Microsoft Security Intelligence Report (Отчет службы безопасности Майкрософт)

Том 13

ЯНВАРЬ - ИЮНЬ 2012

КЛЮЧЕВЫЕ ВЫВОДЫ

www.microsoft.com/sir

Microsoft Security Intelligence Report (Отчет службы безопасности Майкрософт)

Microsoft Security Intelligence Report (Отчет службы безопасности Майкрософт), том 13

Том 13 отчета *Microsoft® Security Intelligence Report* (*SIRv13*) представляет анализ уязвимостей программного обеспечения и эксплойтов, угроз вредоносного кода и потенциально нежелательного программного обеспечения в программных решениях Майкрософт и третьих сторон. Корпорация Майкрософт разработала эти данные на основе подробного анализа тенденций нескольких прошедших лет с акцентом на первом полугодии 2012 г.

Документ обобщает ключевые выводы отчета. Полный отчет включает также глубокий анализ тенденций, обнаруженных более чем в 100 странах и регионах по всему миру и дает рекомендации по управлению рисками для организаций и пользователей.

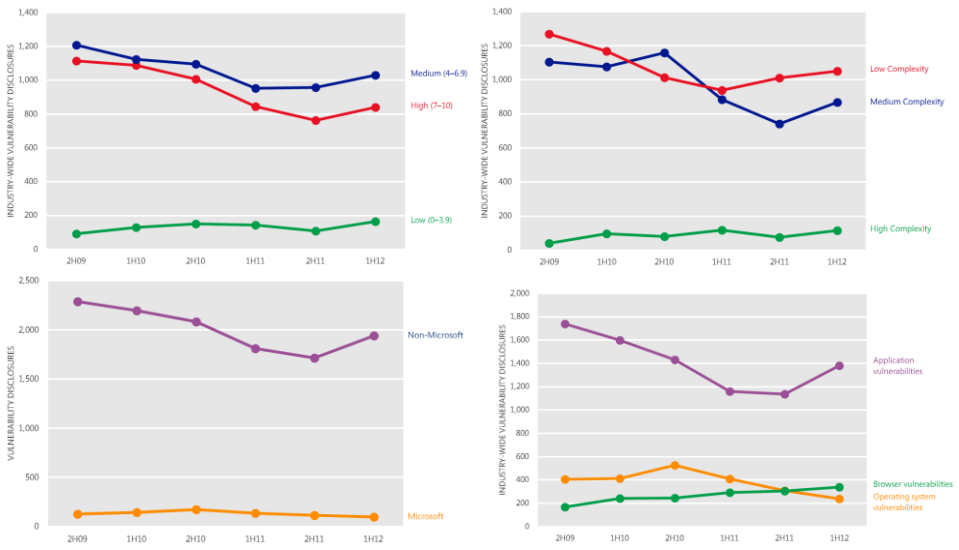
Полный отчет можно загрузить со страницы www.microsoft.com/sir.

Оценка угроз по всему миру

Уязвимости

Уязвимости — слабые места программного обеспечения, позволяющие злоумышленнику подвергнуть риску целостность, доступность или конфиденциальность программного обеспечения или обрабатываемых ими данных. Некоторые из худших уязвимостей позволяют злоумышленнику использовать атакуемую систему, заставив ее выполнить вредоносный код без ведома пользователя.

Рис. 1. Тенденции серьезности уязвимостей (CVE), сложности уязвимостей, сведения по поставщикам, сведения по типам по всей отрасли программного обеспечения, 2П09-1П12[1]



[1] Используемая в отчете номенклатура ссылки на различные отчетные периоды — нПГГ, где нП обозначает либо первое (1), либо второе (2) полугодие, а ГГ — год. Например, 2П09 обозначает вторую половину 2009 года (с 1 июля по 31 декабря), а 1П12 — первую половину 2012 года (с 1 января по 30 июня).

