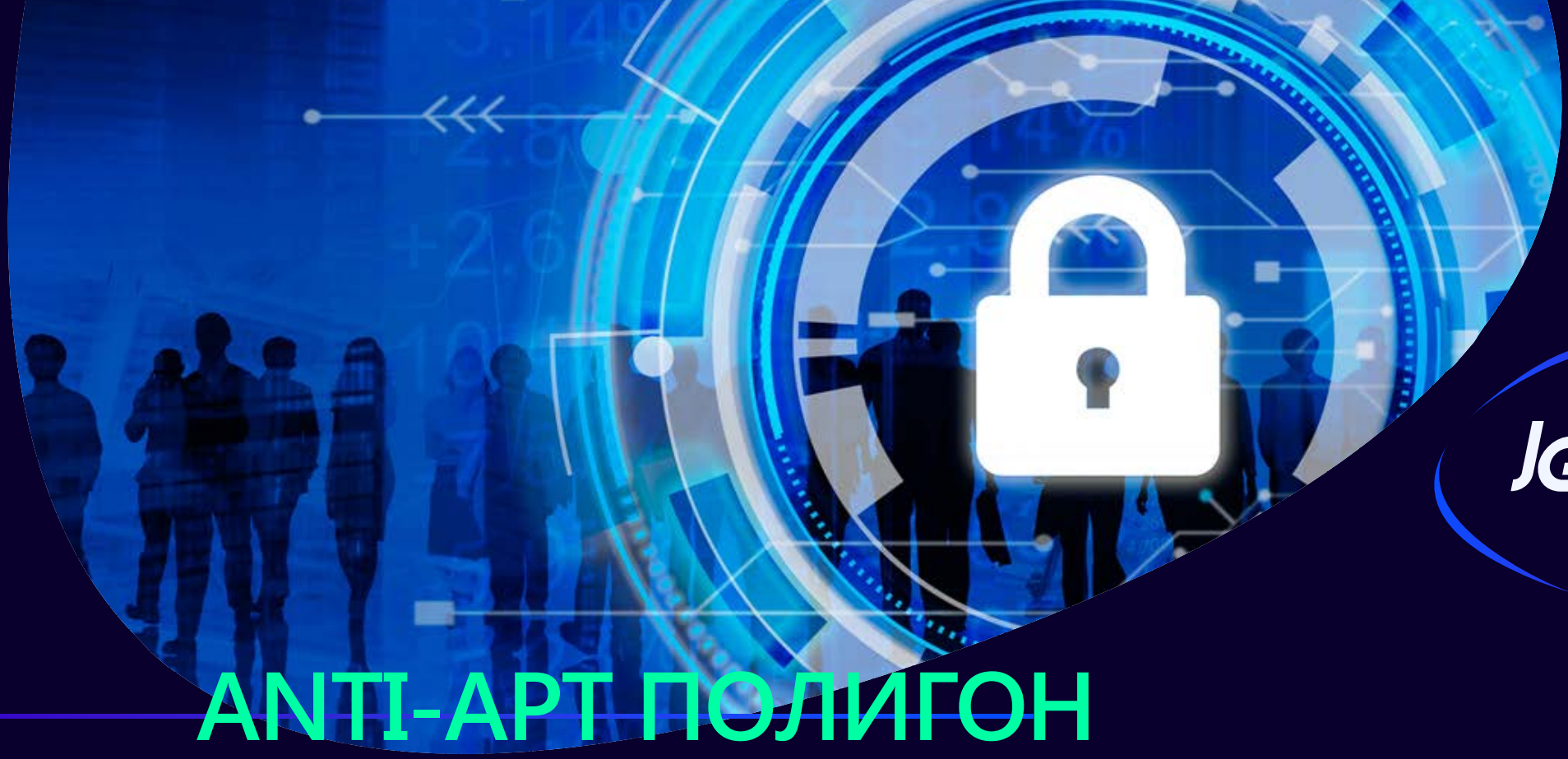


ANTI-APT ПОЛИГОН

14/02/2018

Практический мастер-класс Центра информационной безопасности

Т.: +7 495 411-76-01 | E.: INFO@JET.SU | W.: WWW.JET.SU | 127015, РОССИЯ, МОСКВА, УЛ. БОЛЬШАЯ НОВОДМИТРОВСКАЯ, 14С1, БЦ «НОВОДМИТРОВСКИЙ»

