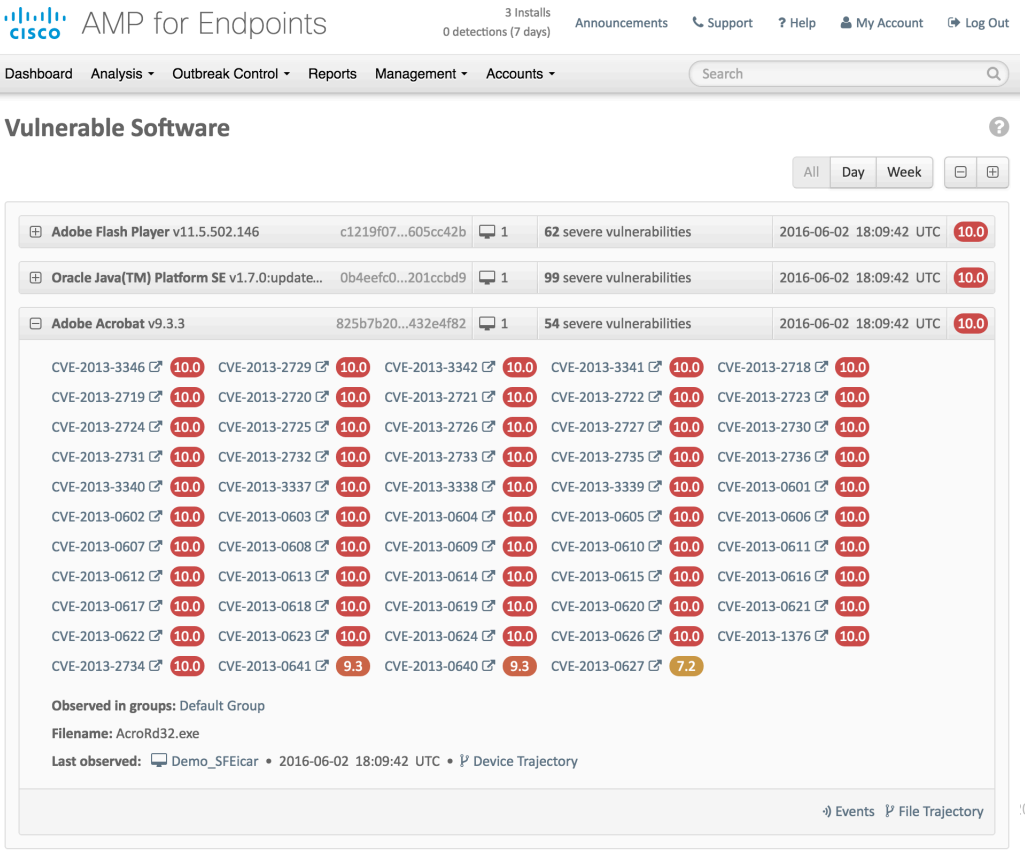



**Интеграция с Enterprise Mobility Management (EMM)**

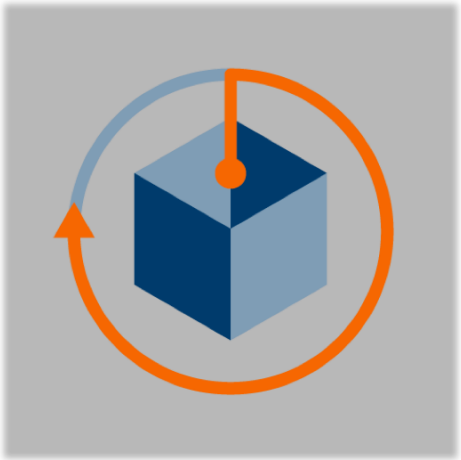
MaaS360 by Fiberlink
airwatch
SAP
IBM
CITRIX
MobileIron
Good
cisco Meraki

# Cisco Advanced Malware Protection

## Уязвимые приложения



# 5. Установка



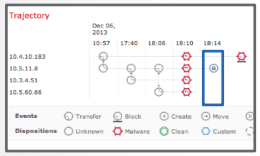
Установка malware в системе

- Руткит
- Уклонение от AV

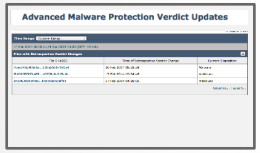
# Защита в сети

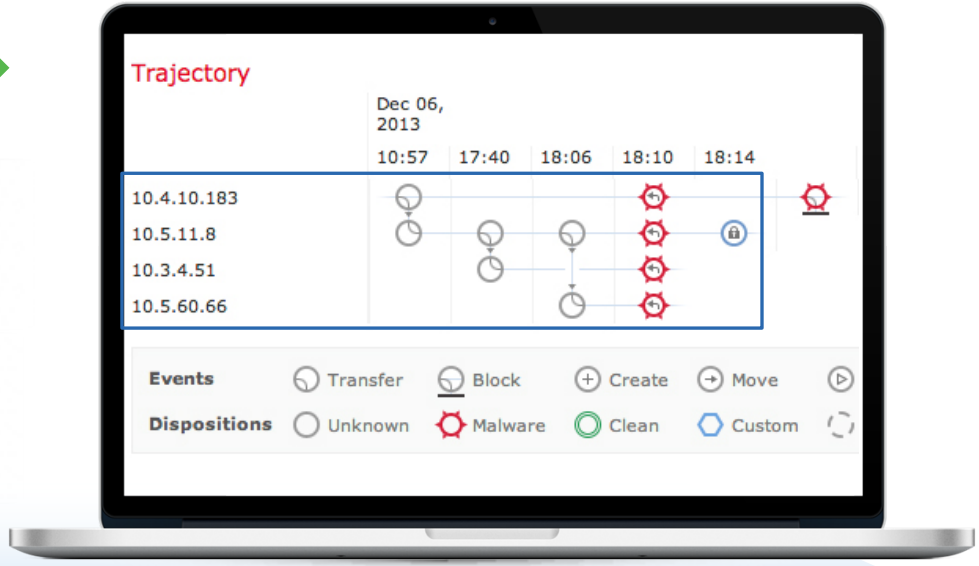
Network


Endpoint




Content



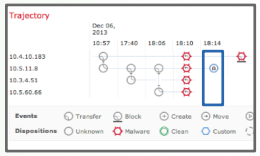




Сетевая платформа использует индикаторы компрометации, анализ файлов. В этом примере файловая траектория показывает, как вредоносные файлы перемещаются по сети.