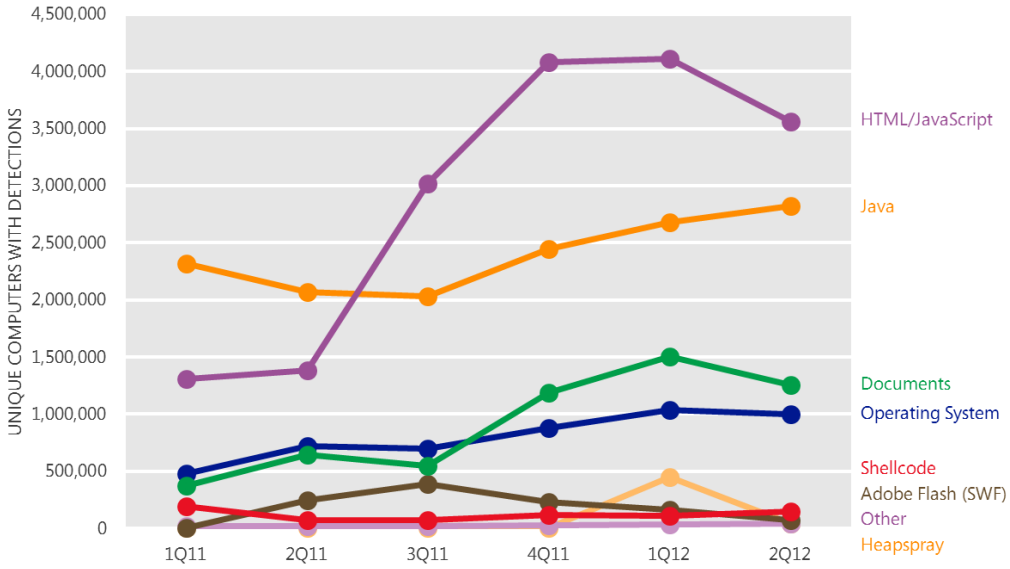
- Раскрытие уязвимостей во всей отрасли выросло в 1П12 на 11,3% по сравнению с 2П11 и на 4,8% по сравнению с 1П11.
- Этот рост сводит на нет тенденцию слабого снижения, наблюдавшуюся в каждом полугодии с 2П09 по 2П11. В основном рост обусловлен уязвимостями приложений, тогда как доля уязвимостей операционной системы продолжает уменьшаться.

Эксплойты

Эксплойт — это вредоносный код, использующий преимущества уязвимостей программного обеспечения для заражения, нарушения работы или полного контроля над компьютером без согласия и обычно без ведома пользователя. Эксплойты нацелены на уязвимости в операционных системах, веб-браузерах, приложениях и компонентах программного обеспечения, установленных на компьютере. Дополнительные сведения можно получить, загрузив полный отчет *SIRv13* со страницы www.microsoft.com/sir.

На рис. 2 показано, какие типы эксплойтов преобладали среди обнаруженных антивирусными продуктами Майкрософт в каждом квартале с 1К11 по 2К12, согласно числу уникальных зараженных компьютеров.

Рис. 2. Число уникальных компьютеров, сообщивших о разных типах эксплойтов с 1К11 по 2К12.



- Число компьютеров, сообщивших об эксплойтах, переданных через HTML или JavaScript, оставалось высоким на протяжении первого полугодия 2012 г., в первую очередь из-за продолжающегося преобладания семейства эксплойтов Blacole, наиболее часто обнаруживаемых в 1П12.
- Вторыми по распространенности в 1П12 были Java-эксплойты, статистика обнаружений которых росла в течение всего периода в основном за счет повышения числа обнаруженных эксплойтов для CVE-2012-0507 и CVE-2011-3544.
- Эксплойты, нацеленные на уязвимости в программах чтения и редактирования документов, стали третьими по численности в 1П12, главным образом из-за обнаружений эксплойтов, нацеленных на более старые версии Adobe Reader.

Семейства эксплойтов

На рис. 3 указаны семейства эксплойтов, наиболее часто обнаруживаемые в первом полугодии 2012 г.

Рис. 3 [TopExploitFamilies] Основные семейства эксплойтов, обнаруженные антивирусными продуктами Майкрософт в 1П12, согласно числу уникальных компьютеров с обнаружениями. Интенсивность фона отображает степень преобладания.

