KASPERSKY lab

Windows: популярность и уязвимости

Version 1.0, August, 2014

Оглавление

Введение: место ПК в Multi-device мире 2
Почему именно Windows? 3
Методология и точность исследования 4
Основные цифры 6
Часть 1: Динамика миграции пользователей: Неспешная Windows 8.1, бессмертная XP 7
Разнообразная Windows: динамика изменения популярности различных версий системы 7
Windows 8.1: в целом медленно, но быстрее Windows 8 10
Windows 8.1: география лидеров 12
Windows XP и ее поразительная живучесть 14
Windows XP: география лидеров 17
Часть 2: Уязвимости и эксплойты 19
Уязвимости в продуктах Microsoft 19
Эксплойты под уязвимости в Windows: далеко от лидеров 21
Эхо Stuxnet 22
Заключение и рекомендации 26

Введение: место ПК в Multi-device мире

Современному человеку давно уже недостаточно одного персонального коммуникационного устройства. Смартфоны и планшеты своим удобством, функциональностью и сравнительно невысокими ценами ежегодно привлекают миллионы пользователей по всему миру. Если раньше для общения в интернете, онлайн-шоппинга, игр и прочих занятий люди использовали только ПК или ноутбук, то теперь для многих из этих целей используются смартфоны, планшеты и другие «подключенные» устройства, разновидностей которых становится все больше – различные переносные устройства, телевизоры, автомобили и т.п.

В этих условиях роль персональных компьютеров в жизни современных пользователей изменилась значительно: теперь это всего лишь одно из устройств, которыми они пользуются ежедневно. Это изменение сказалось и на мировом рынке ПК – в 2013 году он пережил десятипроцентное падение, которое, по оценкам аналитической компании Gartner, стало крупнейшим за всю историю наблюдений. И в 2014 году сокращение рынка ПК и ноутбуков продолжилось: по данным Gartner, в первом квартале 2014 года, поставки ПК сократились на 1,7% по сравнению с тем же периодом 2013 года.

Смещение потребительских предпочтений очевидно, но едва ли этот факт является поводом говорить о приближающейся смерти ПК. Прежде всего, потому, что покупая смартфоны и планшеты вместо новых ПК, пользователи не спешат расставаться со старыми компьютерами. Они остаются в гостиных и детских, где успешно выполняют роль стационарных терминалов для доступа к сети, играм, видео и прочему мультимедийному контенту.

Примерно такая же ситуация сохраняется, когда речь заходит об информационной безопасности: хотя количество устройств на мобильных операционных системах – iOS, Android, Windows Phone – постоянно растет, подавляющее большинство существующих киберугроз направлены прежде всего на пользователей ПК и доминирующей на подобных устройствах операционной системы Windows. Windows – хорошо развитая, глобальная софтверная экосистема, в тени которой за все годы ее существования фактически вырос весь хакерский андерграунд и развился во вполне самостоятельную параллельную экосистему со своим черным рынком программного обеспечения и софтверных услуг нелегального характера.

Эта зависимость киберпреступности от Windows достаточно прочна, чтобы ее не разорвали ни появление конкурентных программных платформ, ни снижение продаж компьютеров и ноутбуков. Тенденция прекрасно просматривается в статистике, которую «Лаборатория Касперского» получает из Kaspersky Security Network – глобальной распределенной инфраструктуре, созданной для обеспечения максимально возможного уровня защищенности пользователей продуктов «Лаборатории Касперского». Более 60 миллионов пользователей по всему миру на добровольной основе делятся данными о том, с какими угрозами им пришлось столкнуться во время работы за ПК. Эта информация помогает «Лаборатории

Касперского» быстрее реагировать на новые угрозы и практически мгновенно доставлять пользователям информацию, необходимую для защиты от этих угроз. Согласно статистике, количество этих угроз – крайне велико: в 2013 году продукты «Лаборатории Касперского» отразили более 5 миллиардов атак. Ежедневно эксперты компании и автоматические системы детектирования обнаруживают около 315 тысяч вредоносных программ. В 2012 году эта цифра составляла около 200 тысяч.

