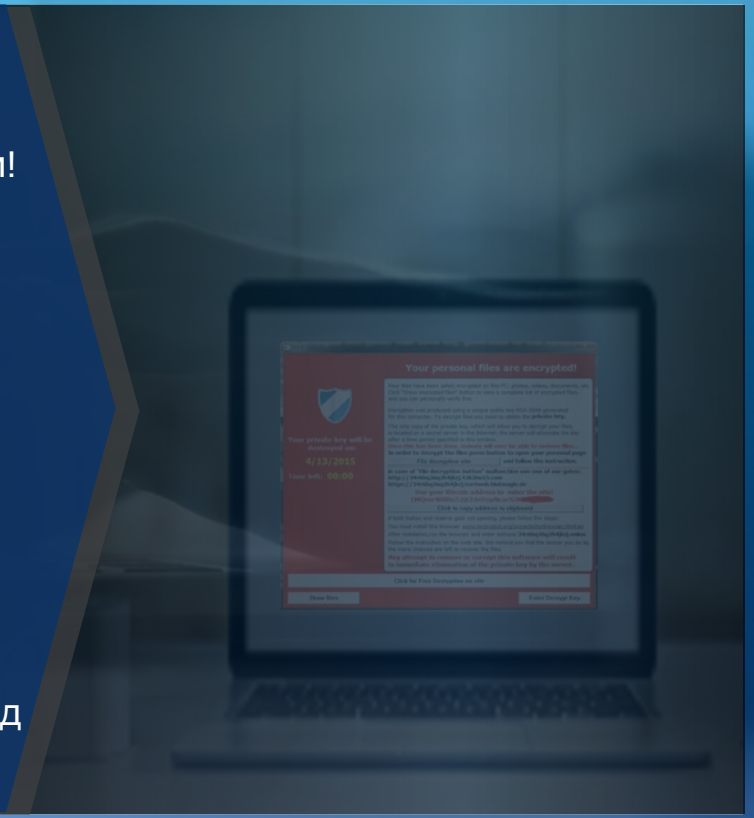
Борьба с современными целенаправленными угрозами – или как защититься ДО, ВО ВРЕМЯ и ПОСЛЕ атаки?

Руслан Иванов
Старший технический консультант по информационной безопасности
24 ноября 2016