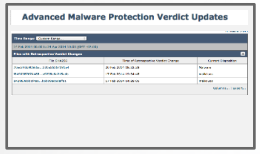
# Защита на узлах

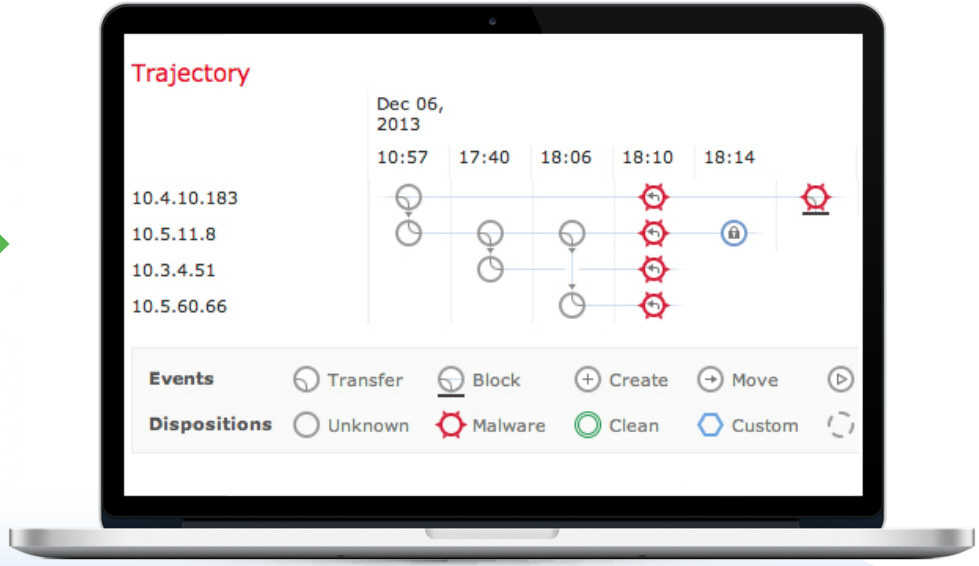
Network


Endpoint




Content

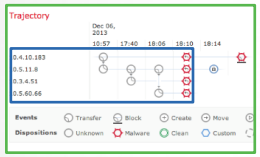


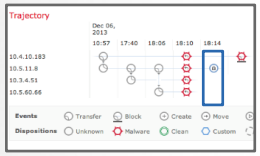

Платформа для защиты узлов имеет траекторию файлов, гибкий поиск и контроль атак. В этом примере показан карантин недавно обнаруженного malware на устройстве с установленным коннектором AMP for Endpoints.

