Стратегия защиты компаний от целенаправленных атак и программ-вымогателей

Владимир Илибман
Cisco Systems

3 ноября 2017 года

АТАКУЮЩИЕ

VS

ЗАЩИТНИКИ

Ландшафт угроз

Как произошел переход от спама и надоедливой рекламы к деструктивным программам

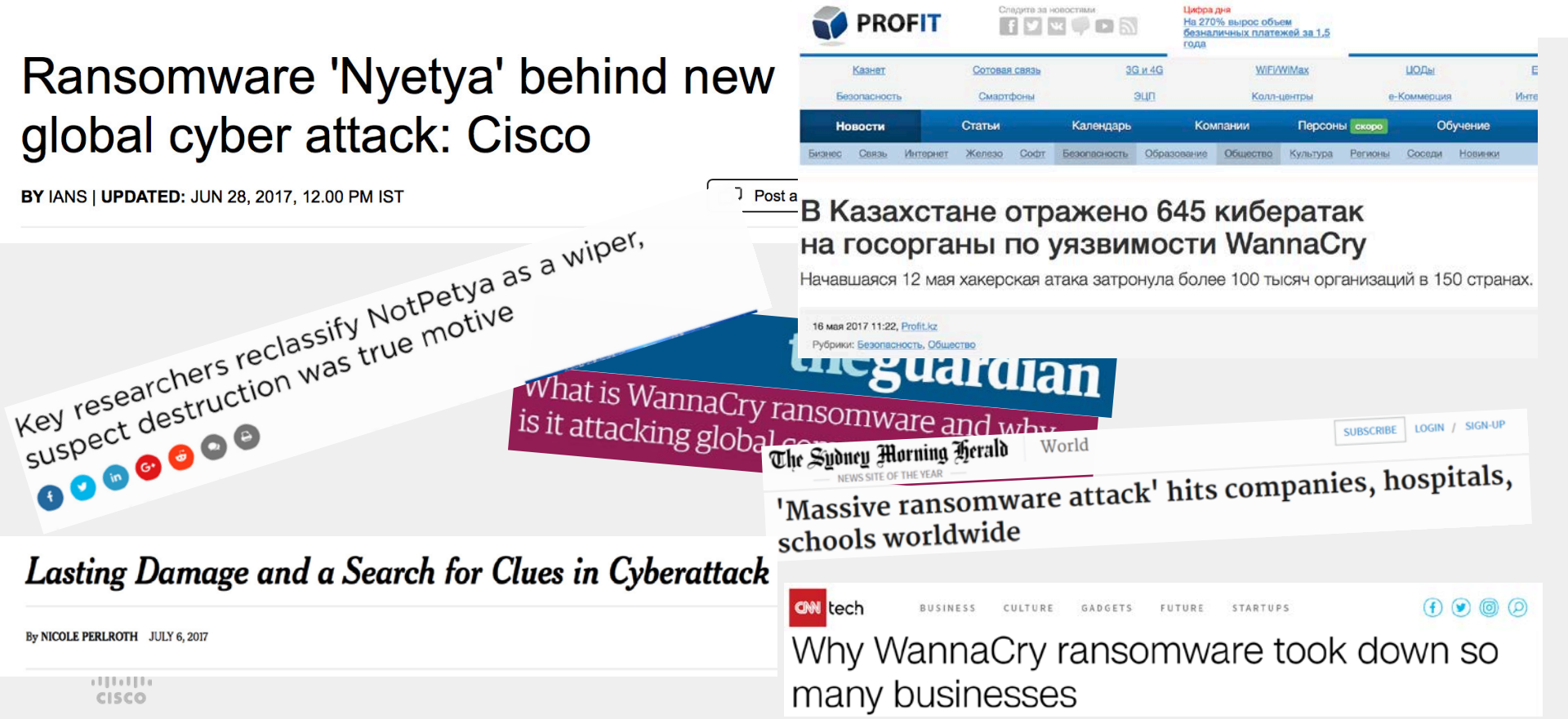
Обзор уязвимостей и спам-вирусов, январь 2016 г.