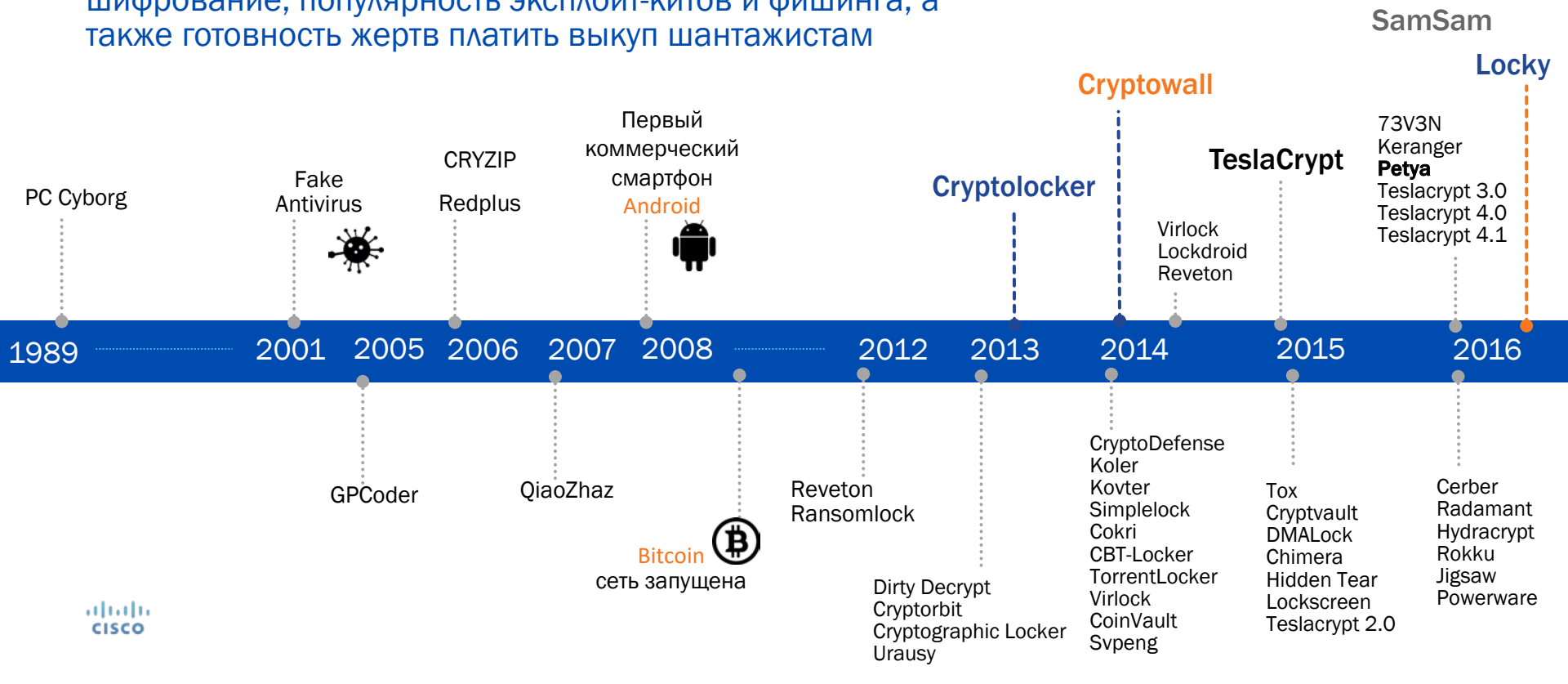
Очень лёгкие деньги для вымогателей

- Наиболее выгодное вредоносное ПО в истории
- Доходы: прямые платежи хакерам!
- Киберкриминал собрал $209 миллионов в первые три месяца 2016 путем вымогания денег у предприятий за разблокировку компьютеров
- Вымогатели зарабатывают до $1 миллиарда в год
- Только один пример:
  - Посмотрите на эксплойт-кит Angler, доставляющий вымогательское ПО
  - $60 миллионов долларов в год