# Защита для Web и Email

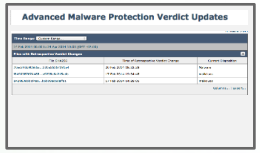
Network

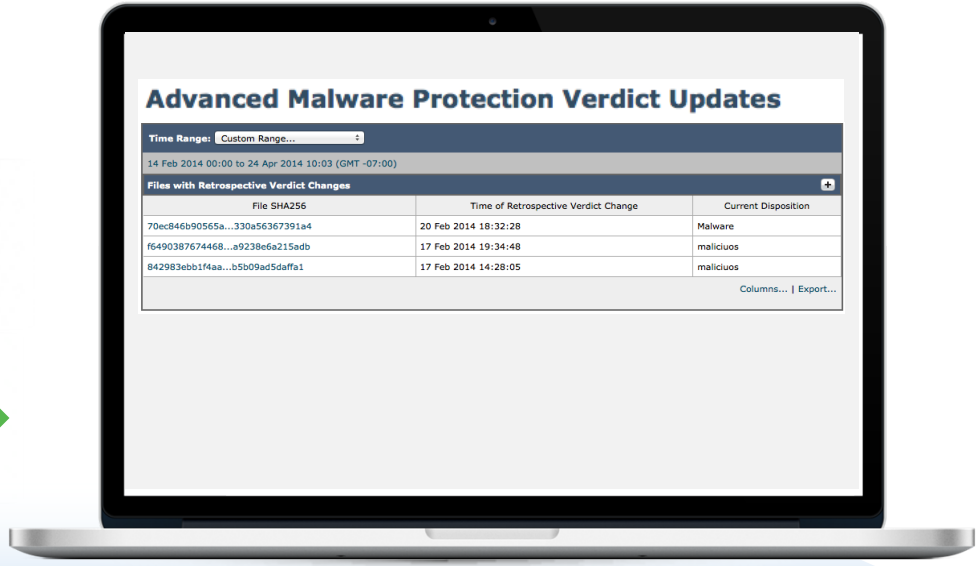



Endpoint



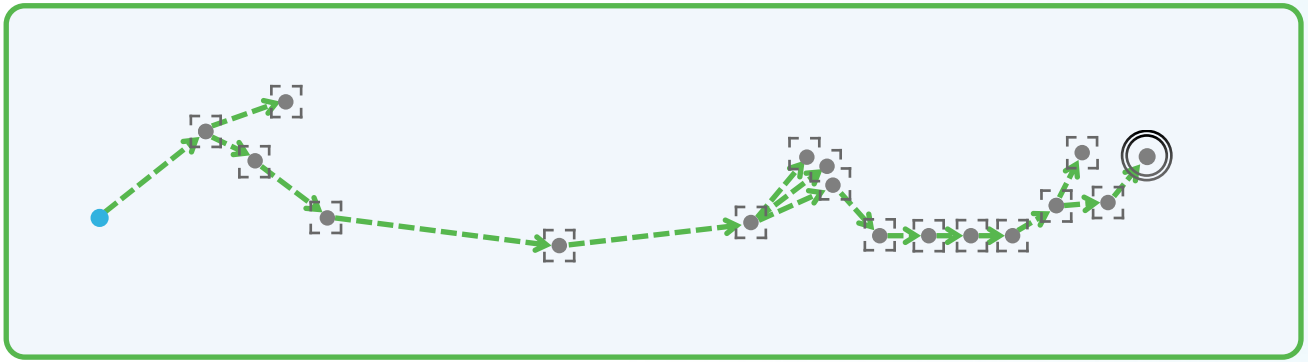

Content




Cisco® AMP для Web и Email защищает от вредоносного содержимого в трафике web и email с помощью блокирования известного malware и выдачи ретроспективных предупреждений, когда обнаруживаются ранее незнакомые пропущенные файлы.

# Ретроспективная безопасность построена на…



| | |
|---|---|
| 1 | Анализ, как только мы увидели файл |
| 2 | Постоянный анализ файла с течением времени, чтобы мы увидели изменение его состояния. |
| 3 | Предоставление непревзойденной видимости пути, действий или связей, который ассоциированы с определенным набором программ. |

# Ретроспектива

**Nov 13 2015 – 12:00**

## FireAMP Cloud

**Processes within a company.org**

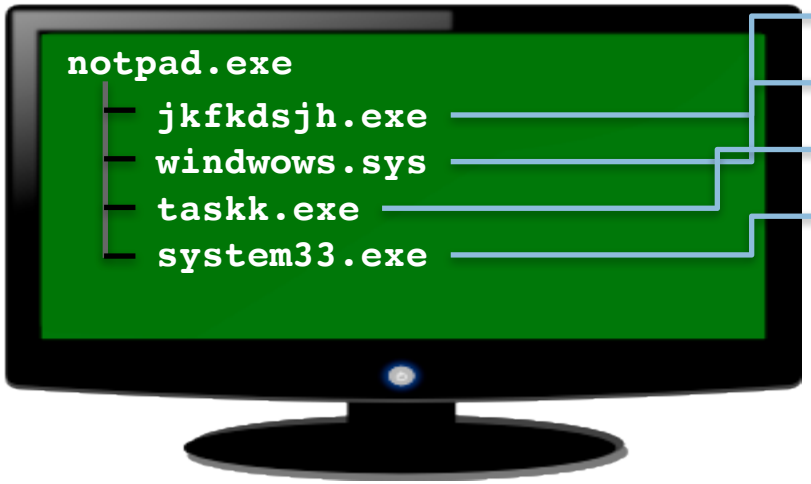
`d7a8fbb…7c9e592` ?