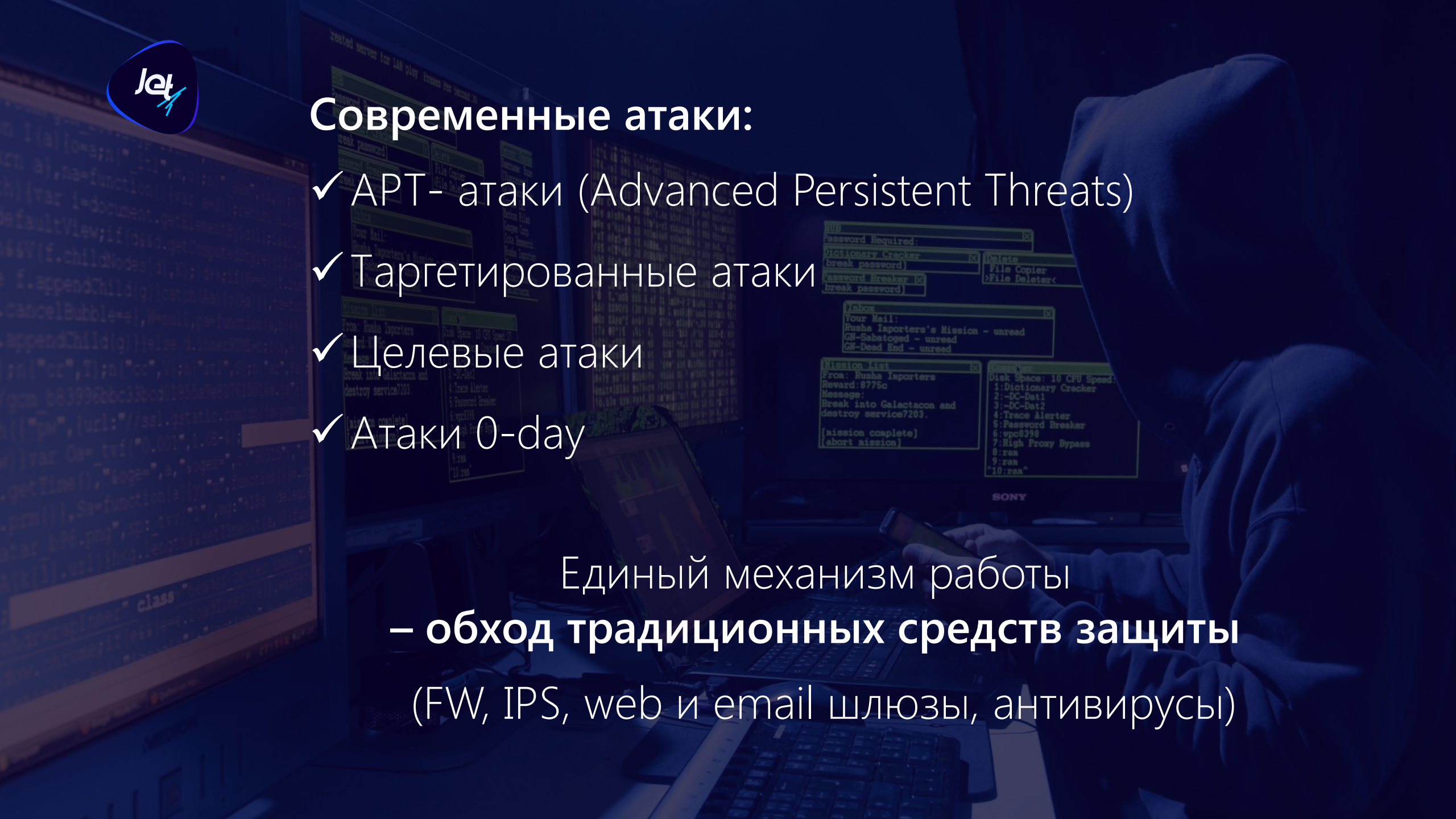
ВЕДУЩИЕ ANTI-APT ПОЛИГОНА

Александр Русецкий

Руководитель направления защиты от направленных атак, компания «Инфосистемы Джет»

Александр Джаганян

Руководитель направления инфраструктурных ИБ-решений, компания «Инфосистемы Джет»



Современные атаки:

- ✓ APT- атаки (Advanced Persistent Threats)
- ✓ Таргетированные атаки
- ✓ Целевые атаки
- ✓ Атаки 0-day

Единый механизм работы

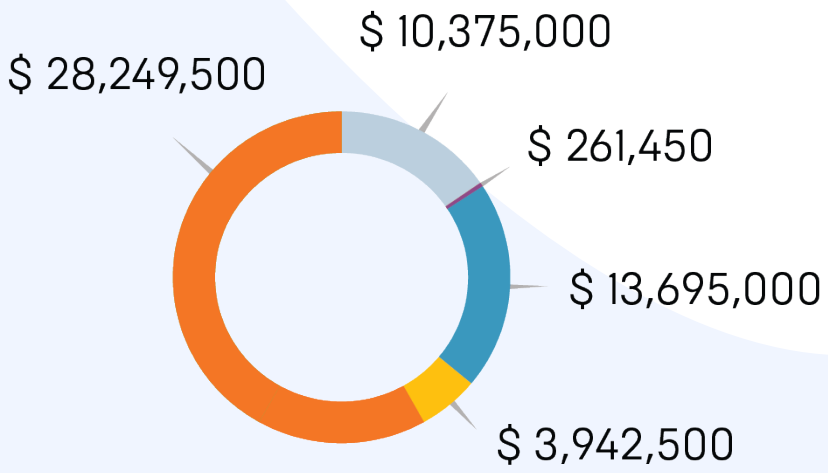
– обход традиционных средств защиты

(FW, IPS, web и email шлюзы, антивирусы)

ОЦЕНКА РОССИЙСКОГО РЫНКА ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ*

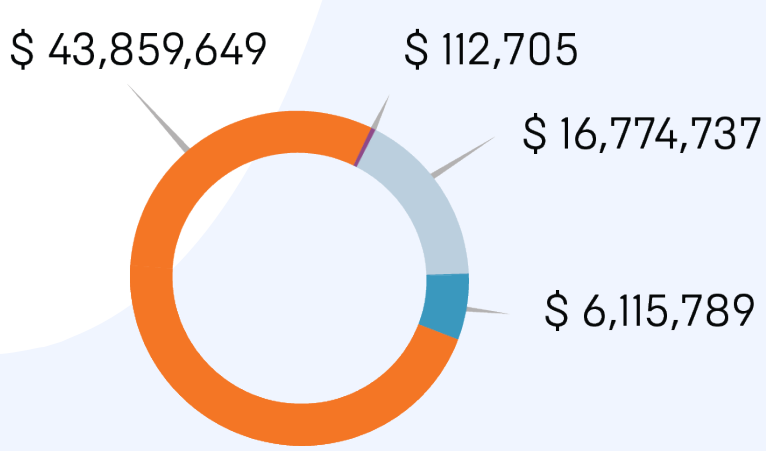
H2 2016 - H1 2017

$ 55,440,617

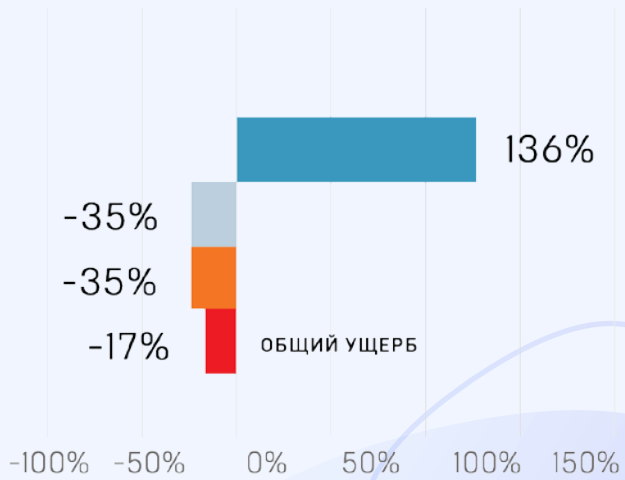


H2 2015 - H1 2016

$ 66,862,880



Изменения по отношению к предыдущему периоду



- ХИЩЕНИЯ В ИНТЕРНЕТ-БАНКИНГЕ У ФИЗИЧЕСКИХ ЛИЦ С ТРОЯНАМИ ДЛЯ ПК
- ХИЩЕНИЯ В ИНТЕРНЕТ-БАНКИНГЕ У ФИЗИЧЕСКИХ ЛИЦ С ANDROID ТРОЯНАМИ
- ХИЩЕНИЯ В ИНТЕРНЕТ-БАНКИНГЕ У ЮРИДИЧЕСКИХ ЛИЦ
- ЦЕЛЕВЫЕ АТАКИ НА БАНКИ
- ФИШИНГ
- ОБНАЛИЧИВАНИЕ ПОХИЩЕННЫХ СРЕДСТВ