Ransomware Downloader Backdoor
Banker Botnet AdFraud
Other

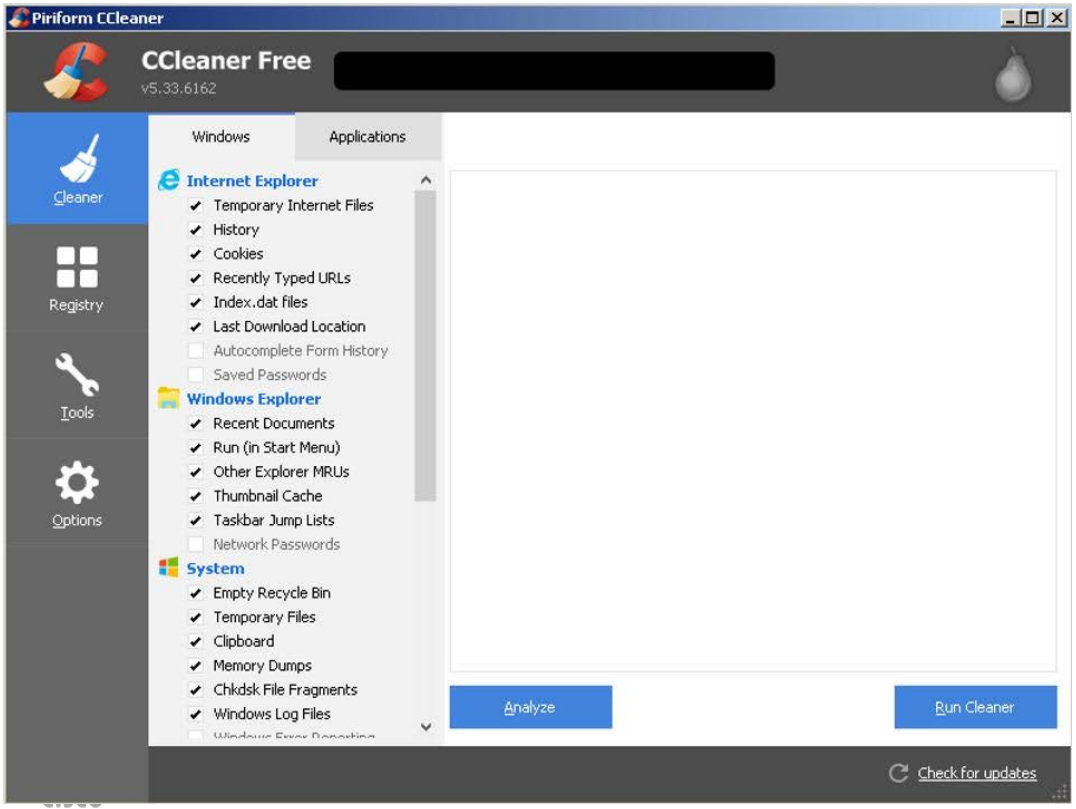
Обзор уязвимостей и спам-вирусов, ноябрь 2016 г.

Ransomware Downloader Backdoor
Banker Botnet AdFraud
Other

Масштабные атаки всегда освещались в новостях



CCleaner. Кандидат на золото. сентябрь 2017



- Cisco Talos обнаружили вредоносный код в популярной утилите CCleaner от компании Avast.
- Бэкдор позволяет злоумышленникам загружать дополнительное вредоносное ПО для шпионажа
- Скомпрометированная версия CCleaner была загружена **2,27 млн раз.**

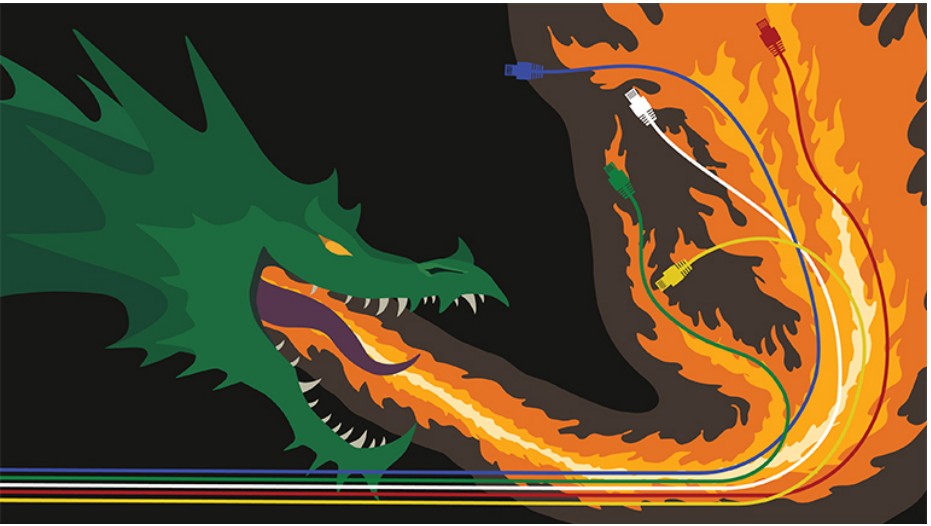
http://blog.talosintelligence.com/2017/07/the-medoc-connection.html