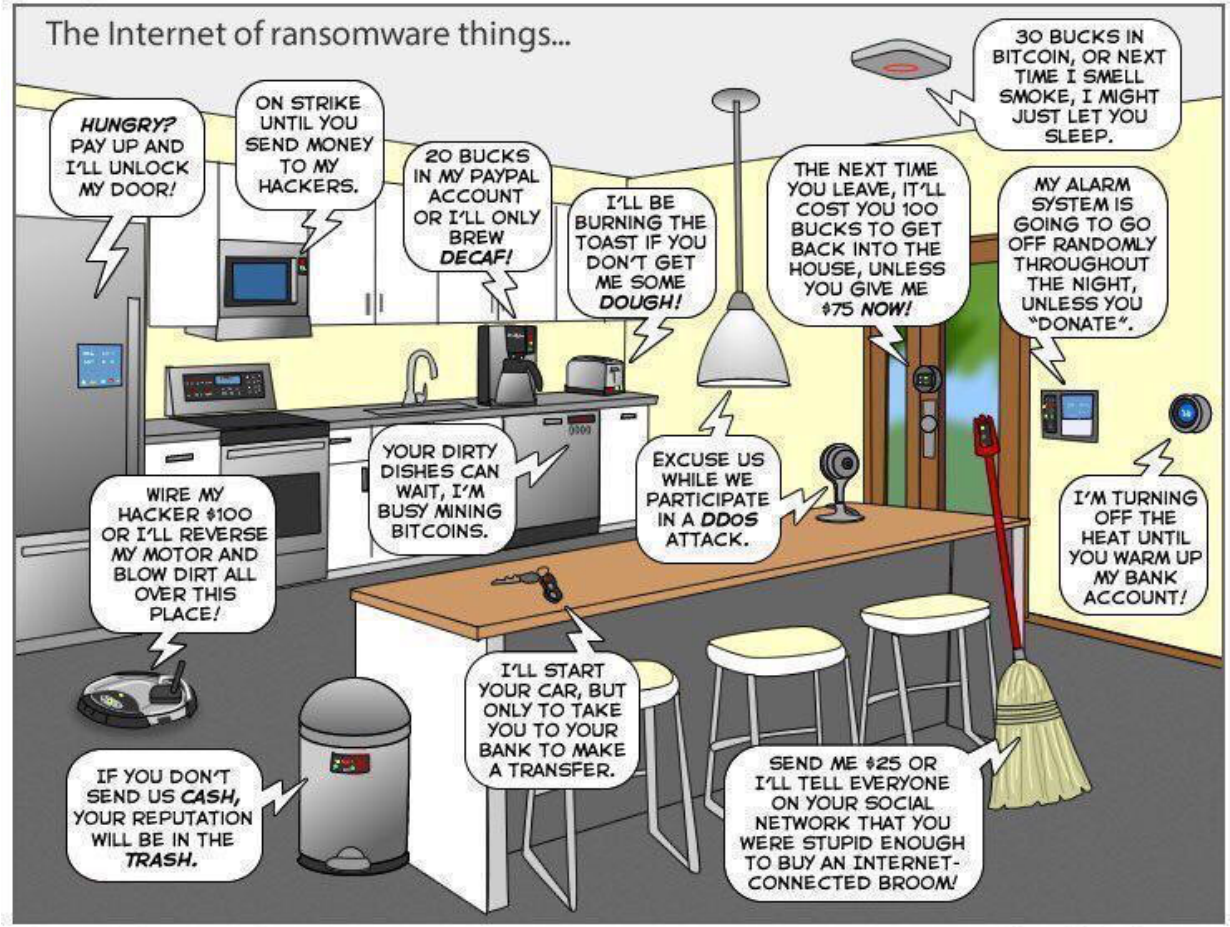


Эволюция вариантов вредоносов-шифровальщиков

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

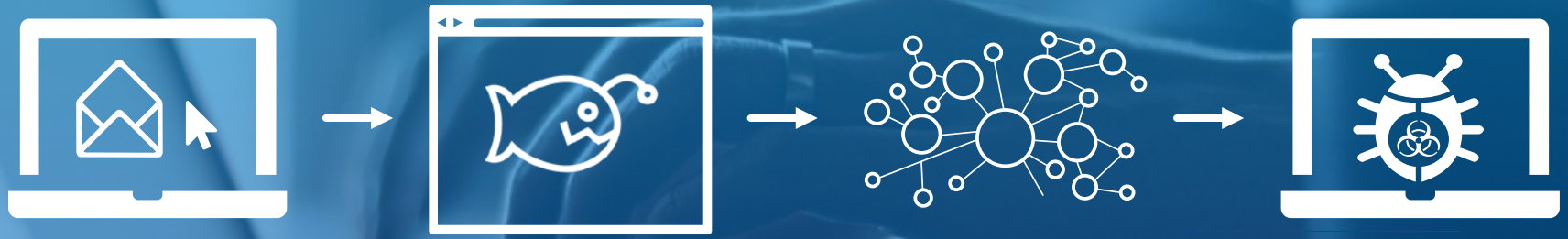


The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

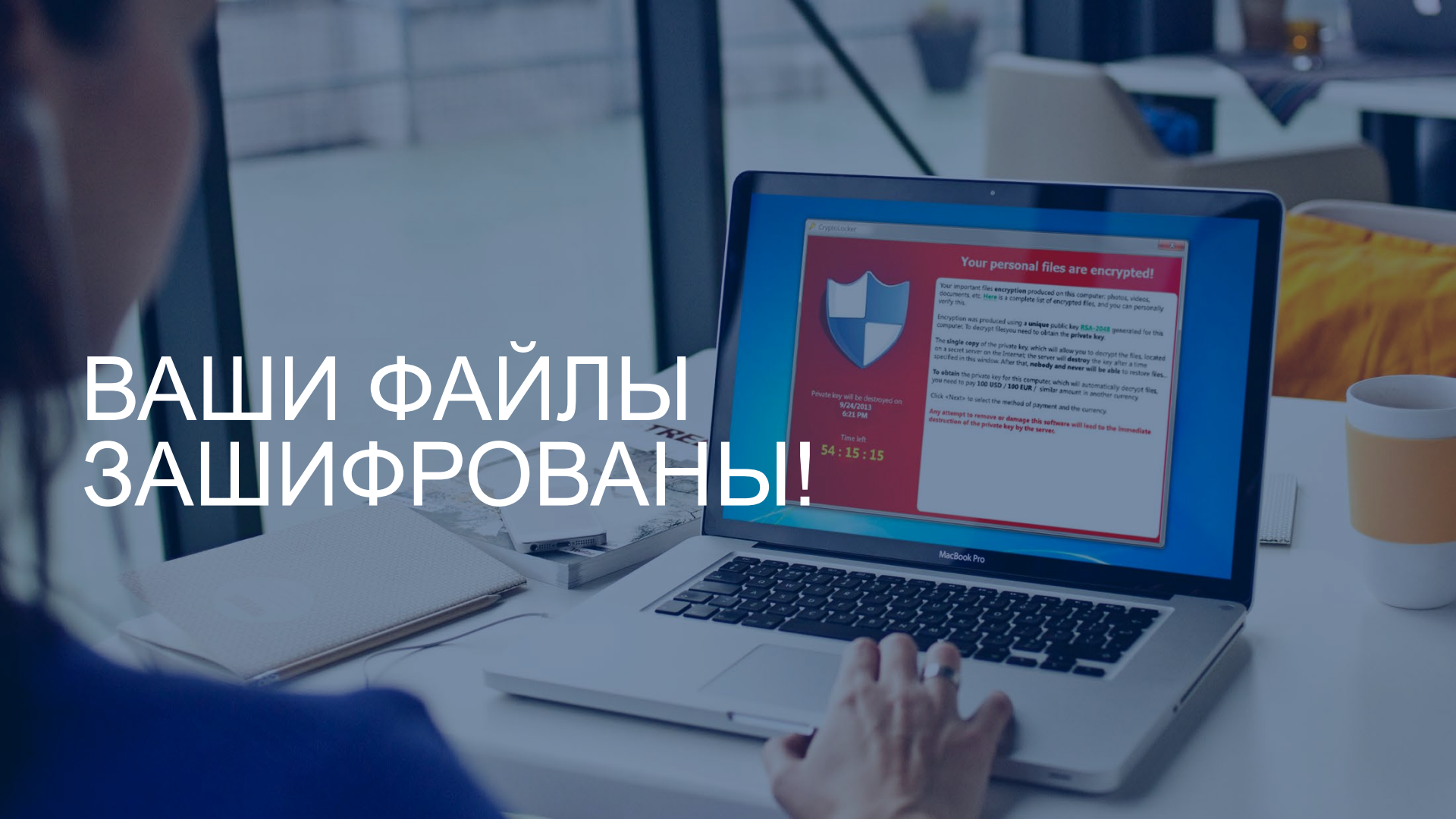


Пользователь кликает по ссылке или открывает вложение в e-mail

Вредоносный код запускается

Вредоносная инфраструктура

Загрузка расширений вредоносного кода


ВАШИ ФАЙЛЫ
ЗАШИФРОВАНЫ!
CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click <Next> to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.
Private key will be destroyed on
9/24/2013
6:21 PM
Time left
54 : 15 : 15
MacBook Pro

Решение Cisco по защите от вымогателей

Решение Cisco по защите от вымогательского ПО – это не серебряная пуля и не гарантирует 100%-й защиты. Однако оно способно помочь:

- Предотвратить попадание вымогательского ПО в сеть или на ПК, когда это возможно
- Остановить его до того, как оно будет управляться извне
- Обнаружить, когда оно появится в сети
- Локализовать его для защиты от распространения по сети
- Обеспечить реагирование для устранения уязвимостей и локализации атакованных участков

[1]Gartner Report “Office 365, Google Apps for Work and Other Cloud Office Key Initiative Overview” July 2015

Элементы решения Cisco по защите от вымогательского ПО

- Threat intelligence – знание о существующих вымогателях и способах их коммуникаций

