Современные угрозы и технологии на страже

Региональный представитель в УрФО и Пермском крае

Александр Орда

Россиянус интернетус юзерус

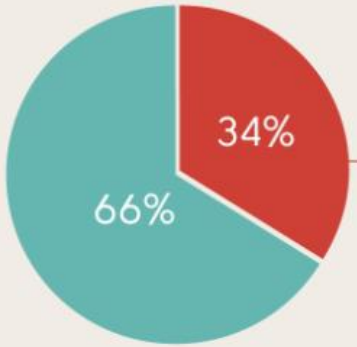
Портрет типичного российского пользователя на основании данных 14,6 млн россиян за 2011 год

55% пользуются Windows XP

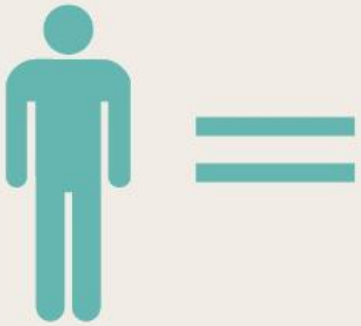
В среднем каждый подвергается **64** сетевым и **10** фишинговым атакам в год

Подвергается фишинговым атакам на поддельных сайтах, выдающих себя за

Каждый пятый пользователь использует один и тот же пароль ко всем аккаунтам, а значит, рискует лишиться их всех. В России бдительность пользователей выше — беспечен лишь 1 из 10, а каждый четвертый соблюдает принцип «1 аккаунт — 1 пароль».



ИСПОЛЬЗУЮТ НЕСТОЙКИЕ ПАРОЛИ



= 5 УЧЕТНЫХ ЗАПИСЕЙ ИЗ КОТОРЫХ 3 В СОЦСЕТЯХ

САМЫЕ ПОПУЛЯРНЫЕ

- 12345
- qwerty
- 1а2б3в
- пароль
- откройся
- отвали

МОЖНО ЛЕГКО УЗНАТЬ

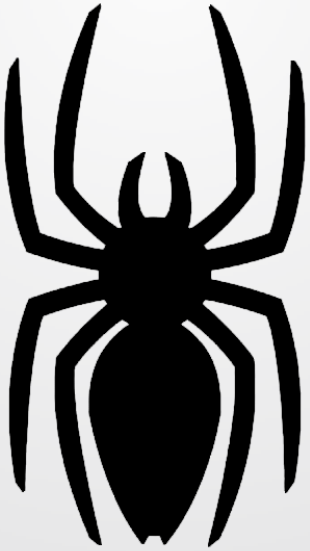
- 17% День рождения
- 10% Номер телефона
- 10% Имя
- 9% Кличка животного

Традиционная Киберприступность

Эволюция зловредного ПО

1994

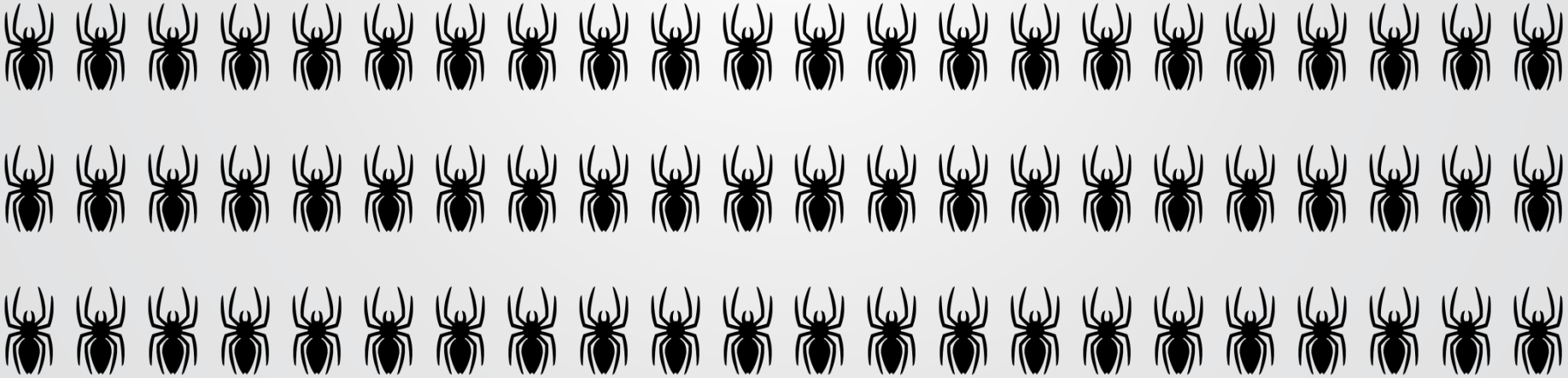
Один новый вирус каждый час



Эволюция зловредного ПО

2006

Один новый вирус каждую минуту



Эволюция зловредного ПО

2011

Один новый вирус каждую секунду

Или 70.000 экземпляров\день

Kaspersky Lab

Ежедневно обрабатывает

200.000

1 345 570 352 угроз в Q1 2013

Эво ПО

Унесенные спамом 2012

В среднем **72%** писем в почте россиян является **спамом**

3,4% писем содержат **вредоносные вложения**

Вредоносные программы для **кражи логинов и паролей** чаще всего оказываются во вложениях в спам-сообщениях

Соцсети больше всех (**24,5%**) подвергаются **атакам фишеров**

Кто отправляет письма в спам?

по данным @mail.ru group

Мужчины **52%**

Женщины **48%**

Азия лидирует по объему **спама**, рассылаемого с территории стран региона

8-е место в мире заняла **Россия** в 2012 году по объему спама, рассылаемого с ее территории

Главные отправители спам-писем*

- купонные сервисы
- сайты знакомств
- онлайн-площадки
- службы бесплатных почтовых рассылок
- сайты для поиска работы

