| Аналитический отчет по безопасности Майкрософт

Том 11

Подробное описание перспектив уязвимостей программного обеспечения и средств их использования, угроз вредоносного кода и потенциально нежелательного ПО за первую половину 2011 г.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

Microsoft

Аналитический отчет по безопасности Майкрософт

Содержание

Аналитический отчет по безопасности Майкрософт, том 11

В 11 томе *аналитического отчета по безопасности Майкрософт®* (*SIRv11*) представлено подробное описание перспектив уязвимостей программного обеспечения, средств их использования, угроз вредоносного кода и потенциально нежелательного ПО в продуктах Майкрософт и сторонних производителей. Корпорация Майкрософт создала этот отчет на основе тщательного анализа тенденций за последние несколько лет с концентрацией на первом полугодии 2011 г.

В этом документе представлены ключевые результаты отчета. Полная версия отчета также содержит тщательный анализ тенденций, обнаруженных более чем в 100 странах или регионах во всем мире и описывает способы управления рисками для вашей организации, программного обеспечения и людей.

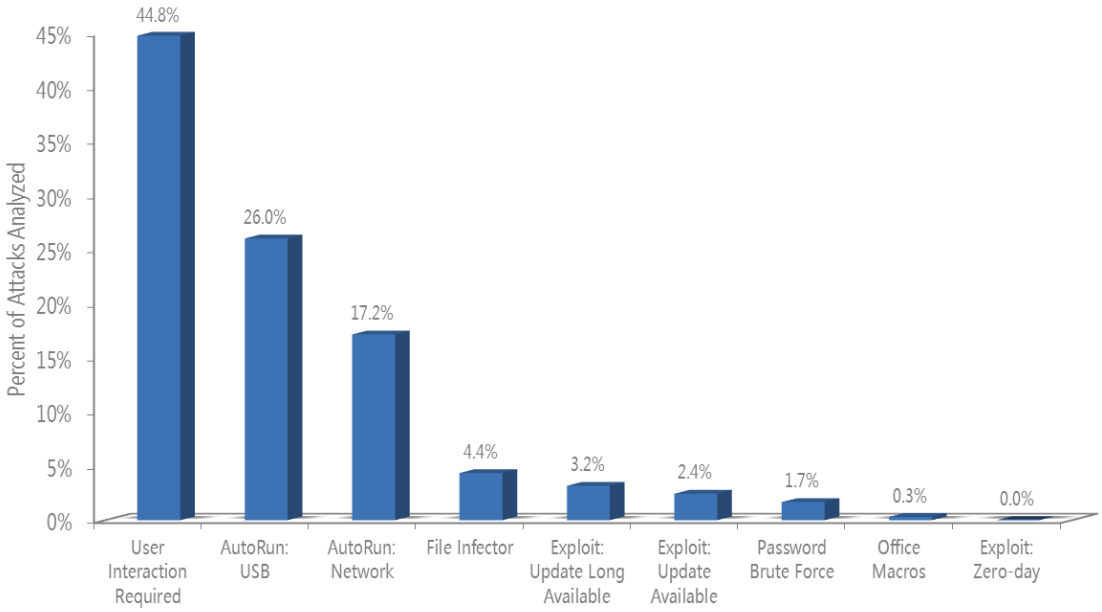
Полный отчет, как и предыдущие тома и связанные видео, можно загрузить с веб-сайта www.microsoft.com/sir.

Обнуление методов распространения вредоносного программного обеспечения

Корпорация Майкрософт выполнила анализ для лучшего понимания частоты эксплуатации нулевого дня и рисков, которые эта угроза представляет для пользователей. Этот анализ был создан, чтобы предоставить специалистам по безопасности информацию, которую они могут использовать для определения приоритетов своих задача и эффективного управления рисками. Как и все остальные, ИТ-отделы встречаются с ограничениями времени, бюджета, кадров и ресурсов при планировании и выполнении своей работы. Точная и обновленная информация об угрозах позволяет специалистам эффективно классифицировать средства защиты и обеспечивать безопасность сетей, ПО и пользователей.

Для этого анализа угрозы, обнаруженные с помощью средства удаления вредоносных программ (MSRT) в течение первого полугодия 2011 г., были классифицированы по средствам распространения каждого семейства угроз для заражения своих жертв. Если было задокументировано, что угроза использует несколько векторов атак для заражения пользователей, то число заражений, определенное MSRT для этого семейства, делилось на равные доли для каждого вектора. На рис. Рис. 1 показаны результаты этого анализа.

