ОБЗОР АКТУАЛЬНЫХ ИТ-УГРОЗ

Поляков Павел

Инженер по предпродажной поддержке в Восточной Европе

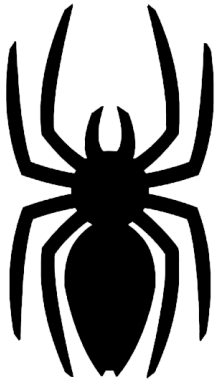
РАЗВИТИЕ ВРЕДОНОСНОГО ПО

Looking Back: 20 Years of Malware Evolution

EVOLUTION OF MALWARE

1994

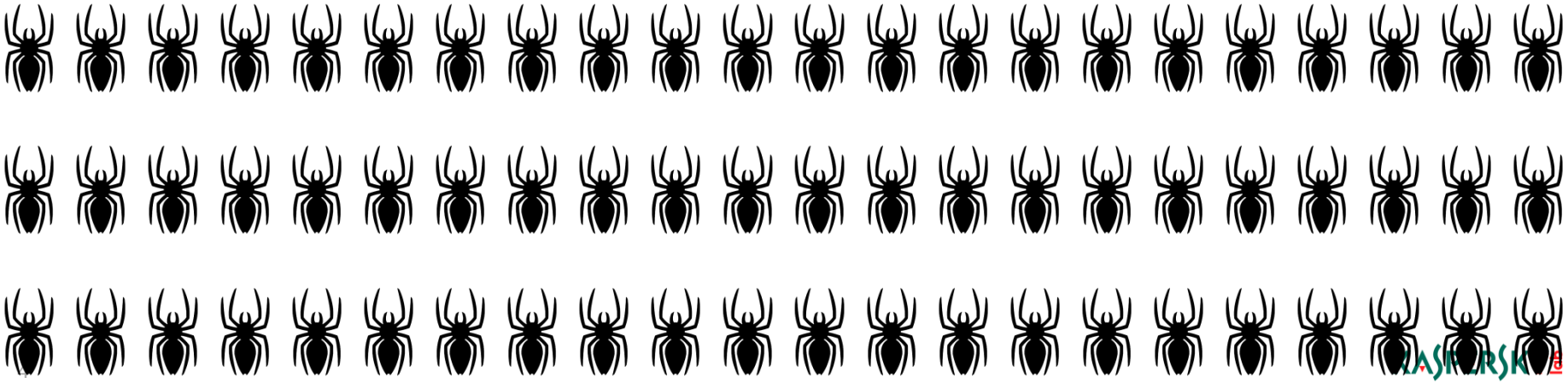
One new virus every hour



EVOLUTION OF MALWARE

2006

One new virus every minute



EVOLUTION OF MALWARE

2011

One new virus every second

Or 70,000 samples/day

What about

2014 ?

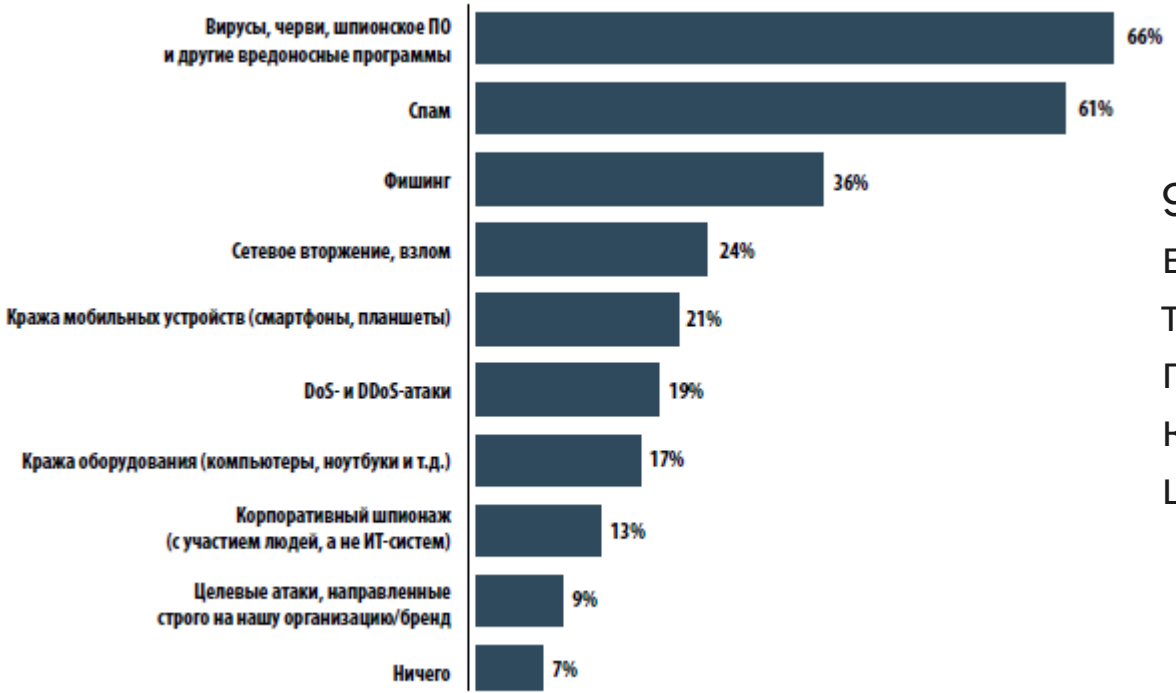
Kaspersky Lab
обнаруживает приблизительно
315,000
новых образцов вредоносного ПО
каждый день

