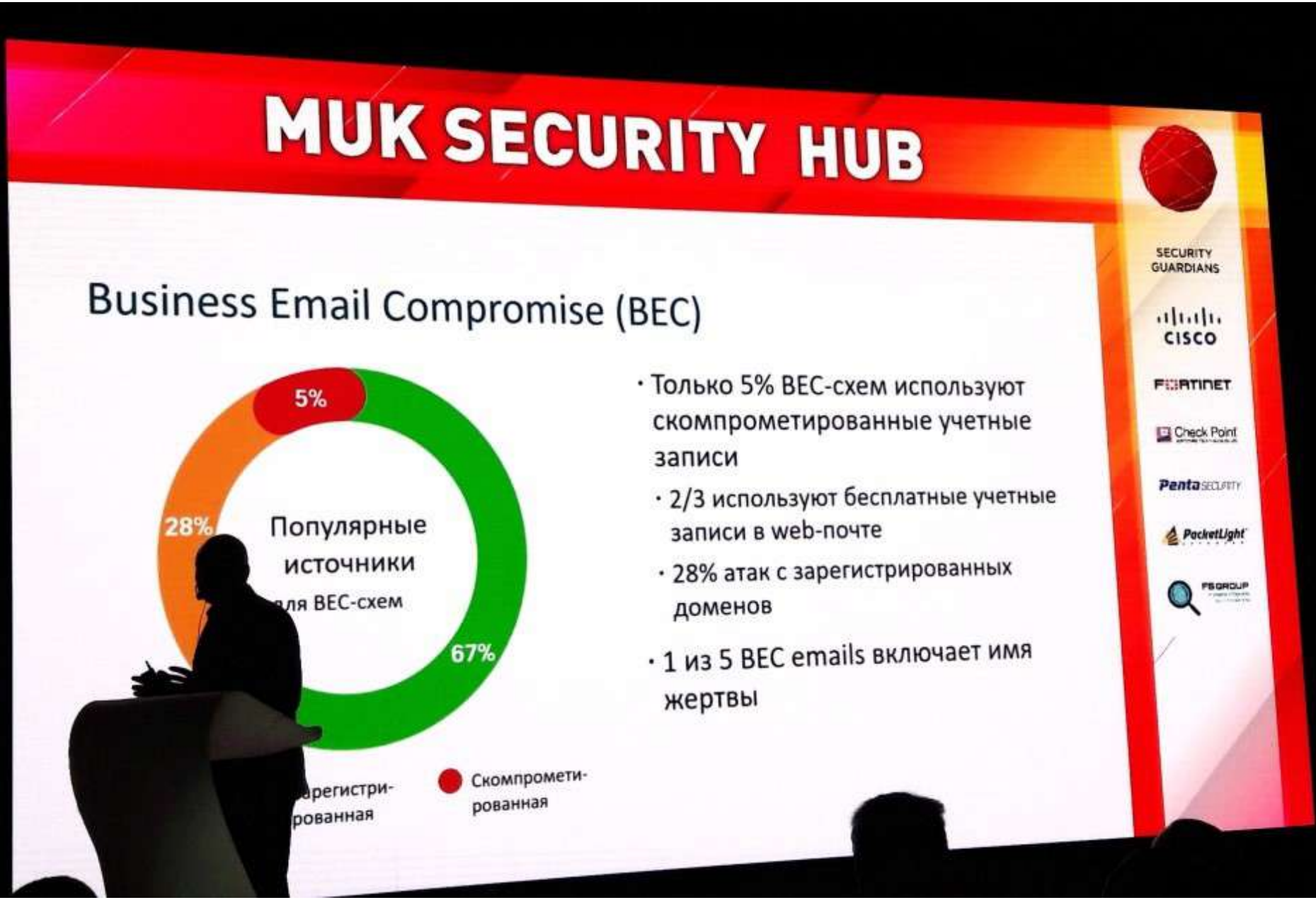

MUK SECURITY HUB
SECURITY GUARDIANS
CISCO
FORTINET
Check Point
PentaSECURITY
PacketLight
FSGROUP
Business Email Compromise (BEC)
5%
28%
67%
Популярные источники
для BEC-схем
Скомпрометированная
• Только 5% BEC-схем используют скомпрометированные учетные записи
• 2/3 используют бесплатные учетные записи 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 вр носных файлов – это докумен Microsoft Office
- Менее 2 ений – бинарные файлы