Рис. 1. Вредоносное ПО, обнаруженное MSRT в 1 полугодии 2011 г. с, по документированным средствам распространения



- Разные методы распространения угроз на рис. Рис. 1 описываются следующим образом:

  - **Требуется участие пользователя**. Когда пользователь должен выполнить действие, чтобы скомпрометировать компьютер. В этом контексте «действие» означает преднамеренное действие, которое каким-то образом отличается от обычного использования компьютера.

  - **Автозапуск: USB**. Угроза использует функцию автозапуска в Windows для заражения USB-устройств и других съемных носителей.

  - **Автозапуск: сеть**. Угроза использует функцию автозапуска для заражения сетевых томов, сопоставленных с буквами диска.

  - **Заражение файлов**. Угроза распространяется за счет изменения файлов (зачастую с расширениями EXE и SCR), заменяя определенные сегменты кода.

- **Средство эксплуатации уязвимости: обновление доступно долгое время**. Производитель выпустил обновление безопасности для устранения уязвимости за год до атаки.
- **Средство эксплуатации уязвимости: обновление доступно**. Производитель выпустил обновление безопасности для устранения уязвимости менее чем за год до атаки.
- **Средство эксплуатации уязвимости: нулевой день**. Производитель не выпустил обновление безопасности для устранения уязвимости во время атаки.
- **Атака пароля методом подбора**. Угроза распространяется, пытаясь напрямую подобрать пароль для доступных томов, например с помощью команды net use .
- **Макросы Office**. Угроза распространяется, заражая документы Microsoft Office вредоносными макросами Visual Basic® for Applications (VBA).
- **Эксплуатация нулевого дня**. Производитель не выпустил обновление безопасности для устранения уязвимости во время атаки.

- Больше трети обнаруженных вредоносных программ, которые были проанализированы, использовали функцию автозапуска в Windows®.
  - Угрозы, эксплуатирующие автозапуск, разделились на те, которые распространяются через съемные носители (26 процентов), и те, которые распространяются через сетевые тома (17 процентов).
  - Для борьбы с этими угрозами корпорация Майкрософт предприняла несколько мер для защиты пользователей, в том числе выпустила обновление для платформ Windows XP и Windows Vista® в феврале 2011 г., чтобы сделать функцию автозапуска более безопасной, как это сделано в Windows 7 по умолчанию.
- Около шести процентов обнаруженных MSRT угроз были классифицированы как *средства эксплуатации уязвимостей* —

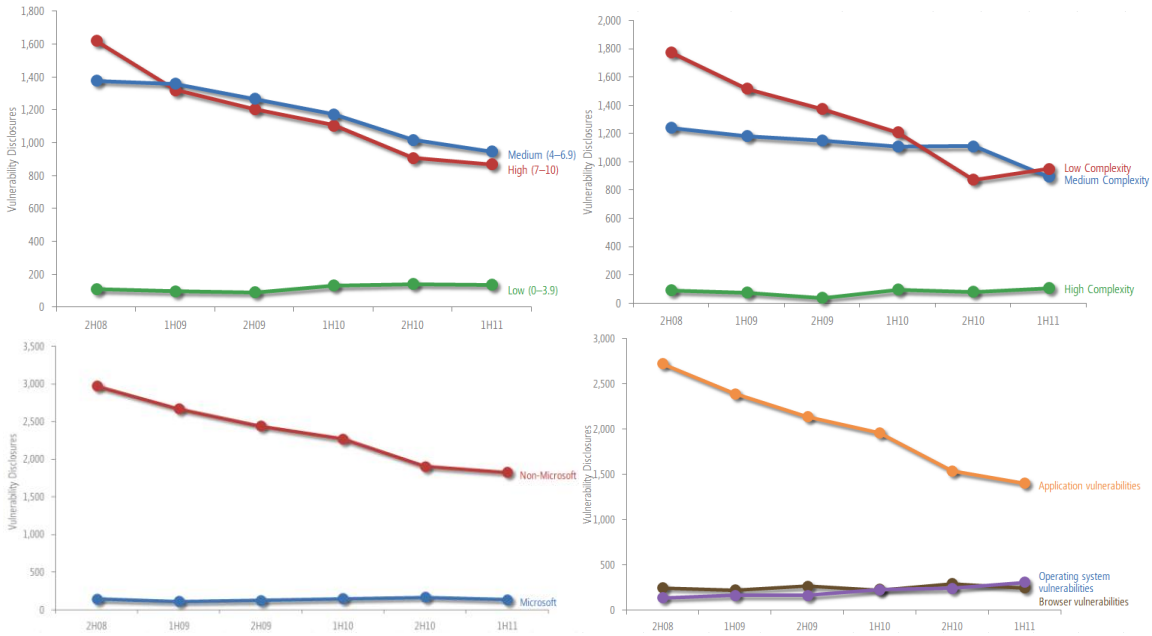
вредоносный код, который пытается эксплуатировать уязвимости в приложениях или операционных систем.