по данным @mail.ru group

KASPERSKY lab

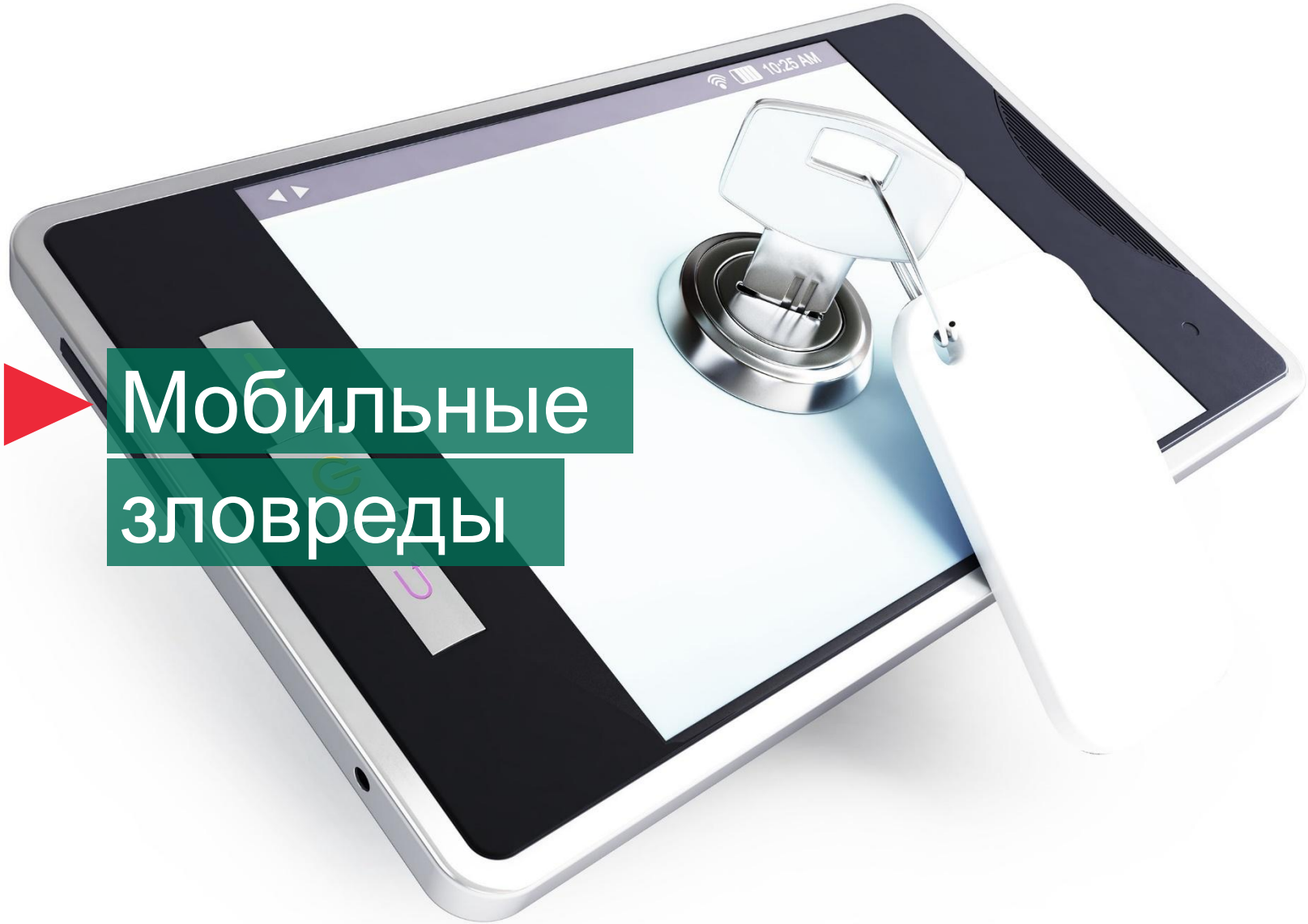
ЗАО «Лаборатория Касперского», 1997–2012

* данные по количеству писем за 1 день

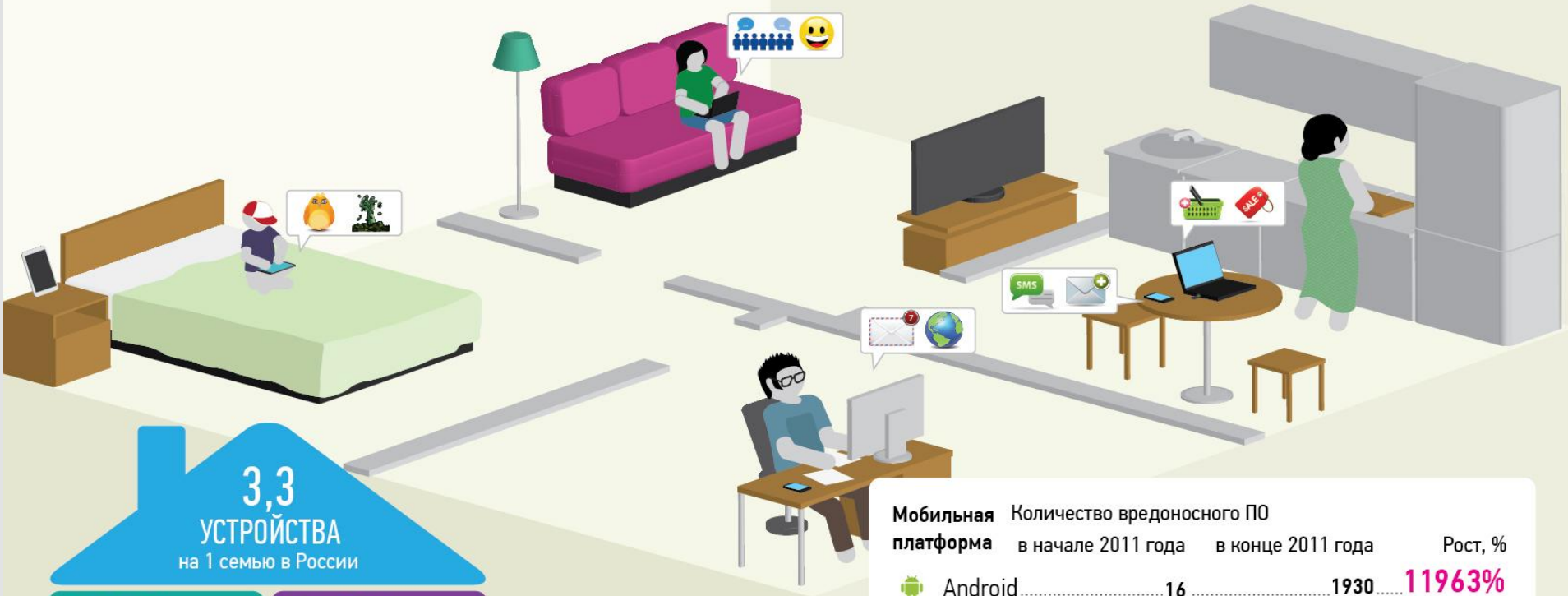
KASPERSKY lab

Социальная инженерия

Мобильные зловреды



Тотальная «ГАДЖЕТизация» населения - источник счастья или опасности ?