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


MUK SECURITY HUB
Современные технологии защиты e-mail
70-80% уровень блокирования
SPF, DKIM & DMARC
CASE
Сканиро-вание несколь-кими движками
Антивирус
Блокирова ние 100% известных вирусов
Блокирова ние по хешам файлов
Свыше 300 признаков поведения
Соцсети, маркетинг, реклама
Правила фильтра-ции
9-12 ч среднее время опереже-ния
Анализ поведения
Антиспуфинг
0-Day BPO
0-Day
Link Validation & Unsubscribe
Track user clicks and report on URLS
Alert on verdict changes and Auto-delete from
Сканирован ие исходящей почты
Блокирова ние 100% известных вирусов
Сканиро-вание несколь-кими
тельных данных
SECURITY GUARDIANS
CISCO
FORTINET
Check Point
Penta SECURITY
PacketLight


MUK SECURITY HUB
Взлом NASA
• В апреле 2018 хакеры проникли во внутреннюю сеть NASA и украли 500 МБ данных по
• В
ве точки входа
ался портативный
ер Raspberry Pi,
ленный в сети NASA
NASA
Office of Inspector General
Office of Audits
CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY
June 18, 2019
Report No. IG-19-022
SECURITY GUARDIANS
CISCO
FORTINET
Check Point
Penta SECURITY
PacketLight
FS GROUP

MUK SECURITY HUB

Nyetya/NotPetya

Опи

е, ассоциированный с

а маскировалась под

инцидент в истории

Инструменты

- Деструктор 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
- Очень быстрое распространение
- Разрушение систем / сетей