Атака WannaCry
Май 2017

https://www.youtube.com/watch?v=_VeKNYBzhw0

[25855, 'RU']
[22986, 'CN']
[7614, 'TW']
[5966, 'UA']
[5054, 'US']
[3087, 'CA']
[2195, 'KR']
[1712, 'FR']
[1394, 'IN']
[1132, 'BR']
[943, 'HK']
[656, 'JP']
[651, 'GB']
[546, 'DE']
[518, 'PL']
[517, 'CL']
[480, 'MX']
[436, 'IT']
[430, 'VN']
[403, 'AM']
[397, 'KZ']
[363, 'RO']
[362, 'AR']
[337, 'MD']
[330, 'PH']

Nyetya. Он же Petya-A. Он же Не-Петя
Июнь 2017



- Использовал доверенный канал бухгалтерского ПО для доставки в организации
- Использовал гибридную методологию распространения
- Шифровал файлы не с целью получения выкупа, а для нанесения урона

Расследование атаки от группы Cisco Talos
http://blog.talosintelligence.com/2017/07/the-medoc-connection.html

24 октября 2017

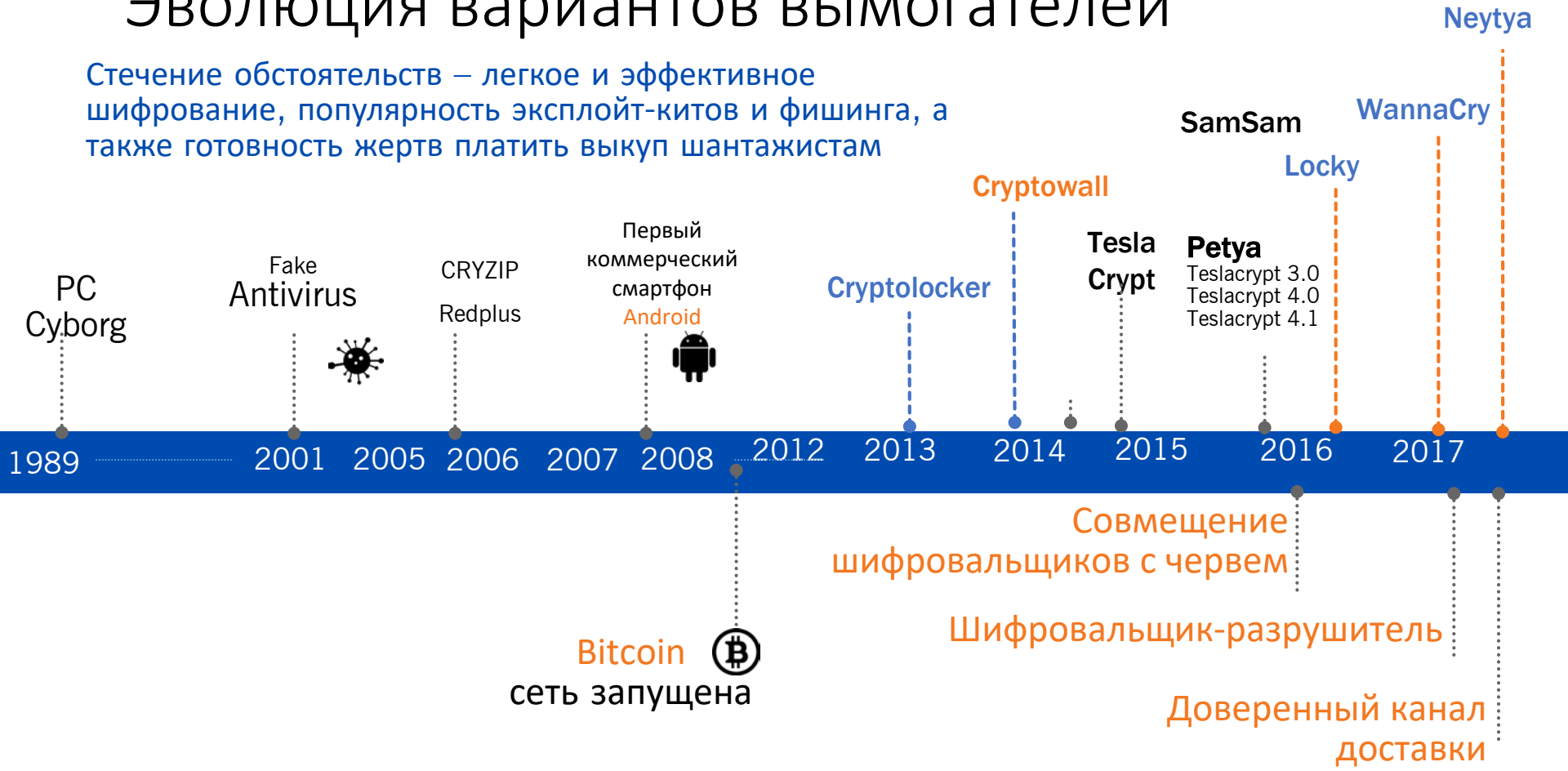
Следуй за «плохим кроликом»!