Семейство эксплойтов	Платформа или технология	3К11	4К11	1К12	2К12
Blacole	HTML/JavaScript	1054045	2535171	3154826	2793451
CVE-2012-0507*	Java	–	–	205613	1494074
Win32/Pdfjsc	Документы	491036	921325	1430448	1217348
Вредоносный код IFrame	HTML/JavaScript	1610177	1191316	950347	812470
CVE-2010-0840*	Java	1527000	1446271	1254553	810254
CVE-2011-3544	Java	–	331231	1358266	803053
CVE-2010-2568 (MS10-046)	Операционная система.	517322	656922	726797	783013
JS/Phoex	Java	–	–	274811	232773
CVE-2008-5353	Java	335259	537807	295515	215593
Шелл-код	Шелл-код	71729	112399	105479	145352

* Эту уязвимость также использует семейство Blacole; в приведенной здесь статистике не учтены обнаружения Blacole.

- Blacole, семейство эксплойтов, используемых т. н. набором эксплойтов «Blackhole» («черная дыра») для передачи вредоносных программ через зараженные веб-страницы, стало наиболее часто обнаруживаемым семейством эксплойтов в первом полугодии 2012 г. Злоумышленники покупают или берут в аренду наборы Blacole на хакерских форумах или через иные незаконные источники. Такой набор состоит из коллекции вредоносных веб-страниц, содержащих эксплойты, нацеленные на уязвимости в различных версиях Adobe Flash Player и Adobe Reader, в компонентах доступа к данным MDAC, в среде выполнения Oracle Java (Oracle JRE) и в прочих популярных продуктах и компонентах. Когда злоумышленник устанавливает набор Blacole на вредоносный или зараженный веб-сервер, те компьютеры, на которых нет регулярно обновляемых средств безопасности, подвергаются риску заражения через попутную загрузку.

Вредоносные и потенциально нежелательные программы

Если не указано иное, информация в этом разделе составлена по данным телеметрии, полученным с более чем 600 миллионов компьютеров по всему миру и некоторых самых активно используемых служб в Интернете. Уровни заражения указаны в единицах CCM, или тысячах, на тысячу очищенных компьютеров (CCM, computers cleaned per mille) и представляют собой число отправивших отчеты компьютеров, очищенных в квартале на каждую 1000 выполнений средства удаления вредоносных программ Windows®, доступного через Центр обновления Майкрософт и веб-сайт Центра обеспечения безопасности Microsoft.

С точки зрения шаблонов заражения, рис. 4 с помощью CCM показывает уровни заражения в регионах по всему миру. Обнаружения и удаления по отдельным странам и регионам могут значительно отличаться от квартала к кварталу.

Рис. 4. Уровни заражения по странам и регионам в 2K12, по CCM

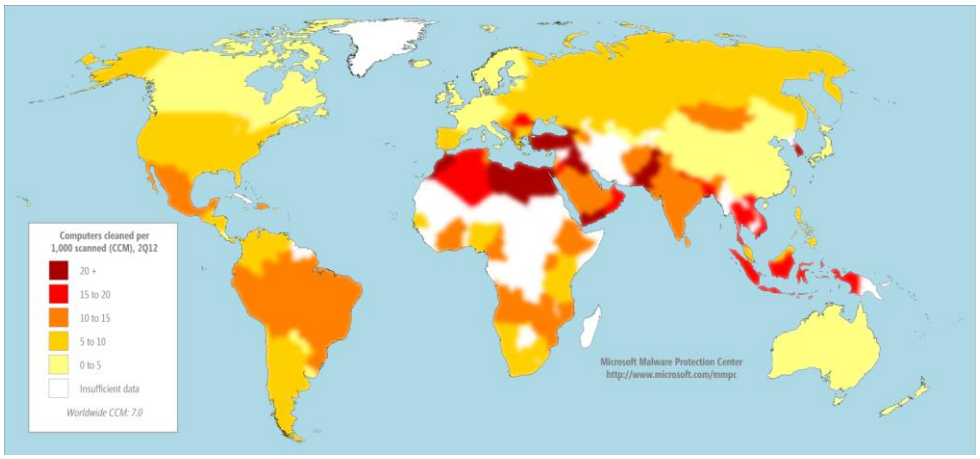
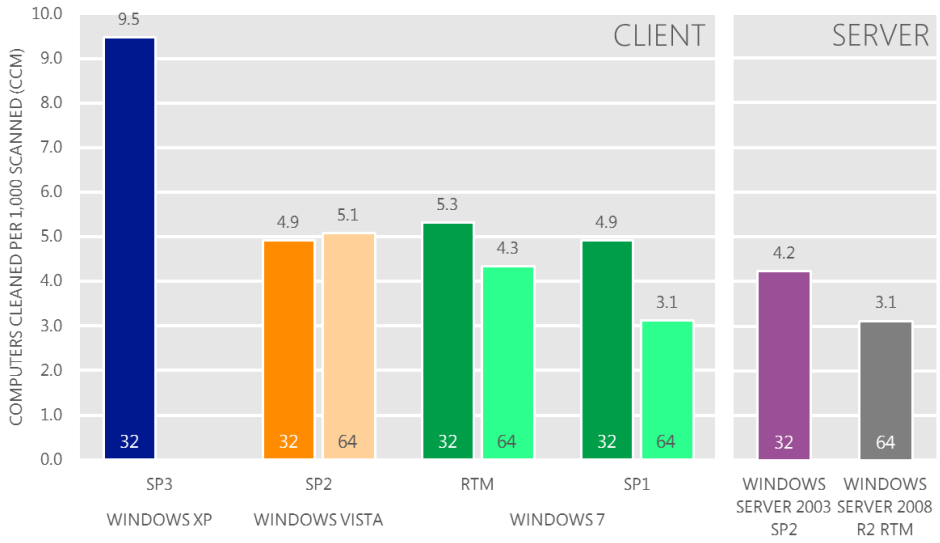