EVOLUTION OF MALWARE

Тенденции развития вредоносного ПО:

- Целевые атаки + кибершпионаж
- Мобильные банковские троянцы/ботнеты
- Кибервымогательство
- Уязвимости и эксплойты
- Кто украл мою частную жизнь?! – облако

ЦЕЛЕВЫЕ АТАКИ + КИБЕРШПИОНАЖ



91% опрошенных организаций в мире хотя бы один раз в течение года подверглись кибератаке, 9% компаний стали мишенью целевых атак.

ЦЕЛЕВЫЕ АТАКИ + КИБЕРШПИОНАЖ

- **NetTraveler:**

Trojan-Spy.Win32.TravNet и Downloader.Win32.NetTraveler, Exploit.MSWord.CVE-2010-333 и Exploit.Win32.CVE-2012-0158.

- **Цель Атаки** - правительства, посольства, научную и военную сферу государств, а также отдельные активистские движения

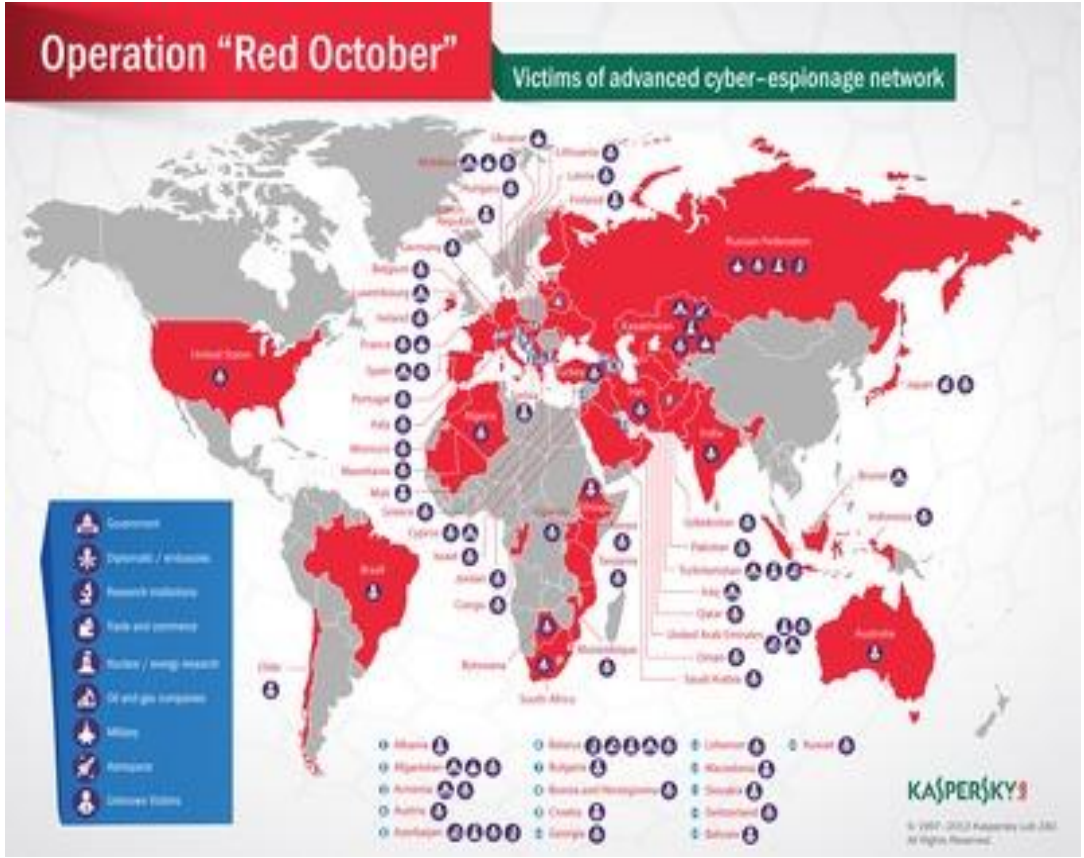
KASPERSKY lab

ЦЕЛЕВЫЕ АТАКИ + КИБЕРШПИОНАЖ

- **Red October**

Java-эксплойт Rhino

- **Цель Атаки** – энергетические компании, правительства, торговые организации

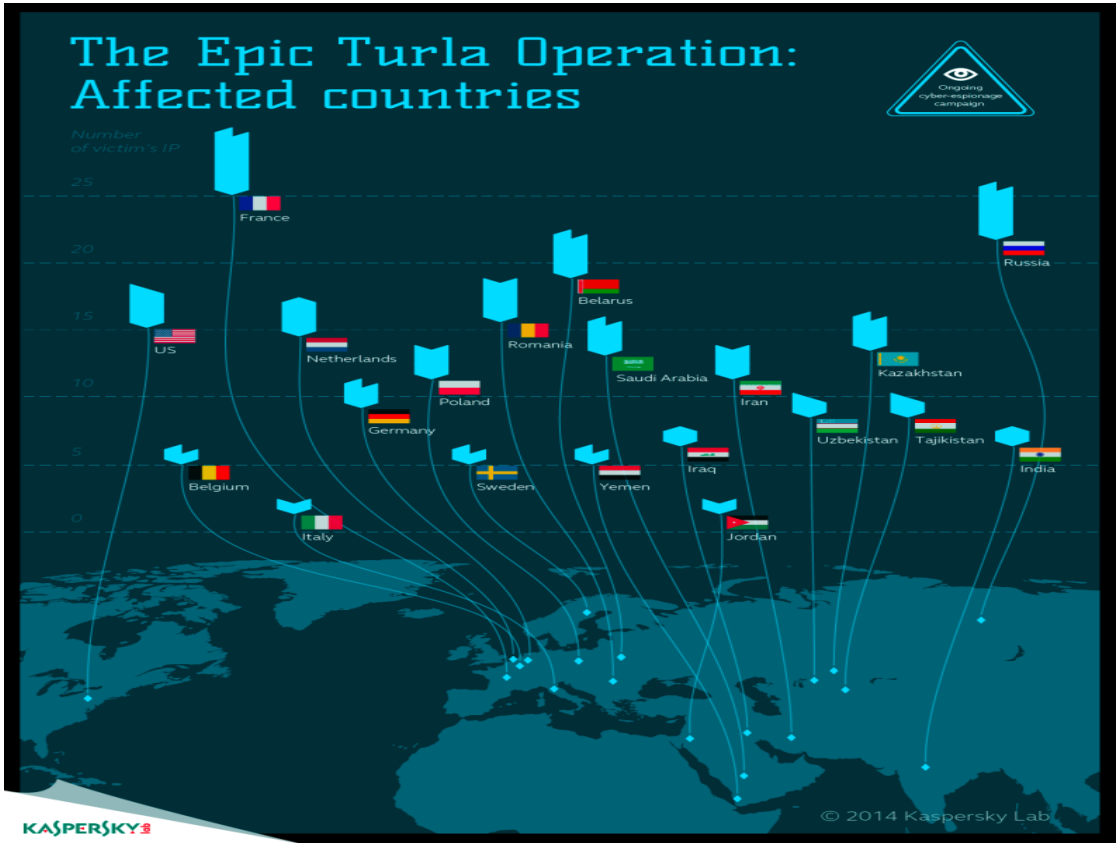


KASPERSKY lab

ЦЕЛЕВЫЕ АТАКИ + КИБЕРШПИОНАЖ

Epic Turla

watering hole, Java-эксплойтов (CVE-2012-1723), CVE-2013-5065 уязвимость XP, PDF-эксплойтами (CVE-2013-3346 + CVE-2013-5065)