- Ни одно из самых распространенных семейств угроз, обнаруженных MSRT, не использовало эксплуатация нулевого дня в 1 полугодии 2011 г.
- Из всех способов использования уязвимостей, обнаруженных MMPC, менее одного проценты были связаны с эксплуатацией нулевого дня.

Анализ угроз во всем мире

Обнаружение угроз

Рис. 2. Тенденции по критичности уязвимостей (CVE), сложности уязвимостей, обнаружения по производителям и обнаружения по типу



- Общая тенденция критичности угроз (которая определяется числом CVE) была положительной. Число уязвимостей среднего и высокого уровня критичности, обнаруженных в 1 полугодии 2011 г., было на 6,8 % и 4,4 % ниже, чем во 2 полугодии 2010 г. соответственно.

- Число уязвимостей малой сложности (самых простых в использовании) упало на 41,2 % по сравнению с предыдущим годом.

- Число обнаруженных уязвимостей операционной системы и браузера было стабильно в течение нескольких лит и составляло 12,7 % и 15, 7 %

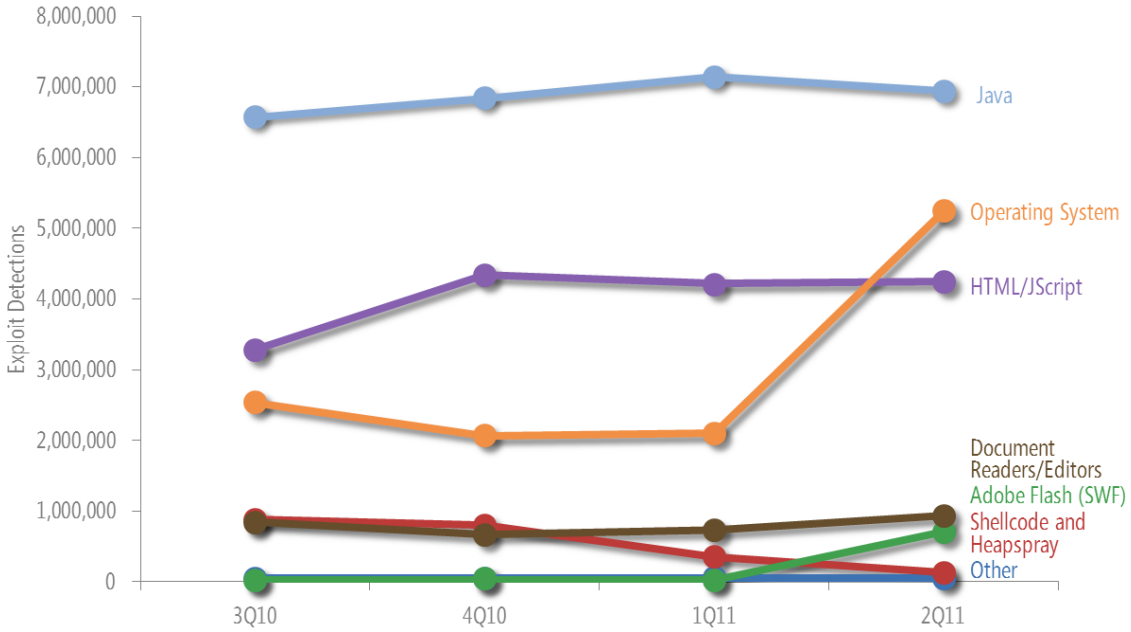
от всех обнаруженных уязвимостей в 1 полугодии 2011 г. соответственно.