*Данные предоставлены компанией Group-IB

BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

41:02:24

Price for decryption:

 = 0.05

HI-TECH CRIME TRENDS 2017*

- ✓ Вымогатели
- ✓ Целенаправленные атаки на банки и платежные системы
- ✓ Атаки на клиентов банков
- ✓ Атаки на криптовалютные сервисы
- ✓ Развитие хакерского инструментария

*По данным компании Group-IB

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ОТ APT

Песочница (SandBox)

ДИНАМИЧЕСКИЙ АНАЛИЗ

Обнаружение изменений реестра
Обнаружение сетевых коммуникаций
Обнаружение активности процессов
Обнаружение изменений файловой системы

СТАТИЧЕСКИЙ АНАЛИЗ

Распаковка
Анализ деассемблированного кода
Анализ пассивного кода
Обнаружение скрытых логических путей

NGFW/Proxy

Сетевой мониторинг

Защита рабочих станций

ПРОВЕДЕНИЕ ANTI-APT ПОЛИГОНА

Цель мастер-класса:
оценить возможности каждого из продуктов и выбрать оптимальное Anti-APT решение

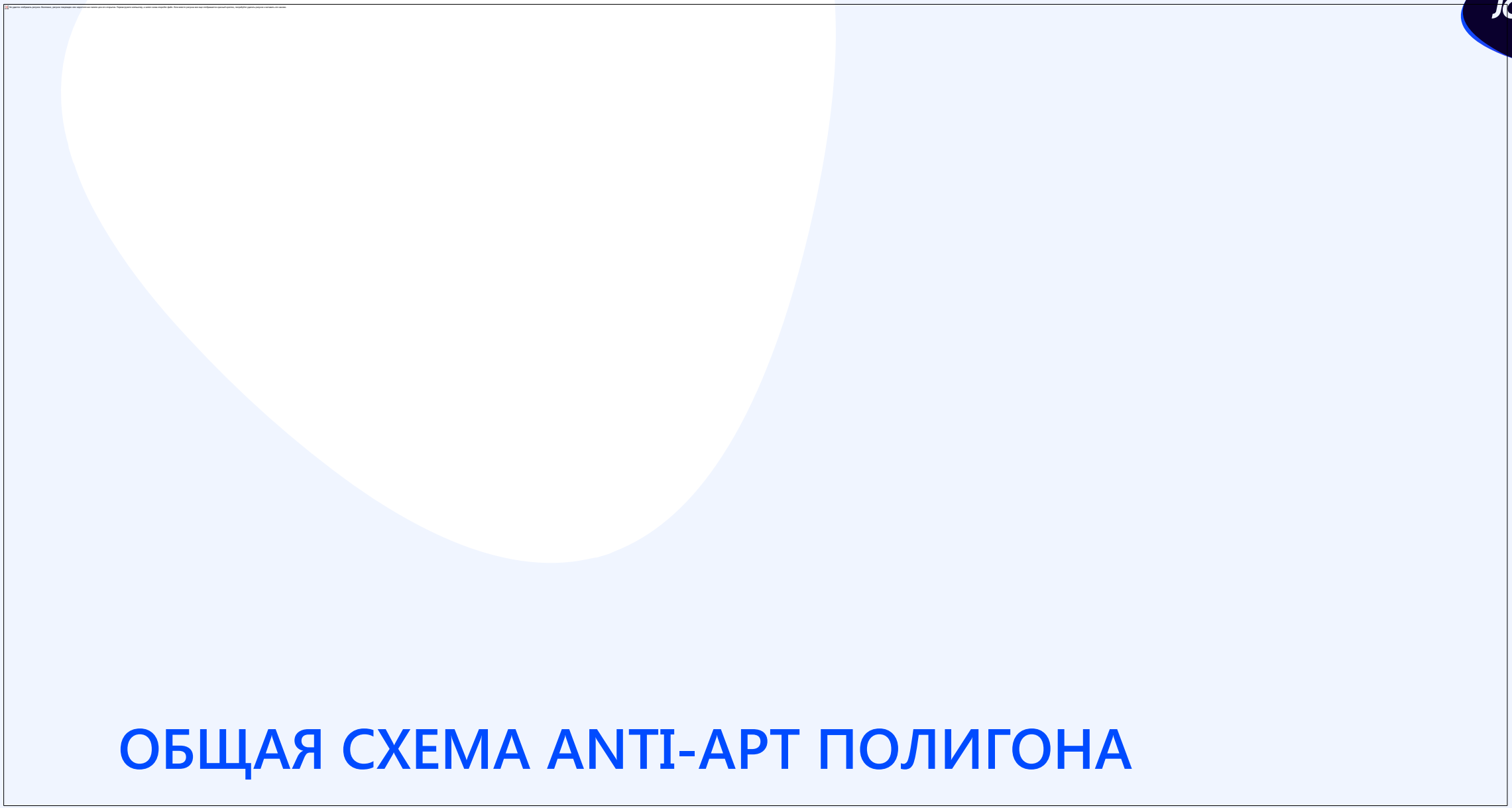
Условия проведения:
ВПО прошло стандартные средства защиты (веб и почтовый шлюзы, антивирус)

УЧАСТНИКИ ANTI-APT ПОЛИГОНА

Check Point SOFTWARE TECHNOLOGIES LTD.