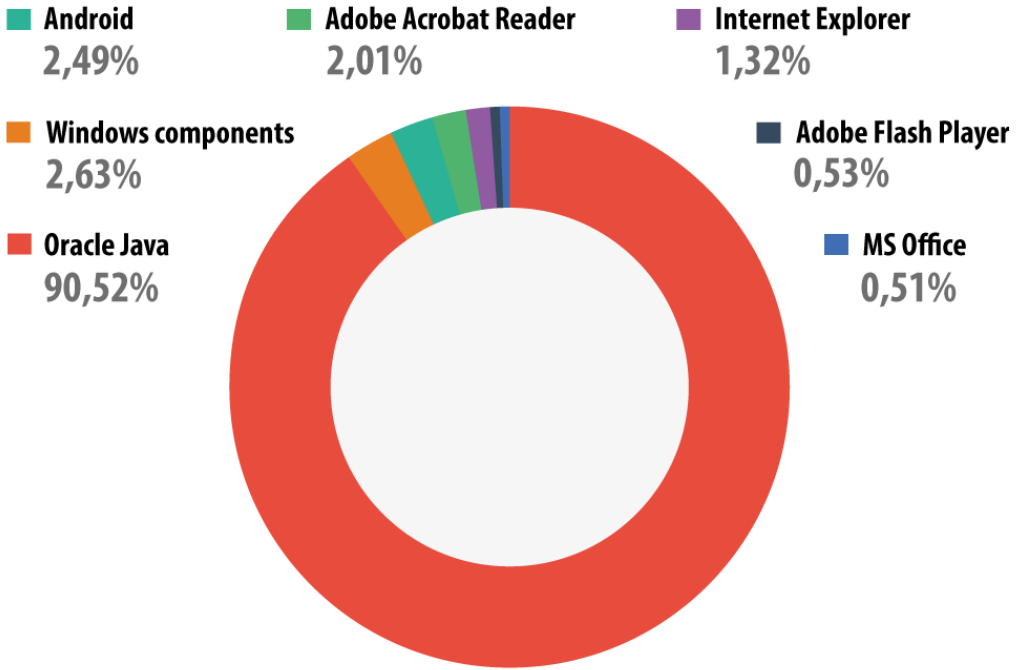
KASPERSKY lab

ЗАЧЕМ АТАКУЮТ

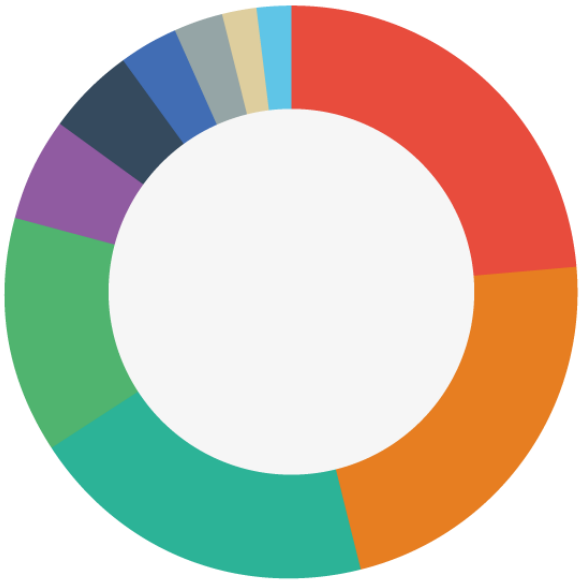
- Кража информации
- Уничтожение данных или блокирование работы инфраструктуры
- Кража денег
- Удар по репутации компании
- Финансовый ущерб

VULNERABLE APPLICATIONS EXPLOITED BY CYBERCRIMINALS

Злоумышленники предпочитают использовать уязвимости в наиболее популярных приложениях, которые пользователи по тем или иным причинам редко обновляют.



DISTRIBUTION OF OPERATING SYSTEMS BY OUR USERS



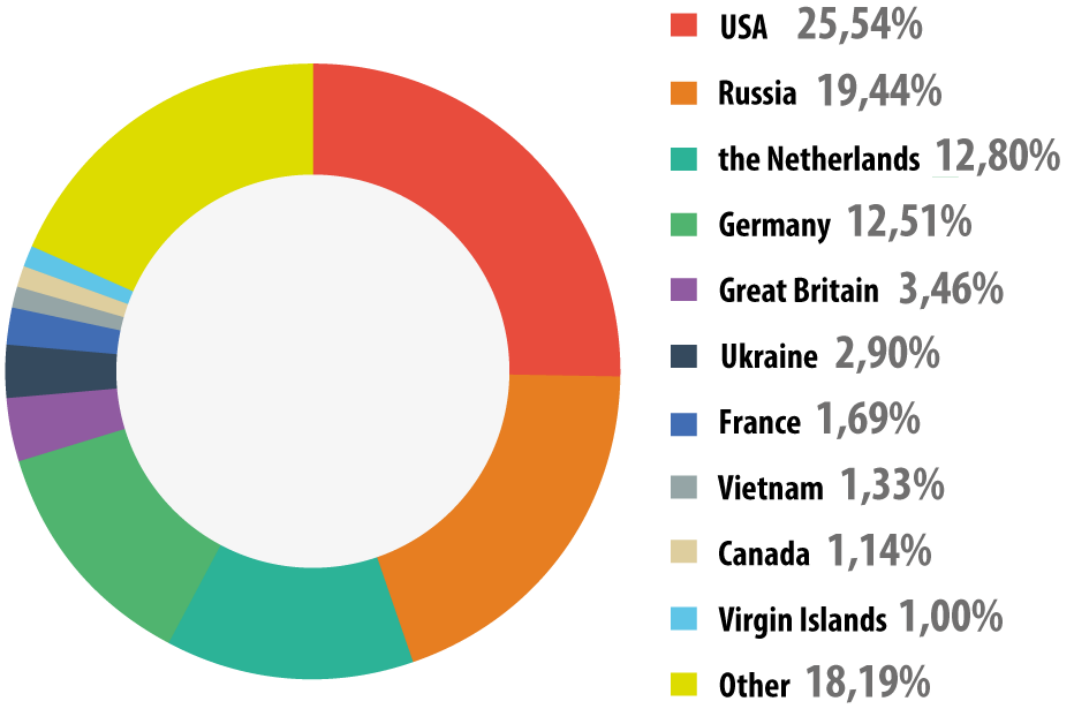
- Windows XP Pro 23,77%
- Windows 7 Home x64 22,38%
- Windows 7 19,74%
- Windows 7 x64 13,39%
- Windows 7 Home 5,96%
- Windows 8 Home x64 4,85%
- Windows Vista Home 3,47%
- Windows XP Home 2,81%
- Windows 8 x64 1,89%
- Other 1,73%

- Согласно информации KSN 61.5% пользователей используют Windows 7
- Более того 26.58% все еще пользуются Windows XP

Microsoft stoped supporting Windows XP in April 2014!

ONLINE THREATS

45% веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США и России.