- Уязвимости в продуктах Майкрософт составляют 6,9 % от всех уязвимостей, обнаруженных в 1 полугодии 2011 г., что меньше 8,2 % во 2 полугодии 2010 г.

Средство эксплуатации уязвимости

На рис. Рис. 3 показана распространенность разных типов использования уязвимостей за каждый квартал между 3 кварталом 2010 г. и 2 кварталом 2011 г.

Рис. 3. Способы использования уязвимостей, обнаруженные и заблокированные продуктами защиты от вредоносного ПО Майкрософт, 3 квартал 2010 г.-2 квартал 2011 г., по целевой платформе или технологии



- Самыми распространенными средствами использования уязвимостей в 1 квартале 2011 г. были нацелены на уязвимости в Oracle (ранее Sun) Java Runtime Environment (JRE), Java Virtual Machine (JVM) и Java SE в пакете Java Development Kit (JDK). Уязвимости Java были ответственны за одну треть и одну вторую всех средств использования уязвимостей, обнаруженных в течение последних четырех кварталов.

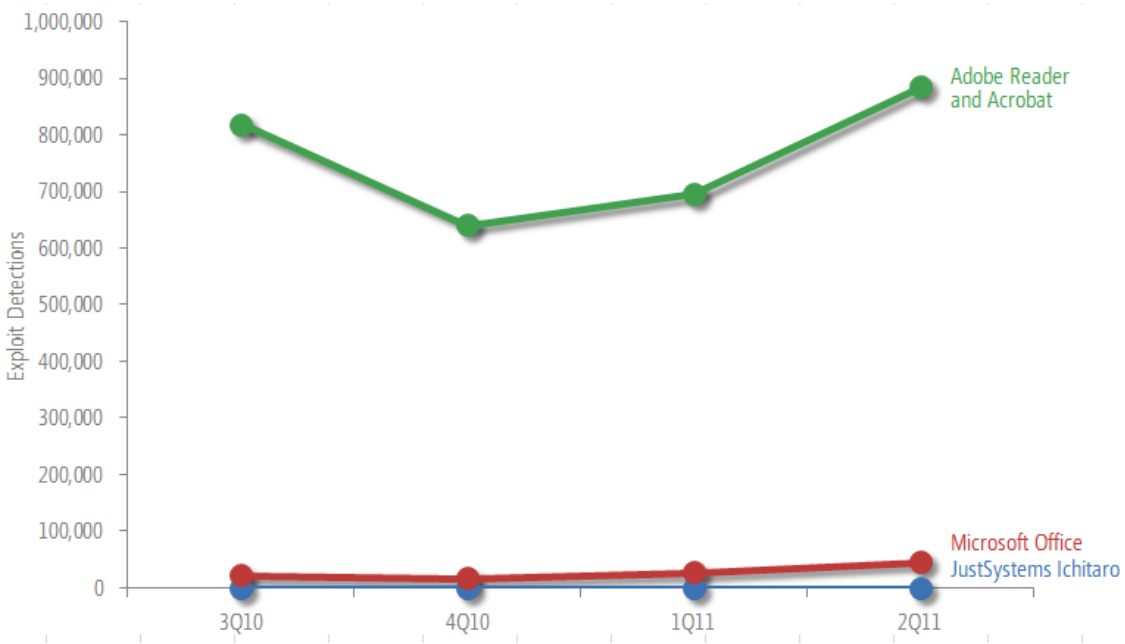
- Число использования уязвимостей операционных систем значительно выросло во 2 квартале 2011 г. из-за частого использования уязвимости CVE-2010-2568.

- Число использования уязвимостей Adobe Flash, которые менее распространены по сравнению с другими типами, увеличилось во 2 квартале 2011 г. более чем на 40 % по сравнению с 1 кварталом 2011 г. из-за эксплуатации пары новых обнаруженных уязвимостей.

- Число использования CVE-2010-2568, уязвимости в оболочке Windows, значительно увеличилось во 2 квартале 2011 г., что стало основной причиной повышения числа использования уязвимостей операционных систем во 2 квартале 2011 г.. Данная уязвимость была впервые обнаружена при использовании семейством вирусов Win32/Stuxnet в середине 2010 г.