Рис. 5. Уровни заражения (CCM) по операционным системам и пакетам обновления в 2K12

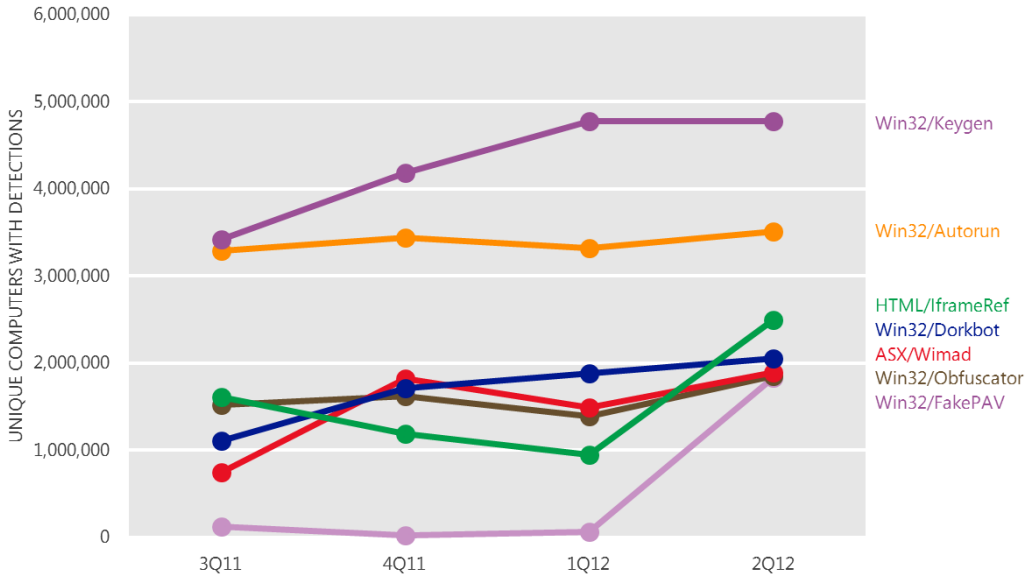


«32»= 32-разрядный выпуск; «64» = 64-разрядный выпуск. SP = пакет обновления. RTM = окончательная первоначальная версия. Показана статистика для операционных систем как минимум с 0,1% от всех выполнений средства удаления вредоносных программ в 2K12.

- Эти данные нормализованы: уровень заражения для каждой версии Windows рассчитывается сравнением равного числа компьютеров на версию (например, 1000 компьютеров с Windows XP SP3 в сравнении с 1000 компьютеров с Windows 7 RTM).

Семейства угроз

Рис. 6. Тенденции обнаружения для нескольких заметных семейств в 3К11-2К12



- Семейства Win32/Keygen и Win32/Autorun обнаруживались чаще всего в 1П12. Keygen представляет собой универсальное обнаружение средств, генерирующих ключи для нелегально приобретаемых версий разнообразных программных продуктов.