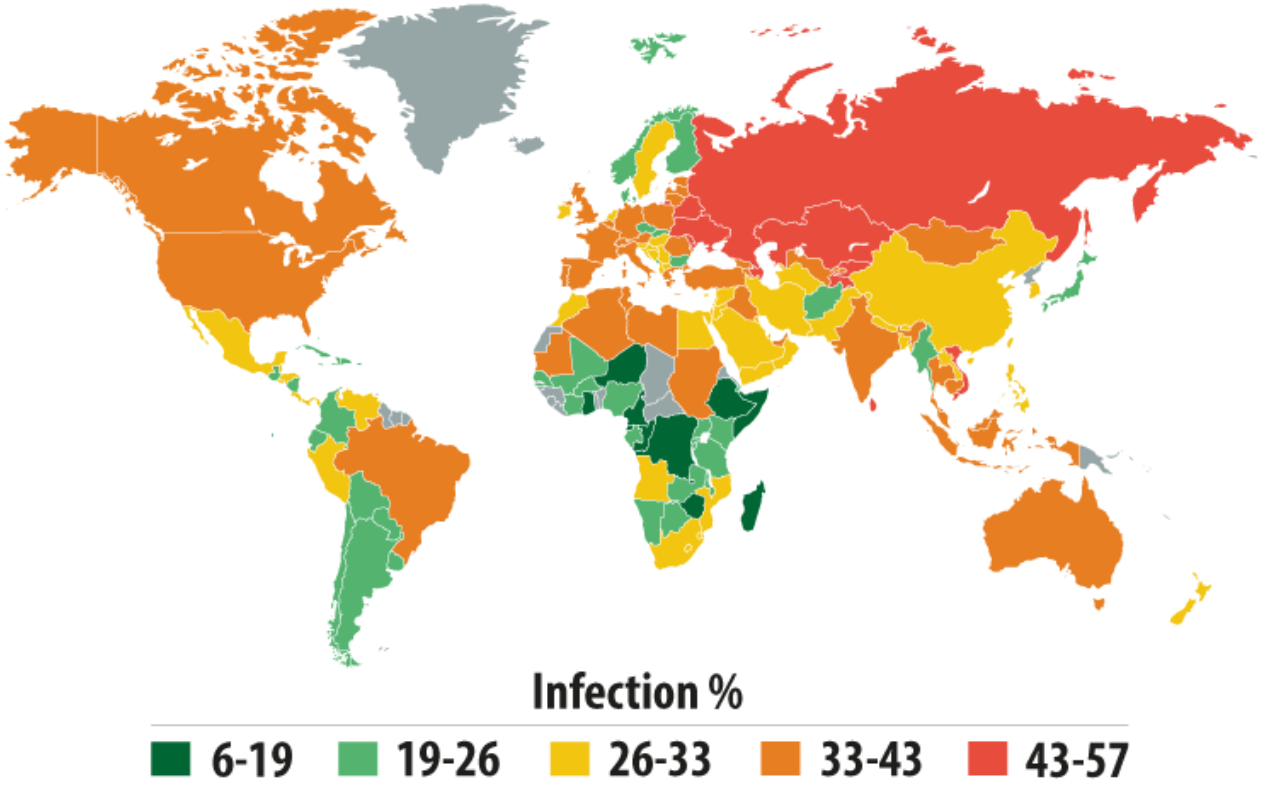


Distribution of online resources seeded with malicious programs, by country

KASPERSKY lab

COUNTRIES' RISK OF ONLINE INFECTION

- Статистика по количеству срабатываний веб-антивируса согласно KSN

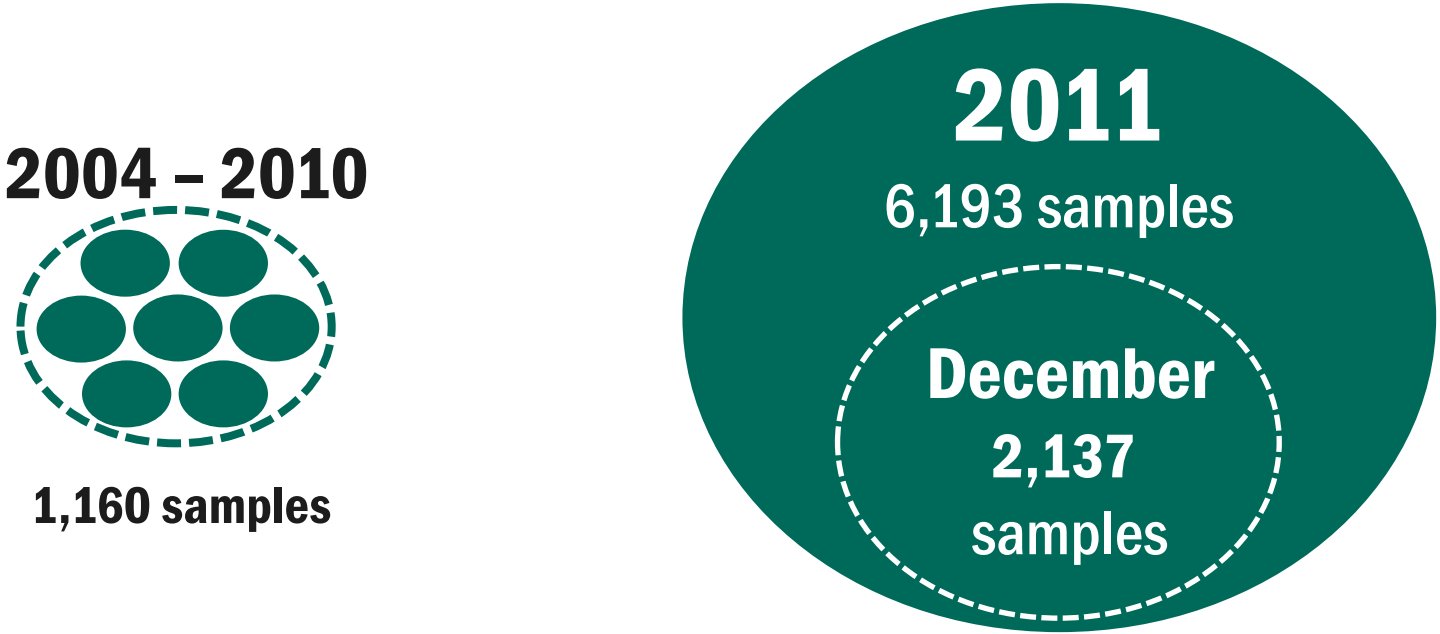


