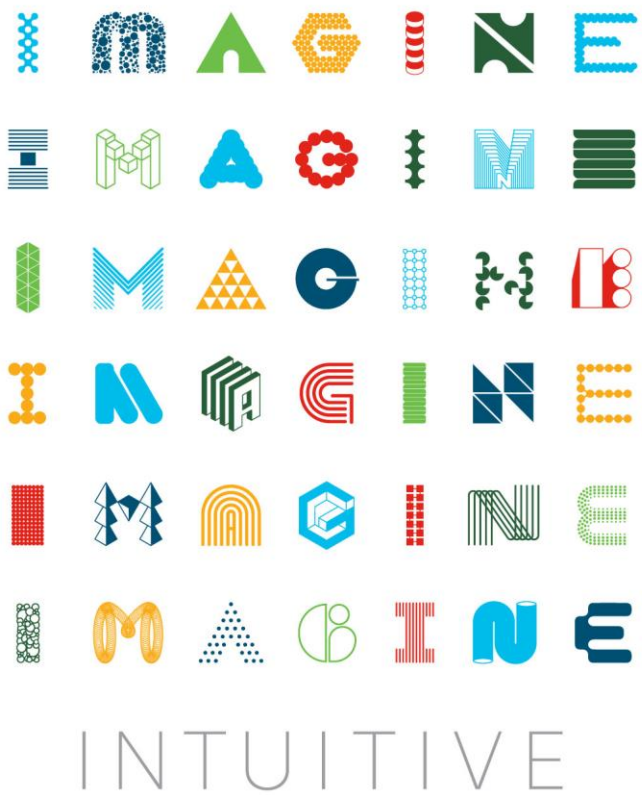
# Основные угрозы кибербезопасности

## Что действительно важно предпринять

Лукацкий Алексей, бизнес-консультант по ИБ




Emotet был в тени долгие годы. Эта тактика позволила ему быстро. Стать сегодня одним из самых успешных семейств вредоносного ПО.

Email остается вектором №1.

Есть некоторая разница между ПО для криптомайнинга, устанавливаемым пользователем и хакерским ПО для криптомайнинга

Olympic Destroyer был очень деструктивным и разработан для уничтожения информации.

VPNFilter показал новый вектор атаки, оставаясь угрозой для многих IoT-проектов

# Emotet

- Emotet был в тени, выйдя на первый план совсем недавно и быстро заняв первое место
- Начался как банковский троян
- Трансформирования в сеть распространения вредоносного кода
- Модульная архитектура с разным назначением модулей
- Доставляется через спам-кампании

# Business Email Compromise (BEC)


- Только 5% BEC-схем используют скомпрометированные учетные записи
  - 2/3 используют бесплатные учетные записи в web-почте
  - 28% атак с зарегистрированных доменов
- 1 из 5 BEC emails включает имя жертвы

