

**KASPERSKY** lab

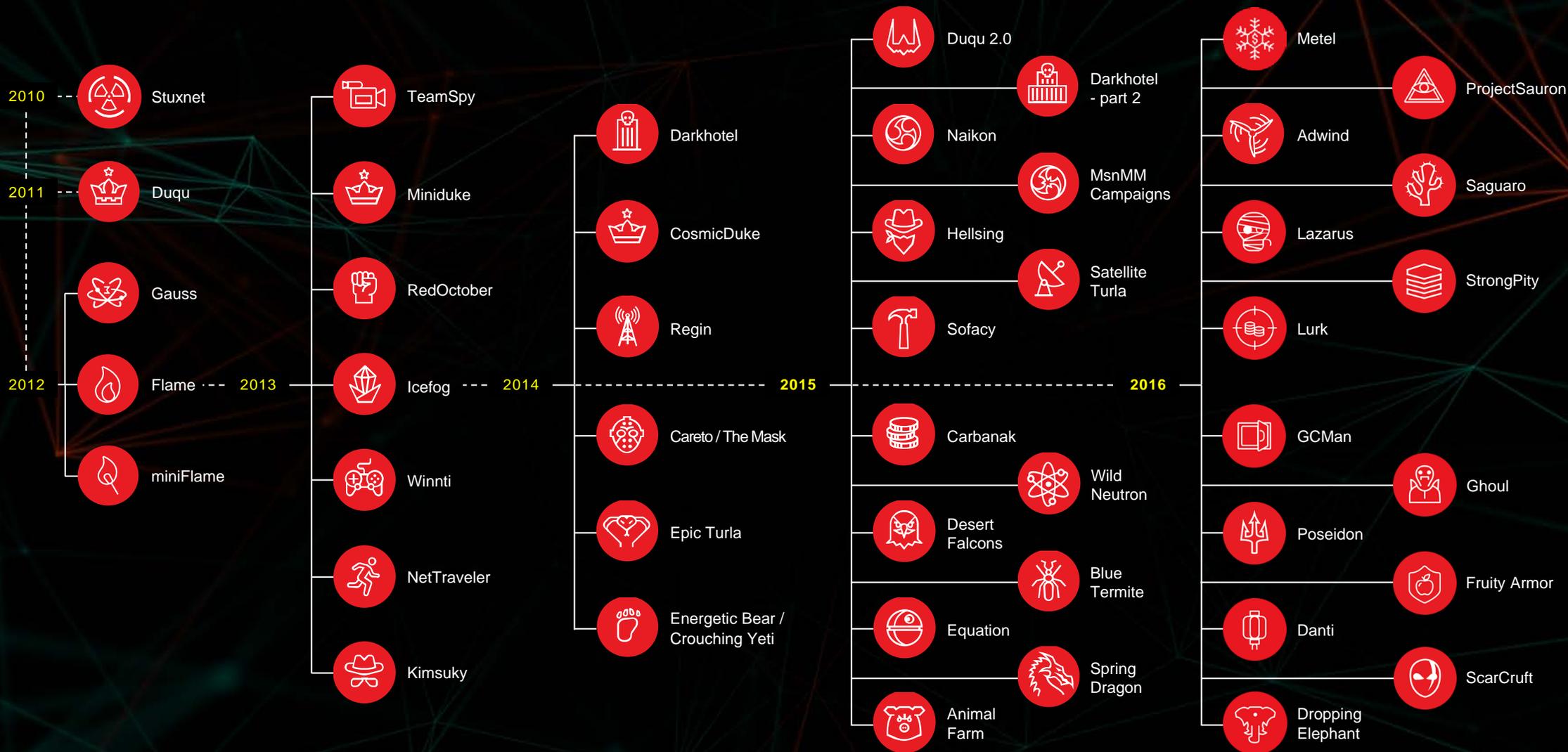


SAVING  
THE WORLD  
FOR 20 YEARS

**Причинять добро и наносить пользу**

**Риски использования мобильных устройств в бизнесе**

# ЭВОЛЮЦИЯ АТАК



# Под угрозой – не только деньги и данные

## ГЛОБАЛЬНЫЕ УГРОЗЫ



Кража денег



Нарушение бизнес-процессов



Потеря доли рынка



Шантаж



Кража цифровой личности



Атаки на клиентов



Мошеннические рассылки от лица оператора