  Autorun представляет собой универсальное семейство вирусов-червей, распространяющихся между подключенными томами за счет функции автозапуска в Windows. Изменения, внесенные недавно в эту функцию в Windows XP и Windows Vista, помогли снизить связанные с ней риски, но злоумышленники продолжают распространять вредоносные программы, нацеленные на эту уязвимость.

- Число обнаружений универсального семейства JS/IframeRef выросло более чем вдвое между 1K12 и 2K12 после нескольких кварталов спада. IframeRef представляет собой обобщенное обнаружение тегов, специально формируемых для встроенных фреймов HTML и указывающих на удаленные веб-сайты, содержащие вредоносный контент.

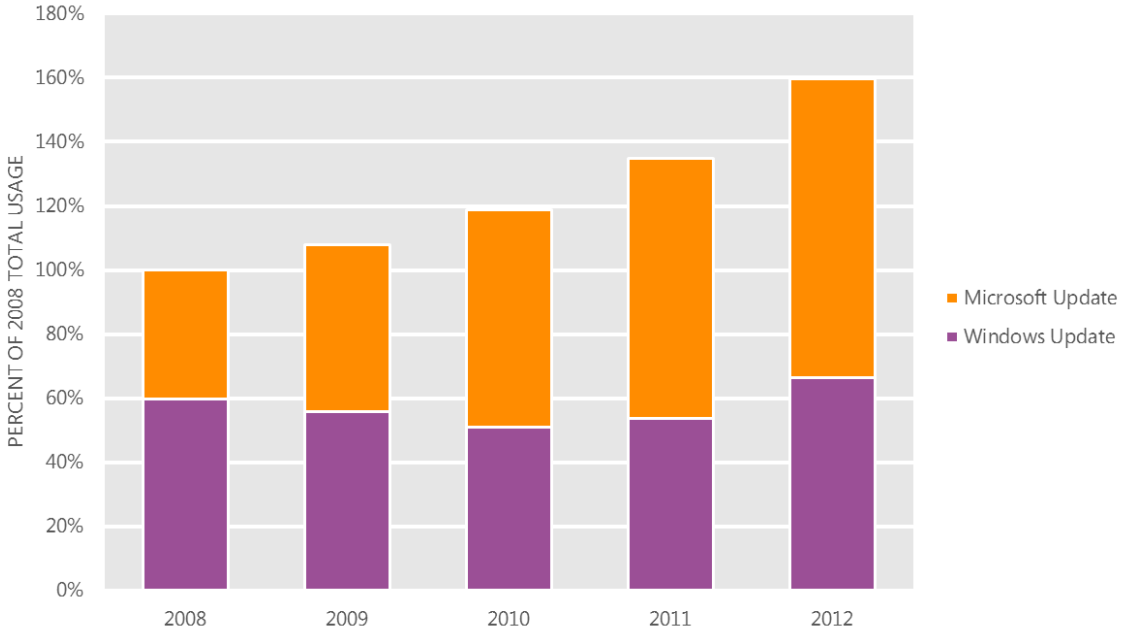
Угрозы для домашних и корпоративных компьютеров

Сравнение угроз, с которыми сталкиваются компьютеры, присоединенные к домену, и компьютеры вне домена, может дать представление о различных способах, применяемых злоумышленниками при атаках на корпоративные и домашние компьютеры, а также о том, какие угрозы чаще всего реализуются в каждой среде.

- Пять семейств являются общими для обоих списков, прежде всего универсальне семейства Win32/Keygen и Win32/Autorun, а также семейство эксплойтов Blacole.
- Семейства, значительно преобладающие на компьютерах, присоединенных к домену, по меньшей мере в течение одного квартала включают универсальное семейство JS/IframeRef и семейство вирусов-червей Win32/Conficker.
- Семейства, значительно преобладающие на компьютерах вне домена, включают Keygen и семейства программ для показа рекламы JS/Pornpop и Win32/Hotbar.

Обращения в Центр обновлений Windows и Центр обновлений Майкрософт

Рис. 7. [WU-MU] Компьютеры под управлением Windows, для которых Центр обновления Windows и Центр обновления Майкрософт выполнили обновления, по всему миру, 2008–2012 гг.