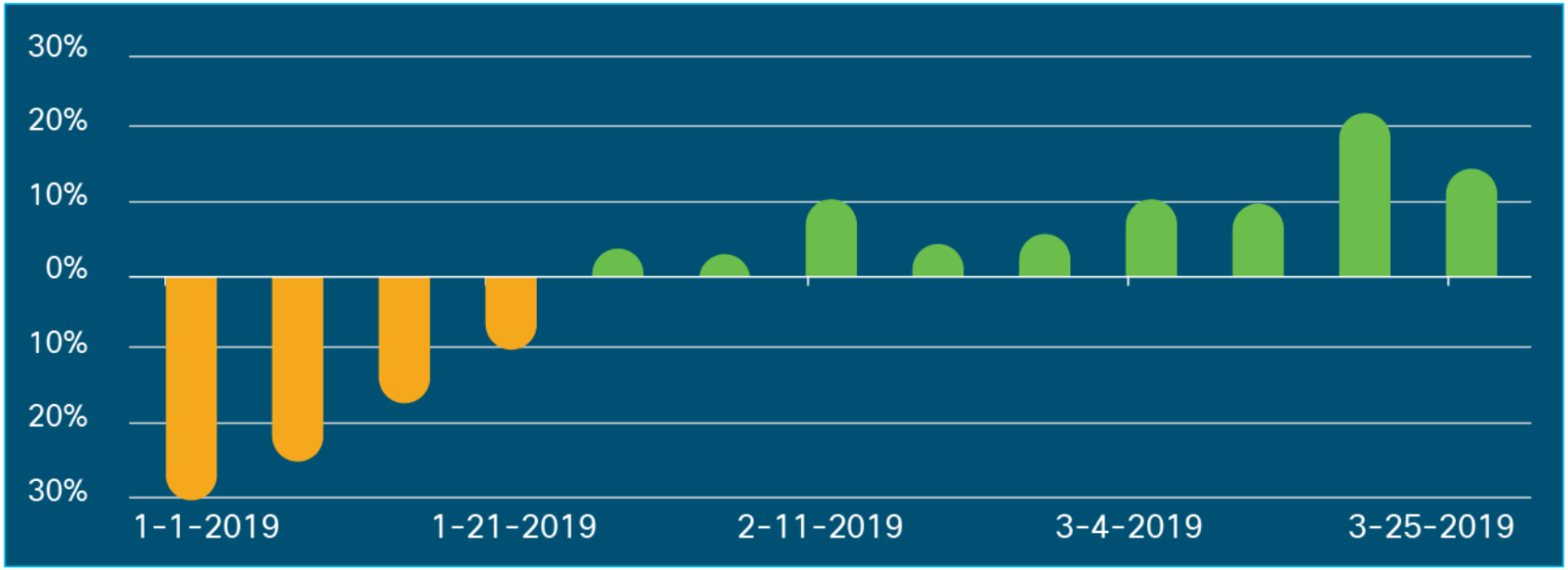
# Вредоносные вложения

- Более чем половина всех вредоносных вложений – это регулярно используемые типы документов
- 2 из 5 вредоносных файлов – это документы Microsoft Office
- Менее 2% вложений – бинарные / исполняемые файлы

| Тип | Процент |
|---|---|
| Office | 42.8% |
| Архив | 31.2% |
| Скрипт | 14.1% |
| PDF | 9.9% |
| Бинарный | 1.77% |
| Java | 0.22% |
| Flash | 0.0003% |