Подделка веб-ресурсов с целью фишинга



Контроль над биллингом

ОПЕРАТОРЫ СВЯЗИ

TELECOM

## МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ



Кража данных о пациентах



Атаки на проекты телемедицины

## ФИНАНСОВЫЕ СТРУКТУРЫ



Кража денег



Кража личности



Шпионаж



Манипуляция открытыми данными



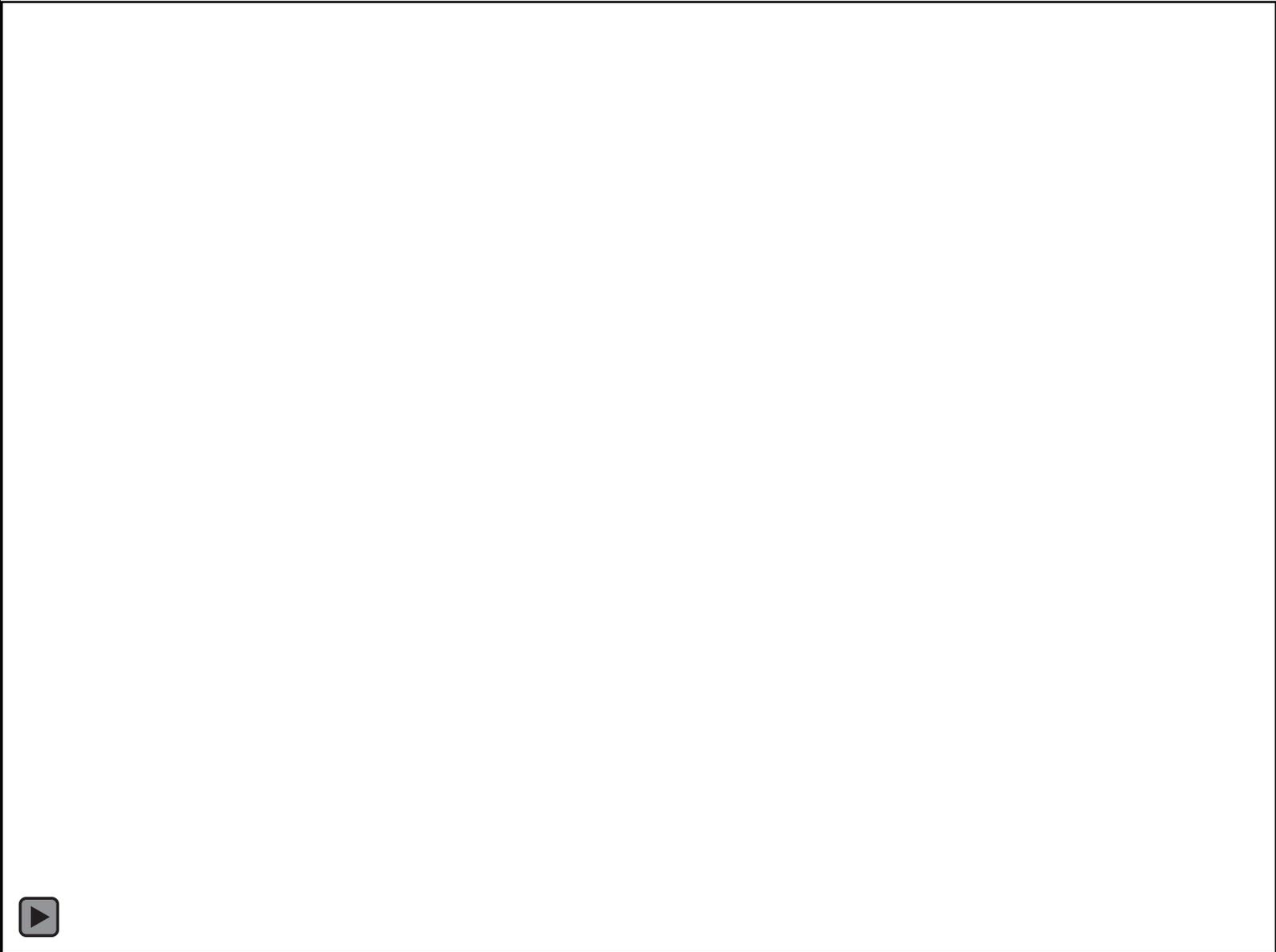
Ограничение доступа к государственным услугам



