

The background of the slide is a close-up, high-angle photograph of a calculator keypad. The keypad is light-colored, possibly white or light grey, and features several dark grey buttons. A prominent feature is a large, dark grey button with a white right-pointing triangle. Other visible buttons include a "MENU" button and a red "STOP" button. The keypad is set against a background of a blue and green grid pattern, which appears to be a digital display or a textured surface. The overall lighting is soft and even.

ПОДХОД ЛАБОРАТОРИИ КАСПЕРСКОГО К ЗАЩИТЕ ВСТРАИВАЕМЫХ СИСТЕМ

Георгий Шебулдаев

Менеджер корпоративных технологических проектов



АТАКИ НА POS И БАНКОМАТЫ

Атаки на POS терминалы

2011: Subway
146 000 карт скомпрометировано

2012: Dexter
(POS в отелях, ресторанах в 40 странах)

2013: Stardust

2014: Jimmy Jones, SuperValu, Albertson

2014: Target (40 млн карт, 70 млн клиентов)

Атаки на Банкоматы

2003: Bank of America проблемы с Банкоматной сетью из-за SQL Slammer

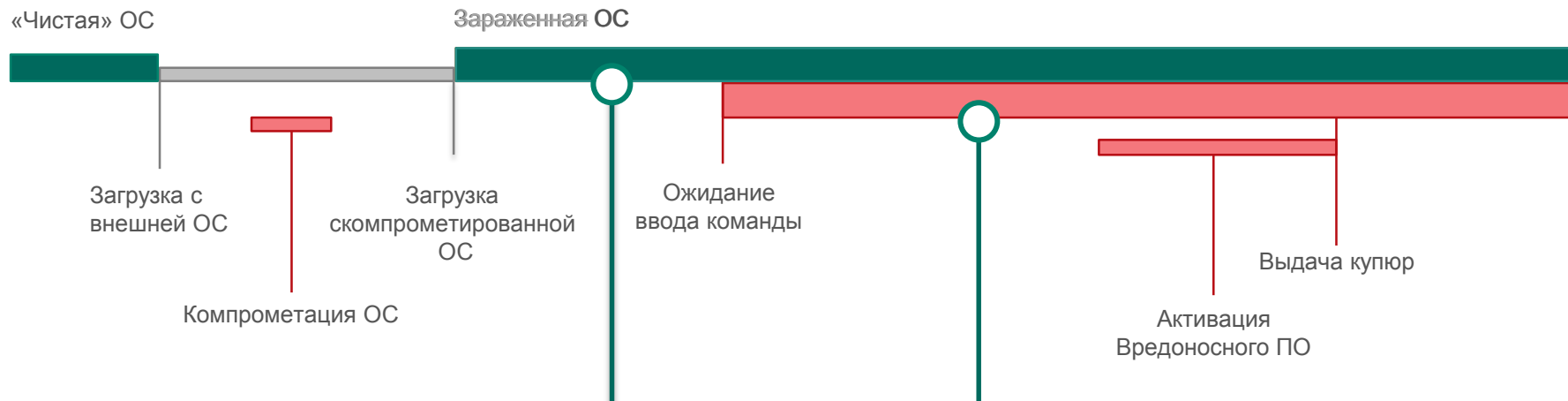
2009: Backdoor.Win32.Skimer - вредоносное ПО установлено при физическом доступе к банкоматам. Россия и Украина.

2010: Brazil - Trojan-Spy.Win32.SPSniffer перехват данных с карт. COM and USB ports

2010: Black Hat demo (Barnaby Jack)

2014: Tyurkin
Манипулирование банкоматами при помощи вредоносного ПО

BACKDOOR.MSIL.TYUPKIN



Антивирусные движки

Статические анализаторы



Exact & Stream Signatures

Анализаторы URL



URL Bases (Anti-Phishing, Malware и т.п.)