# Рост фишинговых доменов

64% рост новых фишинговых доменов в Q1 2019




Ежеквартально появляется около 500 тысяч новых фишинговых доменов

*Источник: Cisco Umbrella*


## Проводите регулярные фишинговые учения

- Сотрудники – это не только жертвы, но и элементы защиты

## Используйте MFA

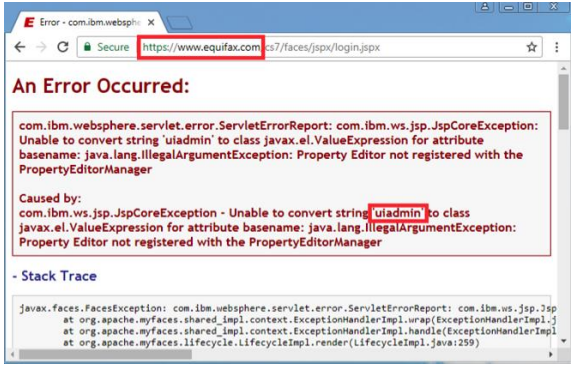
- Помогает предотвратить доступ хакеров

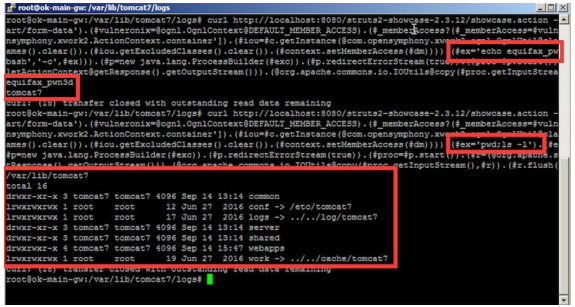
## Обновляйте ПО

- Не только системное и браузеры, но плагины к ним

# Пример: взлом Web-портала Equifax

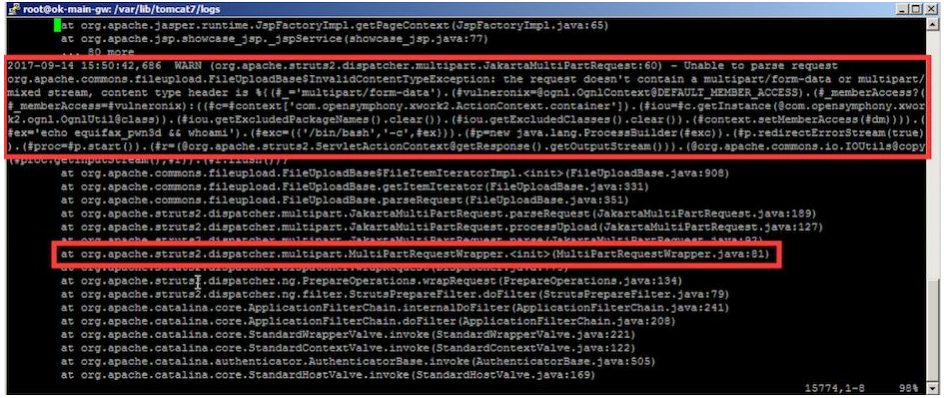
- 10 марта 2017 года злоумышленники нашли известную уязвимость на портале Equifax, позволившую получить доступ к Web-порталу и выполнять на нем команды
- Информация об уязвимости была разослана US CERT двумя днями ранее
- После идентификации уязвимости злоумышленники запустили эксплойт и получили доступ к системе, проверив возможность запуска команд
- Никаких данных украдено еще не было



# Шаг 2 в атаке на Equifax: эксплуатация уязвимости

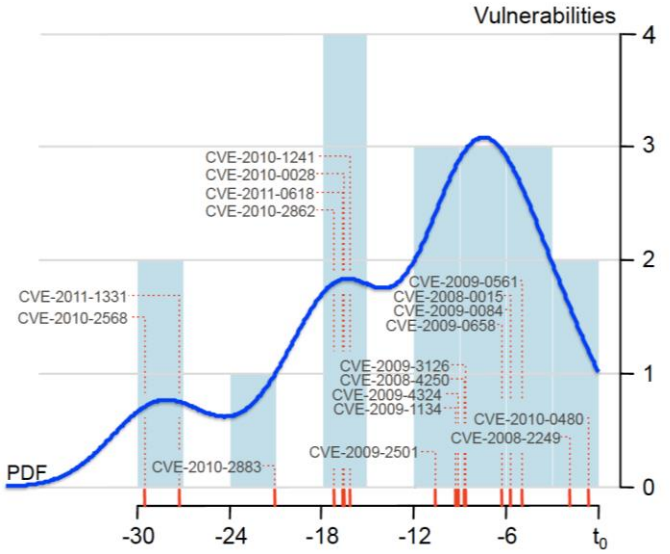
- 13 мая 2017 года злоумышленники эксплуатировали эту уязвимость и проникли во внутренние системы, выполнив ряд маскирующих процедур
- Например, использовалось существующее зашифрованное соединение для генерации запросов/получения ответов




Результат: утечка финансовой информации 146 миллионов человек

# Обновление спасает от многих атак

- Средняя длительность 0day-атаки составляет 312 дней (медиана – 8 месяцев)
- После раскрытия 0day-уязвимости число использующего ее ВПО возрастает в 183-85000 раз, а число атак с ней возрастает на 5 (!) порядков
- Эксплойты для 0day уязвимостей появляются в течение 30 дней после даты раскрытия уязвимости в 42% случаев