- BadRabbit -- массовая ransomware кампания
- Поражены организации в
- России, Украине, Болгарии, Турции
- Основной вектор заражения – поддельное обновление Adobe Flash
- Использует методы последовательного распространения из Petya/Nyetya

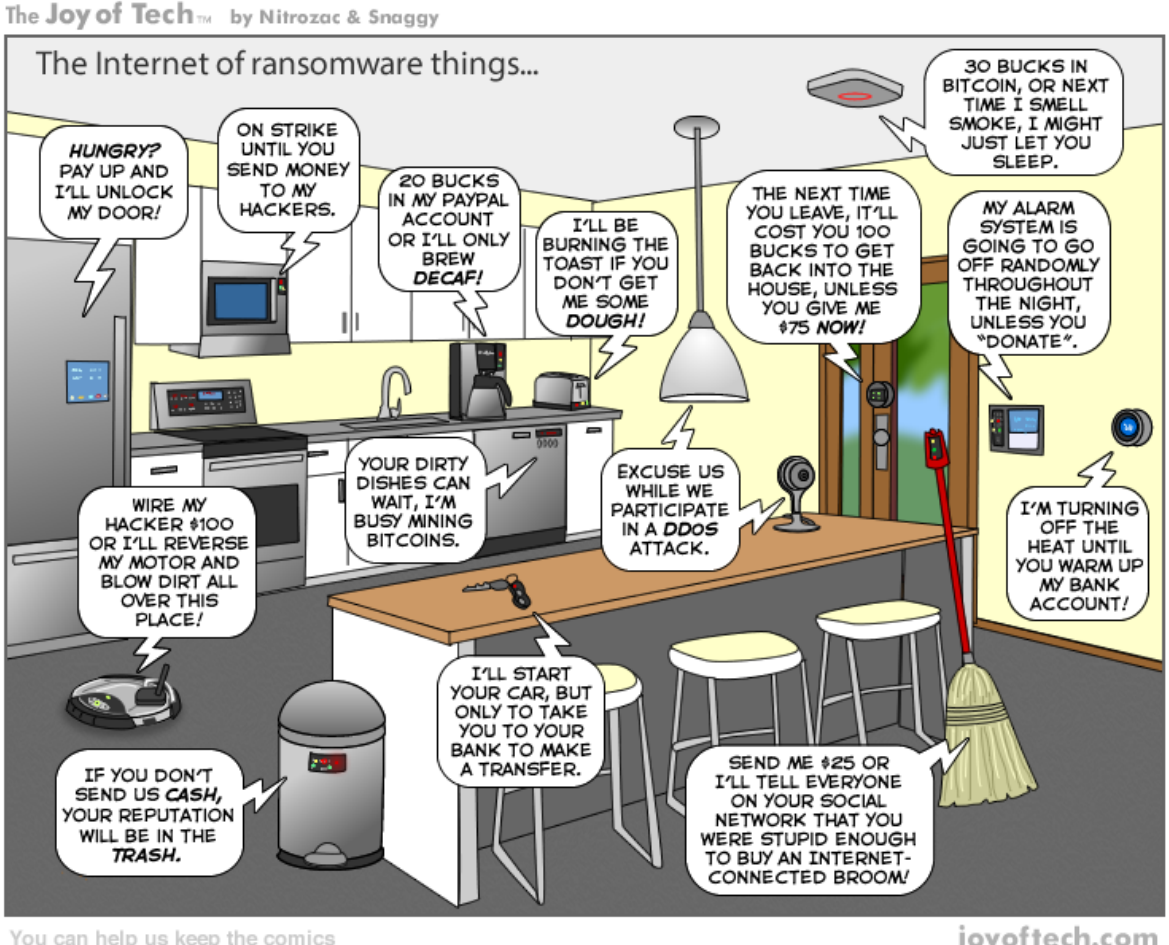
Расследование атаки от группы Cisco Talos
http://blog.talosintelligence.com/2017/10/bad-rabbit.html