Эвристические анализаторы



Heuristic Signatures, Detection & Cure Code

Эмуляторы

Средства очистки



Компоненты контроля запуска и исполнения приложений

PDM | Proactive Defense Module



Behavior Patterns (WL & BL), Signatures

HIPS | Host Intrusion Prevention System



HIPS Policies, IDS Rules

EP | Exploit Protection



Software Categories, Categorization Rules, Security Permissions

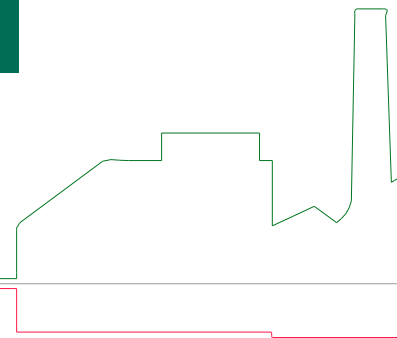
EAC | Enterprise Application Control



KASPERSKY

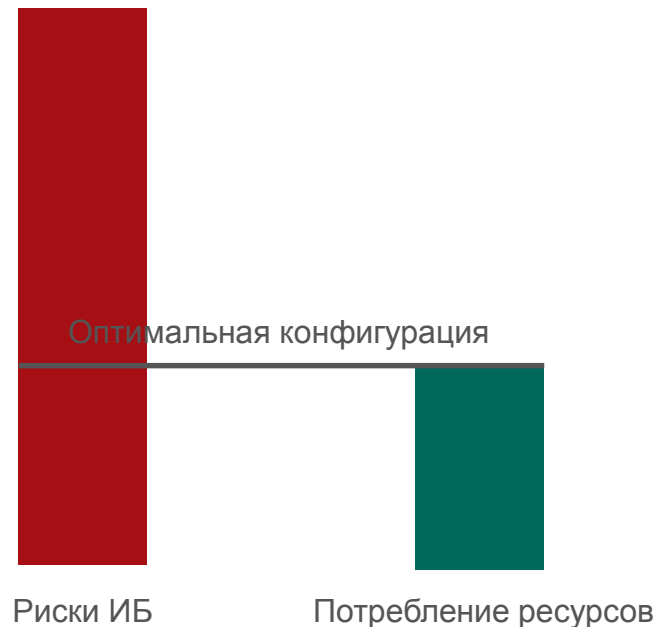
SECURITY

ДЛЯ EMBEDDED СИСТЕМ



ПОДХОД К ЗАЩИТЕ ВСТРАИВАЕМЫХ УСТРОЙСТВ

- 1) Использование стандартного продукта Kaspersky Endpoint Security 10
- 2) Предустановка производителем
- 3) Определение оптимальной конфигурации и тестирование совместимости со сторонним ПО
- 4) Соответствие требованиям Гос регуляторов



РЕШЕНИЯ ЛК ДЛЯ WINDOWS EMBEDDED

Продукт - Kaspersky Endpoint Security 10 для Windows

- Флагманский продукт Лаборатории Касперского
- Сертифицирован ФСТЭК

Расширение поддержки Windows Embedded:

Сейчас:

- Windows Embedded POSReady 7 x86 / x64
- Windows Embedded Standard 7 SP1 x86 / x64
- Microsoft Windows Embedded POSReady 2009

В 2015 году:

- Windows Embedded 8 Standard
- Windows Embedded 8 Industry

КОМПОНЕНТЫ СОВРЕМЕННОГО АВ-СРЕДСТВА



Перехватчики

Драйверы
onAccessScan

Сетевые драйверы
IDC, Firewall

Плагины
почтовые клиенты, браузеры, IM-клиенты



Антивирусные движки

Статические анализаторы



Exact & Stream Signatures

Анализаторы URL



URL Bases (Anti-Phishing, Malware и т.п.)

Эвристические анализаторы

Эмуляторы

Средства очистки



Heuristic Signatures, Detection & Cure Code



Компоненты контроля запуска и исполнения приложений

PDM | Proactive Defense Module



Behavior Patterns (WL & BL), Signatures

HIPS | Host Intrusion Prevention System



HIPS Policies, IDS Rules

EP | Exploit Protection

EAC | Enterprise Application Control



Software Categories, Categorization Rules,
Security Permissions

НОВАЯ МОДЕЛЬ ЛИЦЕНЗИРОВАНИЯ ДЛЯ OEM (РФ)

Традиционный канал

- > Лицензии до 2 лет
- > Срок лицензии с момента активации конечным пользователем
- > Скидка от объема каждого заказа