## Anti-virus

Machine Status: ✔

# Ретроспектива

**Nov 13 2015 – 12:06**




## FireAMP Cloud

**Processes within a company.org**

d7a8fbb…7c9e592

h84hfyd…h7dbw0k

mlpa3hz…jdn9jq1

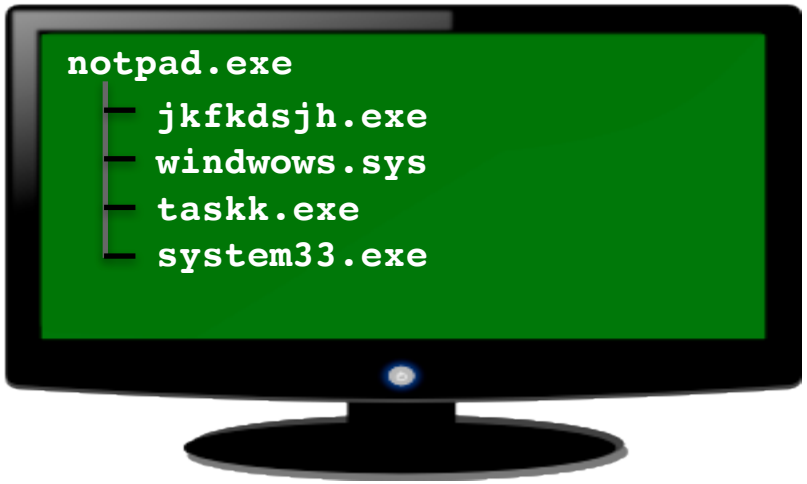
bzhw9hd…nski87d

vsh82ge…mk93gxs

## Anti-virus

Machine Status: ✔

# Ретроспектива




**Nov 14 2015 – 12:00**

## FireAMP Cloud

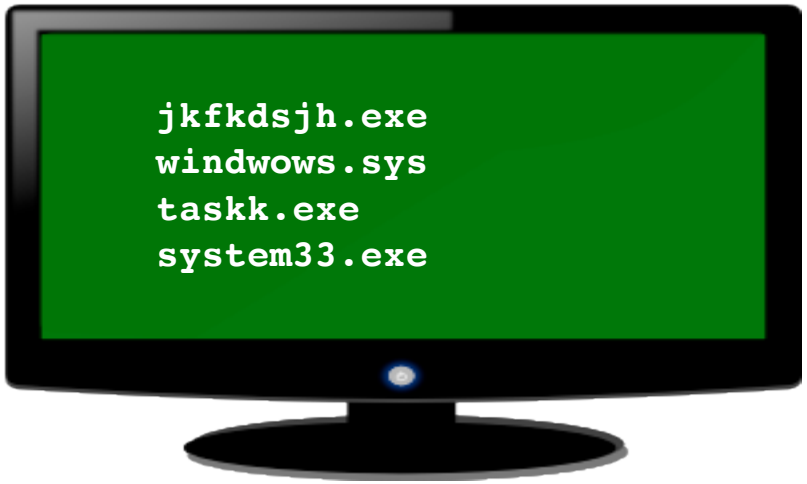
**Processes within a company.org**

```
d7a8fbb…7c9e592
h84hfyd…h7dbw0k
mlpa3hz…jdn9jq1
bzhw9hd…nski87d
vsh82ge…mk93gxs
```

## Anti-virus

Machine Status: ✔

# Ретроспектива




**Nov 14 2015 – 12:00**

## FireAMP Cloud

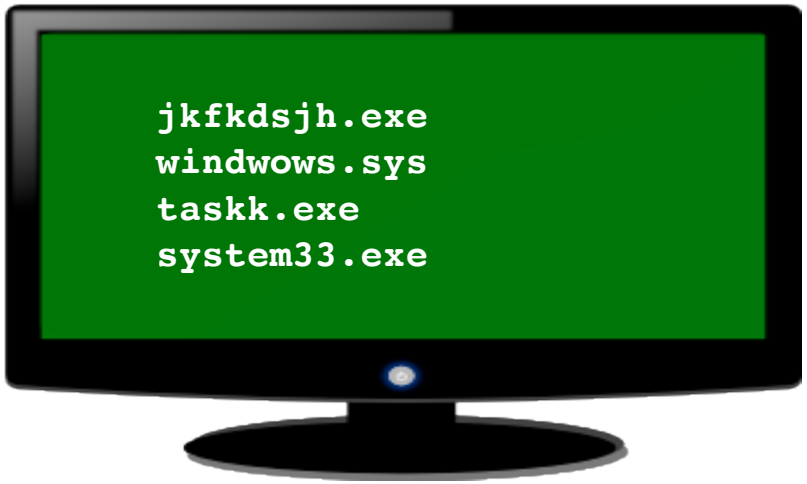
**Processes within a company.org**

```
d7a8fbb…7c9e592
h84hfyd…h7dbw0k
mlpa3hz…jdn9jq1
bzhw9hd…nski87d
vsh82ge…mk93gxs
```

## Anti-virus

Machine Status: ✔

# Ретроспектива




**Nov 15 2015 – 12:00**

## FireAMP Cloud

**Processes within a company.org**

```
d7a8fbb…7c9e592
h84hfyd…h7dbw0k
mlpa3hz…jdn9jq1
bzhw9hd…nski87d
vsh82ge…mk93gxs
```

## Anti-virus

Machine Status: Signature Update

# Ретроспектива

Nov 15 2015 – 12:00

**Retrospective Alert**


## FireAMP Cloud

**Processes within a company.org**

`d7a8fbb…7c9e592` ✗

`h84hfyd…h7dbw0k` ?

`mlpa3hz…jdn9jq1` ?

`bzhw9hd…nski87d` ?

`vsh82ge…mk93gxs` ?

## Anti-virus

Machine Status: ✔

# 6. Command & Control

Канал команд для удаленной манипуляцией системой жертвы.

- Известные легитимные приложения (Twitter, SSH, HTTPS)