Использование уязвимостей документов

Рис. 4. Типы использования уязвимостей синтаксического анализатора документов, обнаруженные и заблокированные продуктами защиты от вредоносного ПО Майкрософт, 3 квартал 2010 г.-2 квартал 2011 г.



- Средства эксплуатации уязвимостей, затрагивающие Adobe Acrobat и Adobe, были основным типом эксплуатации уязвимостей форматов документов в первом половине 2011 г. Почти все эти уязвимости применялись семейством Win32/Pdfjsc.

- Более половины способов эксплуатации уязвимостей Microsoft Office применяли CVE-2010-3333, уязвимость синтаксического анализатора формата RTF в различных версиях Microsoft Word.

Вредоносные и потенциально нежелательные программы

Если не указано иначе, сведения в данном разделе были получены на основе телеметрических данных, сформированных более чем на 600 миллионах компьютеров во всем мире и одних из самых используемых служб в Интернете. Показатели заражений указаны в *единицах CCM* или тысячах и представляют задокументированное число очищенных компьютеров за квартал на 1 000 выполнений средства удаления вредоносных программ (MSRT). Дополнительные сведения об единице измерения CCM см. в разделе «Вредоносное программное обеспечение» *аналитического отчета по безопасности Майкрософт*.

Показатели заражения операционных систем

Рис. 5. Показатели заражения (CCM) по операционным системам и пакетам обновлений во 2 квартале 2011 г.

«32» = 32-разрядная версия, «64» = 64-разрядная версия. SP = пакет обновления. Показаны поддерживаемые операционные системы с общим числом запуска как минимум 0,1 % во 2 квартале 2011 г.

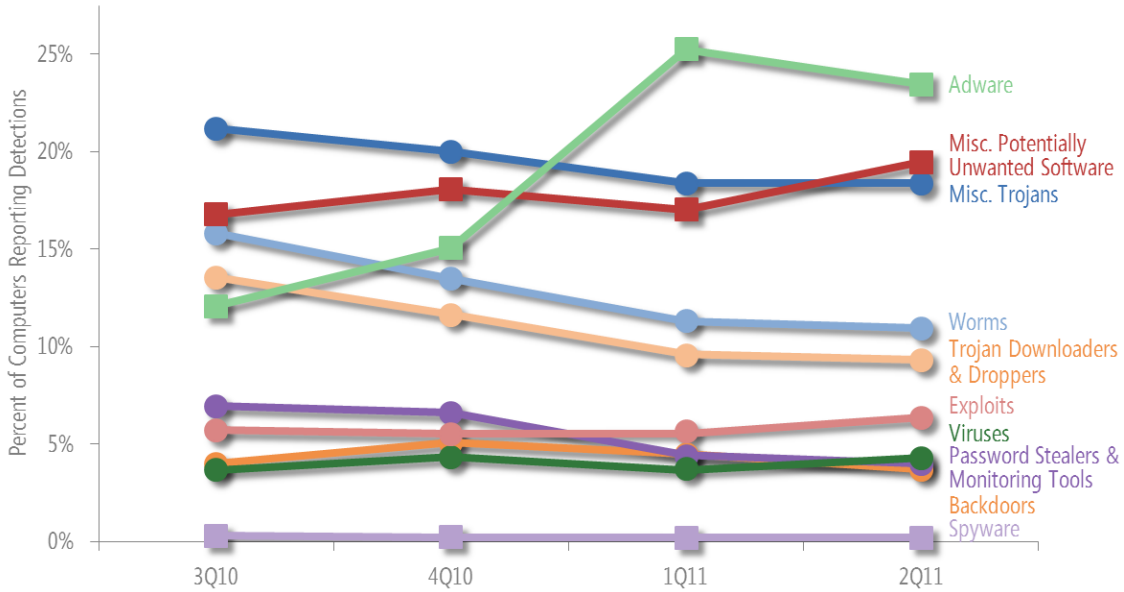
- Как и в предыдущие периоды, показатели заражений для недавно выпущенных операционных систем и пакетов обновлений Майкрософт значительно ниже, чем для старых продуктов, как для клиентских, так и для серверных платформ. Windows 7 и Windows Server® 2008 R2, самые

последние клиентские и серверные версии Windows соответственно, имели самые низкие показатели заражений, как показано на рис. Рис. 4.