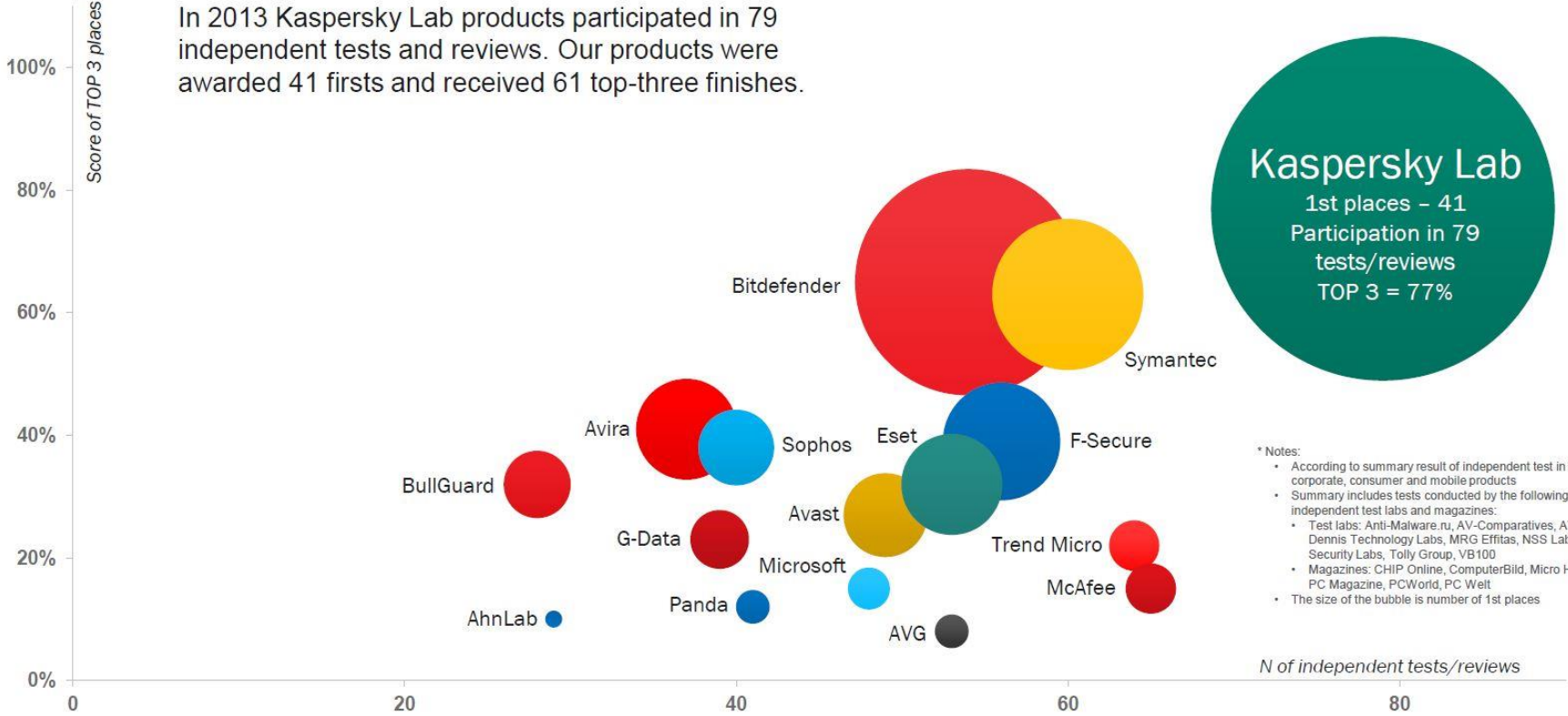
OEM Дистрибьютор (Quarta)

- > Лицензии до 3 лет
- > Активация на этапе сборки устройства + период доставки
- > «Плоское» ценообразование

СПАСИБО ЗА
ВНИМАНИЕ!

KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION*

In 2013 Kaspersky Lab products participated in 79 independent tests and reviews. Our products were awarded 41 firsts and received 61 top-three finishes.



* Notes:

- According to summary result of independent test in 2013 for corporate, consumer and mobile products
- Summary includes tests conducted by the following independent test labs and magazines:
 - Test labs: Anti-Malware.ru, AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, Tolly Group, VB100
 - Magazines: CHIP Online, ComputerBild, Micro Hebdo, PC Magazine, PCWorld, PC Welt
- The size of the bubble is number of 1st places

N of independent tests/reviews