KASPERSKY lab

MOBILE MALWARE

Statistics

EVOLUTION OF MALWARE

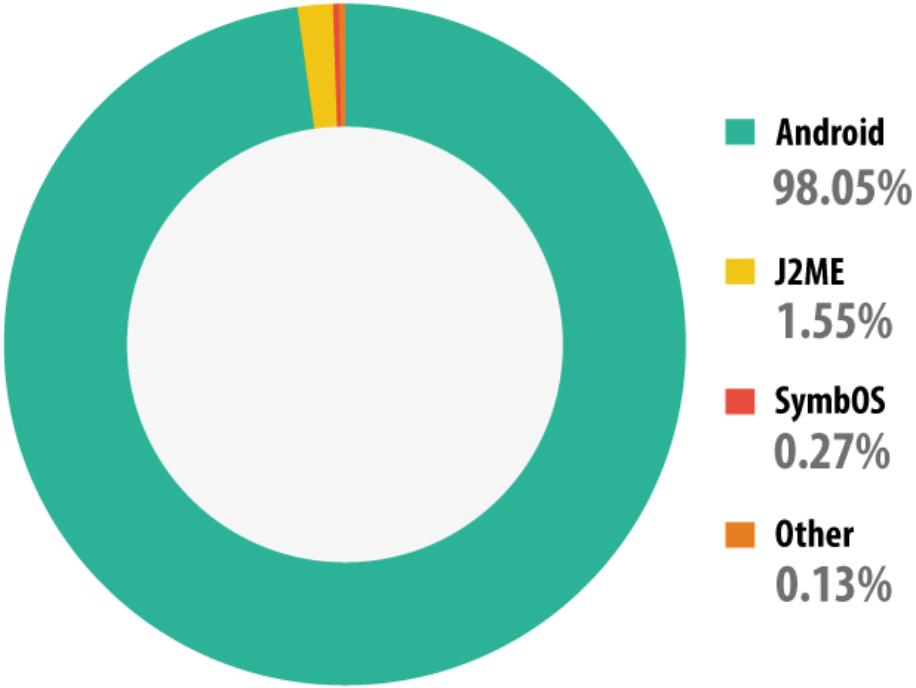


2011 was the year of mobile malware

EVO

2013:
143,211
образцов
вредоносного ПО
обнаружено

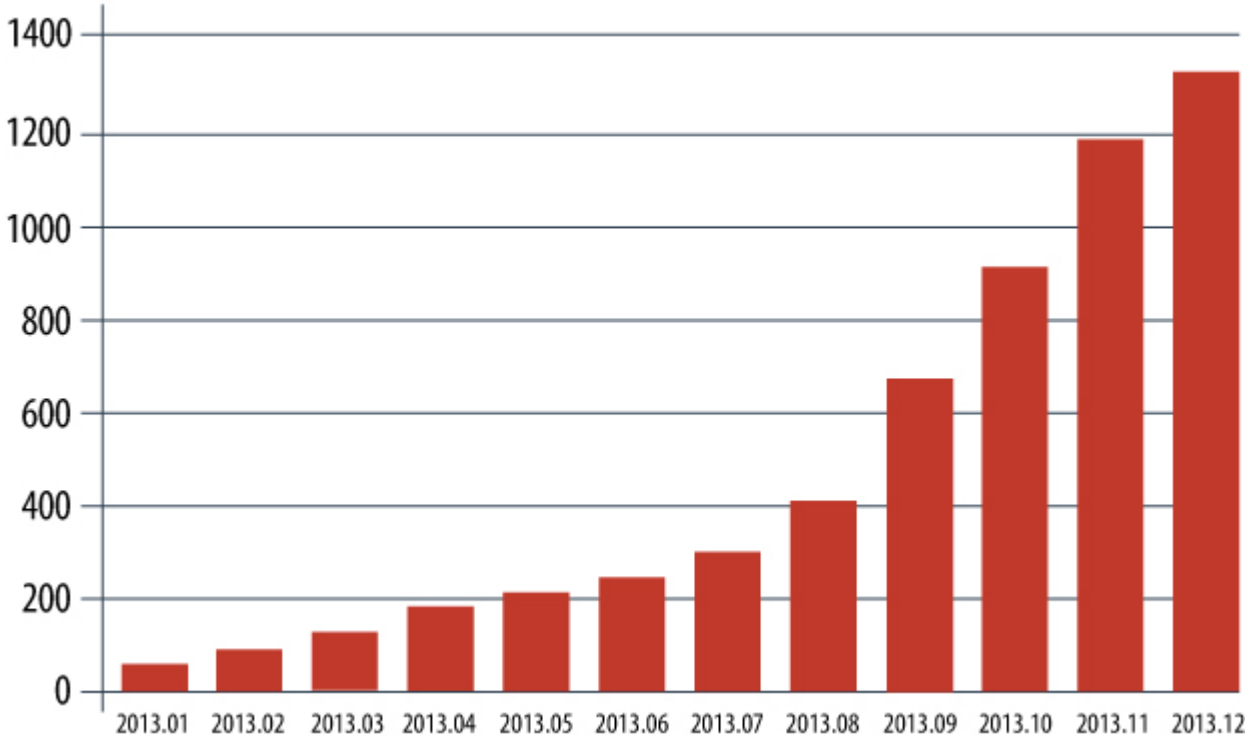