# Глобальное исследование и информация

**100 TB**
Of Data Received Daily

**1.5 MILLION**
Daily Malware Samples

**600 BILLION**
Daily Email Messages

**16 BILLION**
Daily Web Requests


**24 • 7 • 365 Operations**

**250+**
Full Time Threat Intel Researchers

**MILLIONS**
Of Telemetry Agents

**4**
Global Data Centers

**Over 100**
Threat Intelligence Partners

# Cisco Umbrella:
## Самый быстрый и простой путь заблокировать угрозы


### ВЫГОДЫ

Просто настроить DNS без профессиональных сервисов

Не требуется ни программное ни аппаратное обеспечение

Защита любого устройства

Защита как Mac, так и Win устройств

# Cisco Umbrella & Investigate.

## Уникальная аналитика для классификации

### Захват

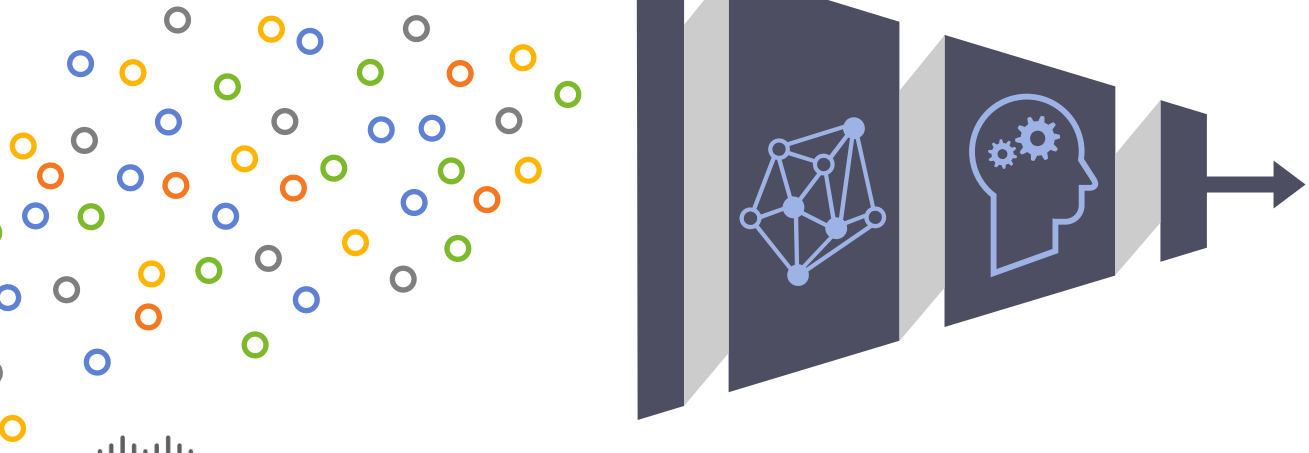
С миллионов точек данных за секунды

### Анализ

Статистические модели и человеческий интеллект

### Идентификация

вероятно вредоносных сайтов




# Мы видим, где начинаются атаки

3D визуализация Dark hotel Attack 2014

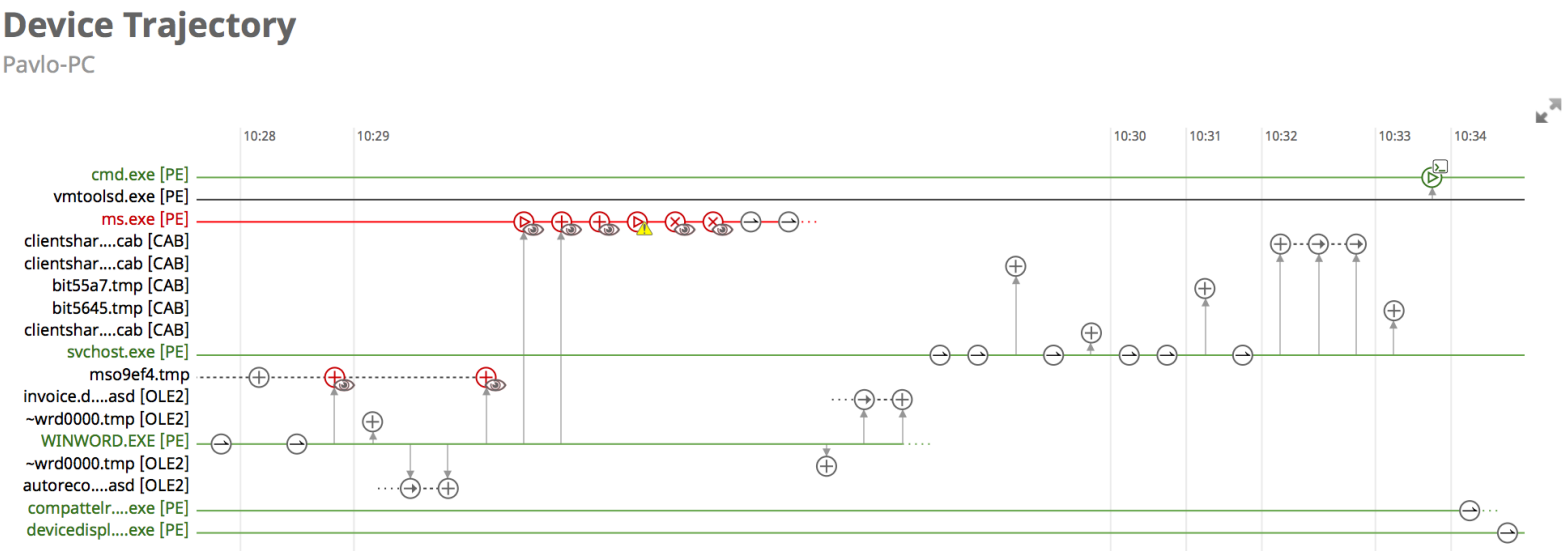
# 7. Действия на целях

С «полным доступом» злоумышленник может использовать и достичь

- Несколько промежуточных узлов для скрытия следов
- Скомпрометировать другие машины
- Экосистемы