И, разумеется, абсолютное большинство обнаруживаемых ежедневно угроз созданы для атак на пользователей операционной системы Windows.

Почему именно Windows?

Выбирая тему для очередного отчета на основе статистики Kaspersky Security Network, мы стараемся обращать внимание на наиболее интересные на данный момент времени угрозы или программные платформы. К примеру, 2012-2013 годы можно было охарактеризовать стремительным ростом числа уязвимостей в программной среде Java и эксплойтов для нее, поэтому мы решили подготовить специальное исследование атак на эту платформу. По итогам 2013 года аналитики «Лаборатории Касперского» отметили рост числа кибератак, направленных на похищение финансовой информации. Это стало поводом для подготовки более подробного исследования подобных атак.

Последние полгода с небольшим были весьма интересны для операционной системы Windows. В октябре прошлого года Microsoft выпустила Windows 8.1 – самую свежую на текущий момент версию системы, которая к тому же стала первой версией в рамках новой стратегии компании по ежегодному выпуску обновлений системы. В апреле компания полностью[1] прекратила поддержку Windows XP – одной из своих самых популярных операционных систем, присутствующей на рынке с 2001 года. Более 13 лет.

Комбинация из не поддерживаемой более производителем операционной системы и опасной уязвимости в одном из ее компонентов или «братском» программном обеспечении – одна из самых худших из возможных, если рассматривать ситуацию с точки зрения информационной безопасности, поэтому для данного исследования эксперты «Лаборатории Касперского» решили остановиться на двух основных темах: распределении версий Windows, которые используют владельцы продуктов «Лаборатории Касперского», динамике перехода на более свежие версии этого ПО, а кроме того, рассмотреть динамику срабатываний продуктов «Лаборатории Касперского» на эксплойты, написанные под уязвимости в Windows и другом программном обеспечении Microsoft, которое есть практически на любом компьютере, работающем под управлением операционной системы компании из Редмонда.

[1] *За исключением Windows XP Embedded Service Pack 3 для встроенных систем, поддержка которой закончится 12 января 2016 года.*

Методология и точность исследования

В качестве объекта исследования выступили версии операционной системы Windows, работающие на компьютерах пользователей[2] продуктов «Лаборатории Касперского», согласившихся предоставлять данные в Kaspersky Security Network. Основными системами стали Windows 8.1, Windows 8, Windows 7, Windows Vista и Windows XP с учетом различных версий системы. Этими системами пользуются около 99% пользователей продуктов «Лаборатории Касперского». Еще одним объектом исследования стали данные о срабатываниях защитных продуктов «Лаборатории Касперского» на эксплойты, использующие уязвимости в Windows и других продуктах Microsoft.

Эти параметры были рассмотрены с точки зрения географического распределения и изменения во времени.

Основным периодом исследования избран промежуток в 8 месяцев с ноября 2013 по июнь 2014 года, однако в некоторых случаях, проводилось сравнение результатов месяц к месяцу (например, результаты в июне 2014 года сравнивались с результатами в июне 2013 года), а кроме того, анализировались данные об изменении различных показателей за всю историю наблюдений.

Конечная цель этого исследования заключалась в том, чтобы выяснить, насколько расторопны пользователи в переходе на более свежие версии системы, а кроме того, насколько велика опасность для пользователей не обновленных систем столкнуться с атаками с помощью эксплойтов для уязвимостей в устаревшем ПО Microsoft.

Всего для исследования была проанализирована информация, полученная более чем от 60 миллионов пользователей по всему миру. Являются ли эти данные достаточным для каких-либо определенных выводов о поведении пользователей Windows?