- Защита E-mail – блокирование вложений и ссылок в сообщениях

- Защита Web – блокирование web-коммуникаций с инфицированными сайтами и файлами

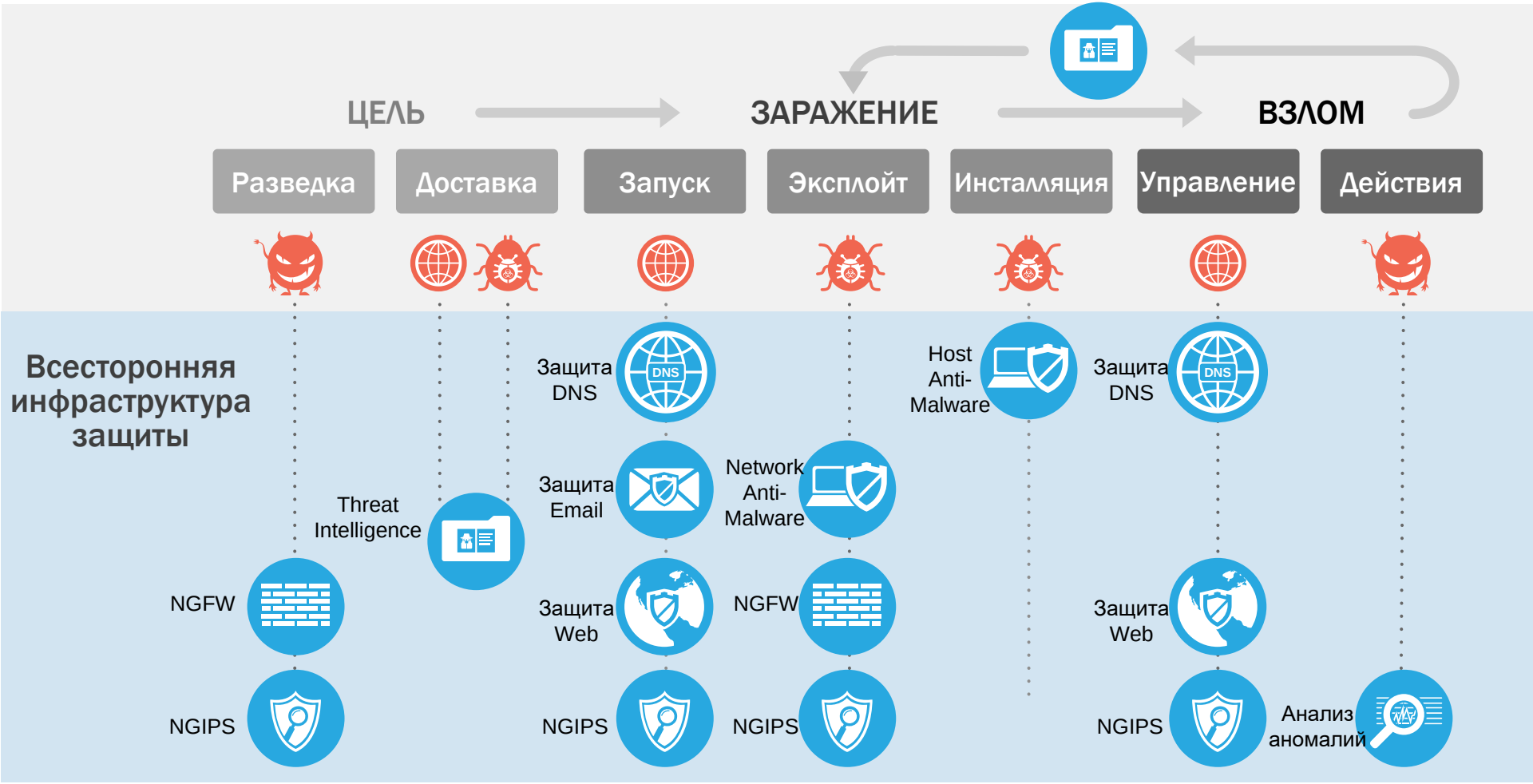
- Защита DNS – прерывание взаимодействия с узлами Command & Control

- Защита ПК – инспектирование файлов, карантин и удаление

- Сегментация – контроль доступа, разделение трафика на базе ролей и политик

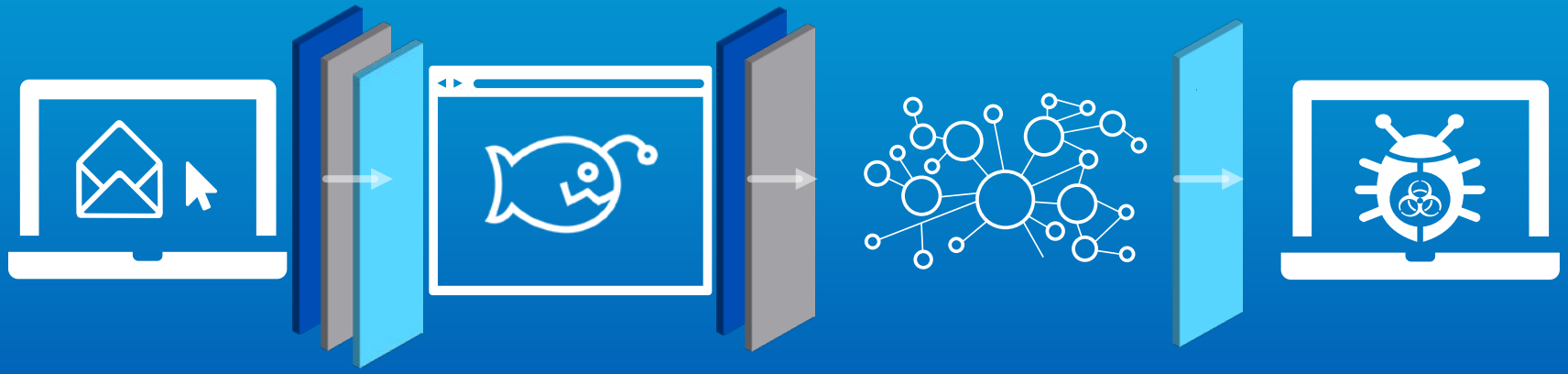
- Предотвращение вторжений – блокирование атак, эксплойтов и разведки