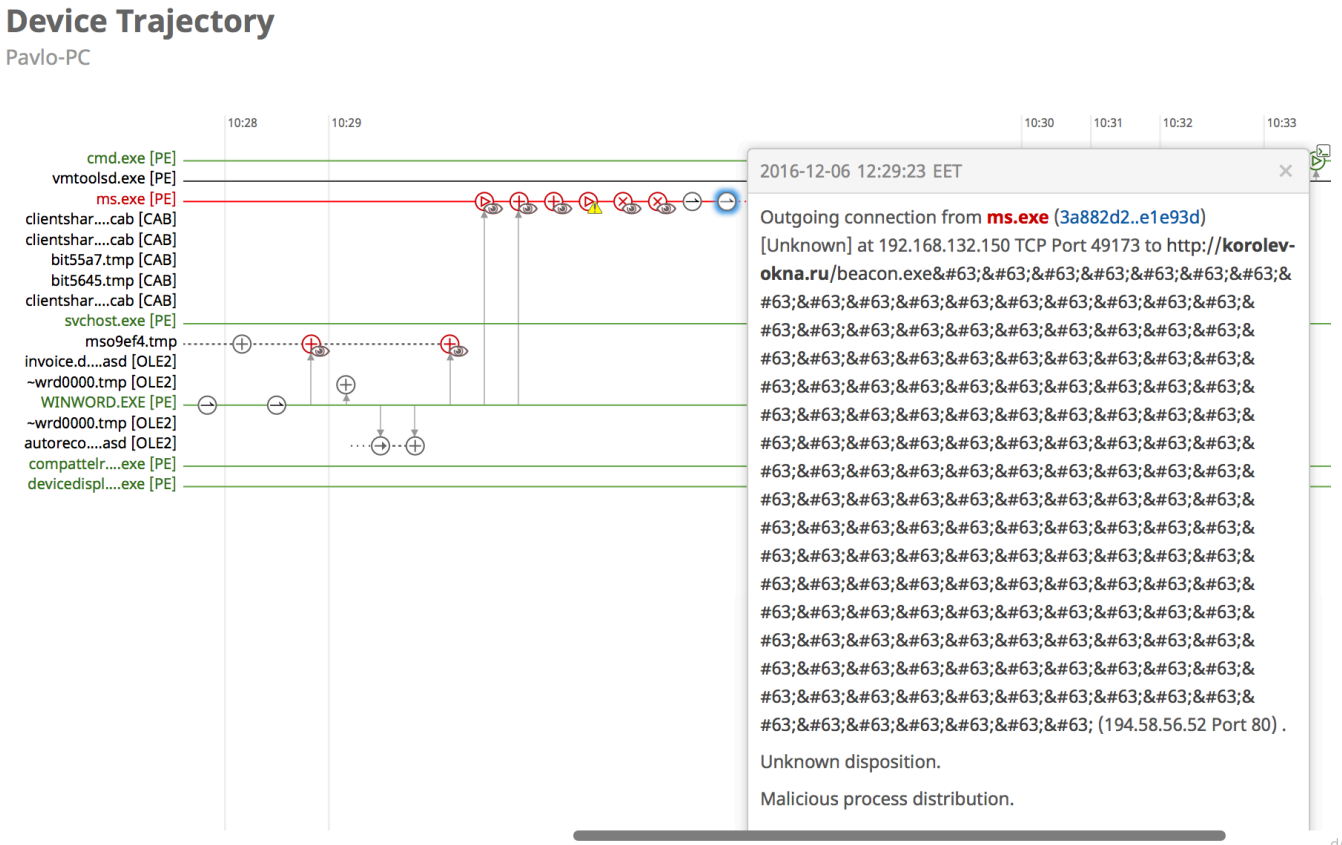
# Cisco Advanced Malware Protection

## Что происходит на узлах

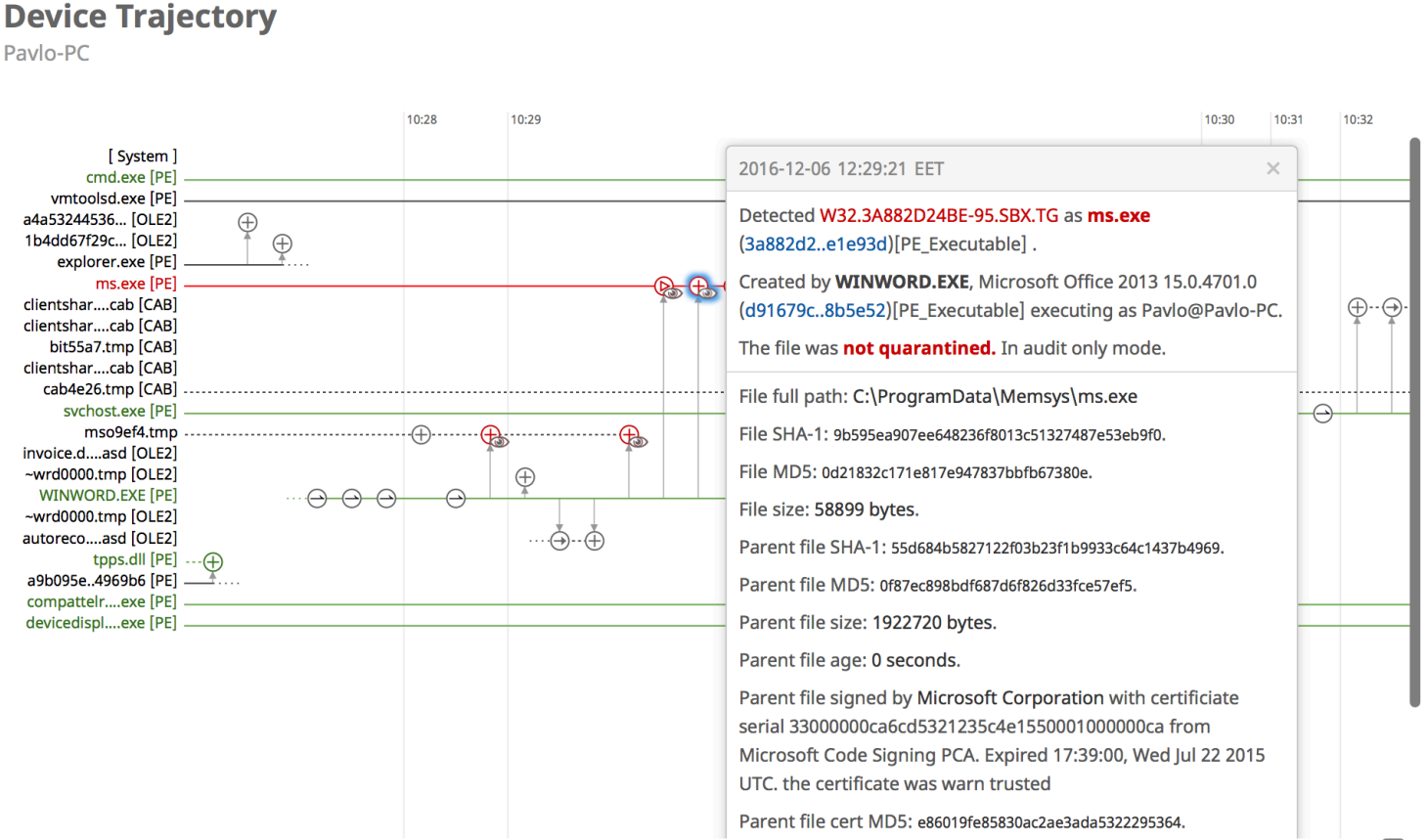


# Cisco Advanced Malware Protection

## Куда обращалось malware?

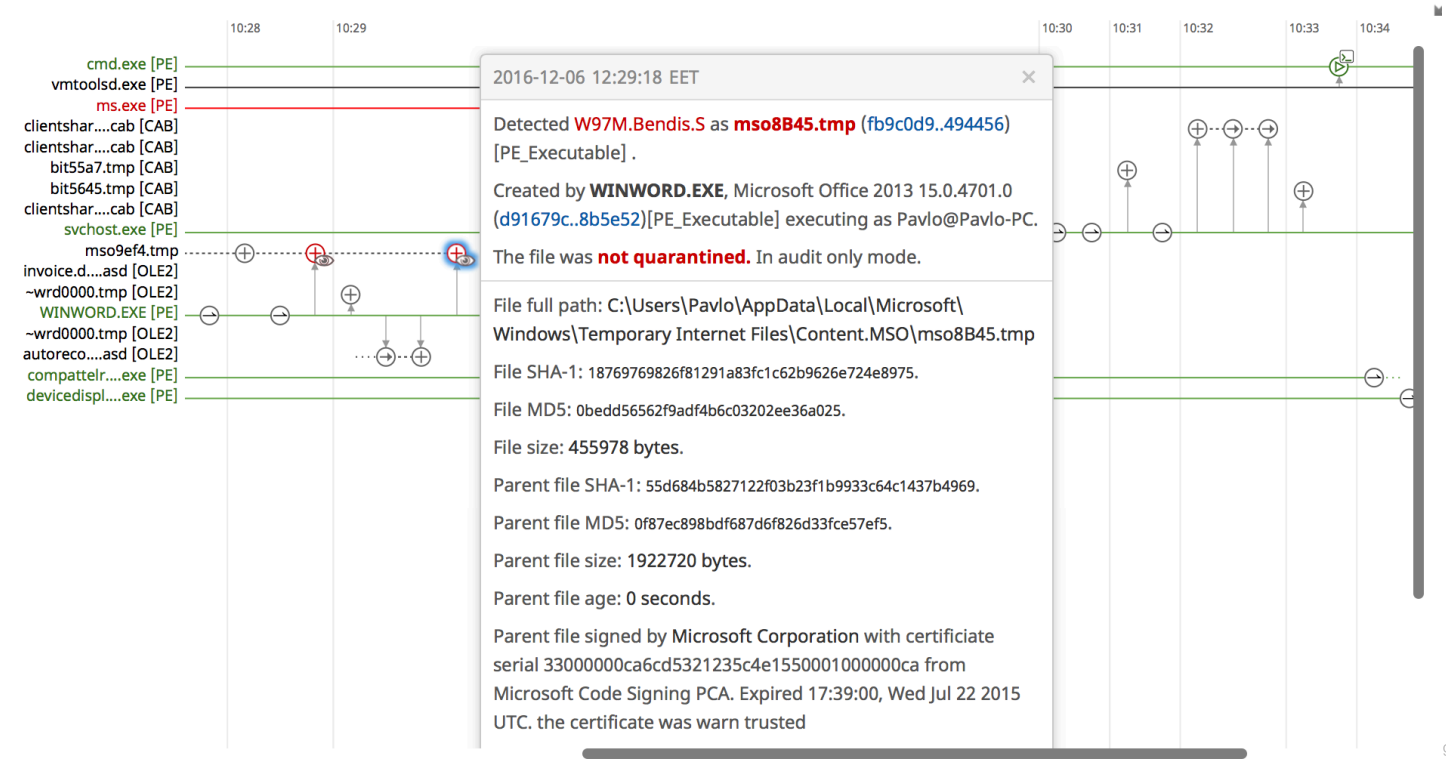


# Cisco Advanced Malware Protection
## История его появления?



# Cisco Advanced Malware Protection

## Как оно попало на компьютер?



# Быстрое время обнаружения

Обнаружить быстреее – меньше времени для атакующих, обеспечение более эффективной безопасности.

| Detection Time Scoring | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Time to Detect | Product A | Cisco | Product B | Product C | Product D | Product E | Product F | Product G | Product H |
| <1min | 44.40% | 67.00% | 0.60% | 48.90% | 46.20% | 5.50% | 7.30% | 6.50% | 3.60% |
| <3min | 75.90% | 91.80% | 2.90% | 88.70% | 84.20% | 31.30% | 17.90% | 17.10% | 26.70% |
| <5min | 86.60% | 96.30% | 6.50% | 91.00% | 88.40% | 47.80% | 27.60% | 27.00% | 66.20% |