Для того чтобы выяснить это, мы обратились к стороннему источнику, в качестве которого выступил известный сервис аналитики StatCounter.com, и сравнили данные о популярности операционных систем по версии KSN и StatCounter. По данным KSN, в июне 2014 года картина выглядела следующим образом:

[2] Учитывались участники Kaspersky Security Network, которые хотя бы раз за исследуемый период столкнулись с вредоносным или Riskware ПО

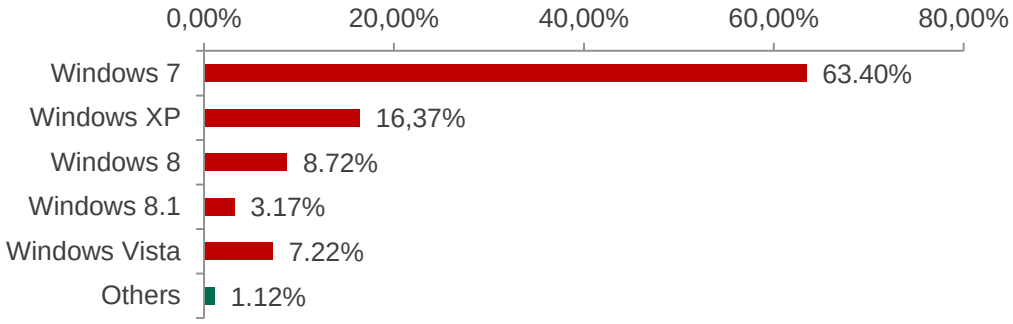


Рис.1: Распределение версий Windows по популярности в июне 2014, по данным KSN (количество уникальных пользователей)

Сервис StatCounter за тот же период времени выдает следующие результаты:

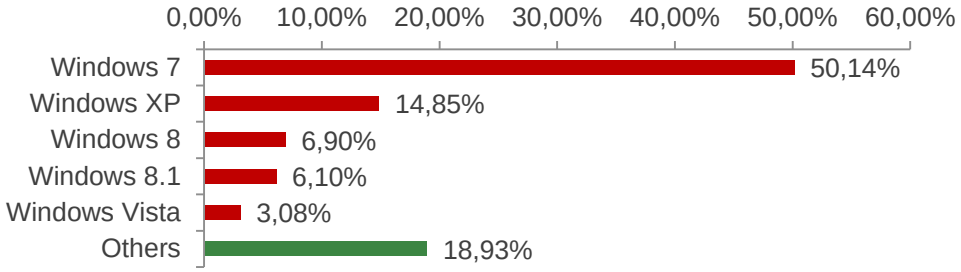


Рис.2: Распределение версий Windows по популярности в июне 2014, по данным StatCounter (количество просмотров веб-страниц).

Конечно, конкретные цифры в двух источниках разнятся. Прежде всего, потому что у StatCounter несколько иной метод сбора данных – сервис ведет подсчет просмотров страниц, в то время как «Лаборатория Касперского» учитывает количество уникальных пользователей. Однако совпадение общей картины и распределения популярности большинства исследуемых ОС в версиях KSN и StatCounter очевидны.

Основные цифры

- Несмотря на то, что поддержка Windows XP прекращена, огромное количество пользователей продолжает пользоваться этой системой – 16,37% пользователей продуктов «Лаборатории Касперского» в июне работали на компьютерах под управлением именно этой системы.
- Более полутора лет спустя после официального релиза, Windows 8 доля пользователей этой ОС составляет 8,72% процента. Доля Windows 8.1 – 7,22%
- Странами лидерами по уровню распространенности новейшей системы Windows 8.1 являются США, Канада, Германия и Великобритания.
- Странами лидерами по доле устаревшей ОС Windows XP являются Вьетнам, Китай, Индия, Алжир и Испания.
- Хотя в Windows и других продуктах Microsoft регулярно обнаруживаются уязвимости, абсолютное большинство срабатываний приходится на эксплойты под всего пять уязвимостей, самая ранняя из которых была обнаружена в 2010 году.
- Четыре года спустя после обнаружения все еще актуальна LNK-уязвимость CVE-2010-2568, использовавшаяся для распространения известного червя Stuxnet. Наибольшее число срабатываний на эксплойты под эту уязвимость регистрируются во Вьетнаме, Индии, Индонезии и Бразилии

Часть 1: Динамика миграции пользователей: Неспешная Windows 8.1, бессмертная XP

Windows 8.1 -это первая система, переход на которую с предыдущей версии осуществляется через обновление в фирменном магазине Windows Store, клиент для доступа в который присутствует в Windows 8.