Процессы

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

SECURITY GUARDIANS

CISCO

FORTINET

Check Point

PentaSECURITY

PacketLight

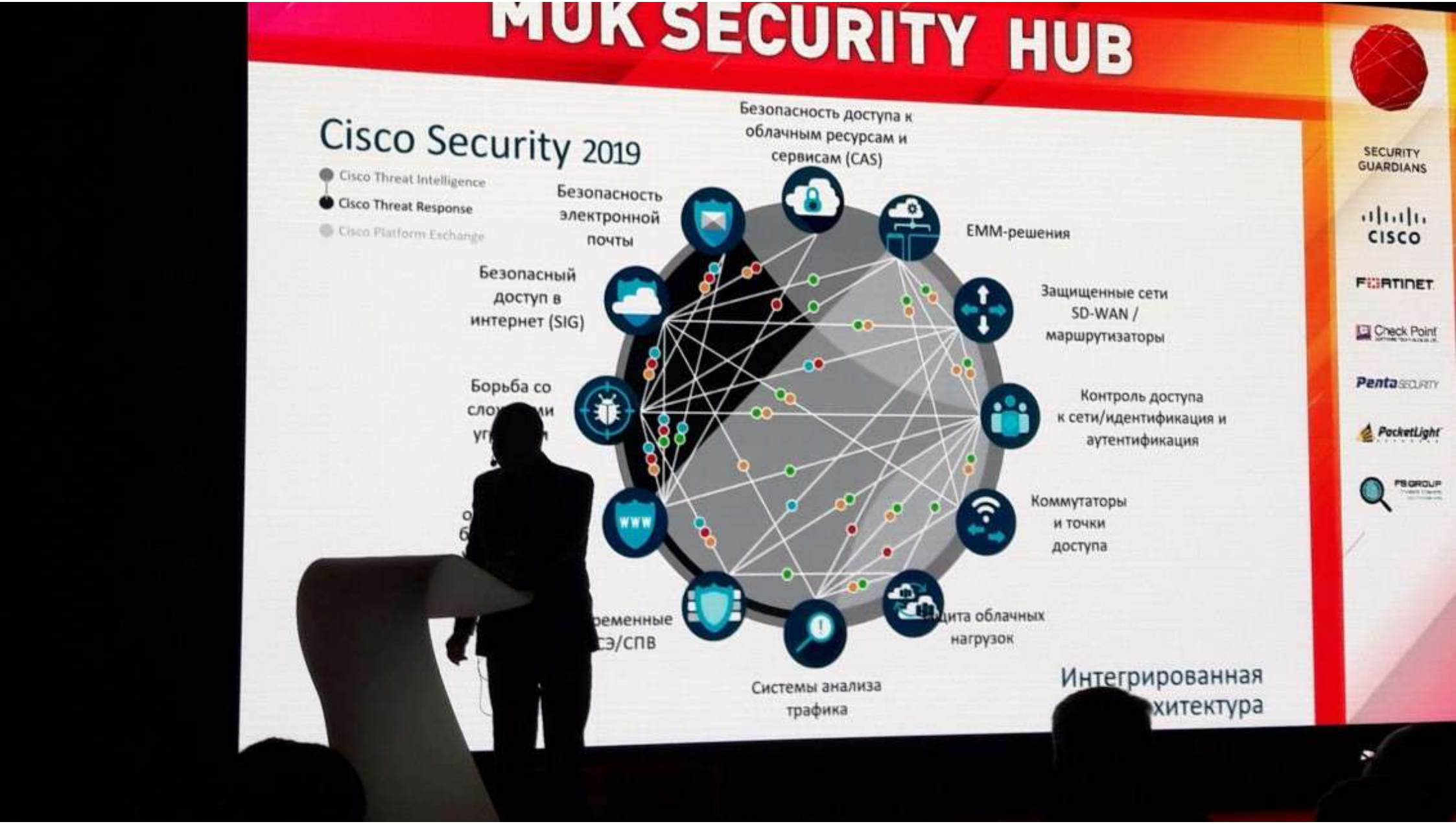
FSGROUP


MUK SECURITY HUB
CCleaner
ние
ый malware, ассоциированный с
ом
ть выполнять сложные и
операции, фокусированные на
теллектуальной 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 «игр
SECURITY GUARDIANS
CISCO
FORTINET
Check Point
PentaSECURITY
PacketLight
FSGROUP


MUK SECURITY HUB
Опыт Cisco: комбинируйте методы обнаружения
В прошлом
Signature
2012
Signature
Flows
Intel
2013+
Behavior
Flows
Signature
Intel
бходимо использовать различные способы изучения угроз
етевые потоки | Поведение | Сигнатуры | Исследования
SECURITY GUARDIANS
cisco
FORTINET
Check Point
PentaSECURITY
PacketLight
FS GROUP


MUK SECURITY HUB
Многоходовые атаки требуют комплексной защиты
Разведка
Вооружение
Определение цели
Доставка
Эксплойт
Инсталляция
C&C
Подготовка
Планирование
Вторжение
SECURITY GUARDIANS
CISCO
FORTINET
Check Point
PantaSECURITY
PocketLight


MUK SECURITY HUB
Эффективная безопасность зависит от общей видимости
ЗНАТЬ
Каждый хост
ВИДЕТЬ
Каждую сессию
Понимать что есть
НОРМА
Быть предупрежденным
при ИЗМЕНЕНИИ
Реагировать на
УГРОЗЫ быстро
Филиал
Облако
Мобильные пользователи
Сеть
Пользователи
Головной офис
Администратор
ЦОД
SECURITY
GUARDIANS
CISCO
FORTINET
Check Point
Penta SECURITY
PacketLight
PS GROUP


MUK SECURITY HUB
Cisco Security 2019
Cisco Threat Intelligence
Cisco Threat Response
Cisco Platform Exchange
Безопасность доступа к облачным ресурсам и сервисам (CAS)
Безопасность электронной почты
EMM-решения
Безопасный доступ в интернет (SIG)
Защищенные сети SD-WAN / маршрутизаторы
Борьба со
Контроль доступа к сети/идентификация и аутентификация
Коммутаторы и точки доступа
Системы анализа трафика
нагрузок
Интегрированная
SECURITY GUARDIANS
CISCO
FORTINET
Check Point
PentaSECURITY
PocketLight
FS GROUP