- Показатели заражений для Windows XP SP3 и Windows Vista упали после выпуска в феврале 2011 г. автоматического обновления, которое изменило способ работы функции автозапуска на этих платформах так же, как это было сделано в Windows 7. Результаты этого изменения можно увидеть в статистике заражений Win32/Rimecud, девятого в списке самых распространенных семейств угроз в мире и часто использующих функцию автозапуска в 1 квартале 2011 г.

Семейства и категории угроз

Рис. 6. Число обнаружений по категории угроз, 3 квартал 2010 г.-2 квартал 2011 г., по проценту от всех зараженных компьютеров



Круглые маркеры обозначают категории вредоносных программ, квадратные маркеры обозначают категории потенциально нежелательных программ.

- Семейство Win32/OpenCandy было самым распространенным семейством угроз, обнаруженным в 1 квартале 2011 г. в целом. OpenCandy — это программа для показа рекламы, которая может быть встроена в определенные программы установки ПО сторонних производителей.

- JS/Pornpop, второе по распространенности семейство угроз в 1 квартале 2011 г — это специально созданные объекты с поддержкой JavaScript, которые пытаются отображать всплывающую рекламу в браузерах пользователей

- Win32/Hotbar, самое распространенное семейство угроз среди обнаруженных во 2 квартале 2011 г. и третье в списке самых распространенных семейств угроз в 1 квартале 2011 г. — это программа для показа рекламы, которая устанавливает панель инструментов браузера, отображающая всплывающую рекламу на основе мониторинга действий в браузере.

- Число обнаружений Win32/FakeRean увеличилось более чем на 300 процентов с 1 квартала по 2 квартал 2011 г., что сделало это семейство самым распространенной фальшивой программой обеспечения безопасности во втором квартале.

Корпоративные угрозы

- Семейства червей, которые относятся к трем самым распространенным семействам вредоносных программ, обнаруженных на компьютерах, подключенных к доменам (это больше свойственно корпоративным, а не домашним средам).

- К семействам вредоносных программ, которые преобладают на компьютерах, подключенных к доменам, относится Win32/Conficker и потенциально нежелательная программа Win32/RealVNC. RealVNC — это программа, позволяющая удалять компьютером удаленно (аналогично службе удаленного рабочего стола). Ее можно использовать и в легальных целях, но злоумышленники также применяли ее для управления компьютерами пользователей в преступных целях.

- Семейство вирусов Win32/Sality, которое не вошло в десятку самых распространенных для подключенных к домену компьютеров в 2010 г., в 2011 г. заняло десятое место.

Угрозы электронной почты

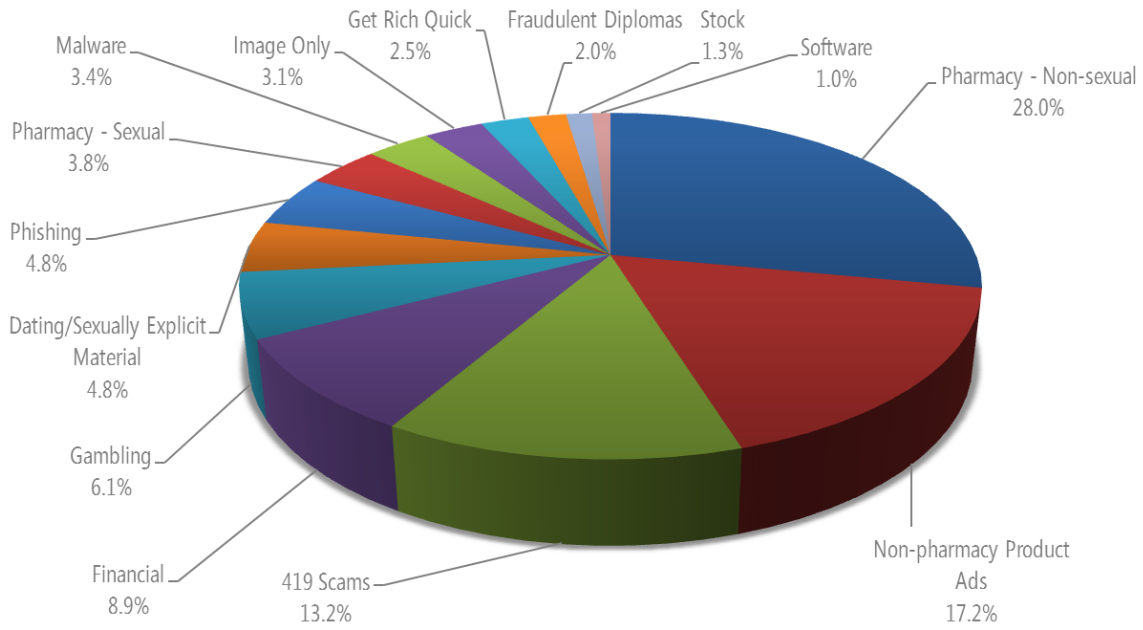
- Объем нежелательной почты, заблокированной Microsoft Forefront® Online Protection for Exchange (FOPE), значительно сократился за последние 12 месяцев с 89,2 миллиарда сообщений в июле 2010 г. до 25 миллиардов сообщений в июне 2011 г. в основном благодаря разрушению двух крупных ботнетов: Cutwail, который был разрушен в августе 2010 г., Rustock, разрушенного в марте 2011 г. после периода бездействия, который начался в январе. [1]