Такая схема ввиду своей предельной простоты должна была бы повлиять на скорость перехода пользователей на наиболее новую систему. Кроме того, на скорость перехода на новую ОС положительно должно было повлиять, прекращение поддержки Windows XP, произошедшее в апреле этого года. Однако, как показывают данные KSN, реальность несколько отличается от продиктованных логикой ожиданий.

Разнообразная Windows: динамика изменения популярности различных версий системы

Общая динамика изменений уровня популярности различных версий Windows за исследуемый период выглядит следующим образом:

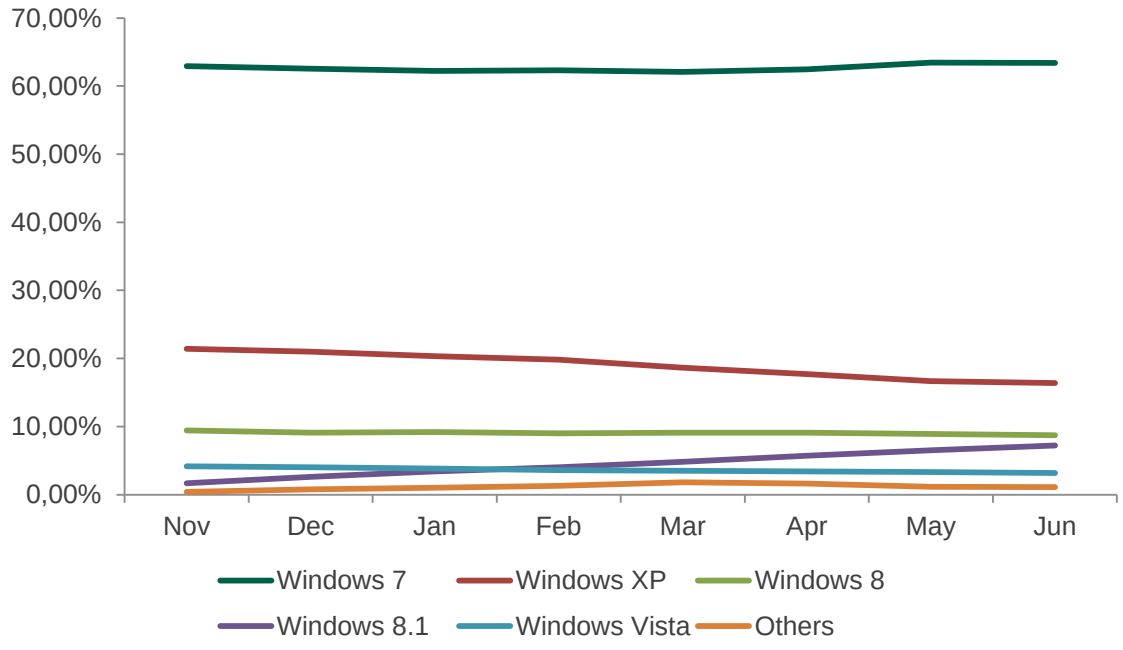


Рис. 3: Популярность различных версий Windows в период с ноября 2013 по июнь 2014

Как видно, абсолютным лидером является Windows 7, и доля ее даже растет: в ноябре минувшего года у нее было 62,91%, а по итогам июня 2014 года – уже 63,4%. Впрочем, если рассматривать абсолютные цифры, то прирост в июне по сравнению с ноябрем оказался незначительным: буквально несколько тысяч пользователей, что не позволяет говорить о каком-то важном изменении. Но число пользователей Windows 7 остается стабильно высоким даже в условиях присутствия на рынке более современных систем. Примечательно, что ситуация с доминированием Windows 7 постоянна: например, в июне 2013 года у этой системы было 63,22% пользователей, практически столько же, сколько и через год, т.е. в июне 2014-го.

С уровнем популярности других версий Windows ситуация складывалась иначе. Для большей наглядности мы исключили показатели Windows 7 из нижеследующего графика.