FORTINET

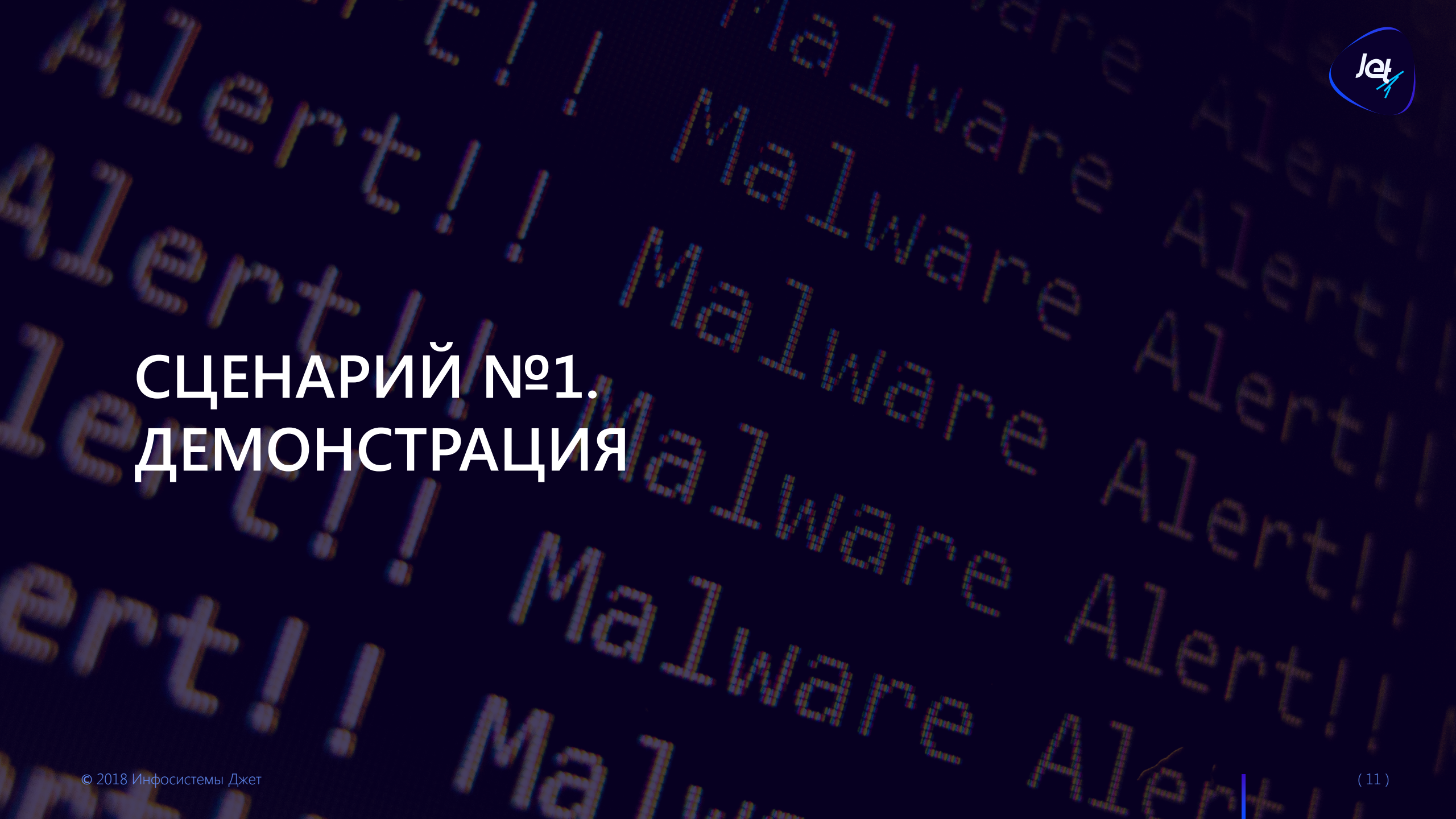
KASPERSKY lab PLATINUM PARTNER



ОБЩАЯ СХЕМА ANTI-APT ПОЛИГОНА

СЦЕНАРИЙ №1. АНАЛИЗ ПОЧТЫ

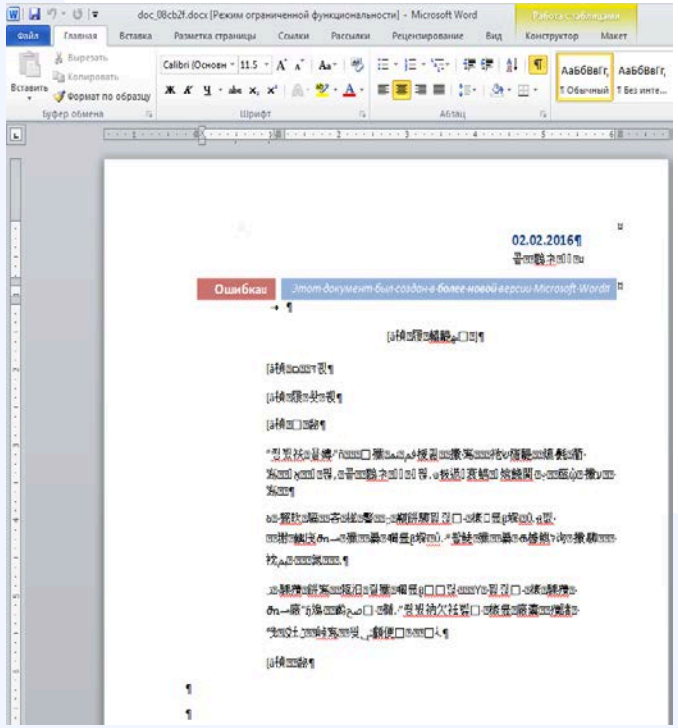
- ✓ фишинговое письмо с архивом, защищенным паролем (пароль указан в теле письма)
- ✓ фишинговое письмо со ссылкой на web-страницу



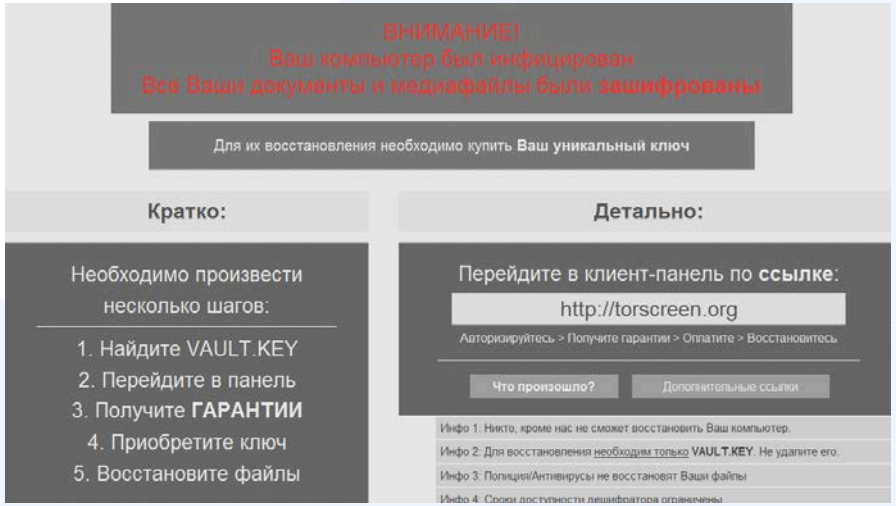
СЦЕНАРИЙ №1. ДЕМОНСТРАЦИЯ

ANTI-APT: ПРАКТИКА ВНЕДРЕНИЙ

Шифровальщик семейства VAULT



- ✓ Пересылка письма нескольким адресатам внутри компании
- ✓ Не обнаружено установленными СЗИ компании



