Подходы к обеспечению безопасности банковских приложений и систем

Вячеслав Ан

Специалист по продаже решений
Майкрософт Россия

Что происходит в мире?

- 39% компьютеров в мире заражены вредоносным кодом
- Каждый 14-й файл скачиваемый из интернет содержит вредоносный код
- Более 1 млн. компьютеров взламывается каждый день. Каждые 14 секунд один компьютер

Что происходит в мире?

- **Участники Anonymous, Lulzsec и прочих групп регулярно взламывают крупнейшие компании в мире и международные организации не прилагая особого труда**
- **В этом году 90% процентов крупнейших компаний в мире имели инциденты ИБ в своей инфраструктуре**
- **Убытки от киберпреступности 114 миллиардов долларов в год**

Источник: 16 security problems bigger than Flame

Откуда мы это знаем?

- **600 000 000 сенсоров антивируса Microsoft**
- **300 000 000 сенсоров собирающих образцы вредоносного ПО из почты Outlook.com**
- **Поисковые роботы Bing**
- **SmartScreen в Windows 8 собирает хэши файлов скачиваемых и запускаемых файлов**

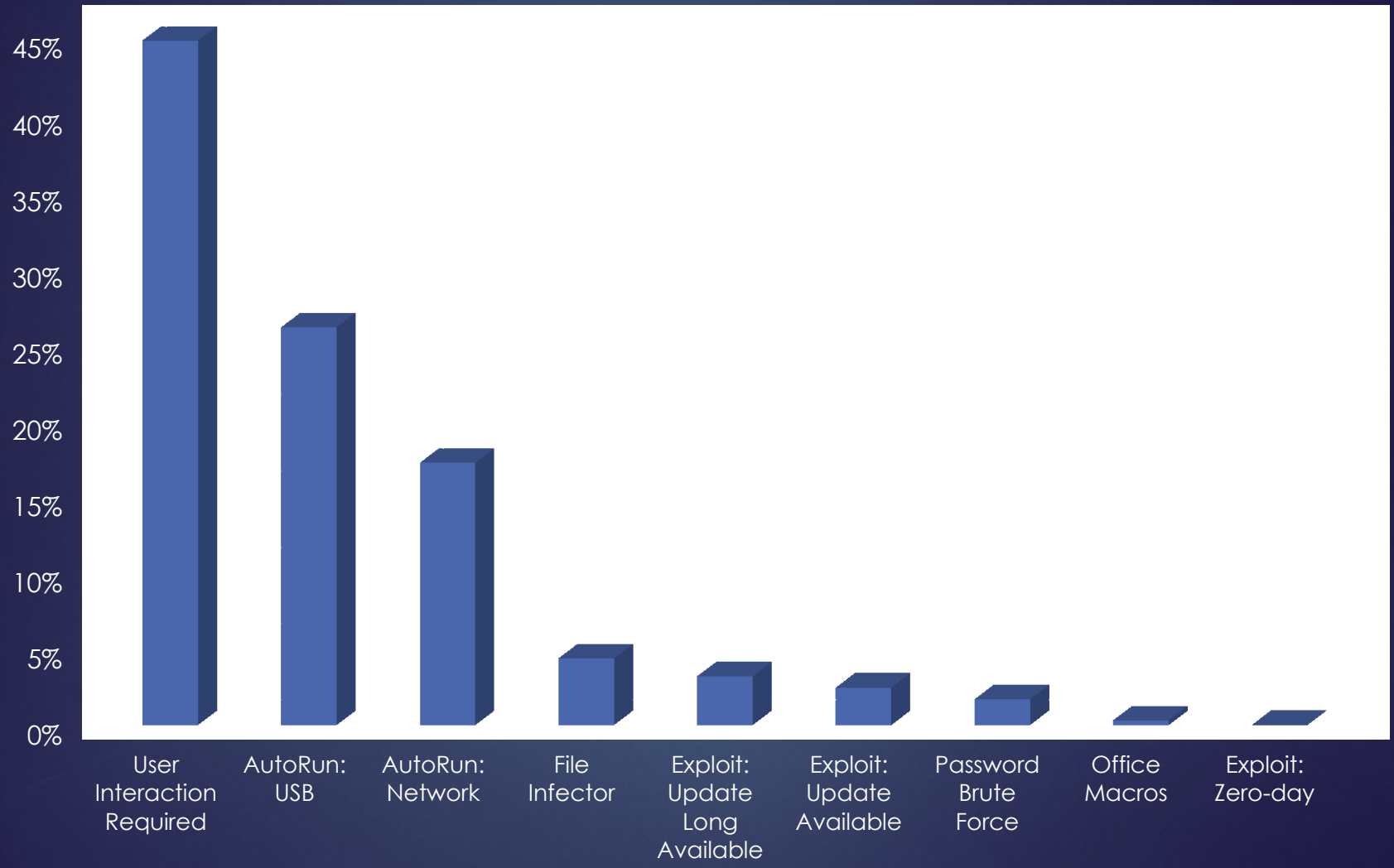
Аналитика и угрозы в OTIS

- Online Threat Information Sharing
- **Бесплатно**
- Список рассылки о проблемах безопасности
- Участвуют группы разработки MS и специалисты ИБ
- Канал между специалистами ИБ клиентов использующих наши продукты и специалистами ИБ Microsoft
- Требует подписания NDA

Для финансовых учреждений SAFI

- Security Alliance for Financial Institutions
- **Бесплатно**
- Позволяет банкам и другим организациям финансового сектора анонимно обмениваться данными
- Предназначена для обсуждения текущих и новых угроз для предприятий финансовой сферы
- Ежемесячный отчет, приоритетная поддержка и специальные тренинги
- Требует подписания NDA

Методы распространения зловредного кода



Microsoft Security Intelligence Report выпуск 11

SmartScreen блокирует 99,9% известных зловредов

Both Figure 1 and Figure 2 illustrate this challenge.

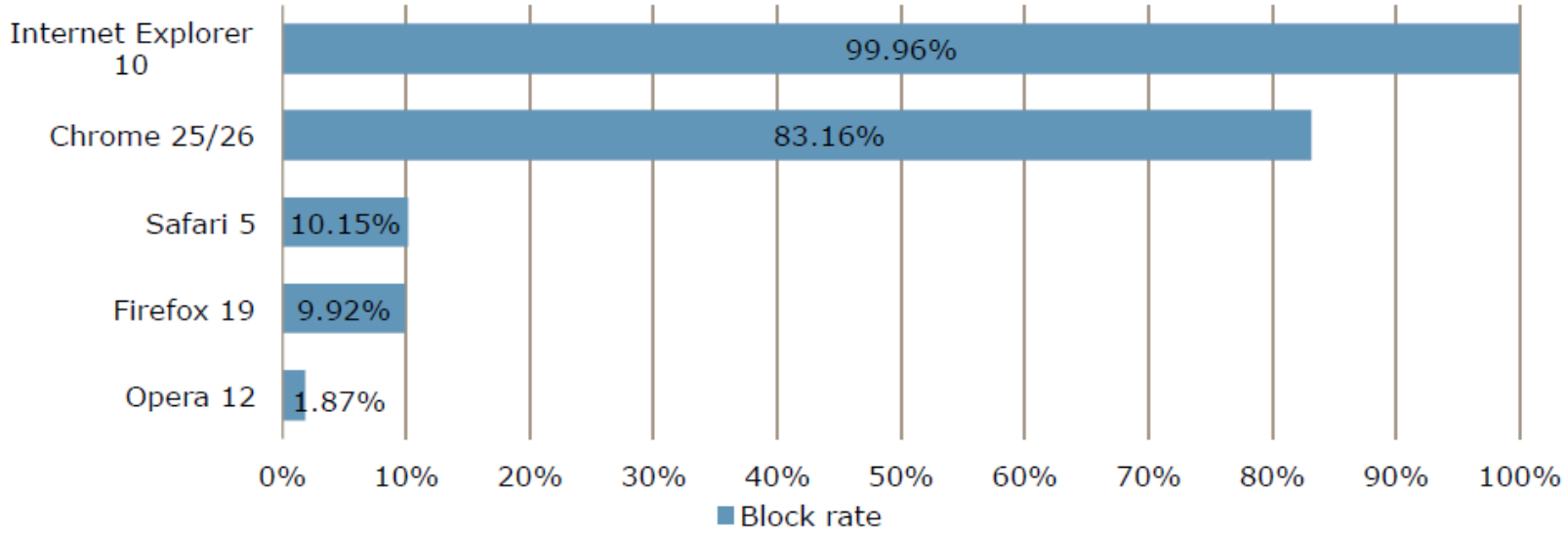


Figure 1 - Overall Malware Block Rate By Browser (Higher Values Are Better).