- Мониторинг аномалий – идентификация и оповещение об аномалиях в сети


ЦЕЛЬ
ЗАРАЖЕНИЕ
ВЗЛОМ
Разведка
Доставка
Запуск
Эксплойт
Инсталляция
Управление
Действия
Всесторонняя инфраструктура защиты
Защита DNS
Host Anti-Malware
Защита DNS
Threat Intelligence
Защита Email
Network Anti-Malware
NGFW
Защита Web
NGFW
Защита Web
NGIPS
NGIPS
NGIPS
NGIPS
Анализ аномалий

Джентльменский набор Cisco

Cisco Umbrella Next-Gen Firewall AMP

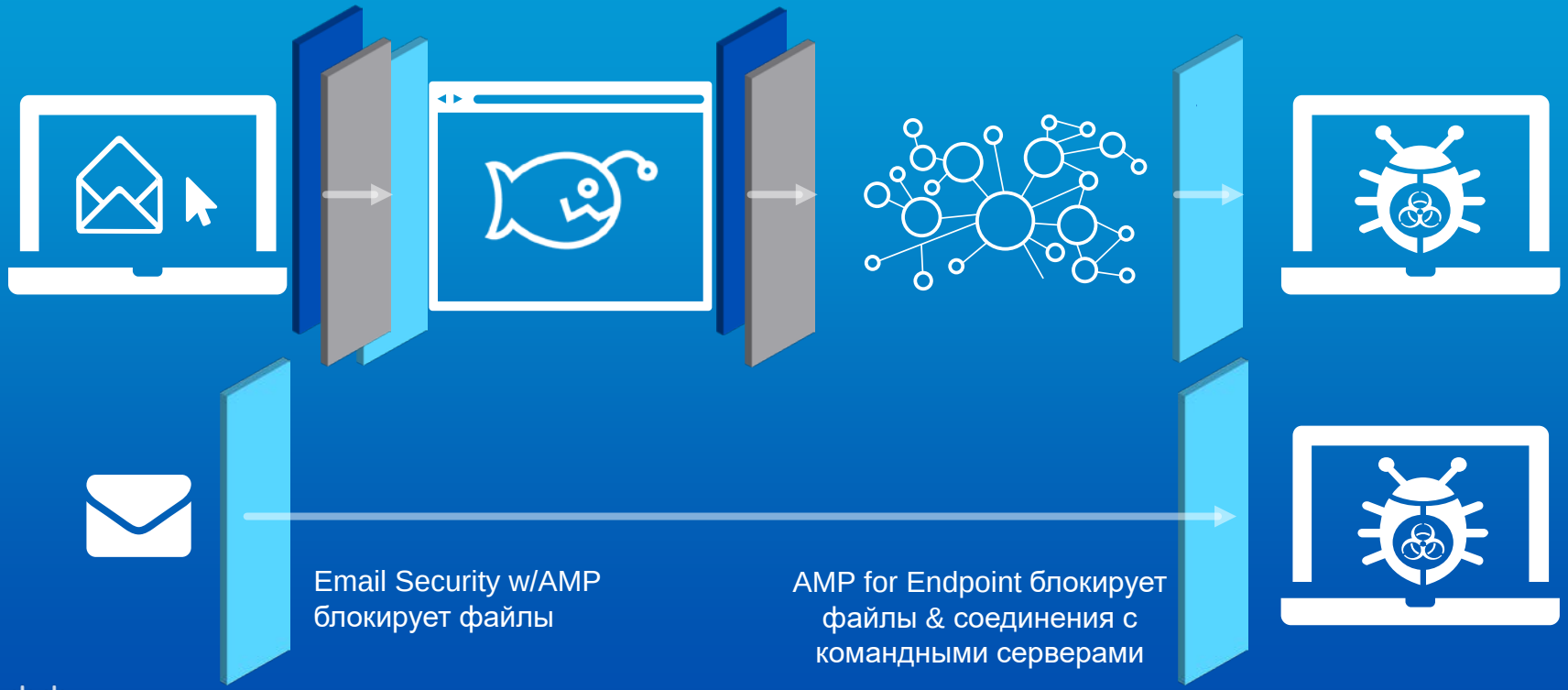


OpenDNS блокирует запросы
NGFW/NGIPS блокирует соединения

OpenDNS блокирует запросы
NGFW/NGIPS блокирует соединения

AMP for Endpoint блокирует файлы & соединения с командными серверами

Cisco Umbrella Next-Gen Firewall AMP



Email Security w/AMP
блокирует файлы

AMP for Endpoint блокирует
файлы & соединения с
командными серверами


Cisco Umbrella
CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click <Next> to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.
Private key will be destroyed on
9/24/2013
6:21 PM
Time left
54 : 15 : 15
MacBook Pro

Какие протоколы используют вымогатели?

Шифрование канала управления ботнетом				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

Cisco Umbrella

Новый уровень обнаружения проникновений с возможностью внутри сети видеть то, что обычно видно только в Интернет

Расширение ATDs (AMP Threat Grid, FireEye, Check Point) за периметром и получение немедленного ответа на ваши IOCs

Обнаружение целевых атак на вашу компанию по сравнению с тем, что происходит в мире

Расследование атак, используя «живую» карту Интернет-активности

Что отличает Cisco Umbrella?

UMBRELLA

Применение политик

Предотвращение угроз
Не просто обнаружение угроз

Защита внутри и вне сети
Не ограничивается устройствами, передающими трафик через локальные устройства

Постоянное обновление
Устройству не нужно обращаться к VPN на локальном сервере для получения обновлений

Блокировка каждого домена для всех портов
Не только IP-адреса или домены только через порты 80/443