Результат целевых BEC атак

facebook

$100,000,000

Google

$23,000,000

$37,000,000

$3,200,000

Письма идут по уязвимым почтовым серверам

Man-in-the-middle

Конфиденциальные данные в открытке

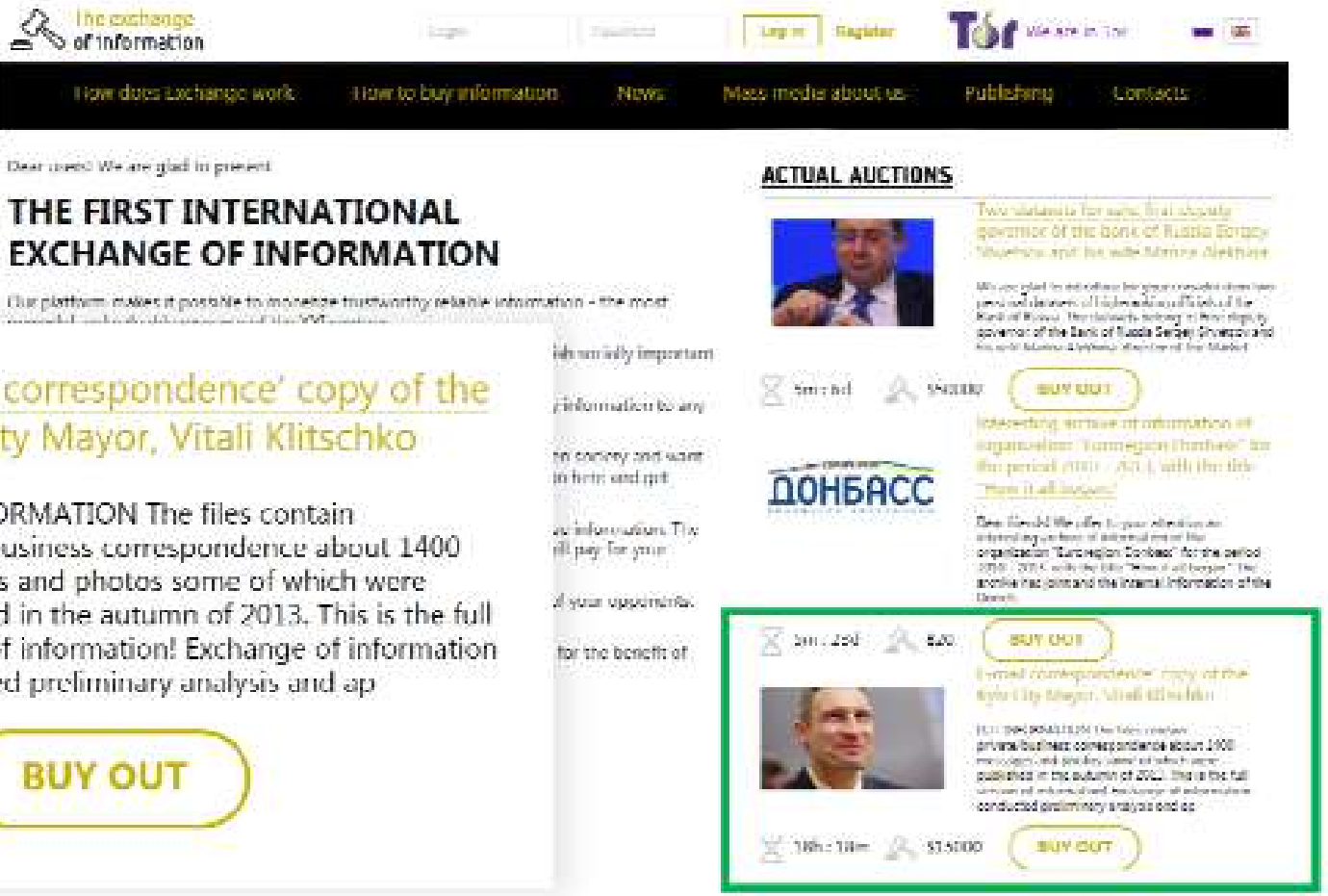
Содержание электронных писем передаётся в открытом виде как у открыток в реальном мире.