- Рис. 7 иллюстрирует рост числа компьютеров, для которых Центр обновления Windows и Центр обновления Майкрософт выполнили обновления, по всему миру за последние четыре года по сравнению с 2008 г.
- С 2008 г. объем обращений в Центр обновлений Windows и Центр обновлений Майкрософт вырос на 60% по всему миру. Этот рост достигнут преимущественно за счет повышения объема обращений в Центр обновлений Майкрософт, который составил 53% с 2008 по 2012 г., тогда как для Центра обновлений Windows этот показатель составил 6%.

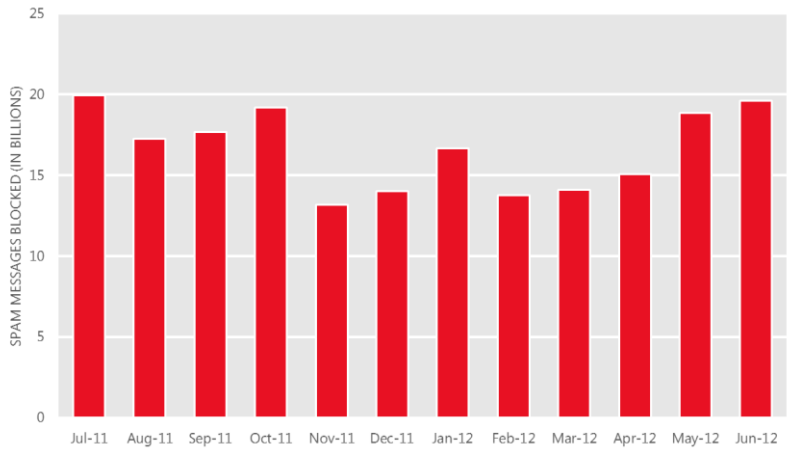
- Центр обновлений Windows обеспечивает обновление для компонентов Windows и для драйверов устройств, предоставляемых как корпорацией Майкрософт, так и поставщиками оборудования. Центр обновлений Windows также распространяет обновления подписей для антивирусных программ и ежемесячные выпуски средств удаления вредоносных программ. По умолчанию, если пользователь задал автоматическое обновление, клиент обновления сам подключается к Центру обновлений Windows.
- Центр обновлений Майкрософт предоставляет все обновления, предлагаемые Центром обновлений Windows, а также обновления для прочих программных продуктов Майкрософт, таких как Microsoft Office, Microsoft SQL Server и Microsoft Exchange Server. Пользователи могут задать автоматические обновления либо при установке программ, обслуживаемых Центром обновлений Майкрософт, либо на сайте Центра обновлений Майкрософт (update.microsoft.com/microsoftupdate). Корпорация Майкрософт рекомендует пользователям задавать для компьютеров обращение в Центр обновлений Майкрософт вместо Центра обновлений Windows, чтобы гарантированно получать своевременные обновления безопасности для продуктов Майкрософт.

Угрозы, связанные с электронной почтой

Блокирование нежелательной почты

Информация этого раздела отчета составлена по данным телеметрии, предоставленным службой Microsoft Exchange Online Protection. FOPE поставляет тысячам корпоративных клиентов Майкрософт службы фильтрации нежелательной почты, фишинга и вредоносных программ и ежемесячно обрабатывает десятки миллиардов сообщений.

Рис. 8. Число сообщений, заблокированных службой Exchange Online Protection с июля 2011 по июнь 2012 г.



- Объем заблокированной почты в 1П12 сопоставим с объемом в 2П11 и остается намного ниже показателей, отмечавшихся ранее, до конца 2010 г. Резкое снижение объемов нежелательной почты, наблюдаемое в последние полтора года, обусловлено успешной ликвидацией нескольких крупных спамботов, особенно Cutwail (в августе 2010 г.) и Rustock (в марте 2011 г.).