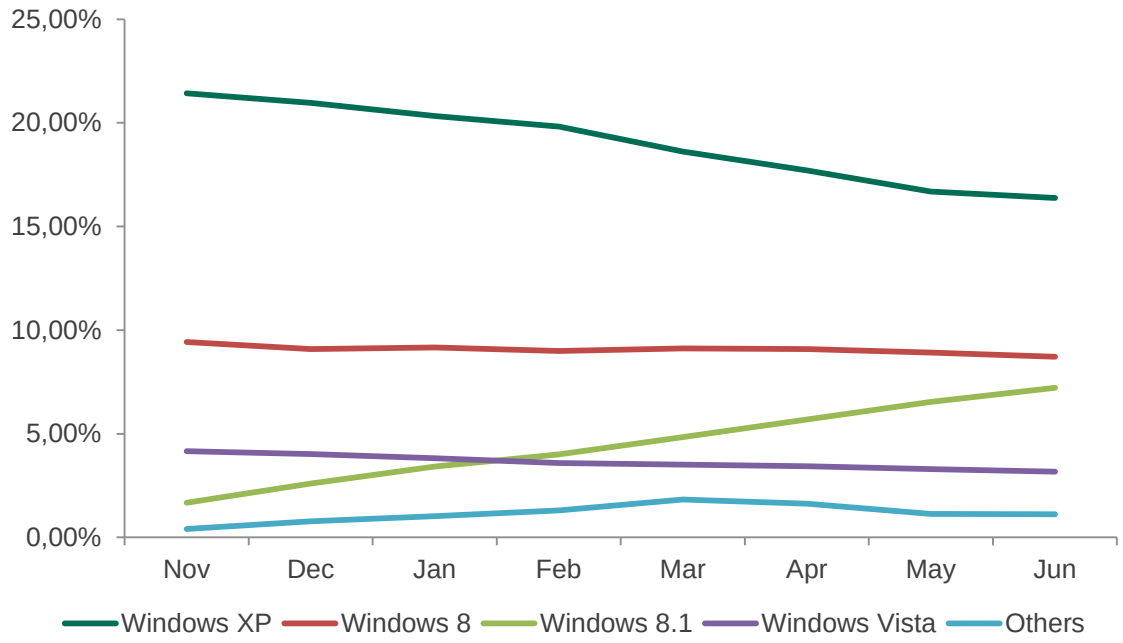


Рис. 4: Популярность различных версий Windows в период с ноября 2013 по май 2014 (без Windows 7)

Как видно, доля «древней» Windows XP наконец-то начала заметно снижаться – с 21,42% в ноябре 2013 года до 16,37% в июне 2014 года. Значительно менее заметно уменьшилась доля Windows Vista – с 4,16% в начале периода до 3,17% в его конце. Windows 8, несмотря на присутствие на рынке более свежей версии ОС, не желает сдавать позиции и держится на уровне 8-9%. Windows 8.1 на правах новичка заметно увеличивает свое присутствие с 1,67% в ноябре до 7,22% в июне.

Такова общая картина популярности версий Windows чуть больше чем за последние полгода. И хотя условно актуальными сейчас можно считать целых пять версий Windows (их использует абсолютное большинство пользователей Windows-продуктов

«Лаборатории Касперского»), в особый фокус этого исследования попадут две системы: самая новая Windows 8.1 и очень старая, но практически легендарная Windows XP. Динамике использования этих систем и будут посвящены следующие главы.

Windows 8.1: в целом медленно, но быстрее Windows 8

Итак, по итогам июня 2014 года, более чем полгода спустя после выпуска Windows 8.1, распределение версий ОС от Microsoft по популярности выглядит следующим образом.