Обычные письма:

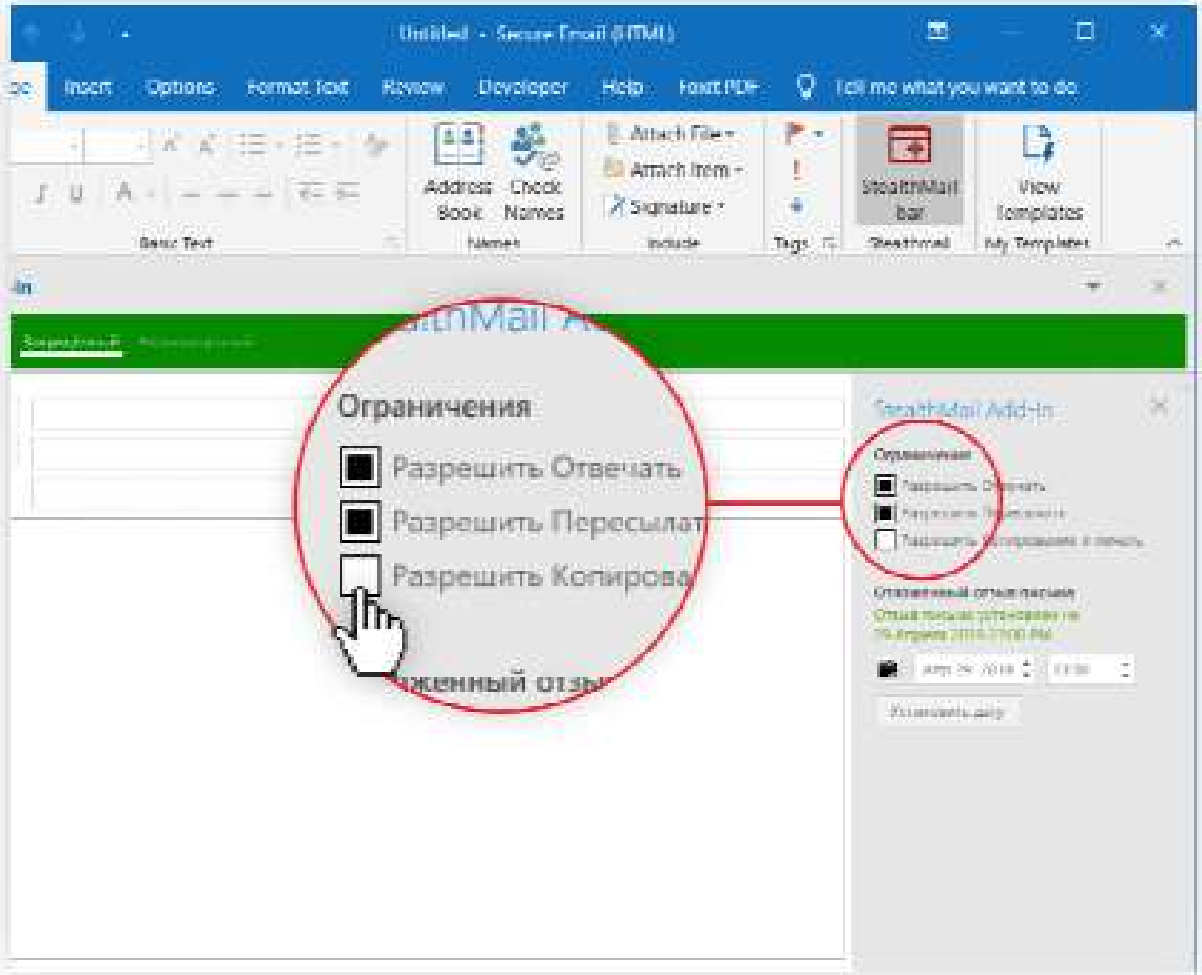
- Отправляются открытым текстом
- Перемещаются через уязвимые почтовые сервера
- Невозможно отозвать
- Уязвимы для сбора и обработки данных

Подробности в RFC 3207

Утечка данных



https://joker.buzz/



Установка

ОГРАНИЧЕНИЙ НА

- ✕ Ответ
- ✕ Пересылку
- ✕ Копирование
- ✕ Скриншот

StealthMail Курс Обучения Сотрудников

Обновляемые руководства от экспертов по кибербезопасности со всего мира избавят Вас от необходимости тратить много времени на обучение кибер-гигиене Ваших сотрудников.