Рис. 9. [FOPEBlockedHistoric] Число сообщений, заблокированных службой Exchange Online Protection в каждое полугодие 2П08–1П12

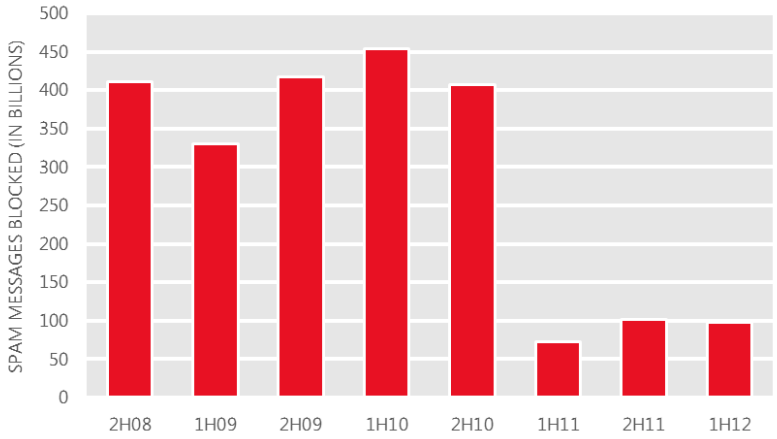
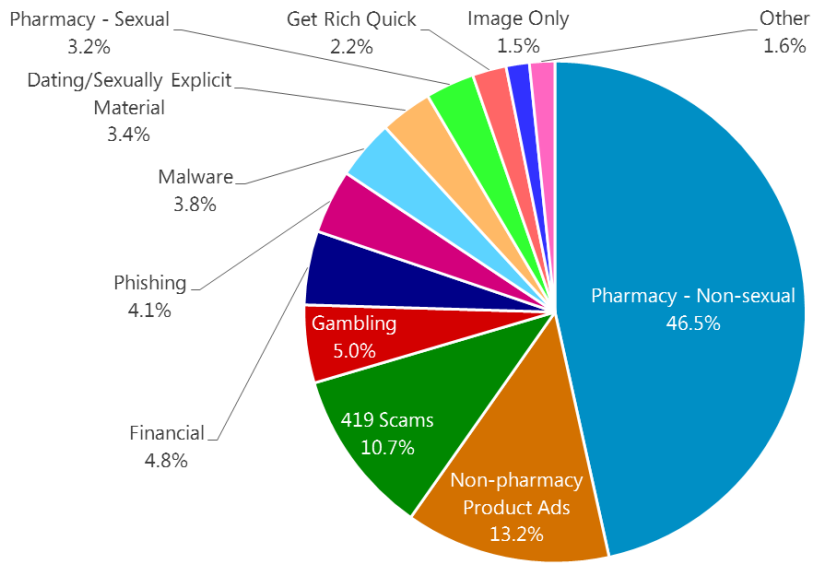


Рис. 10. Входящие сообщения, заблокированные фильтрами Exchange Online Protection в 1П12, по категориям

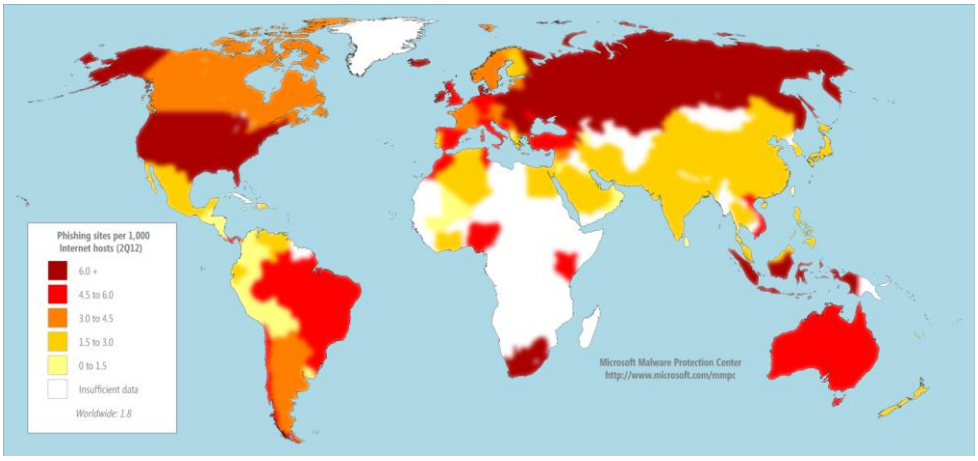


- Фильтры контента FOPE распознают несколько различных общих типов нежелательных сообщений. На рис. 10 показаны наиболее распространенные типы нежелательных сообщений, обнаруженных в 1П12.