Кража личности

ГОСУДАРСТВЕННЫЕ ОРГАНИЗАЦИИ

STATE SECTOR



# Роль мобильного устройства

- › Рабочее место (почта, отчеты, контроль)
- › Платежное средство (ЭЦП, мобильный банкинг)
- › Точка аутентификации(пропуск, NFC)
- › Рабочий инструмент (навигация, справочник)
- › Часть инфраструктуры (M2M, интеграция с поставщиками)
- › Точка продажи
- › Средство досуга

# Вектора атаки

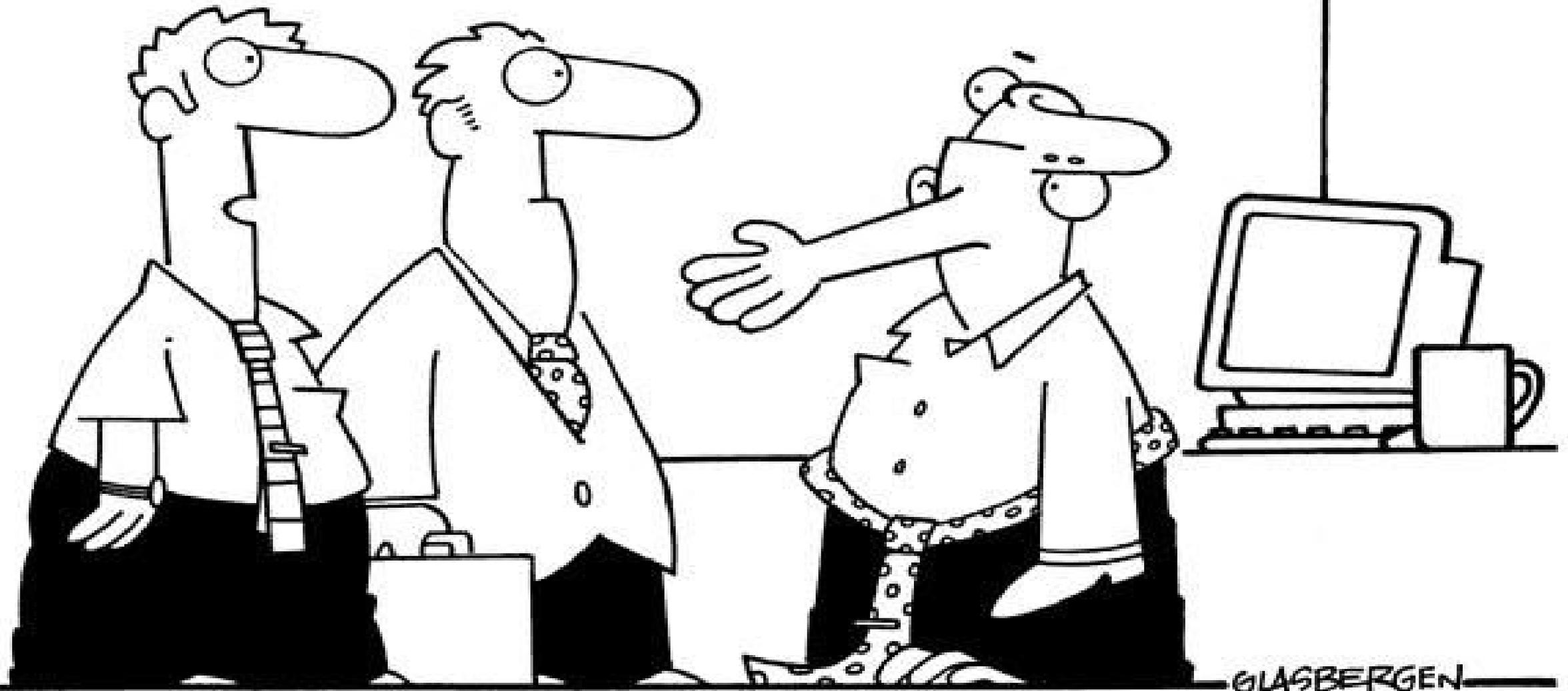
- › Электронная почта
- › SMS/MMS
- › Коммуникаторы
- › Профильные форумы
- › Социальные сети
- › Публичный Wi-Fi
- › Инфраструктуры партнерских сетей
- › Физический доступ