3,3
УСТРОЙСТВА
на 1 семью в России

18,8%
2 и более ПК

24,5%
2 и более смартфона

16,2%
2 и более ноутбука

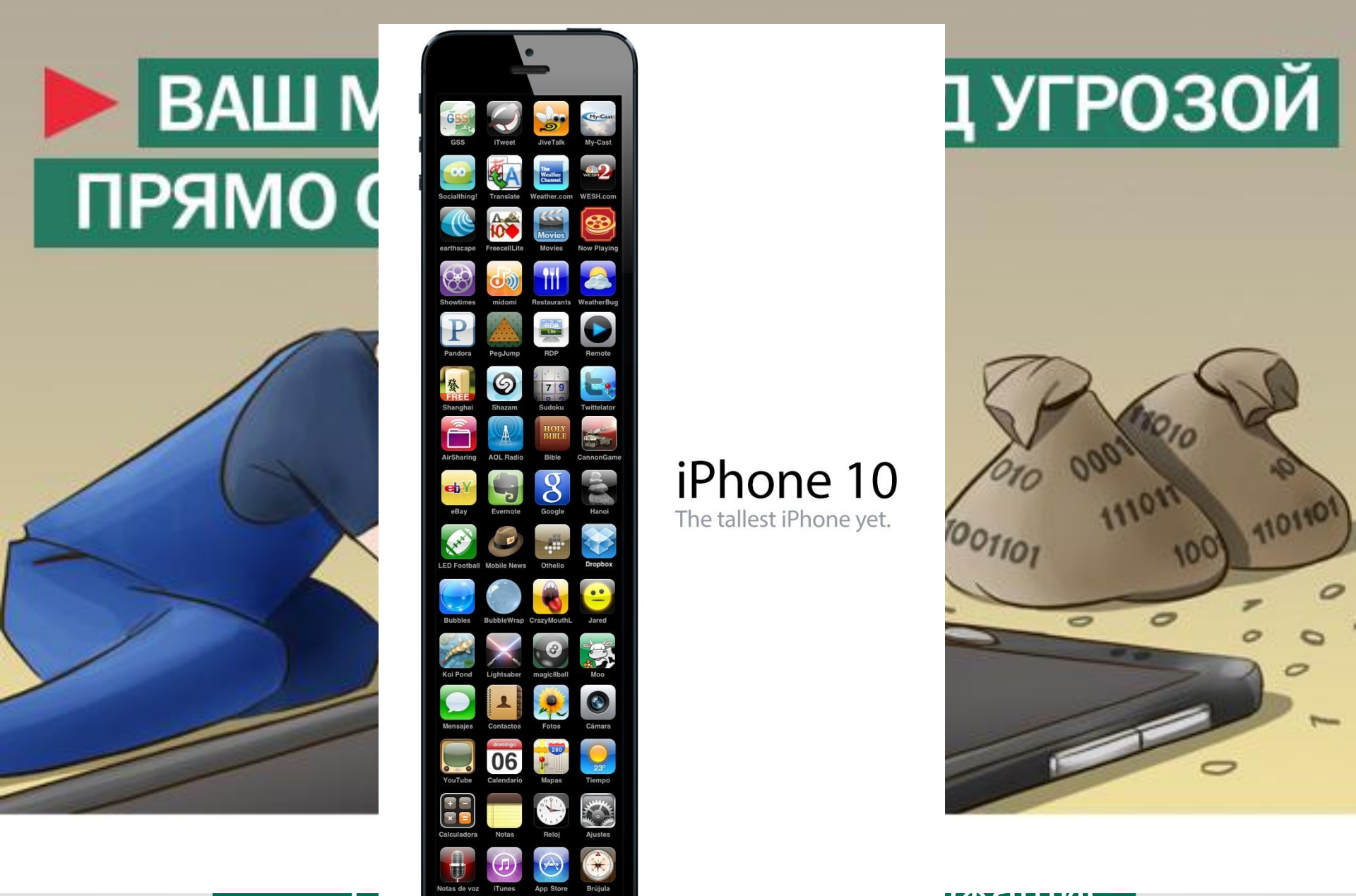
10,7%
уже есть планшет

6,5% СЕМЕЙ
домашний ПК, ноутбук, смартфон, планшет

Мобильная платформа	Количество вредоносного ПО в начале 2011 года	в конце 2011 года	Рост, %
Android	16	1930	11963%
Java2ME	620	1612	160%
Symbian	314	364	16%
Windows Mobile	72	81	13%

Операционная система	Количество вредоносного ПО в начале 2011 года	в конце 2011 года	Рост, %
Windows	2975764	5345105	80%
Mac OS	138	186	35%

KASPERSKY lab



KASPERSKY lab

iOS Взлом за 1 минуту !!!

Смотрите BlackHat новости за июль или youtube.com

KASPERSKY lab

Частна

Что делать? Мобильные устройства

- **ТОП 5 «Нельзя, ни в коем случае!»:**

1. Взламывать / джейлбрейкать смартфон или планшетник!
2. Использовать публичные Wi-Fi сети без пароля для деловой переписки (можно подслушать трафик)
3. Использовать простой или короткий PIN
4. Устанавливать приложения из не доверенных источников
5. Хранить конфиденциальные документы


Банковские
зловреды

A problem has been detected and Windows has been shut down to prevent damage of your comuter.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer, If this screen appears again, follow these steps:

Chceck to make sure any new hardware or software is properly installed.If this is a new installation, ask your ha software manufacturer for any windows updates you might need.

If problems continue, disable installed hardwre od software. Disable BIOS memor ng or shadowing.If you need to use Safe Mode to remove start your computer, press F8 to select Advanced Start ct Safe Mode.Technical information:

*** STOP: 0x000000D1 (0x000 5A89)

*** gv3.sys - Adress B5000, DateStamp 3dd991eb

Beginning dump of physical memory

Physical memory dump complete.

Зловреды для MAC


MacDefender
Mac Security
MacGuard
FAKE AVs

MAC OSx Ботнет Flashfake

- 700,000 зараженных машин
- Распространение через зараженные веб сайты под видом Java Applet