Вредоносные вебсайты

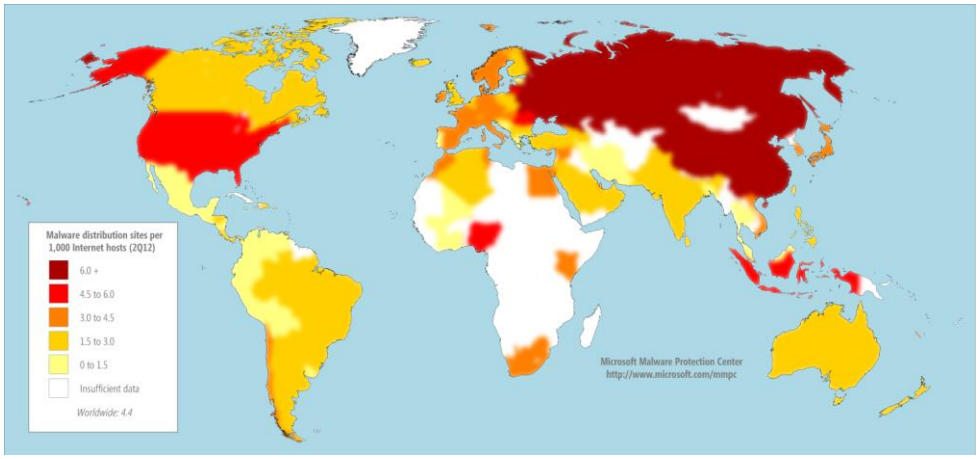
Фишинговые сайты размещены по всему миру на ресурсах, предлагающих бесплатный хостинг, на зараженных веб-серверах и в различных других контекстах.

Рис. 11. Фишинговые сайты на 1000 интернет-хостов по всему миру в 2K12



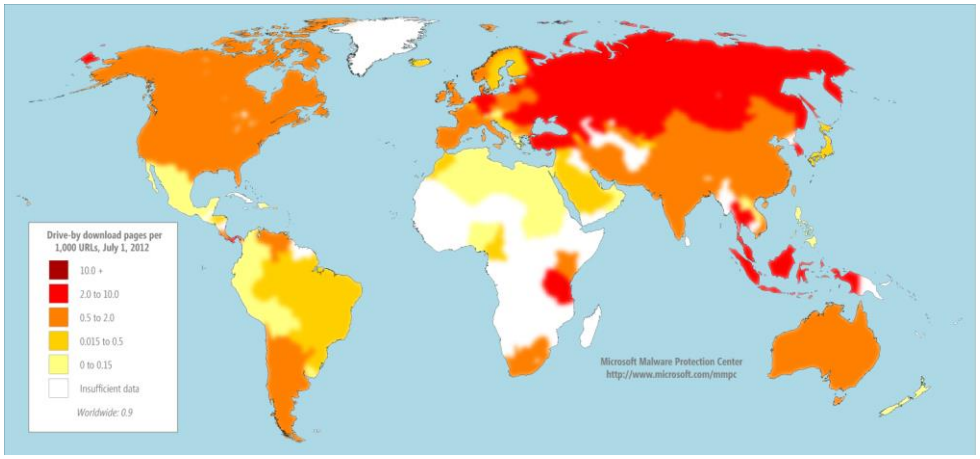
В США, где находится больше всего хостов, имеется и больше всего фишинговых сайтов (2,9 на 1000 интернет-хостов в 2K12); Китай находится на втором месте по числу хостов, но концентрация фишинговых сайтов там намного ниже (0,6 на 1000 интернет-хостов).

Рис. 12. Сайты распространения вредоносных программ на 1000 интернет-хостов по всему миру в 2K12



Сайт *попутной загрузки* — это веб-сайт, на котором размещены один или несколько эксплойтов, нацеленных на уязвимости веб-браузеров и их надстроек. Уязвимые компьютеры могут быть заражены вредоносной программой просто при посещении такого веб-сайта, даже без попытки что-либо загрузить.

Рис. 13. Страницы попутной загрузки, индексированные сайтом Bing.com в конце 2K12 на 1000 URL-адресов в каждой стране или регионе



Документ обобщает ключевые выводы отчета. Полный отчет включает также глубокий анализ тенденций, обнаруженных более чем в 100 странах

и регионах по всему миру и дает предложения по управлению рисками для вашей организации, программного обеспечения и людей.

Полный отчет можно загрузить со страницы www.microsoft.com/sir.

Microsoft

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security