- Как и в предыдущие периоды, реклама фармацевтических продуктов, не связанных с сексом (28 % от общего числа), и нефармацевтических продуктов (17,2 %) составила большинство нежелательных сообщений, заблокированных фильтрами контента FOPE в 1 квартале 2011 г.

- Число нежелательных сообщений, содержащих только изображения, упало до 3,1 % в 1 квартале 2011 г. с 8,7 % в 2010 г.

[1] Дополнительные сведения о разрушении Cutwail см. в *аналитическом отчете по безопасности Майкрософт, том 10 (июль-декабрь 2010 г.)*. Дополнительные сведения о разрушении Rustock см. в статье «Борьба с угрозой Rustock», доступной в центре загрузки Майкрософт.

Рис. 7. Входящие сообщения, заблокированные фильтрами FOPE в 1 квартале 2011 г. по категории



Вредоносные веб-сайты

- Злоумышленники, занимающиеся фишингом, традиционно нацеливались в основном на финансовые сайты, но самая большая доля посещений фишинговых сайтов в 1 квартале 2011 г. была связана с сайтами социальных сетей и составила 83,8 % в апреле. (Под посещением фишингового сайта имеется в виду одна попытка пользователя посетить известный фишинговый сайт с помощью Windows Internet Explorer®, которая была заблокирована фильтром SmartScreen®. Дополнительные сведения см. в разделе «Вредоносные веб-сайты» аналитического отчета по безопасности Майкрософт.) В целом, атаки, направленные социальные сети, составили 47,8 % от всех фишинговых атак в 1 квартале 2011 г., а на втором месте расположились атаки на финансовые организации (35 %).

- Фишинговые сайты, связанные с финансовыми организациями, составили в среднем 78,3 % от всех активных фишинговых сайтов, отслеженных в 1 квартале 2011 г., а число фишинговых сайтов, связанных с социальными сетями, составило всего 5,4 %. Фишинговые атаки могут быть направлены на сотни финансовых организаций, для

каждой из которых требуется свой подход. Число популярных социальных сетей намного меньше, поэтому злоумышленники могут эффективно проводить атаки для большего числа пользователей на каждом сайте. Возможность прямого нелегального доступа к банковским счетам жертвы означает, что финансовые организации всегда будут популярными целями фишинговых атак и число посещений таких сайтов всегда будет самым большим или вторым в списке каждый месяц.

- Этот феномен также присутствует в меньшем масштабе с веб-службами и игровыми сайтами. Небольшое число веб-служб формируют большую часть трафика на такие сайты, поэтому фишинговые сайты, направленные на веб-службы, получили 11 % посещений, тогда как число подобных сайтов всего 3,6 %. Трафик веб-игр распространяется на большее число сайтов, поэтому число фишинговых сайтов, направленных на игровые сайты, составило 8,9 % от числа активных сайтов, но доля посещений была равна всего 4,3 %.

Число фишинговых сайтов, направленных на сайты электронной коммерции, составило всего 3,8 % от числа активных сайтов с долей посещений 1,9 %, что означает, что злоумышленники не считают такие сайты прибыльными целями.

Сведения о защите вашей организации, программного обеспечения и пользователей см. в разделе «Управление рисками» *аналитического отчета по безопасности Майкрософт*.
http://www.microsoft.com/sir

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