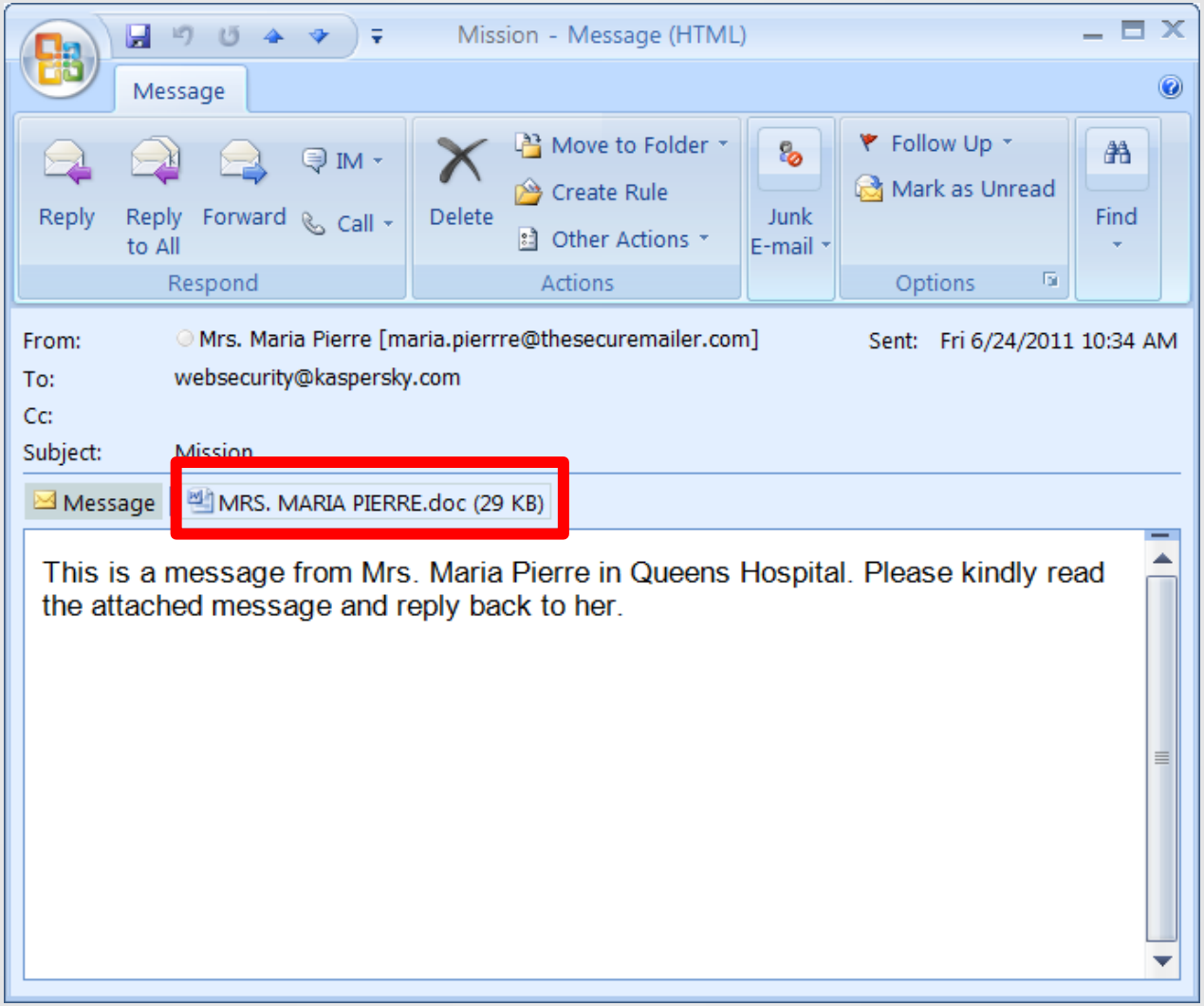
3,5 % всех пользователей MAC заражены

Представьте себе заражение 3,5% пользователей Windows …

KASPERSKY lab


Таргетированные атаки
на организации

Targeted Attacks — начнем с упражнения



KASPERSKY lab


SOS на мыло
UAS@NONPARTISAN.COM
Салют буржуа ! Наши быстроходные катера,атаковали ваш файловоз.
Ваш компьютер взят на абордаж командой Замбийских пиратов .
Ваши файлы зашифрованы нашим морским криптографом Нид Фудом
Если вы, не вонючий ябеда,то мы готовы обменять вашу
драгоценную инфу, на жалкие бумажки именуемые бабосами.
Бабосы - кокосы, колитесь -делитесь, добром обернитесь...
Любовь или месть, жадных Вуду станет есть...
У кого дела не спорятся, в Африке за вас помолятся...
Алчных и неадекватов, за борт всех без адвокатов.
Весёлый роджер на волнах качается ,
весёлым и находчивым скидка полагается.
САМОУНИЧТОЖЕНИЕ ФАЙЛОВ НАЧНЁТСЯ ЧЕРЕЗ 35 ЧАСОВ

Los Angeles Times

LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT F

TRENDING NOW ▲ TORNADOES | SPURS-GRIZZLIES | INTERNAL REVENUE S

Premium content. Unique experiences. Exclusive offers.

David McNew / Getty Images

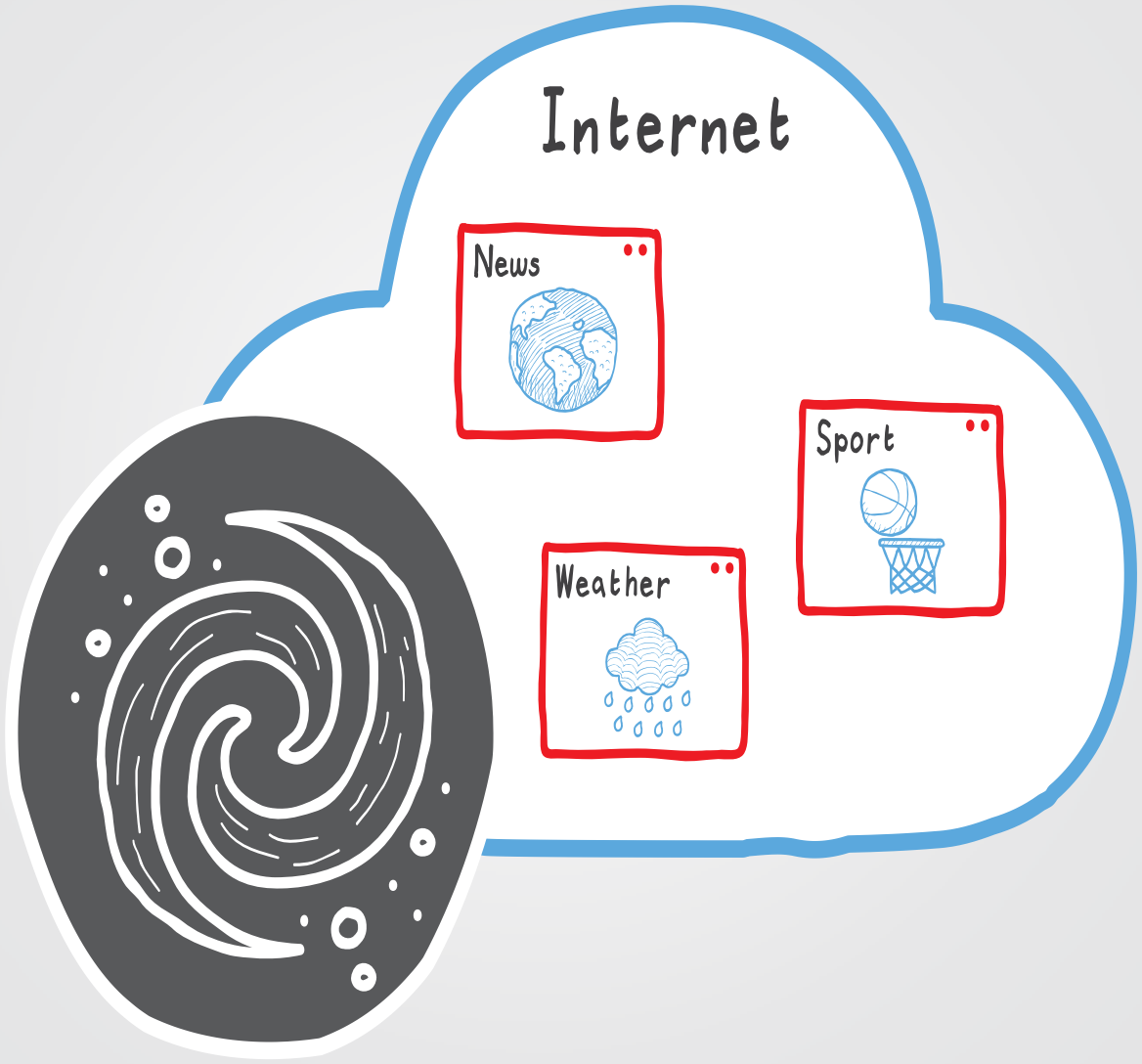
Health
cause
gaps in
By Anna Gor
Common life
incomes to f
married or d
or losing a jo
million low-i
lapses in hea
bounce betw
insurance ex