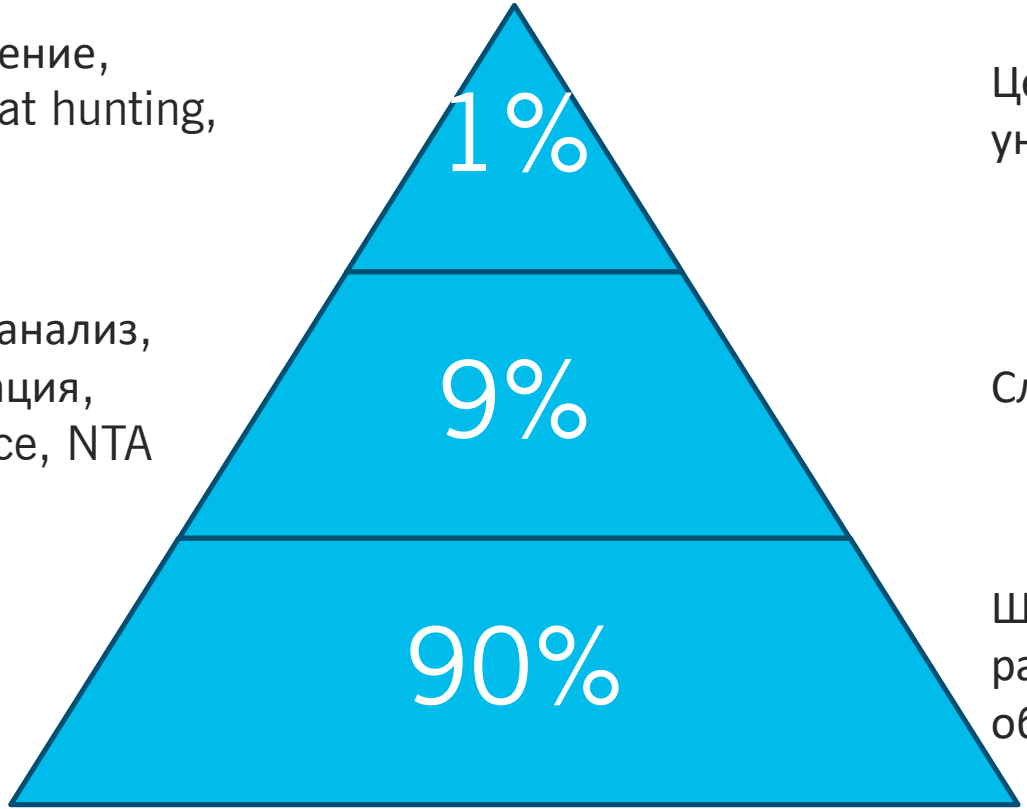
Длительность 0day-атак

# Для борьбы с 0-Day тоже есть методы

Машинное обучение, песочницы, threat hunting, forensics

Поведенческий анализ, облачная репутация, Threat Intelligence, NTA

Сигнатуры и правила

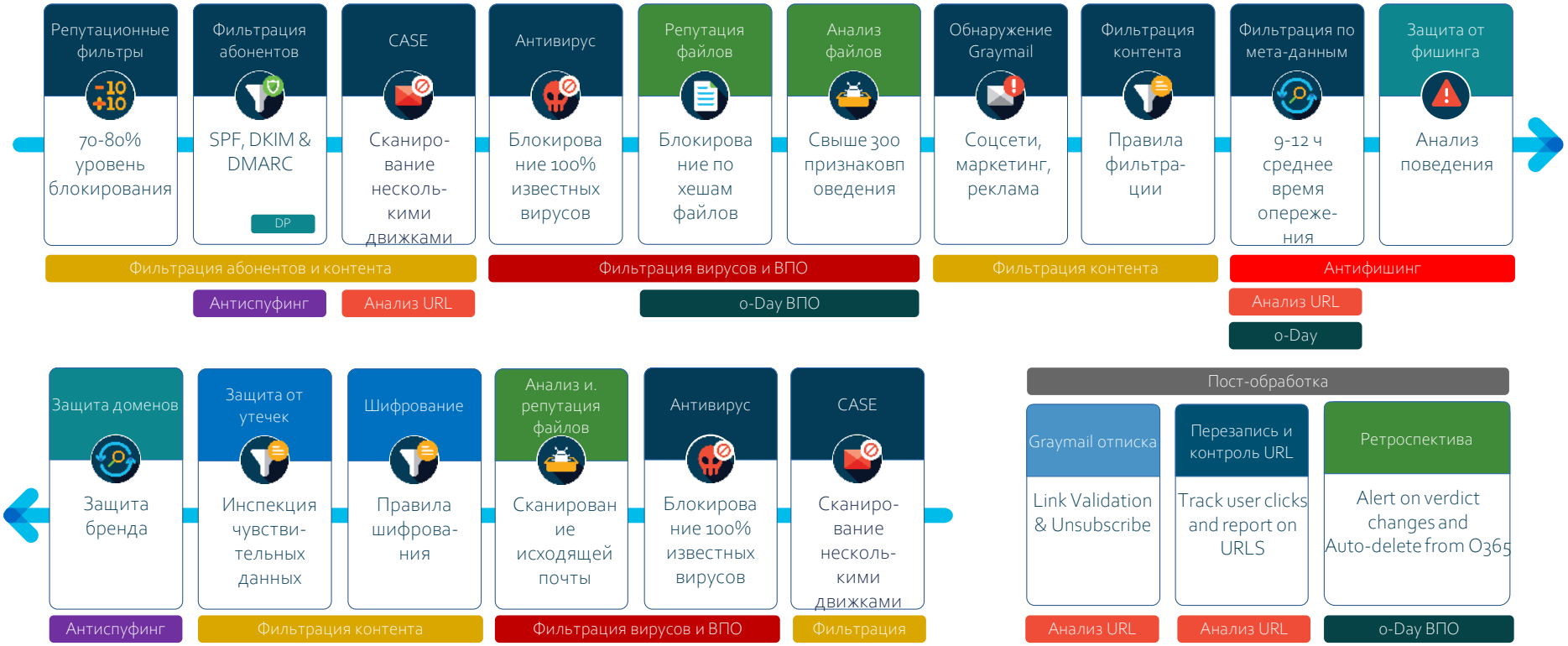



Целевое и уникальное ВПО

Сложное ВПО

Широко распространенное, обычное ВПО

# Современные технологии защиты e-mail



# VPNFilter

## Описание

- Ботнет из периметровых сетевых устройств и систем хранения
- Инфицировано свыше 500K уязвимых устройств (не Cisco)

## Инструменты

- Фреймворк для построения собственных ботнетов
- Модульная архитектура для обновления