# Итоги атаки

- › Ваши (и чужие!) деньги или данные похищены
- › Вы не контролируете ваше устройство
- › Гаджет является частью чужой атаки
- › Вы заражаете чужие сети и устройства
- › От вас уходит недостоверная информация
- › Информация приходит с критической задержкой

# Риски

- › Финансовые потери
- › Потеря доли рынка
- › Имиджевые риски (шантаж, публичный урон)
- › Административная и уголовная ответственность



«Это наш ИТ-директор. Он зашифрован в целях безопасности»

KASPERSKY lab



SAVING  
THE WORLD  
FOR 20 YEARS

Что делаем?

# Единая платформа защиты, мониторинга, разведки, расследования инцидентов и обучения на базе решений и сервисов Kaspersky Lab (Kaspersky Threat Management & Defense)

ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА

ПЛАТФОРМА НАВЫКОВ  
И ЗНАНИЙ



ПЛАТФОРМА ДОСТУПА  
КО ВСЕЙ ИНФОРМАЦИИ  
О КИБЕР-УГРОЗАХ

# Что делаем?

- › Шифруем все, что можно и нужно
- › Создаем внутри устройства безопасные контейнеры данных
- › Отражаем внешние атаки через любой канал угрозы
- › Контролируем местоположение устройства
- › Мониторим все места, которые посещает владелец
- › Определяем, где, когда и каким образом владелец имеет доступ к интернету, приложениям и прочему функционалу
- › Привязываем профиль устройства к политикам безопасности компании
- › Вовремя и удобно ставим все патчи и апдейты (но безопасные!)
- › Не даем перепрошить гаджет
- › Регулярно резервируем и быстро удаляем данные в случае ЧП



# ПЛАТФОРМА НАВЫКОВ И ЗНАНИЙ УРОВЕНЬ 1. СТРАТЕГИЧЕСКИЕ СИМУЛЯЦИИ ДЛЯ ПЕРВЫХ ЛИЦ



- Стратегическая симуляция для первых лиц организаций
- Обучение стратегическому комплексному подходу к ИБ

СЦЕНАРИИ	
КОРПОРАЦИЯ	Защита крупных организаций (бизнес, квази-гос.сектор)
БАНК	Защита финансовых организаций от внешних и внутренних мошенников и преступников
ГОСУДАРСТВО	Защита сегмента e-GOV от кибер-террористов и мошенников
ПРОМЫШЛЕННОСТЬ	Защита различных отраслевых систем (энергетика, нефть/газ, водоочистка, телеком)

# ПЛАТФОРМА НАВЫКОВ И ЗНАНИЙ

## УРОВЕНЬ 2. ИБ-ТАКТИКА. СИМУЛЯЦИИ ДЛЯ МЕНЕДЖМЕНТА



### Понимание

Принятие мер безопасности как необходимых, правильных, требуемых исходя из текущей ситуации



### Наблюдение

Взгляд на все происходящее в департаментах через призму ИБ



### Безопасное принятие решений

ИБ как часть текущих бизнес-процессов организации



### Лидерство

Советы и менторство по части ИБ над коллегами

# ПЛАТФОРМА НАВЫКОВ И ЗНАНИЙ УРОВЕНЬ 3. ОСНОВЫ КИБЕР-ГИГИЕНЫ ДЛЯ ПЕРСОНАЛА



МОДУЛИ ПРАКТИКИ

+

СИМУЛЯЦИЯ АТАК

СРЕЗ КИБЕР-КУЛЬТУРЫ

ОТЧЕТЫ И АНАЛИТИКА

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ

Платформа обучения сотрудников, разработанная «Лабораторией Касперского», позволяет получить базовые навыки в области цифровой безопасности и тем самым помогает защитить вашу организацию от наиболее распространенных киберугроз.