Suburbs now home to majority of poor

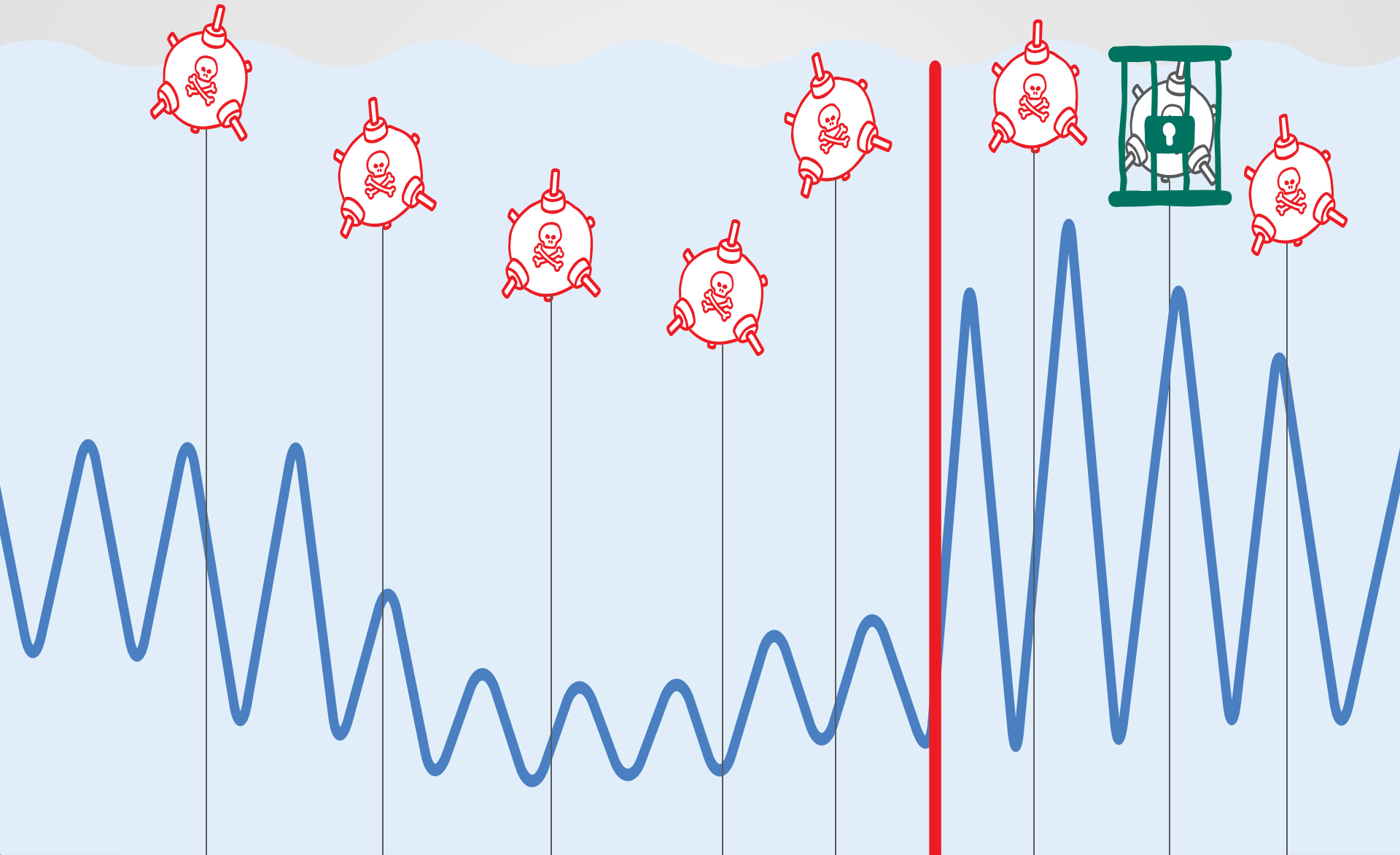
ARE MY LOVELY

WEB SITES DANGEROUS?

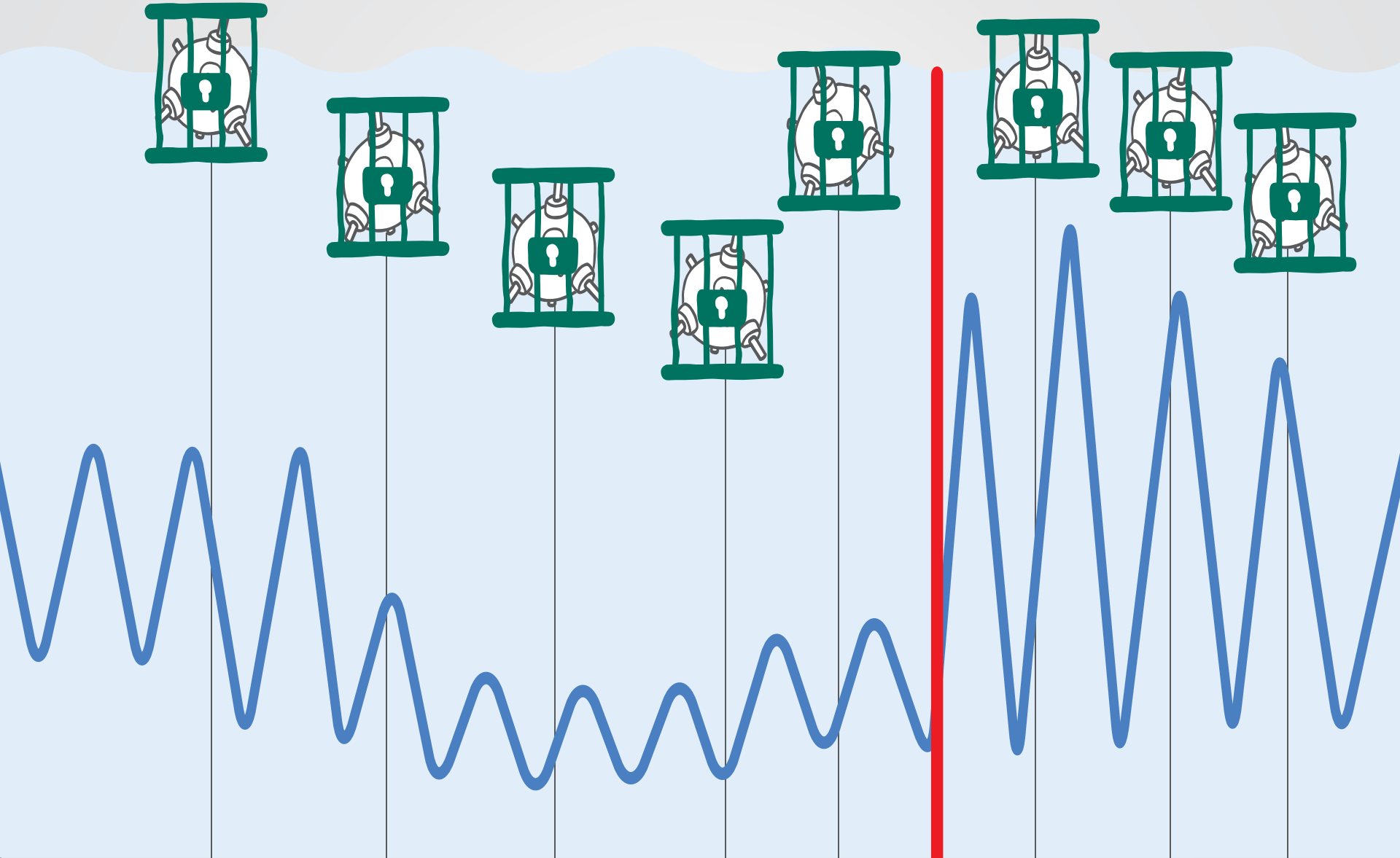
Опасны ли мои любимые сайты?