Эволюция вариантов вымогателей

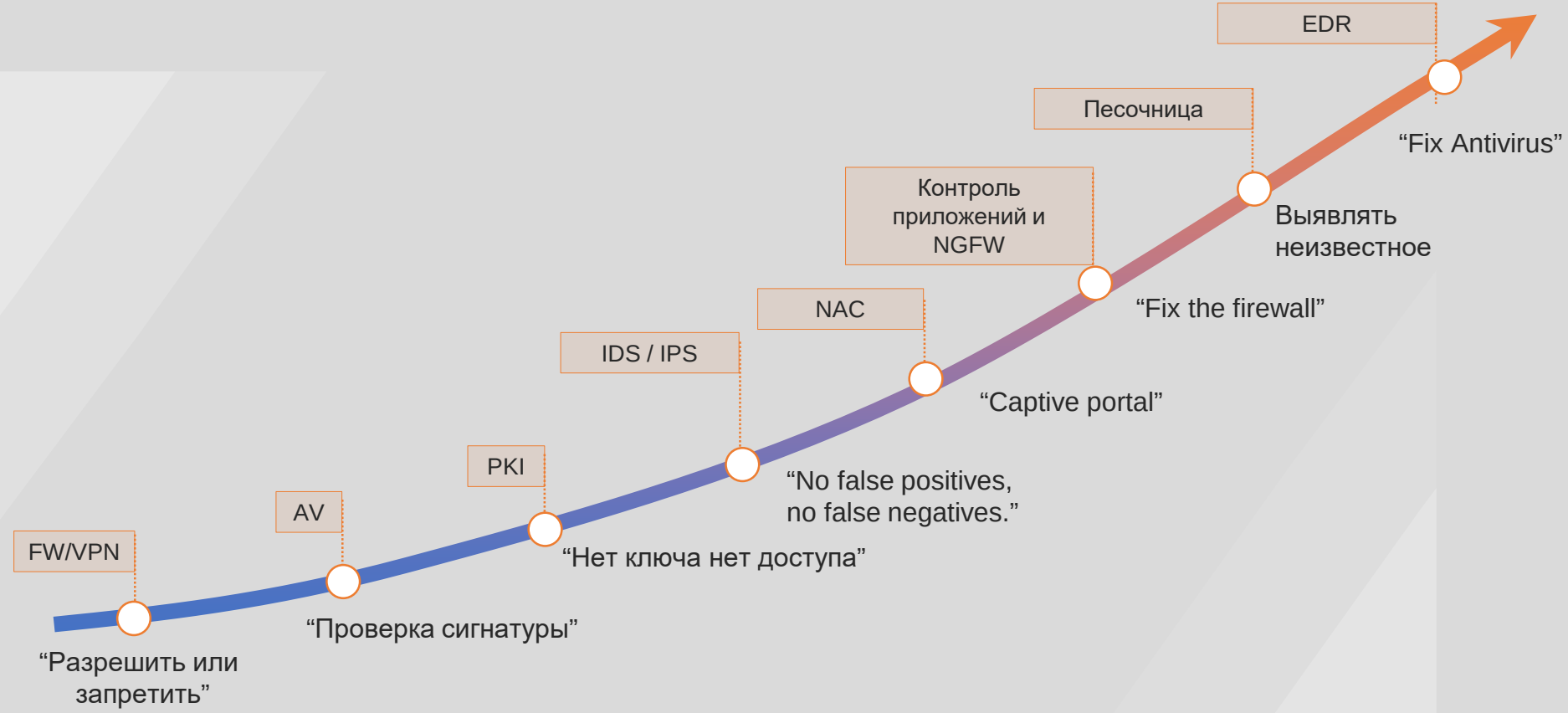
Стечение обстоятельств – легкое и эффективное шифрование, популярность эксплойт-китов и фишинга, а также готовность жертв платить выкуп шантажистам