- Сложная C2 & многоходовая платформа

## Тактики

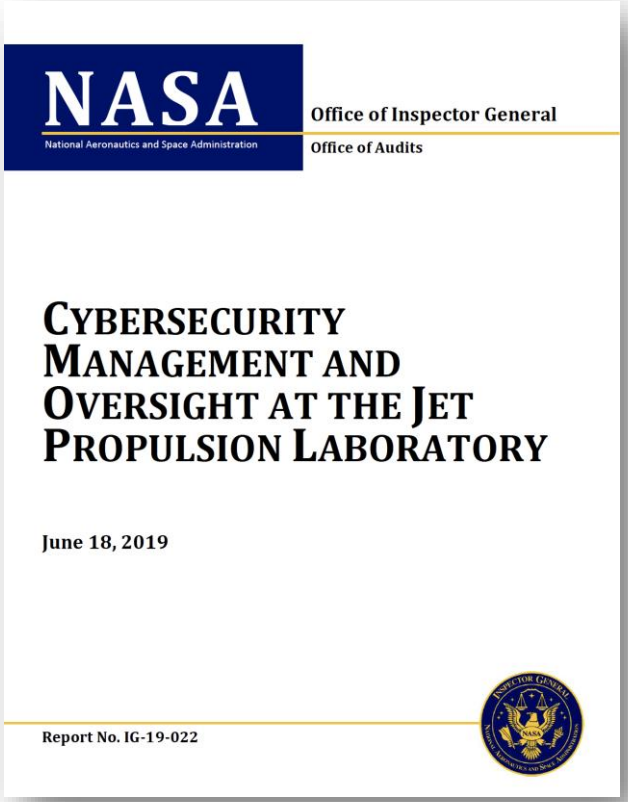
- Направлена на периметровые устройства
- Перенаправляет и изменяет сетевой трафик

## Процессы

- Брать все, искать интересующее
- Заразить и закрепиться

# Взлом NASA

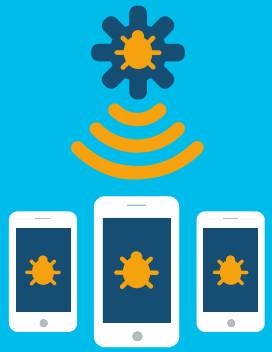
- В апреле 2018 хакеры проникли во внутреннюю сеть NASA и украли 500 МБ данных по миссии на Марс
- В качестве точки входа использовался портативный компьютер Raspberry Pi, установленный в сети NASA


NASA
National Aeronautics and Space Administration
Office of Inspector General
Office of Audits
CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY
June 18, 2019
Report No. IG-19-022