Are my lovely web sites dangerous? Java 0 day

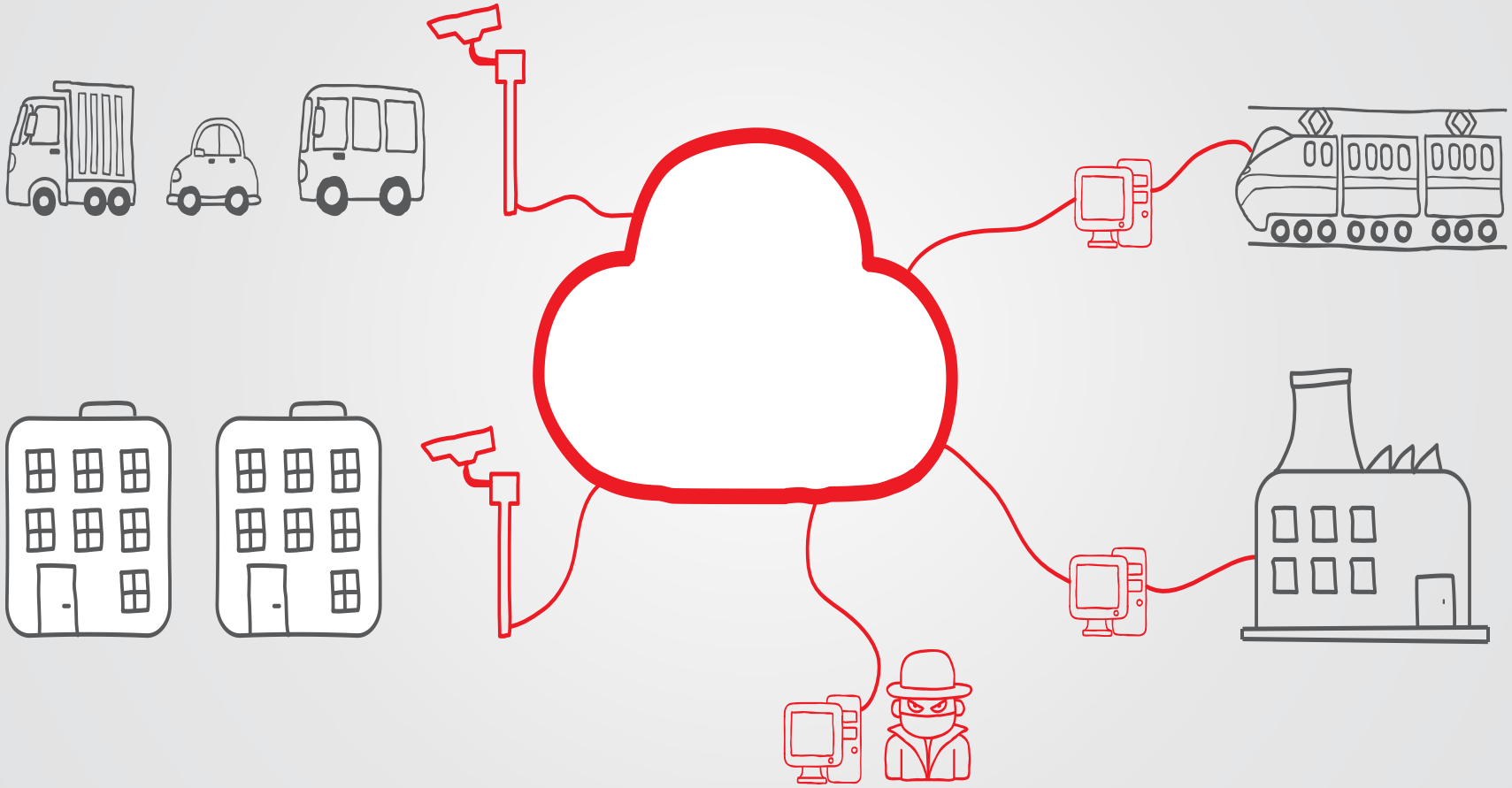


Are my lovely web sites dangerous? AEP efficiency

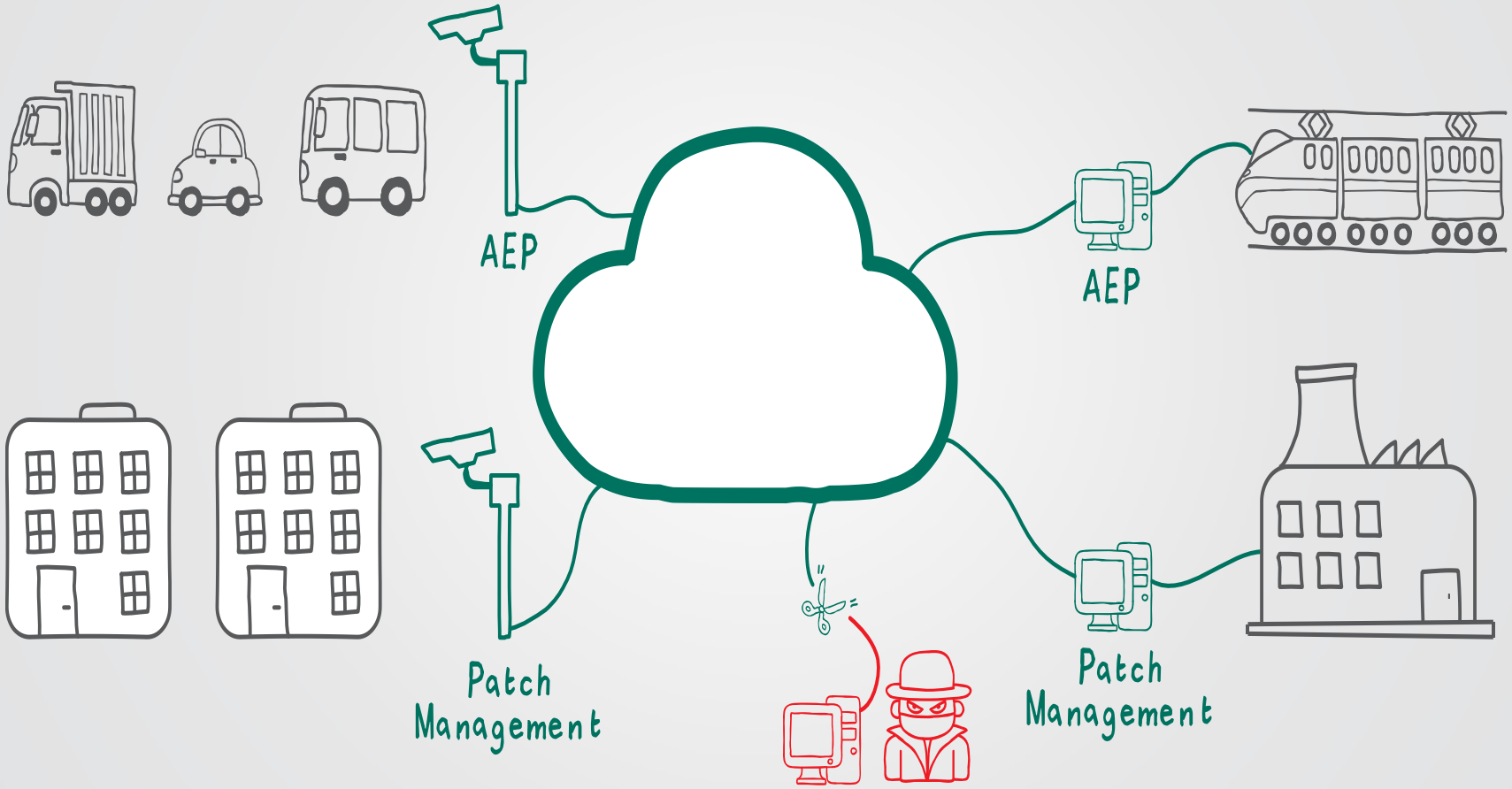



VIRUS на дежурстве
Или недобросовестная конкурентная борьба

Вирус на дежурстве



Есть решение



KASPERSKY lab

Автоматизированные системы управления технологическими процессами (АСУ ТП) – – проблемы кибербезопасности