| <10min | 97.40% | 96.60% | 15.20% | 95.60% | 91.30% | 85.00% | 43.10% | 42.50% | 90.10% |
| <30min | 97.90% | 97.10% | 85.80% | 98.50% | 93.10% | 96.90% | 76.40% | 75.40% | 94.00% |
| <60min | 98.20% | 97.90% | 90.80% | 98.70% | 93.10% | 98.20% | 97.90% | 89.20% | 96.30% |
| <120min | 98.50% | 98.50% | 90.80% | 98.90% | 94.30% | 98.40% | 98.50% | 89.70% | 96.60% |
| <240min | 98.90% | 99.20% | 91.60% | 99.00% | 97.60% | 98.90% | 98.50% | 89.70% | 96.80% |
| <480min | 99.00% | 99.40% | 95.80% | 99.00% | 98.70% | 99.40% | 98.90% | 90.00% | 99.70% |
| <720min | 99.20% | 99.70% | 96.40% | 99.40% | 98.70% | 99.50% | 98.90% | 90.10% | 99.80% |
| <1080min | 99.40% | 99.80% | 96.80% | 99.40% | 98.70% | 99.80% | 98.90% | 90.10% | 99.80% |
| <1440min | 99.40% | 100.00% | 96.80% | 99.40% | 99.00% | 100.00% | 98.90% | 90.10% | 99.80% |
| Overall Detection Score | **99.40%** | **100.00%** | **96.80%** | **99.40%** | **99.00%** | **100.00%** | **98.90%** | **90.10%** | **99.80%** |