Интеграция с партнерским и пользовательским ПО
Не требует услуг профессионалов при настройке

Cisco Advanced Malware Protection (AMP)

Непрерывный анализ и ретроспективная безопасность

Через все точки контроля


Email

Web


Сеть


ПК


Мобильные устройства

Воспользуйтесь ключевыми возможностями


Идентификация точки входа


Слежение за распространением угрозы


Обнаружение точек заражения/компрометации


Анализ поведения


Оперативные локализация и восстановление

Для ответа на вопросы, которые действительно вас волнуют…

Усильте безопасность за счет передовых технологий исследований угроз

100 ТБ
данных ежедневно

1.5 МИЛЛИОНОВ
семплов ежедневно

600 МИЛЛИАРДОВ
сообщений Email ежедневно

16 МИЛЛИАРДОВ
Web-запросов ежедневно

TALOS

24 • 7 • 365 операции

250+
исследователей угроз

МИЛЛИОНЫ
агентов телеметрии

4
Глобальных ЦОДов

Свыше 100
партнеров Threat Intelligence

Глобальное сканирование

30 лет построения сетей по всему миру

Защита от вымогательского ПО от ПК до облака

Email Security

В сети или в облаке

Блокирует до 99% спама, уровень ложных срабатываний - 1 на 1 миллион писем

Umbrella

Безопасность из облака

Блокирует 95% угроз до того, как они нанесут ущерб

Next-Gen Firewall/IPS

Приоритезация угроз

Автоматический ответ

Улучшенное обнаружение вредоносного ПО

AMP

Увидев угрозу однажды, блокирует её везде

Наиболее эффективное решение для известных и целевых угроз

Что дальше?

- Подпишись на вебинары Cisco Security Expert, чтобы больше узнать о том, как технологии Cisco помогают решать ваши задачи

(http://www.cisco.com/c/m/en_uk/events/2016/securityexperts/index.html)

- Запланируйте тестирование OpenDNS

(https://www.opendns.com/enterprise-security/)

- Узнайте больше о решении Cisco по борьбе с вымогателями http://www.cisco.com/c/en/us/solutions/enterprise-networks/ransomware-defense/index.html
- Остались вопросы? Пишите на security-request@cisco.com

Просто | Открыто | Автоматизировано | Эффективно

CISCO SECURITY