В последнее время выявлено огромное число проблем информационной безопасности в различных компонентах самых распостраненных АСУ ТП

Существует риск серьезных последствий связанных с неполадками в АСУ ТП критически важных объектов

Лаборатория Касперского проводит исследования, направленные на существенное повышение уровня кибербезопасности АСУ ТП КВО

Компоненты АСУ ТП информационная безопасность

Уязвимости АСУ ТП, PLC: исследования Digital Bond

- Allen-Bradley: ControlLogix & MicroLogix
- Schneider Electric: Modicon Quantum
- General Electric: D20ME
- Schweitzer: SEL-2032
- Koyo: Direct LOGIC H4-ES

✗ – обнаружено, легко использовать
! – обнаружено, трудно использовать
✓ – не обнаружено

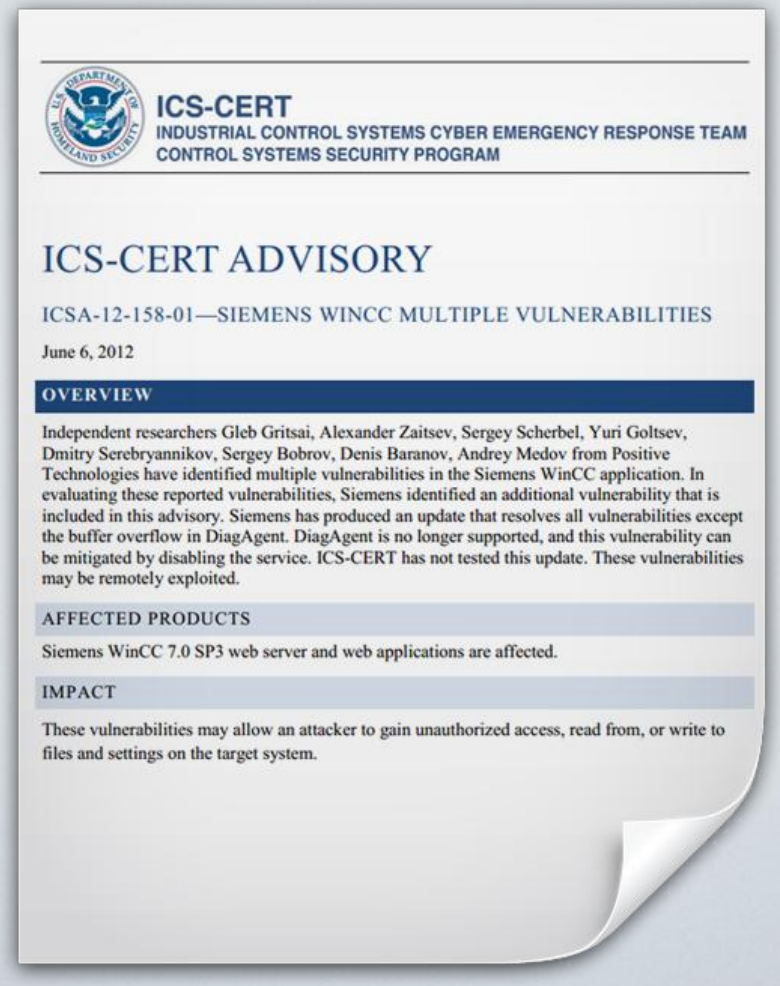
	A-B	Schneider Electric	GE	SEL	Koyo
Встроенное ПО	!	✗	!	!	!
Комбинационная Логика	!	!	✗	!	✗
Бекдоры	!	✗	✗	✓	✓
Ложные данные Fuzzing	✗	✗	✗	!	!
WEB	!	✗	N/A	N/A	✗
Базовое реконфигурирование	!	!	✗	!	!
Перегрузка	✓	✓	✗	✓	✓
НДВ	!	✗	✗	!	!

СОДЕРЖИТ УЯЗВИМОСТИ

Источник: http://www.wired.com/threatlevel/2012/01/scada-exploits/

Компоненты АСУ ТП информационная безопасность

Уязвимости АСУ ТП, софт: исследования Positive Technologies



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-158-01—SIEMENS WINCC MULTIPLE VULNERABILITIES

June 6, 2012

OVERVIEW

Independent researchers Gleb Gritsai, Alexander Zaitsev, Sergey Scherbel, Yuri Goltsev, Dmitry Serebryannikov, Sergey Bobrov, Denis Baranov, Andrey Medov from Positive Technologies have identified multiple vulnerabilities in the Siemens WinCC application. In evaluating these reported vulnerabilities, Siemens identified an additional vulnerability that is included in this advisory. Siemens has produced an update that resolves all vulnerabilities except the buffer overflow in DiagAgent. DiagAgent is no longer supported, and this vulnerability can be mitigated by disabling the service. ICS-CERT has not tested this update. These vulnerabilities may be remotely exploited.

AFFECTED PRODUCTS

Siemens WinCC 7.0 SP3 web server and web applications are affected.

IMPACT

These vulnerabilities may allow an attacker to gain unauthorized access, read from, or write to files and settings on the target system.