Интернет вещей-вымогателей



В безопасности не существует единой серебряной пули



Мифы ИБ, развенчанные атаками 2017

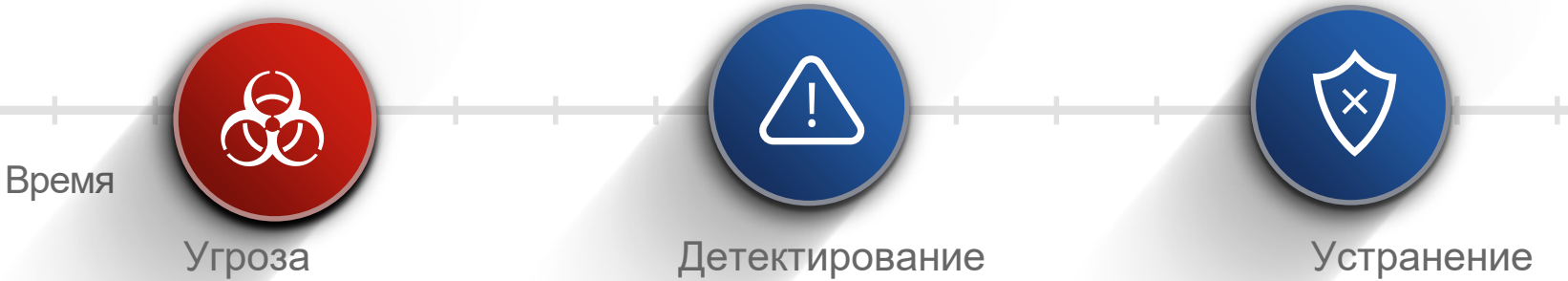
1. Обновлений ОС хватает для защиты
2. Антивирусы с эвристикой могут предотвратить заражение
3. Файервол нового поколения останавливает атаку
4. Песочница – это панацея
5. Пользователь и фишинг – причины всех бед