# Сетевая инфраструктура может быть не только системой защиты, но и мишенью

0. Не ограничивайтесь периметром
1. Используйте Netflow или IPFIX
2. Используйте несемплированный Netflow
3. Проверьте загрузку оборудования
4. Начните с уровня доступа
5. Если российское, то с поддержкой flow (или хотя с поддержкой SPAN)
6. Комбинируйте NTA и COB/COA
7. Думайте о зонировании, а не о МСЭ
8. Интегрируйте средства мониторинга сети и контроля сетевого доступа
9. Учитывайте стратегию развития своей сети

# Mobile Device Management



- MDM-функции используются для управления корпоративными устройствами
- Плохие парни нашли способ использовать MDM
- Установка модифицированных версий популярных мобильных приложений
- MDM-атаки уже зафиксированы для:
  - WhatsApp
  - Telegram

# Olympic Destroyer


## Описание

- Направлен на Олимпийские игры в Ю.Корее
- Авторство приписывают Северной Корее


## Инструменты

- PSEXEC / WMI / Creds stealer / Browser stealer
- Использование **легальных** системных утилит
- Mimikatz и воровство учетных данных

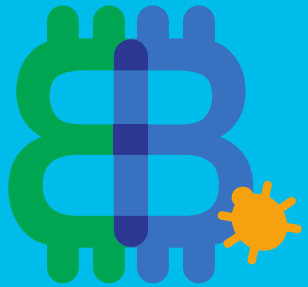
## Тактики

- Цепочка поставок
- Расширение плацдарма через WMI и PSEXEC
- Автоматическое расширение плацдарма с украденными учетными данными

## Процессы

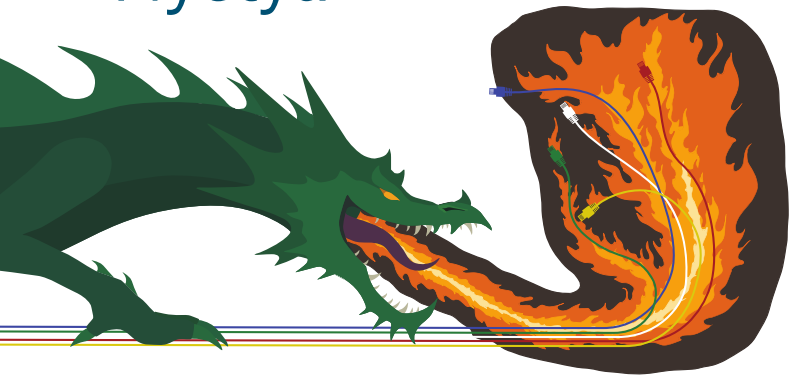
- Кража учетных данных и расширение плацдарма
- Фокусированная атака, направленная на получение политической выгоды

# Вредоносный криптомайнинг



- Отличия легального и вредоносного криптомайнинга: наличие разрешения/согласия
- Отрицательное воздействие на производительность и энергопотребление
- Влияние на пропускную способность сети
- Может стать точкой входа для других вредоносных программ (за счет модульности)

# Nyetya



## Описание

- Продвинутый актор, ассоциированный с государством
- Деструктивная атака маскировалась под Ransomware
- Наиболее дорогой инцидент в истории

## Инструменты

- Ransomware с тактикой червя
- Спроектирован для распространения внутри, не снаружи
- Использование Eternal Blue / Eternal Romance и Admin Tools (WMI/PSExec)

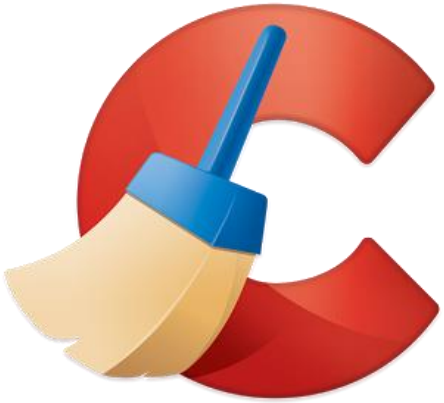
## Тактики

- Цепочка поставок и от жертвы к жертве
- Быстрое распространение
- Разрушение систем / сетей

## Процессы

- Разработан для максимально быстрого и эффективного нанесения ущерба
- Похож на вымогателя, но является деструктивным по сути

# CCleaner



## Описание

- Продвинутый актор, ассоциированный с государством
- Возможность выполнять сложные и длинные операции, фокусированные на краже интеллектуальной собственности