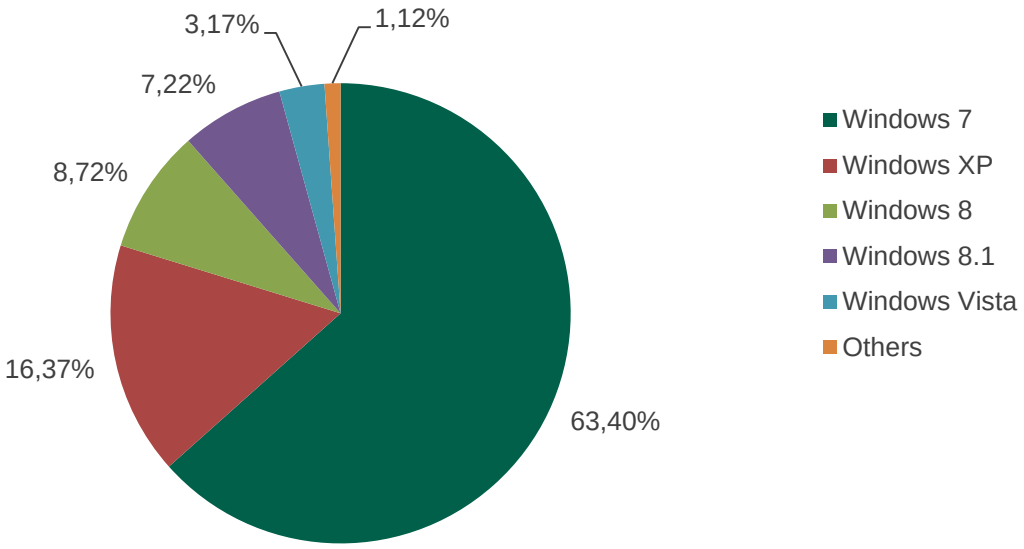


Рис 5.: Популярность Windows в июне 2014 г. (Здесь и далее данные из Kaspersky Security Network)

На Windows 8.1 приходится лишь 7,22% пользователей, на Windows 8 – 8,72%, в то время как абсолютное большинство пользователей (63,4%) все еще отдают предпочтение Windows 7.

Более чем полгода назад, через полтора месяца после запуска Windows 8.1, картина складывалась следующим образом:

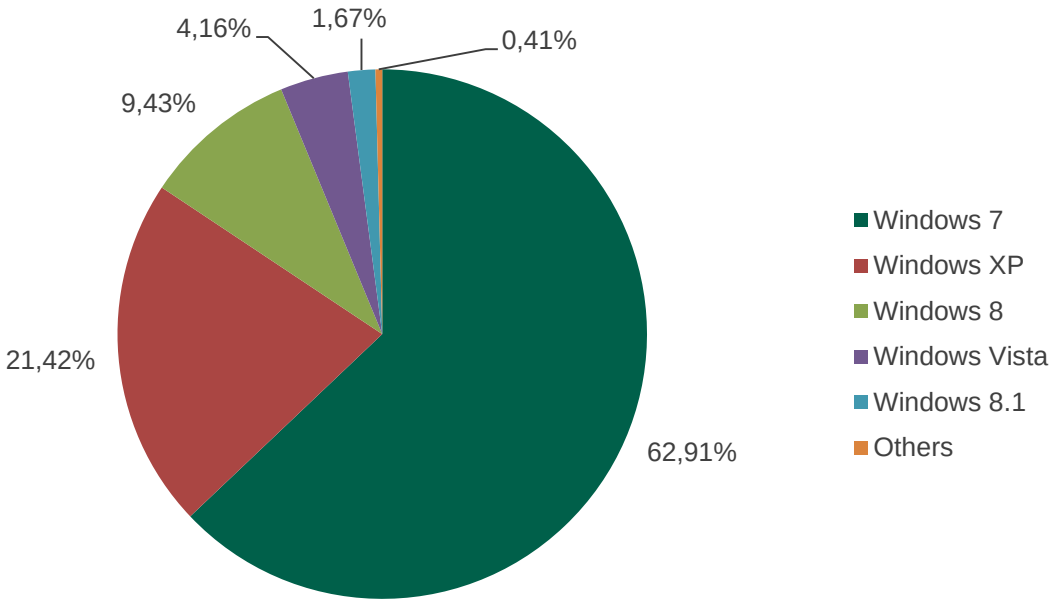


Рис. 6: Популярность Windows в ноябре 2013

Без малого за шесть недель с момента старта Windows 8.1 удалось набрать 1,67% пользователей. За шесть последующих месяцев Windows 8.1 набрала еще 5,55 процентных пункта. Для того чтобы понять, много это или нет, стоит посмотреть, как за тот же период годом ранее росло количество пользователей Windows 8.