MOBILE MALWARE REPORT



- Android по-прежнему остаётся основной целью для вредоносных атак — на эту платформу нацелено уже 98,05% всех известных зловредов.

KASPERSKY lab

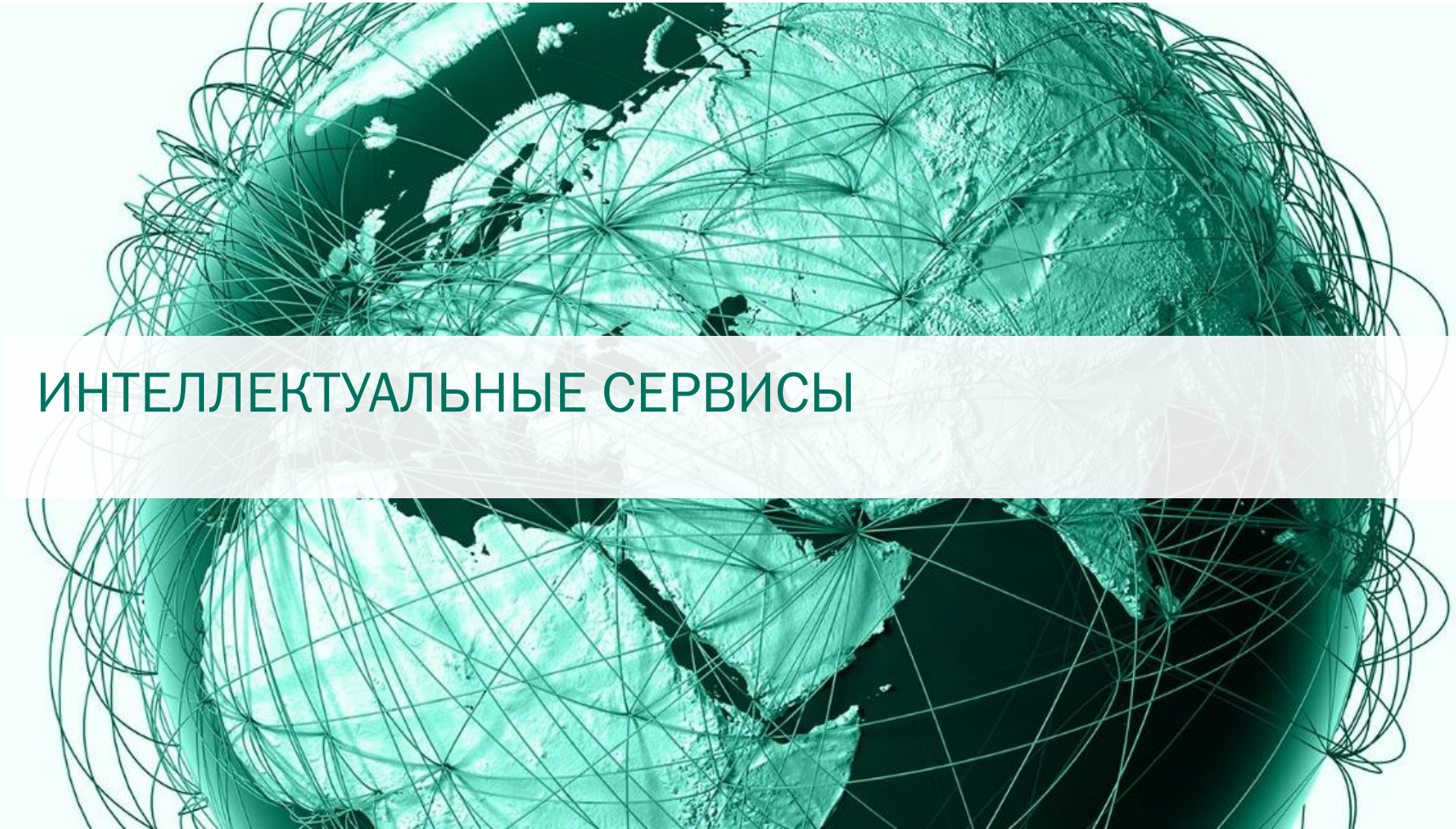
MOBILE TREND OF THE YEAR – MOBILE BANKING TROJANS