## Инструменты

- Целевой фишинг
- Комплексная разведка и профилирование цели
- Кейлогер и вор пользовательских учетных данных

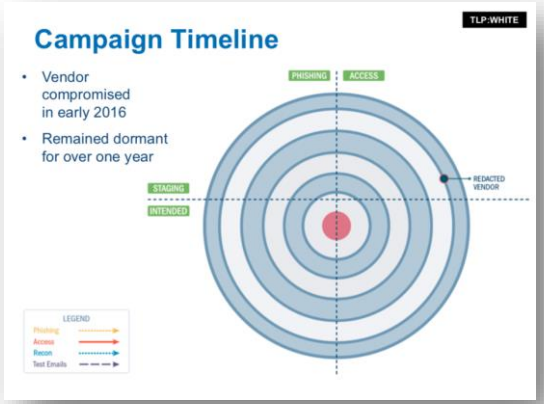
## Тактики

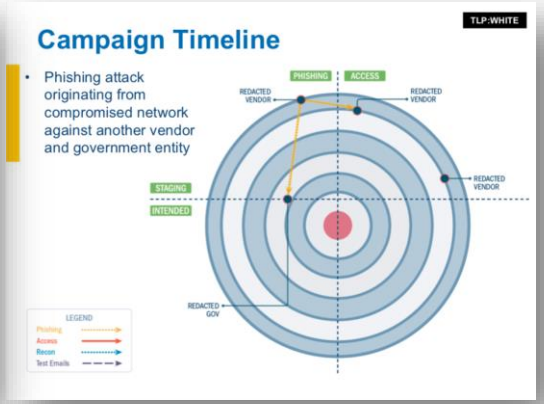
- Цепочка поставок и от жертвы к жертве
- Медленная внутренняя разведка
- Сложная многоходовая атака

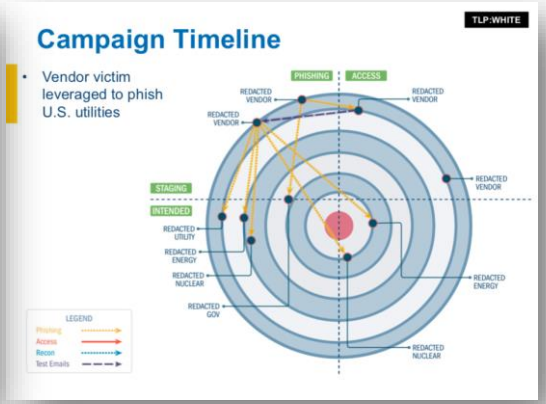
## Процессы

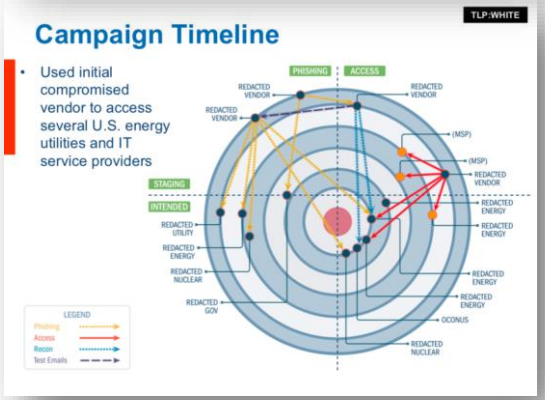
- Высокоточная идентификация жертв через датамайнинг
- Ориентирован на скрытность, рассчитан на долгую «игру»

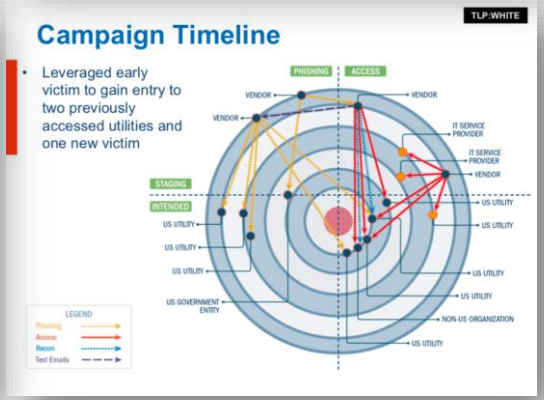
# Атака «водопой» (water hole)