Более эффективная стратегия это нарушить алгоритм злоумышленников

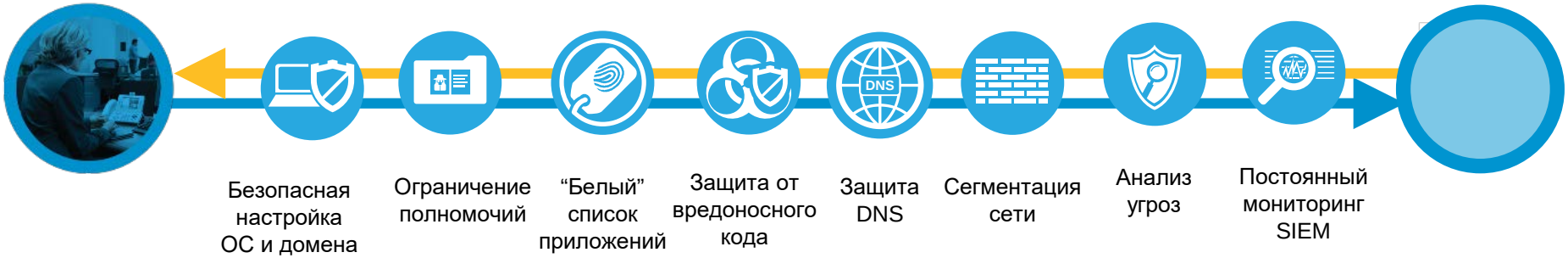
Цепочка атаки – Kill Chain

Целостный подход позволяет разрушить цепочку атаки

Рассматривайте ВРЕМЯ реагирования как новую метрику эффективности ИБ

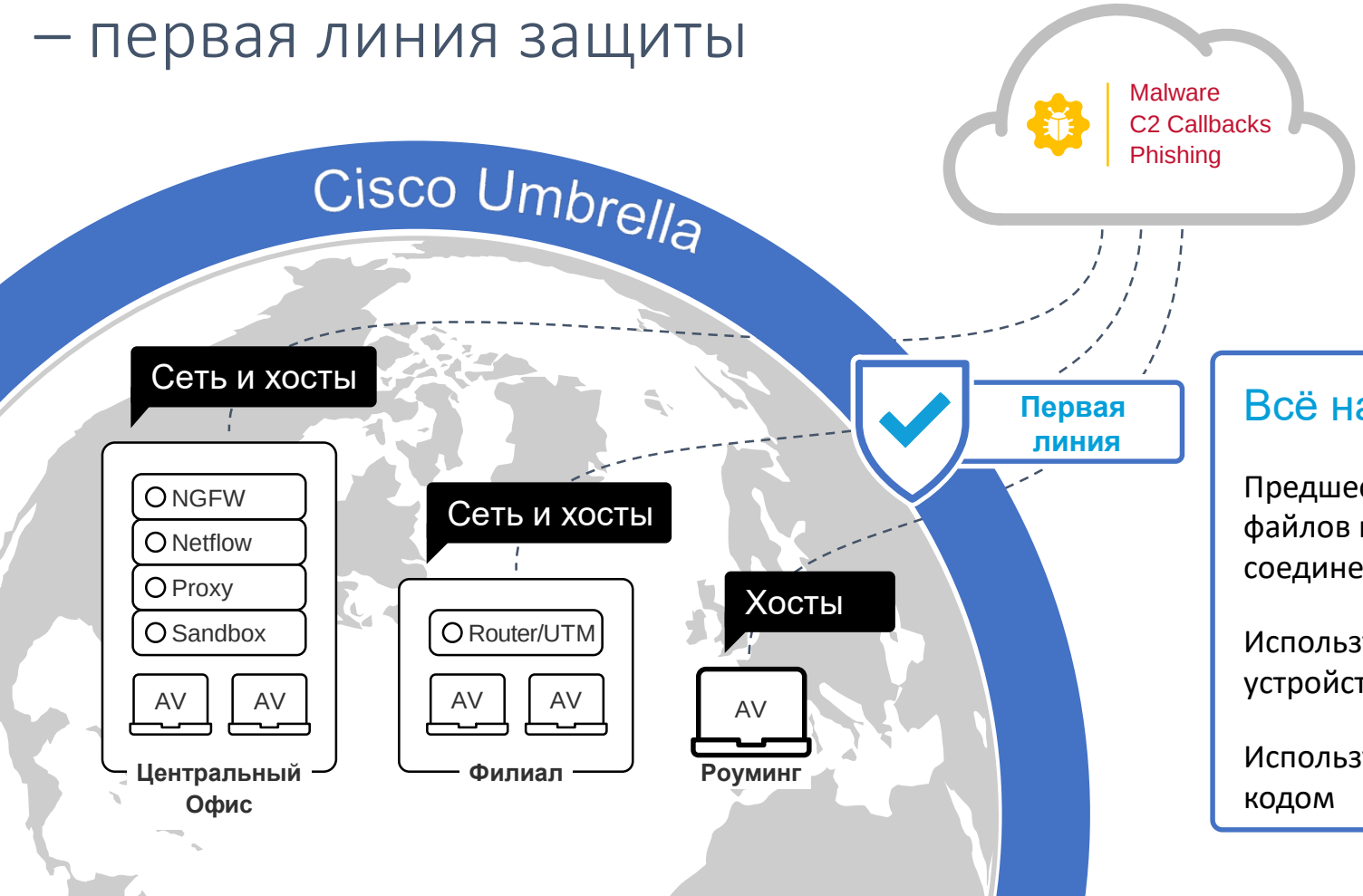


Какие технологии помогают до, во время и после атаки программы-вымогателя



Фильтрация запросов по DNS и IP – первая линия защиты

DNS



Всё начинается с DNS

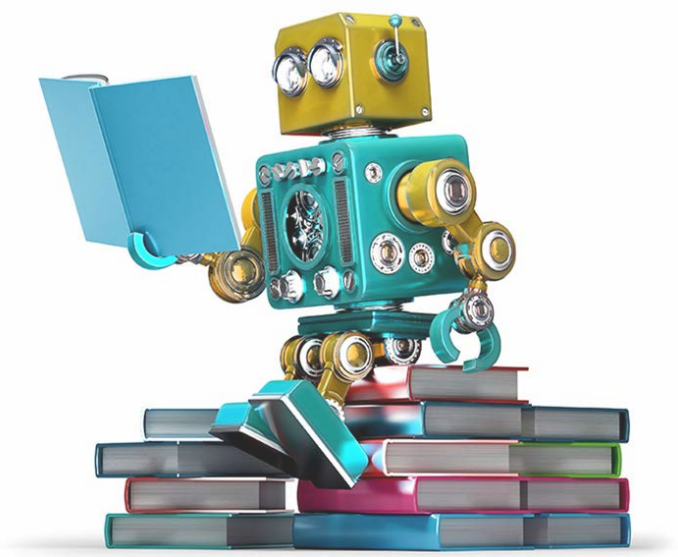
Предшествует открытию файлов и установлению IP соединения