Вывод: необходимо устанавливать Anti-APT решение в режиме «блокировки»

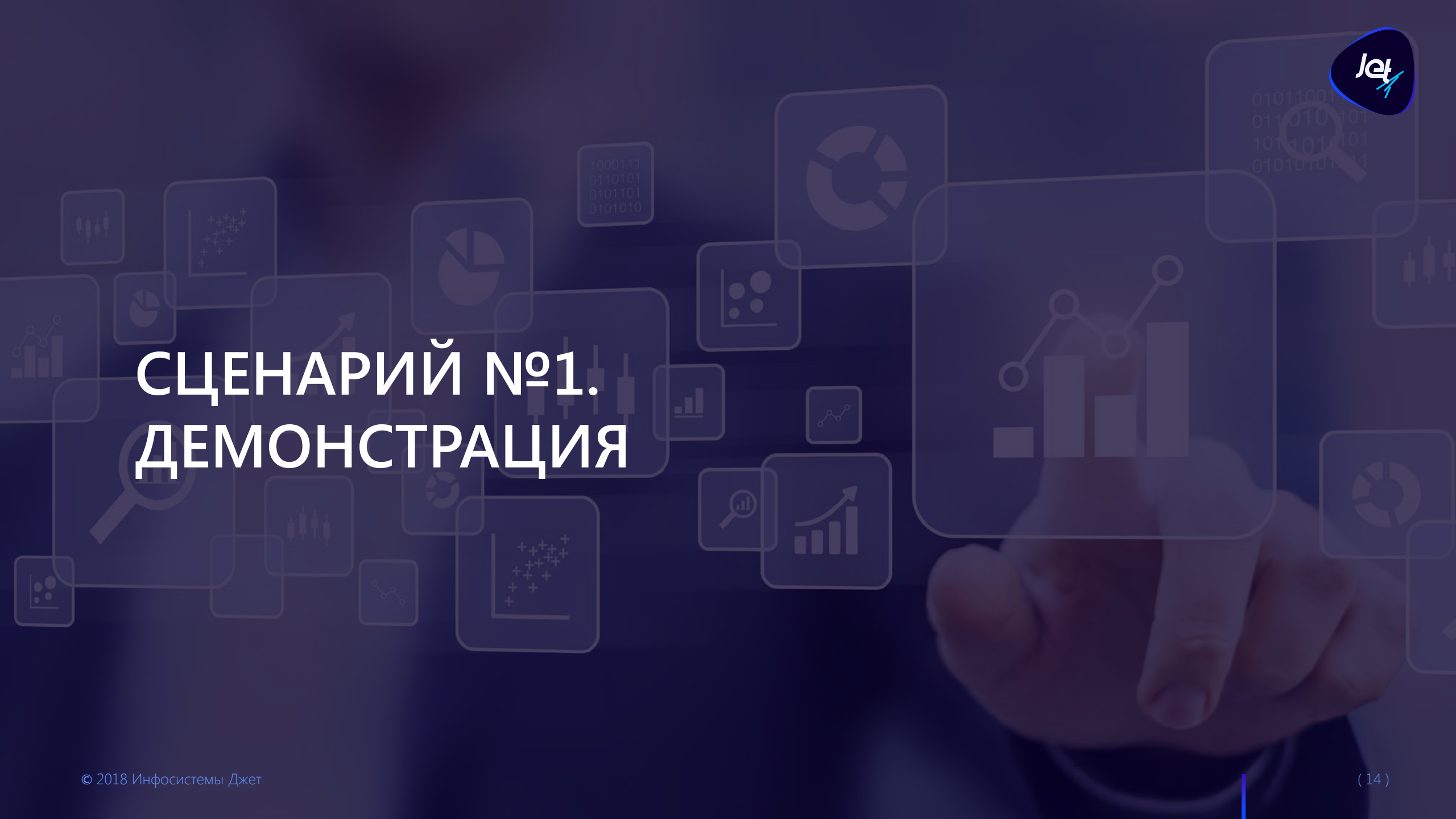
СЦЕНАРИЙ №1. АНАЛИЗ ПОЧТЫ

Check Point SOFTWARE TECHNOLOGIES LTD.

FORTINET

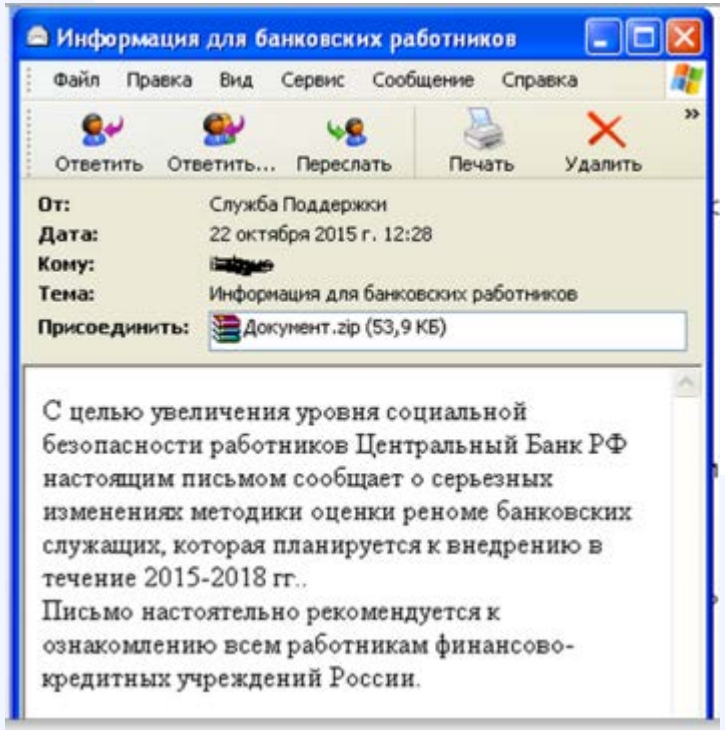
KASPERSKY lab PLATINUM PARTNER

СЦЕНАРИЙ №1. ДЕМОНСТРАЦИЯ



ANTI-APT: ПРАКТИКА ВНЕДРЕНИЙ

Вредоносное ПО Buhtrap



Кастомизированный образ АРМ в песочнице:

- ✓ Сбор логинов и паролей от доменных учетных записей
- ✓ Поиск систем с ПО АРМ КБР
- ✓ Подмена платежных документов в адрес Банка России
- ✓ Вывод из строя зараженных ПК

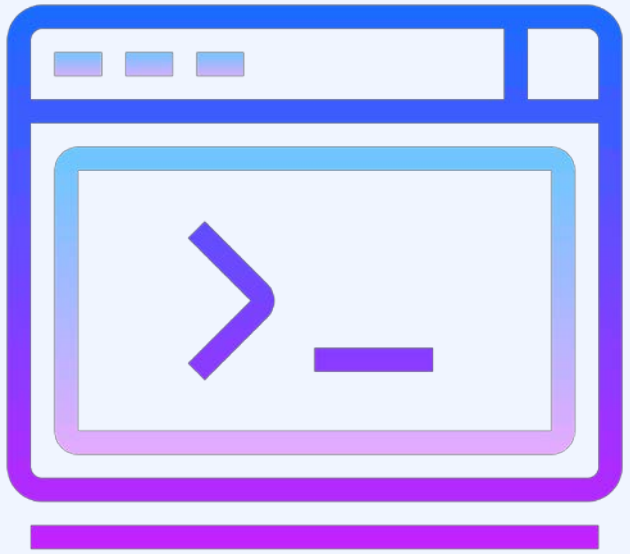
СЦЕНАРИЙ №1. АНАЛИЗ ПОЧТЫ

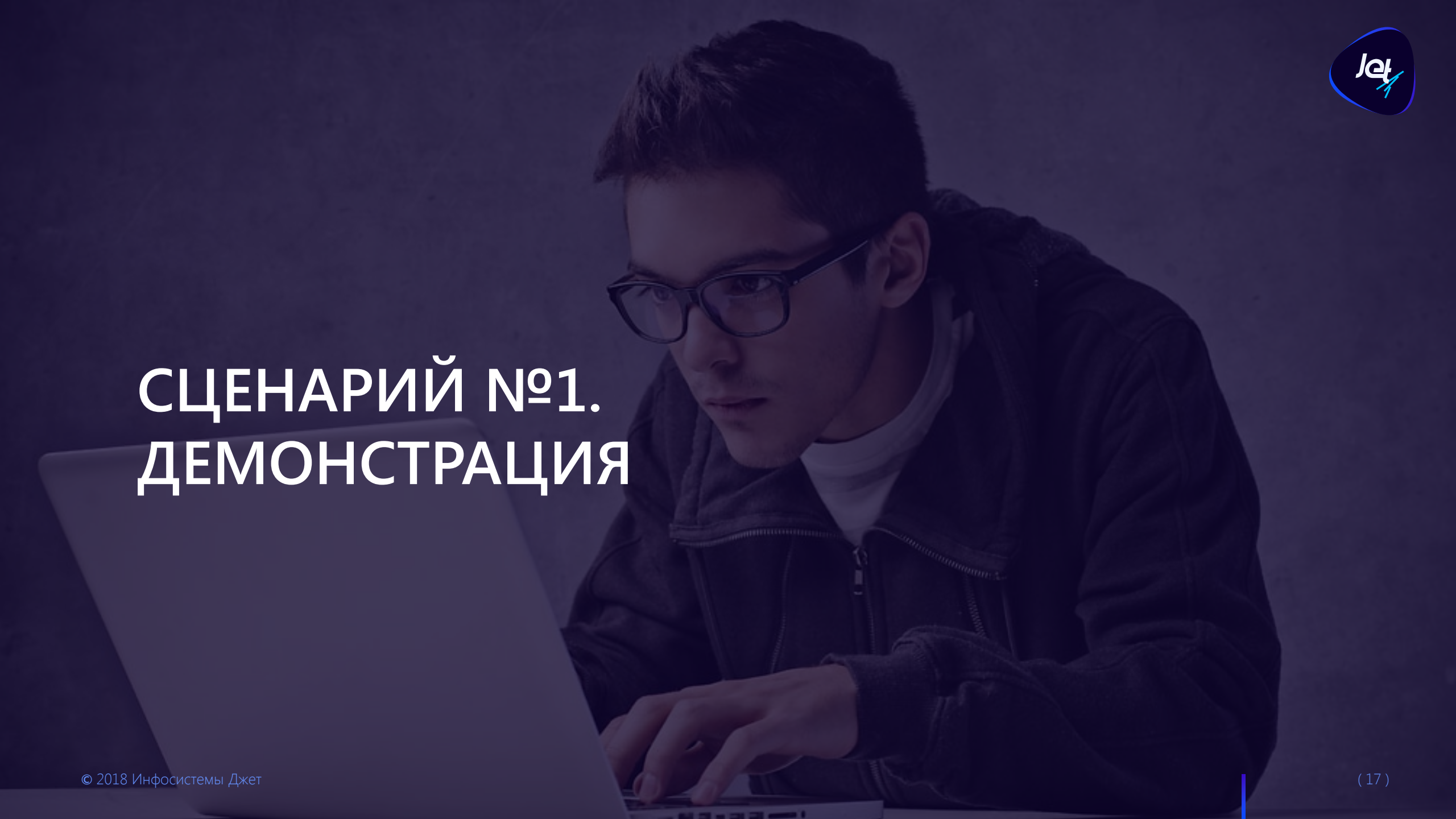
Кастомизация образов

Check Point SOFTWARE TECHNOLOGIES LTD.