- Мы блокируем атаки быстрее

| | |
|---|---|
| | = > 90% |
| | = 80 - 89% |
| | = 60 - 79% |
| | = 40 - 59% |
| | = < 40% |

NSS Labs Security Value Map for Breach Detection Systems - 2016

# Cisco Stealthwatch

## Обнаружение подозрительной сетевой активности


Active Alarms

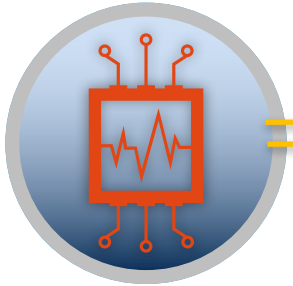
Alarms

Приложения

Тренд сбора потоков

# StealthWatch.

Превратите сеть в сенсор безопасности!



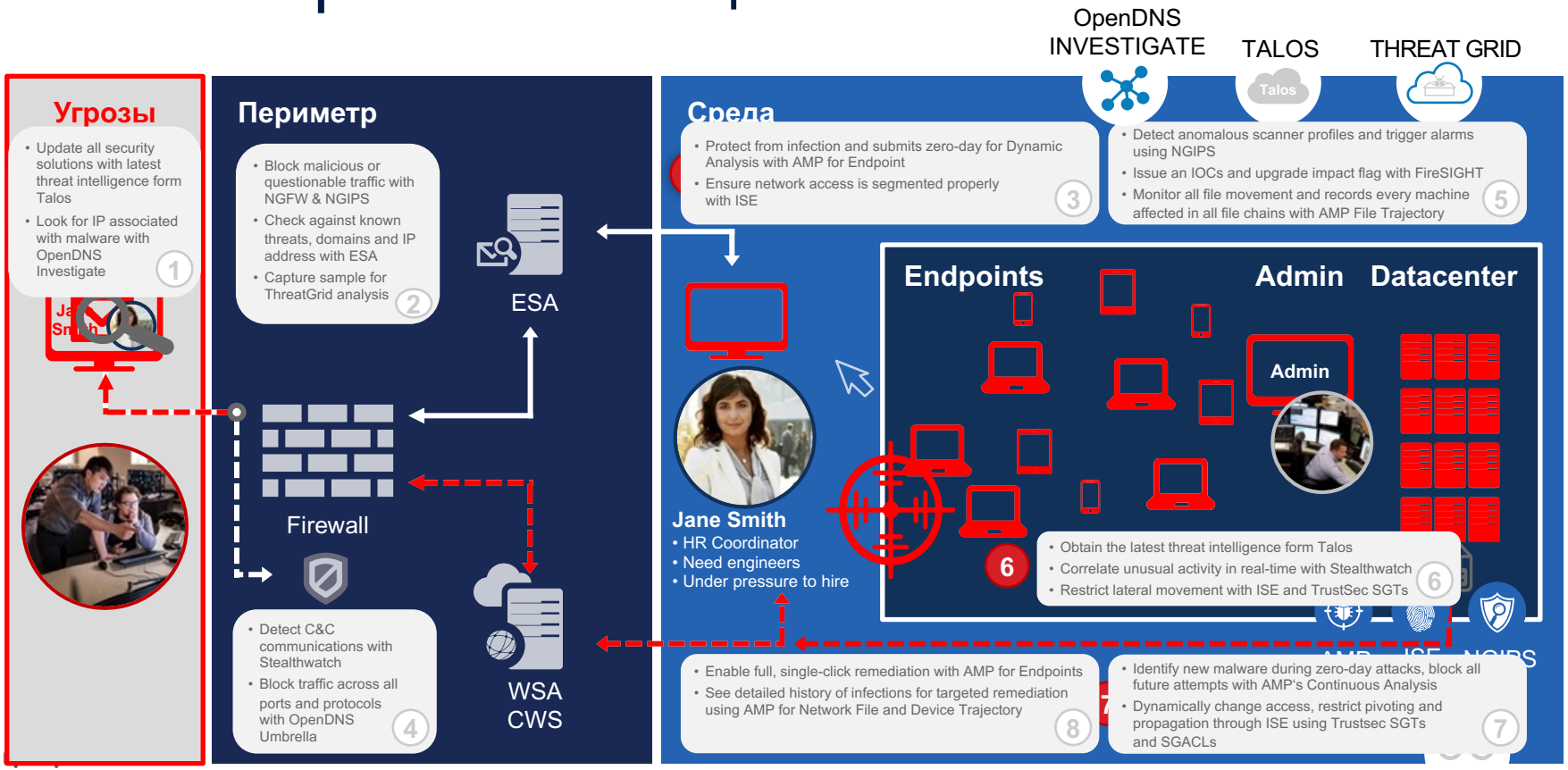
**Обнаружить Аномальные потоки трафика, Malware**

пример связь с вредоносными хостами, Распространение Malware внутри, Вывод (хищение) данных

**Обнаружить Использование приложений, Нарушение политики доступа пользователем**

пример Временный контрактник получает доступ к Финансовым Данным

# Эшелонирование защита




CISCO