MUK CLOUD HUB

Движущие силы цифровой трансформации

DATA

163 zettabytes ежегодно до 2025

ANALYTICS

$200 billion глобальные рынки до 2020

CLOUD

Переход в облако обеспечит более
$1 trillion IT расходов до 2020

MUK CLOUD HUB

Дорожная карта цифровой трансформации

1. Определение целей и ценности трансформации для компании	2. Старт и ускорение	3. Масштабирование
Получение поддержки высшего руководства	Старт пилотного проекта с управляемыми рисками и высоким ожидаемым эффектом	Запуск последовательности инициатив с быстрым возвратом инвестиций
Установка четких целей	Назначение высококлассной команды пилотного проекта	Создание новых возможностей работы
Резервирование инвестиций	Реклама внутри компании новых, удобных и гибких способов работы	Адаптация новой модели работы (люди, процессы, правила и технологии)
	Воспитание цифровой культуры	

MUK CLOUD HUB

С чего начать (или развить) работу с облаком? Рекомендации для стартапов и компаний с историей

У вас стартап? Вам повезло!

- Можете начать использовать технологии прямо здесь и сейчас
- В любой момент можете отключить подписку
- Подключайте внешних пользователей для совместной работы
- Корпоративные продукты и безопасность для SMB

У вас компания с историей – получите преимущество с облаком Microsoft!

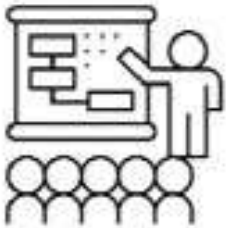
- Расширьте возможности инфраструктуры за счет масштабирования в облако
- Получите корпоративную безопасность без высоких затрат
- Получите преимущества гибридного использования Windows Server
- Перенесите капитальные затраты в операционные

MUK CLOUD HUB

Безопасность и сохранность Ваших данных в облаке. Здесь и сейчас

Что угрожает корпоративной почте?

StealthMail защита

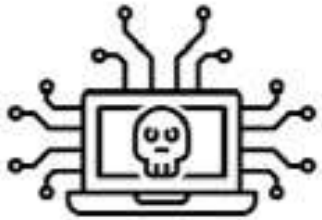


«Человеческий фактор»

- Предотвратите утечку данных, в любой момент отозвав ошибочно отправленные электронные письма.
- Курс по Email безопасности предоставляет учебные материалы, которые помогут пользователям распознавать и избегать угроз.
- Простые для понимания серия книг для самообучения сотрудников вопросам безопасности Email.

Социальная инженерия

- Фишинг легко обнаруживается и игнорируется, так как отправитель всегда проверяется.
- Данные остаются защищенными, даже если учетные данные электронной почты были скомпрометированы.
- Все подозрительные действия, связанные с учетными записями StealthMail, обрабатываются администраторами компании.



Хакерские атаки

- Зашифрованная пользовательская переписка не может быть доступна, даже если пользовательское устройство было взломано.
- К зашифрованным данным нельзя получить доступ, даже если хранилище компании было взломано.
- Распределенного серверная инфраструктура защищает решение от попыток взлома.

MUK CLOUD HUB

Безопасность и сохранность Ваших данных в облаке. Здесь и сейчас

Что мы предлагаем?

Ключевые преимущества StealthMail

Защита от угроз

- Business Email Compromise (BEC);
- Email Account Compromise (EAC);
- Man-in-the-Middle (MITM);
- Спуфинга;
- Фишинга.

Безопасная миграция в облако

- Данные шифруются на устройстве пользователя;
- Данные хранятся в облаке только в зашифрованном виде;
- Полный контроль над ключами шифрования и доступом к данным;
- Резервное копирование данных в режиме реального времени одновременно выполняется на шести разных серверах.

Управление правами доступа

- Отзыв отправленных писем;
- Ограничение прав доступа к содержимому письма (блокировка копирования, пересылки, скриншота);
- Данные защищены в пути, на сервере, и на устройстве;
- Содержимое электронной почты никогда не покидает защищенный периметр компании.