KASPERSKY lab PLATINUM PARTNER

FORTINET





СЦЕНАРИЙ №1. ДЕМОНСТРАЦИЯ

СЦЕНАРИЙ №2. АНАЛИЗ WEB

- ✓ скачивание файла из интернета
- ✓ расшифровка SSL

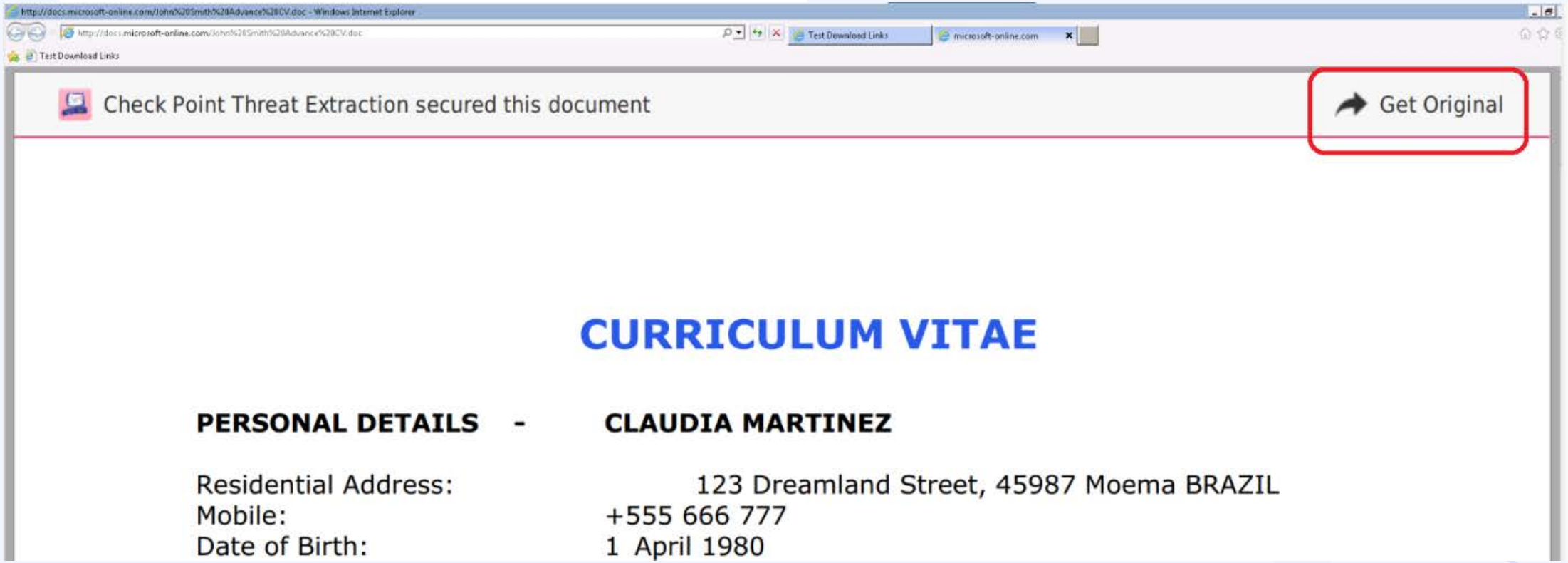
KASPERSKY lab
PLATINUM PARTNER

FORTINET

Check Point
SOFTWARE TECHNOLOGIES LTD.

СЦЕНАРИЙ №2. АНАЛИЗ WEB

Threat Extraction



ANTI-APT: ПРАКТИКА ВНЕДРЕНИЙ

Вредоносное ПО Metel

CallBack:

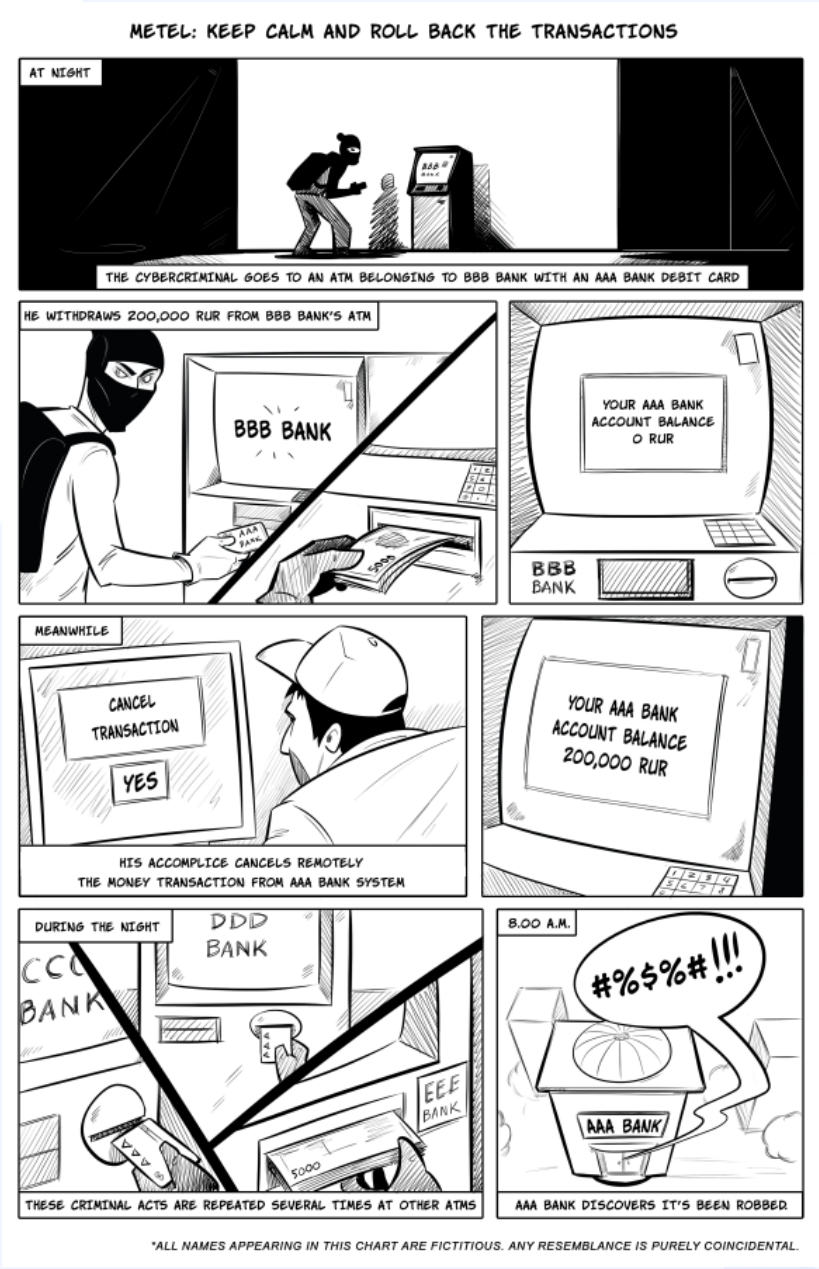
«lev1tan.com»