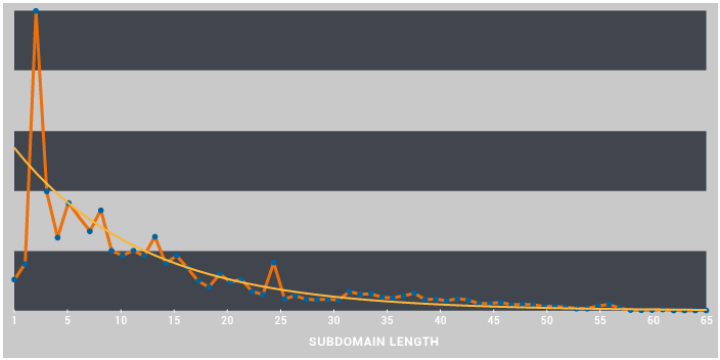



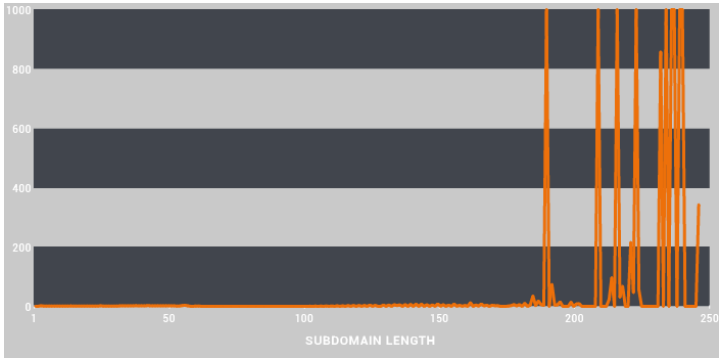

Взлом ASUS, Avast, поставщиков промышленного ПО и др.

# DNS как неконтролируемый канал

Утечка данных кредитных карт, получение обновлений ВПО и т.п.




Нормальное распределение длин поддоменов




Аномалии в названии поддоменов

log.nu6timjqgq4dimbuhe.3ikfsb---отредактировано---cg3.7s3bnxqmavqy7sec.dojfgj.com
log.nu6timjqgq4dimbuhe.otlz5y---отредактировано---ivc.v55pgwcschs3cbee.dojfgj.com

Что скрывается в этой строке на 231 символ?

# 17 каналов проникновения плохих парней в вашу организацию

1. E-mail
2. Web
3. Site-to-Site VPN
4. Remote Access VPN
5. Sharing resources
6. USB
7. Wi-Fi
8. Warez
9. BYOD
10. Embedded
11. Клиент-сервер с шифрованием
12. DevOps
13. Подрядчики
14. Уязвимость на портале
15. «Водопой» (Waterhole)
16. DNS
17. Облако

# Что надо делать компаниям?

- Начать с пересмотра стратегии кибербезопасности
  - Понять мотивацию злоумышленников для их предприятия
  - Учесть тактику, техники и процедуры (TTP), используемые злоумышленниками
  - Идентифицировать слабые звенья в организации, в сети, в системе защиты
  - Думать как злоумышленники – действовать как безопасники (применяйте Red Team / Blue Team)
  - Учитывать жизненный цикл атаки «ДО – ВО ВРЕМЯ - ПОСЛЕ»

# Что надо делать компаниям?

- Пересмотреть систему защиты
  - Сбалансировать технологии защиты (предотвращение, обнаружение и реагирование) – вместо соотношения 80-15-5 перейдите к 33-33-34
  - Задуматься о безопасности внутренней сети, а не только о защите периметра
  - Мониторить даже то, чего по политике нет (Wi-Fi, мобильные устройства, 3G/4G-модемы, облака и т.п.)
  - Внедрить систему Threat Intelligence для раннего предупреждения об угрозах

У меня нет времени смотреть на новые решения по ИБ – мне с угрозами бороться надо!


Исследование приватности данных и ПДн в разных странах для Chief Privacy Officer


Анализ тенденций по ту сторону баррикад за 12 месяцев - для людей, принимающих решения


Ключевые факты и данные о возможностях ИБ и реагировании на инциденты


Анализ тенденций в области фишинга и атак на электронную почту

https://www.cisco.com/c/ru_ru/products/security/security-reports.html

# Спасибо!

security-request@cisco.com

CISCO

INTUITIVE