Посмотрите, как работает Платформа, с помощью бесплатной интерактивной демо-версии. Обратите внимание, что это не полная версия обучающего курса. Полная версия состоит из более чем 20 обучающих модулей, каждый из которых рассчитан на 15 минут времени, а также из инструментальной оценки, автоматического назначения обучающих модулей в зависимости от результатов, подготовки отчетов и аналитики. Демо-версия подготовлена на английском языке, но сама платформа работает на 22 языках, включая русский.

ИНТЕРАКТИВНЫЕ ОБУЧАЮЩИЕ МОДУЛИ

1. Безопасность электронной почты
2. Упоминания по URL адресам
3. Базовые правила безопасности
4. Защита и учетные данные
5. Безопасность мобильных приложений
6. Безопасность мобильных устройств
7. Безопасность паролей
8. PCI DSS
9. Ограничиваем информацию о состоянии здоровья
10. Физическая безопасность
11. PHI
12. Безопасность в социальных сетях
13. Безопасный просмотр веб-сайтов
14. Безопасность вне офиса
15. Социальная инженерия
16. Базовые правила безопасности руководителей
17. Anti-Phishing Phish
18. Anti-Phishing Phylis

СВЯЗАТЬСЯ С ОТДЕЛОМ ПРОДАЖ

**From:** Early Check-In [mailto:dontreply@4.early-checkin.com]

**Sent:** Friday, March 25, 2016 1:54 PM

**To:** Nancy Drubitch <nancy1982@gmail.com>

**Subject:** Preview: Flight Confirmation

Thank you for your purchase. We encourage you to review this information before your trip.

If you need to contact us or check on your flight information, go to [early-checkin.com](http://early-checkin.com), call 800212252 or call the number on the back of your Reward card.

Now, managing your travel plans just got easier. You can exchange, reissue and refund electronic tickets at [early-checkin.com](http://early-checkin.com).

Take control and make changes to your itineraries at [early-checkin.com/itineraries](http://early-checkin.com/itineraries). Speed through the airport.

[Check-in online for your flight.](#)

Flight Information

CONFIRMATION #: MWGJ03

TICKET #: 28195438641658

Day Date Flight Status Bkng Class City Time Meals/Other Seat/Cabin

-----  
Sun 8 JUL 116 OK U LV NYC-KENNEDY AR SAN FRANCISCO 515P 916P F  
45A COACH

# ПЛАТФОРМА НАВЫКОВ И ЗНАНИЙ УРОВЕНЬ 4. БАЗОВЫЕ ИБ-НАВЫКИ ДЛЯ ИТ-ПЕРСОНАЛА



Malware Hunting EDUCATION PROGRESS KASPERSKY

**RANSOMWARE**

You have recently launched unknown file and suppose that it could be a ransomware.

Try to find working cryptor.

More information on ransomware features is available here

Enter suspicious process PID:

Process: chrome.exe

I suppose that this process is malware. First of all, it [has high CPU load](#). Secondly it is strange that it [does not have description](#). And it [choose answer](#) [choose answer](#)