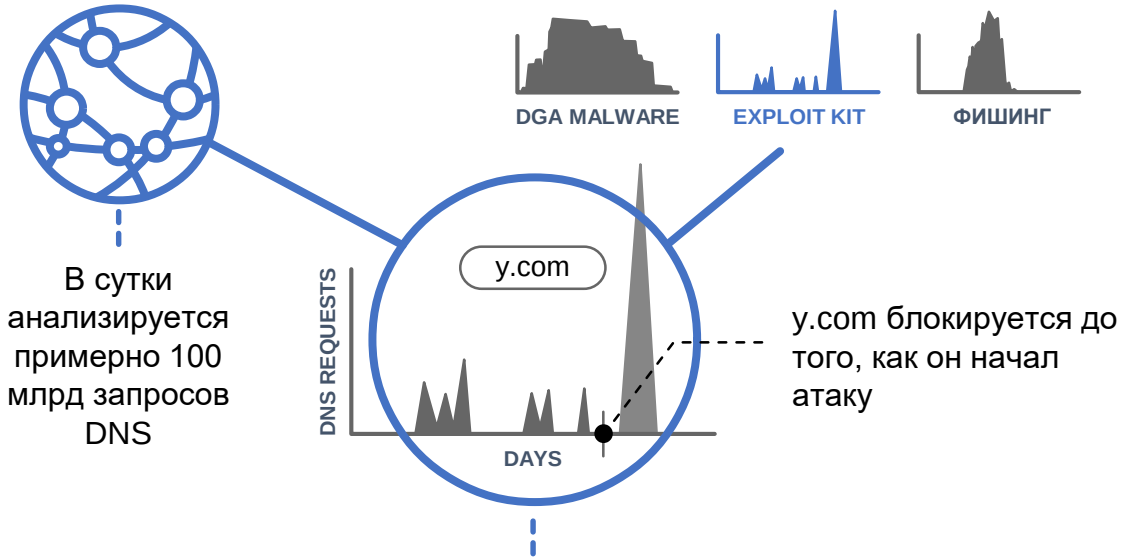
Используется всеми устройствами

Используется вредоносным кодом

Предупреждение будущих атак

Шаблоны плохих ресурсов





В сутки анализируется примерно 100 млрд запросов DNS

y.com блокируется до того, как он начал атаку

Изучается структура DNS запросов по известным машинным шаблонам

Следуй за «Плохим кроликом»

Details for 1dnscontrol.com

SEARCH IN GOOGLE

SEARCH IN VIRUSTOTAL

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 5.61.37.209

This domain is currently in the Umbrella block list

This domain is associated with the following type of threat: Ransomware

Classifier prediction: benign

Umbrella risk score: +100

DNS queries

DNS queries/hour

2k

1k

Tuesday, Oct 24, 17:00
Queries: 1,375

28. Sep 30. Sep 2. Oct 4. Oct 6. Oct 8. Oct 10. Oct 12. Oct 14. Oct 16. Oct 18. Oct 20. Oct 22. Oct 24. Oct

Модель подводной лодки в безопасности

Ограничить сферу распространения malware

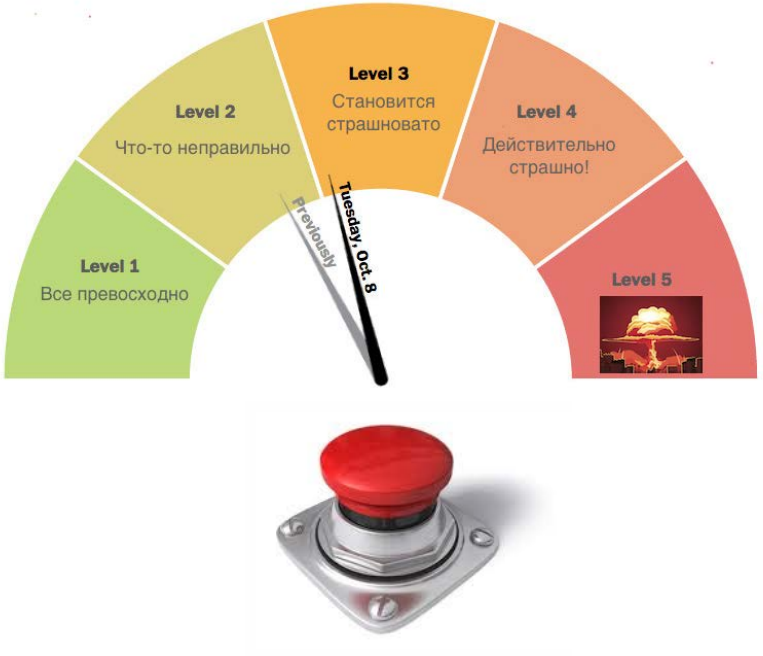
- Разбейте сеть на небольшие сегменты
- Ограничивайте трафик между сегментами (запрещено все, что не разрешено)
- Динамическая мигросегментация

Динамическая микросегментация

Политики в зависимости от уровня угрозы DefCon

Standard Policy

Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	✓	–	–	–	–	✓	✓	–
LoB 2 Employee	–	✓	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	✓	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

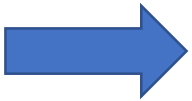


DEFCON3 Policy

Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	–	–	–	–	–	✓	✓	–
LoB 2 Employee	–	–	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	–	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

Процесс реагирования на инциденты

Киберучения для специалистов



Ключевой вопрос для внедрения стратегии

Почему кибербезопасность – это основа бизнеса

Потери от WannaCry составили $1млрд

McClatchy

Потери от Petya.A составили $850 млн

Страховая компания Lloyd's

Глобальная кибератака может спровоцировать экономические потери в среднем на $53 млрд

Страховая компания Lloyd's