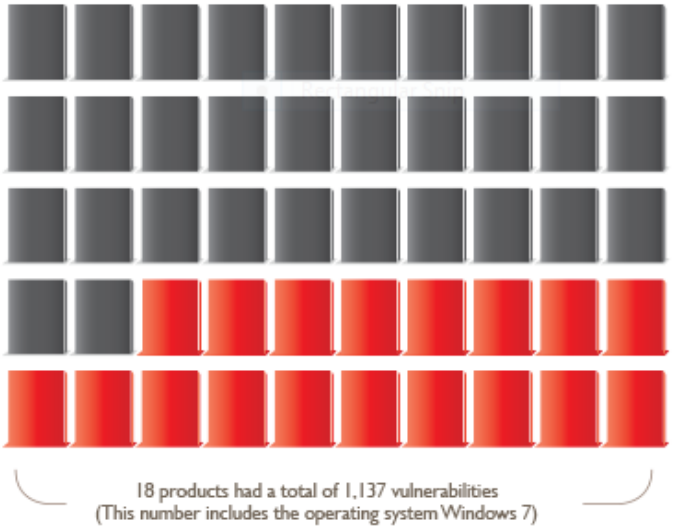
Уязвимости ОС на 5 апреля 2013 по Secunia

Продукт	Уязвимостей
Sun Solaris 10	**1663**
Red Hat Enterprise Linux Server v.5	**2119**
FreeBSD 6.x	**86**
Microsoft Windows Server 2008	**410**
Microsoft Windows Server 2012	**87**
Apple Mac OS X	**1838**
Red Hat Enterprise Linux Client v.5	**2349**
Ubuntu Linux 8.04 (выпуск 2008 год)	**1667**
Windows XP (выпуск 2001 год)	**599**
Windows 7	**276**
Windows 8	**84**

Уязвимости БД и файерволов на 5 апреля 2013 по Secunia

Продукт	Уязвимостей
Oracle Database 11.x	**354**
IBM DB2 9.x	**121**
MySQL 5.x	**145**
Microsoft SQL Server 2008	**4**
Microsoft SQL Server 2012	**1**
Cisco ASA 7.x	**89**
Microsoft ISA Server 2006	**7**
Microsoft Forefront TMG	**2**

Уязвимости на клиентских ПК



18 products had a total of 1,137 vulnerabilities
(This number includes the operating system Windows 7)

GOOGLE CHROME	291
MOZILLA FIREFOX	257
APPLE ITUNES	243
ADOBE FLASH PLAYER	67
ORACLE JAVA JRE SE	66
ADOBE AIR	56
MICROSOFT WINDOWS 7	50
ADOBE READER	43
MICROSOFT INTERNET EXPLORER	41
APPLE QUICKTIME	29
MICROSOFT .NET FRAMEWORK	14
VLC MEDIA PLAYER	11
MICROSOFT EXCEL	10
MICROSOFT VISIO VIEWER	7
MICROSOFT SILVERLIGHT	5
MICROSOFT WORD	3
SKYPE	1
MICROSOFT XML CORE SERVICES (MSXML)	1

In the top 50 portfolio the total number of end-point vulnerabilities in 2012 was

1137

In the 5 year trend, this shows an increase of

98%

The 1,137 vulnerabilities were discovered in 18 of the Top 50 products - an average of 63 vulnerabilities per product.

Источник Secunia TOP 50 vulnerability review 2012

Zero day уязвимости - фетиш ИБ индустрии?

Распределение эксплоитов используемых в зловредном ПО

Microsoft Security Intelligence Report выпуск 11

Что сейчас выгодно атаковать?

5 продуктов с множественными уязвимостями не обновленных на пользовательских ПК и наиболее часто атакуемых злоумышленниками

- Oracle Java
- Adobe Flash Player
- Apple QuickTime
- Apple iTunes
- Winamp
- Adobe Shockwave Player

23% пользователей посещают интернет с устаревших браузеров. 14.5% используют предыдущую версию, 8.5% отстают на несколько версий .

Kaspersky IT Threat Evolution Q3 2012

Как дела с обновлениями в мире?