14:14 21/06/2017

192.168.152.2 - Remote Administration

Process Hacker 2

Name	PID	CPU	I/O Total ...	Private by...	User name	Description	Verified Signer	Verification s...
chrome.exe	1698	90.58	4.3 KB/s	868.7 KB	WIN-658C...	Google Chrome		
System Idle Process	1	11.57			NT AUTHO...			
chrome.exe	2204	0.42	2.5 KB/s	1.3 MB	WIN-658C...	Go		
Skype.exe	1948	0.12	791.6 KB/s	2.5 MB	WIN-658C...	Sky		
firefox.exe	2732	0.1	671.3 KB/s	4.5 MB	WIN-658C...	Fire		
svchost.exe	1424	0.08		122.9 KB	NT AUTHO...	Ho		
csrss.exe	412	0.05		453.6 KB	NT AUTHO...	Cle		
CyberArticle.exe	1912	0.04		1.0 MB	WIN-658C...	Cyt		
Interrupts		0.04				Int		
System	4	0.04		2.0 KB	NT AUTHO...	NT		
svchost.exe	520	0.02		696.0 KB	NT AUTHO...	Ho		
AcroRd32.exe	2664	0.02		3.2 MB	WIN-658C...	Ad		
lsass.exe	1272	0.02		162.4 KB	NT AUTHO...	Loc		
explorer.exe	1564			2.0 MB	WIN-658C...	Wi		
csrss.exe	352			62.9 KB	NT AUTHO...	Cle		
svchost.exe	1008			234.9 KB	NT AUTHO...	Ho		
svchost.exe	3660			321.7 KB	NT AUTHO...	Ho		
wordpad.exe	2368			408.9 KB	WIN-658C...	Wi		
lsm.exe	904			57.5 KB	NT AUTHO...	Loc		
wordpad.exe	2508			431.3 KB	WIN-658C...	Wi		
svchost.exe	628			116.3 KB	NT AUTHO...	Ho		
audiodg.exe	3580			700.8 KB	NT AUTHO...	Wi		
svchost.exe	1076			546.5 KB	NT AUTHO...	Ho		
WinRAR.exe	1976			269.4 KB	WIN-658C...	Wi		
spoolsv.exe	1224			229.5 KB	NT AUTHO...	Sp		

Properties

chrome.exe

57.0.2987.133

Image file name: C:\temp\uhcqijkjds\chrome.exe

Process

Command line: "C:\temp\uhcqijkjds\chrome.exe"

Current directory: C:\temp\uhcqijkjds

Started: 23 seconds ago (7:23:31 PM 4/13/2017)

PEB address: 0x7ffde000 Image type: 64-bit

Parent: explorer.exe (1564)

Mitigation policies: DEP (permanent)

Protection: None

Тренинги для ИТ-команд:

- Первая линия обороны в части реакции на инциденты
- Снижение количества инцидентов в силу неправильных настроек ПО и оборудования
- Развитие критического мышления по части ИБ у ИТ-команд

# ПЛАТФОРМА НАВЫКОВ И ЗНАНИЙ

## УРОВЕНЬ 5. ПРОФЕССИОНАЛЬНЫЕ НАВЫКИ ЦИФРОВЫХ РАССЛЕДОВАНИЙ ДЛЯ СПЕЦИАЛЬНЫХ ПОДРАЗДЕЛЕНИЙ



### ЦИФРОВАЯ ФОРЕНЗИКА

АНАЛИЗ ЦИФРОВЫХ УЛИК, РЕКОНСТРУКЦИЯ АТАКИ, ХРОНОЛОГИЯ И ЛОГИКА, РАСКРЫТИЕ ПРИЧИН ИНЦИДЕНТА



### ПРОФЕССИОНАЛЬНЫЕ ТРЕНИНГИ



### АНАЛИЗ ВРЕДНОСНОГО КОДА

ПОЛНОЕ ПОНИМАНИЕ ПОВЕДЕНИЯ И ЗАДАЧ ВРЕДНОСНЫХ ОБЪЕКТОВ



### РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

ВЕДЕНИЕ ПОЛНОГО ЦИКЛА РАССЛЕДОВАНИЯ ИНЦИДЕНТА ДЛЯ ПОЛНОГО УСТРАНЕНИЯ ДАЛЬНЕЙШИХ УГРОЗ ОРГАНИЗАЦИИ



HAPPY MONDAY FAMILY

МЕСТО, ГДЕ  
СЛУЧАЮТСЯ  
ЧУДЕСА

ЗОНА  
ТВОЕГО  
КОМФОРТА



Вопросы?

KASPERSKY



SAVING  
THE WORLD  
FOR 20 YEARS