The number of mobile banking Trojans in our collection

KASPERSKY lab

KASPERSKY



ИНТЕЛЛЕКТУАЛЬНЫЕ СЕРВИСЫ

КАРТА СЕРВИСОВ

URL адреса вредоносных ссылок
MD5-хэши вредоносных объектов

ПОТОКИ ДАННЫХ ОБ УГРОЗАХ

Мониторинг Ботнет-Угроз

РЕПУТАЦИОННЫЕ СЕРВИСЫ

АНАЛИТИЧЕСКИЕ ОТЧЕТЫ

Финансовые Угрозы
APT исследования

ЭКСПЕРТНЫЕ СЕРВИСЫ

Образовательная программа (набор тренингов) по IT-безопасности
Анализ вредоносного ПО
MSA (экспертная поддержка продуктов ЛК)

ТРЕНИНГИ ПО IT БЕЗОПАСНОСТИ

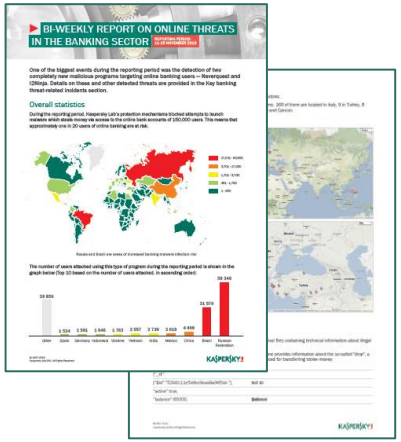
KASPERSKY lab

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПО IT-БЕЗОПАСНОСТИ: СТРУКТУРА

АНАЛИТИЧЕСКИЕ ОТЧЕТЫ

KASPERSKY lab

АНАЛИТИЧЕСКИЕ ОТЧЕТЫ: ТИПЫ ОТЧЕТОВ



- **Подписка на непубличные отчеты от GReAT по исследованиям APT**
- **Подписка на отчеты по финансовым (банковским) угрозам**

KASPERSKY lab

АНАЛИТИЧЕСКИЕ ОТЧЕТЫ: ТИПЫ ПОДПИСОК

APT	Годовая подписка на отчеты по теме **APT исследования** (ежеквартально) ✓ Краткий отчет ✓ Углубленный анализ инструментов злоумышленников и статистика кибер-угрозы ✓ Углубленный анализ инфраструктуры C&C ✓ Показатели компрометации
Фин. Угрозы	Годовая подписка на отчеты по теме **Финансовые Угрозы** (ежеквартально) ✓ Краткий отчет ✓ Описание наиболее значительных кибер-угроз за отчетный период ✓ Статистика кибер-угроз за отчетный период ✓ Экспертная оценка новых уязвимостей ПО, найденных за отчетный период, охватывающая практически все популярные программы и их версии

Уровни подписки

АНАЛИЗ ВРЕДОНОСНОГО ПО

KASPERSKY lab

АНАЛИЗ ВРЕДОНОСНОГО ПО

Возможность понять поведение и цели конкретных вредоносных файлов, нацеленных на вашу организацию

Услуга предоставляет возможность рассмотреть подозрительный файл под микроскопом экспертного анализа вредоносного ПО от ЛК. Ваш персональный Менеджер Технического Сопровождения (TAM) от лица вирусных аналитиков предоставит подробный отчет – в срок до 40 часов.

Состав отчета

- Свойства образца файла: краткое описание и вердикт.
- Детальное описание: функции вредоносного ПО, поведение и цели зловреда, информация необходимая для нейтрализации данного вредоносного ПО.
- Сценарий восстановления: шаги по обеспечению безопасности от данного и аналогичного вредоносного ПО.

SLA

- Годовая подписка
- Техническая поддержка TAM-ом в режиме 8x5
- Предоставление отчета в течение 5 рабочих дней

Варианты подписок

- 10 отчетов на анализ файла
- 20 отчетов на анализ файла

ИСТОРИИ УСПЕХА

KASPERSKY lab

ИСТОРИЯ УСПЕХА — ТЕЛЕФОНИКА

Текущая подписка на Интеллектуальные сервисы

- **Страна** – Испания
- **Заказчик** – Телефоника
- **Состав услуг** – Годовая подписка на услуги: Потоки Данных об Угрозах, Мониторинг Ботнет-Угроз, Аналитические отчеты

http://www.kaspersky.com/about/news/business/2014/Kaspersky-Lab-and-Telefonica-join-forces-to-improve-cyber-protection-for-European-and-Latin-America-customers

http://www.eurocomms.com/industry-news/49-online-press/9898-telefonica-signs-cyber-security-deal-with-kaspersky-lab

ИСТОРИЯ УСПЕХА — ПОЛИЦИЯ ЛОНДОНА

Образовательная программа по ИБ

- **Страна** – Великобритания
- **Заказчик** – Городская Полиция Лондона (COLP)
- **Тип тренинга** – Уровень 2 - Основы расследования инцидентов и анализа вредоносного ПО

http://www.kaspersky.com/about/news/virus/2014/City-of-London-Police-and-Kaspersky-Lab-lead-the-way-in-combatting-fraud

http://www.computerworlduk.com/news/security/3539039/city-of-london-police-brings-in-kaspersky-to-train-officers-to-tackle-cybercrime/

ВОПРОСЫ?

KASPERSKY lab