Источник: http://www.us-cert.gov/controlsystems/pdf/ICSA-12-158-01.pdf

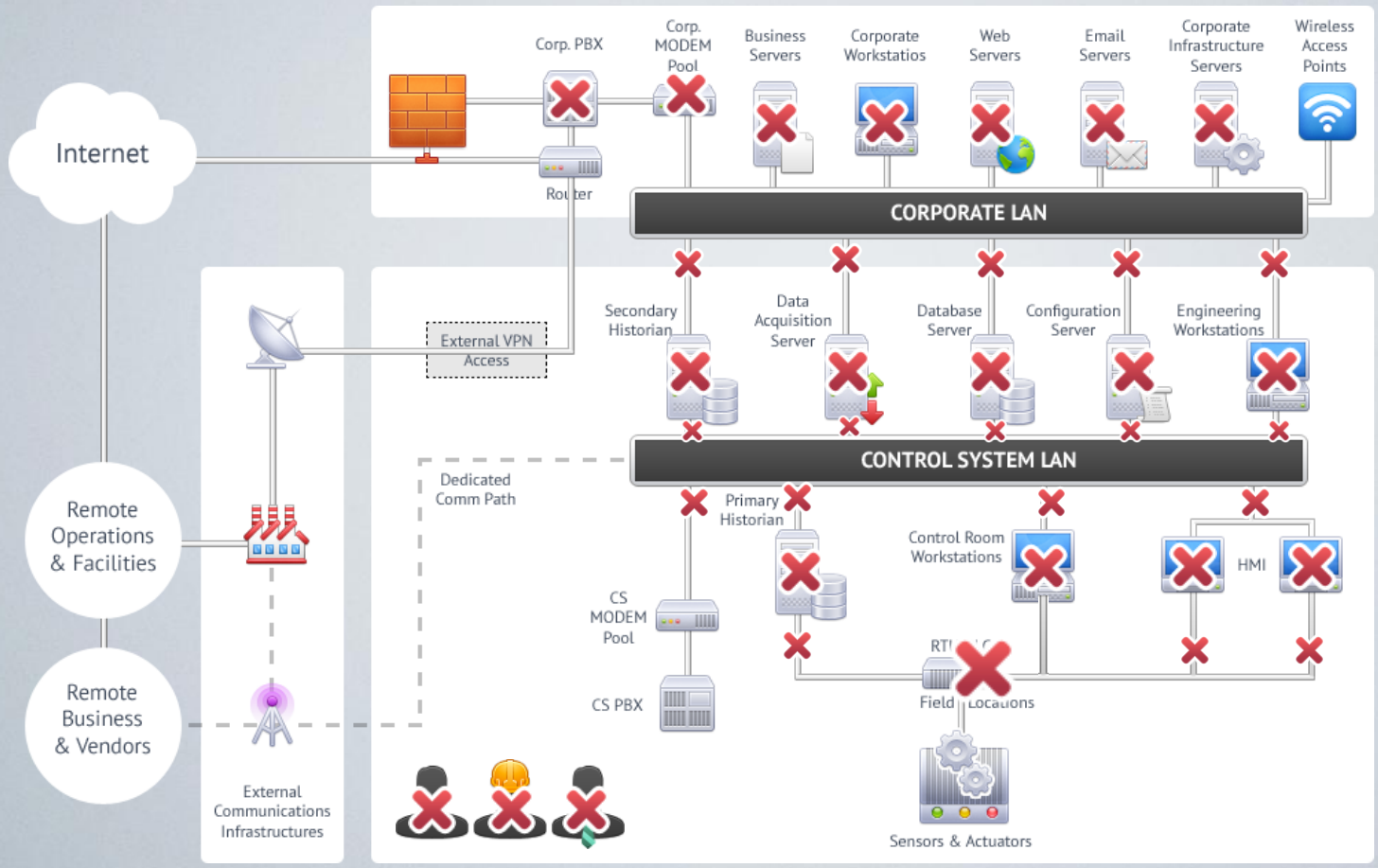
Компоненты АСУ ТП информационная безопасность

Уязвимости АСУ ТП, персонал: разные исследователи

Former Employees Are Identified as Sources of Recent Cyber-Attacks on Critical Infrastructures	http://voices.yahoo.com/former-employees-identified-as-sources-recent-10665979.html
Downsizing within corporations, has brought on high number of disgruntled employees or ex-employees. An internal attack could result from changes made to the system thru personal computers or PLC interfacing; a disgruntled employee can change settings, turn off motors or pumps, or implant a virus or worm.	http://cmu95752.wordpress.com/2012/04/11/are-scadax-systems-secured/
In 2000, former employee Vitek Boden release a million liters of water into the coastal waters of Queensland, Australia.	http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf
In 1992, former Chevron employee disabled it's emergency alert system in 22 states, which wasn't discovered until an emergency happened that needed alerting	http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf
Computers and manuals seized in Al Qaeda training camps full of SCADA information related to dams and related structures	http://www.blackhat.com/pres 06/BH-Fed-06-Maynor-Graham

Компоненты АСУ ТП информационная безопасность

Обобщенная схема



- PLC – софт, железо
- АСУ ТП – софт
- АСУ ТП – протоколы
- Персонал
- Офисное ПО

Проблема?

Если наша цель сделать АСУ ТП безопасной с т.з защиты информации, то интуитивно кажется, что у нас есть проблема

Проблема очень простая

В АСУ ТП нет ни одного компонента, которому можно было бы доверять

Безопасная операционная система

Лаборатория Касперского разрабатывает собственную, безопасную операционную систему

- Разработана “с нуля”
- Микроядерная архитектура
- Все приложения, в том числе и системные, состоят из верифицируемых модулей
- Прямые связи между модулями недопустимы
- Каждый программный модуль ассоциируется с корректным сценарием поведения
- Поведение любого программного модуля проверяется на соответствие сценарию
- Гарантии невозможности исполнения “недокументированного поведения”


EXPLOITS

Не обновленный софт на компьютере в РФ

По данным «Лаборатории Касперского», H1 2012

31%

Oracle Java

29%

Adobe Flash

20%

Winamp

20%

VLC Media Player

17%

Microsoft Office

KASPERSKY lab

Стоимость атаки снижается

WIRED.CO.UK

- DDoS атака: $30-$70 день, от $1200 – месяц
- Рассылка SPAM: от $10 за миллион адресов
- Боты для Бот сетей: от $200 за 2000 Ботов
- Исходный код ZeuS: от $200
- Взлом корпоративного почтового ящика: от $500

Счет за одну успешную атаку

Последствия	Цена для крупного бизнеса/СМБ
Вынужденный простой	$791,000 / $13,000
Упущенные возможности (и потерянные контракты)	$375,000 / $16,000
Дополнительные услуги специалистов	$26,000 / $6,600
Счет за одну атаку в среднем	$695,000 / $14,000

Что будет следующей целью таргетированных атак?

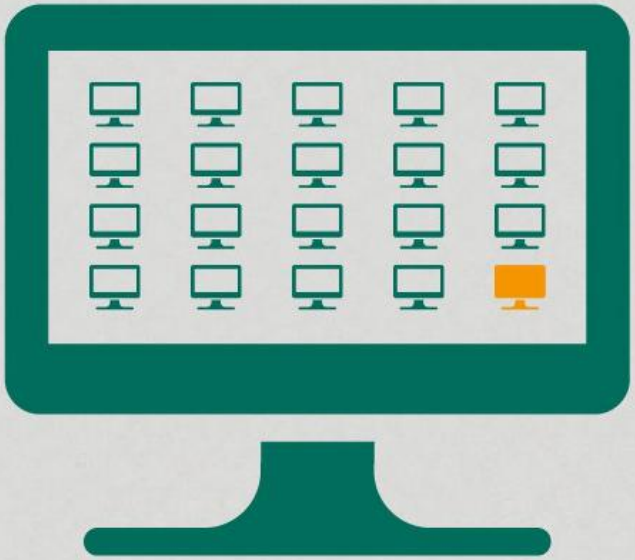
Медицинское оборудование?

Офисы под управление «умных» систем?

Автомобили?

НЕ ВСЕ АНТИВИРУСЫ ОДИНАКОВО ЭФФЕКТИВНЫ

5% компьютеров, защищенных антивирусом, все же заражены вирусом.



Среди компьютеров, не имеющих антивируса, активное заражение обнаружено на 13%

Как противостоять?

- Обновлять ПО (операционные системы, Flash, Acrobat, и т.д.)
- Разграничивать права для пользователей
- Использовать правило сложных паролей
- Установить лицензионный антивирус на все компьютеры и устройства корпоративной сети
- Обучать пользователей базовым правилам безопасной работы
- Использовать политики безопасности (в том числе для мобильных устройств)
- Осуществлять централизованный контроль сети

Спасибо

Вопросы?

Региональный представитель в УрФО и Пермскому краю
Александр Орда

KASPERSKY lab