Статус обновления безопасности	Microsoft Windows	Microsoft Word	Adobe Reader	Oracle Java	Adobe Flash Player
Нет последнего обновления	34%	39%	60%	94%	70%
Нет последних трех обновлений	16%	35%	46%	51%	44%

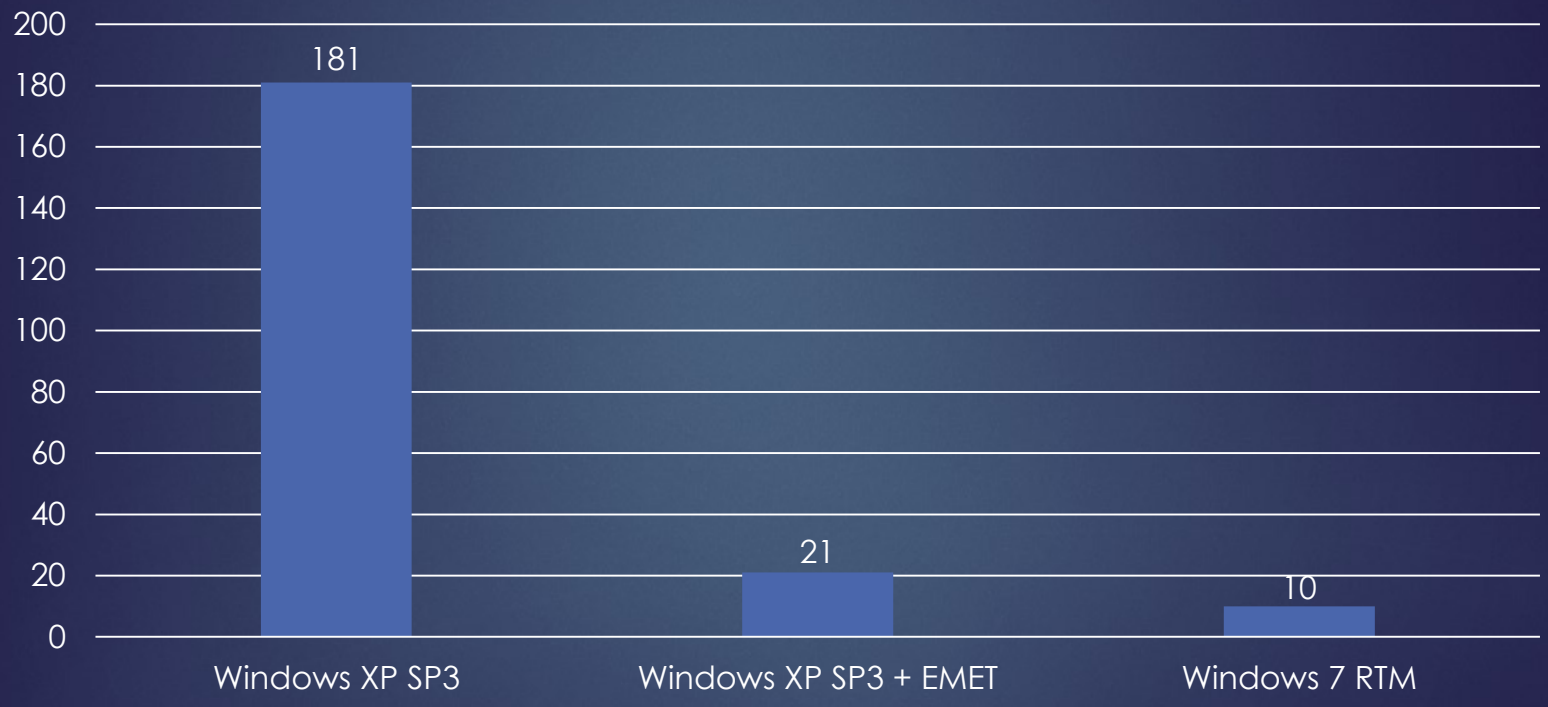
Статистика по состоянию на октябрь 2011. Последнее обновление ядра Windows выпущено за 9 месяцев до даты сбора статистики, обновление для Word выпущено за год до этого.

Microsoft Security Intelligence Report выпуск 13

Упрощение обновлений SUVP

- Security Update Validation Program
- **Бесплатно**
- Можно получать обновления для продуктов Microsoft за месяц до их официального выпуска. Это позволяет тестировать их тщательнее перед развёртыванием их у себя в инфраструктуре.
- Включение в программу по приглашениям. Необходимо подписать соглашение о неразглашении

EMET блокирует 89% эксплоитов



Для тестирования EMET использовались 184 наиболее популярных эксплоита

Контроль приложений Applocker и SRP

- Запуск только разрешенных приложений
- Контроль по издателю, версии, хэш сумме

Итоги!

У вас уже есть множество средств защиты в новых продуктах.

Microsoft может существенно помочь в сфере обеспечения безопасности ваших инфраструктур.

Присоединяйтесь к ИБ программам.

Спасибо

E-mail:
van@microsoft.com