«bloombergloop.biz»

«archimedus.com»

«uorenbuffets.com»

«wizardtesla.com»



СЦЕНАРИЙ №2. АНАЛИЗ WEB

YARA-правила

СЦЕНАРИЙ №2. ДЕМОНСТРАЦИЯ

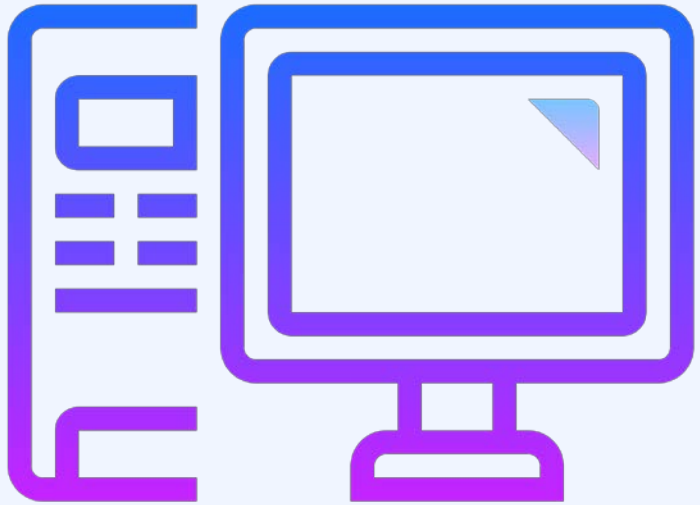
СЦЕНАРИЙ №3. ЗАЩИТА РАБОЧИХ СТАНЦИЙ

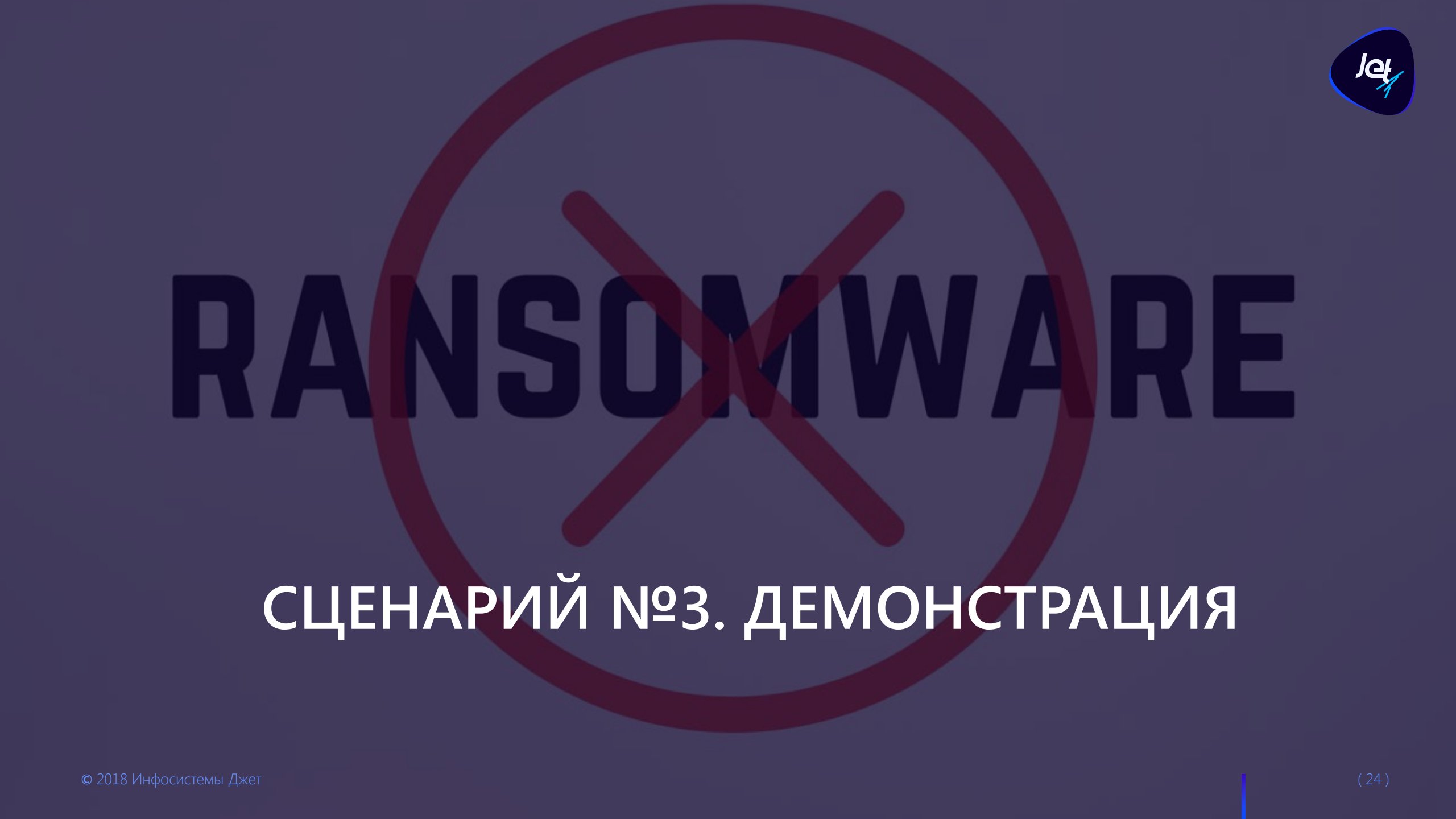
EDR-агент

KASPERSKY lab
PLATINUM PARTNER

FORTINET + CARBON BLACK
ARM YOUR ENDPOINTS

Check Point
SOFTWARE TECHNOLOGIES LTD.





СЦЕНАРИЙ №3. ДЕМОНСТРАЦИЯ

СЦЕНАРИЙ №4. ЗАЩИТА ФАЙЛОВЫХ ХРАНИЛИЩ

Карантин подозрительных файлов

Возможность сканирования по расписанию

✓ Автоматическое перекладывание чистых файлов из одного хранилища в другое

FORTINET

Ждем ваши флешки с вредоносным ПО!

ИНФОСИСТЕМЫ ДЖЕТ

14/02/2018

Спасибо за внимание!