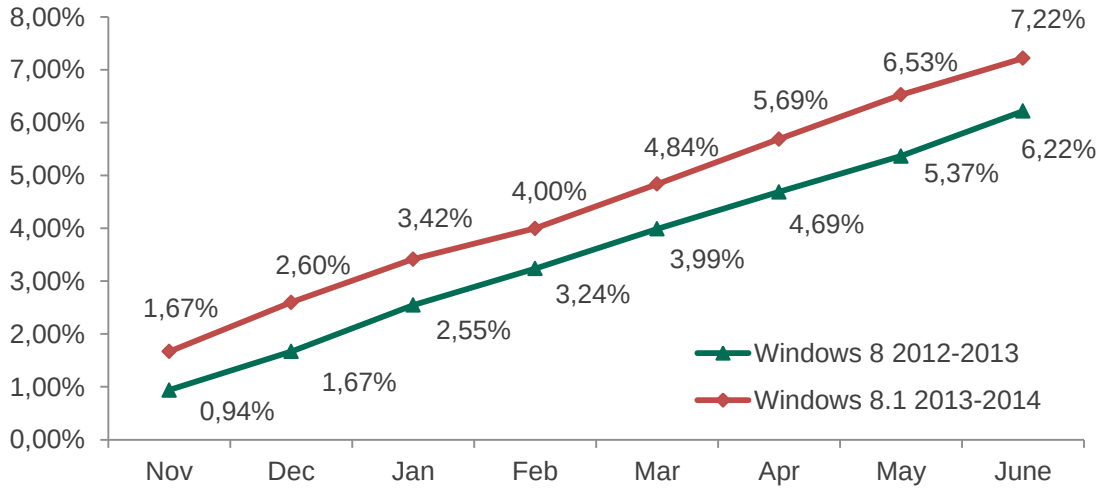


Рис. 7: Динамика увеличения доли Windows 8 vs. Windows 8.1 в общем объеме пользователей

Как видно на графике, Windows 8.1 продемонстрировала чуть более активную динамику, чем ее предшественница: ежемесячно эта система отвоевывала у «конкурентов» на 0,7-1 п.п. пользователей больше, чем Windows 8. В абсолютном выражении это преимущество вылилось в то, что Windows 8.1 понадобилось всего лишь 6 месяцев на то, чтобы набрать такое же количество пользователей, на которое у Windows 8 ушло восемь месяцев. Не исключено, что в дальнейшем прирост увеличится. По крайней мере, динамика увеличения количества пользователей Windows 8.1 в сравнении с динамикой снижения количества пользователей Windows 8 ясно демонстрирует уверенное сближение двух параметров. Если текущая скорость сохранится, количество пользователей двух систем сравняется уже осенью, в сентябре-октябре 2014 года.

И хотя в общем объеме пользователей доля Windows 8.1 все еще довольно мала, на отдельных территориях доля этой системы более значительна.

Windows 8.1: география лидеров

Чтобы понять, где доля пользователей Windows 8.1 самая большая, «Лаборатория Касперского» выявила страны с наибольшим абсолютным количеством пользователей этой системы, а потом провела анализ того, какую долю в общем числе пользователей Windows в стране занимают пользователи более новой системы.

Согласно этому методу, список стран с наибольшим числом пользователей продуктов «Лаборатории Касперского», работающих на компьютерах под Windows 8.1, по состоянию на июнь 2014 года выглядит следующим образом:

United States
Russian Federation
Germany
France
Brazil
United Kingdom
India
Mexico
Canada
Italy

Однако при вычислении доли, которую пользователи Windows 8.1 занимают в общем объеме пользователей Windows в стране, чарт выглядит совершенно иным образом.

United States	**16,2%**
Canada	**13,5%**
Germany	**11,1%**

United Kingdom	**10,8%**
France	**10,3%**
Mexico	**9,6%**
Brazil	**8,4%**
Italy	**8,1%**
Russian Federation	**5,1%**
India	**2,9%**

США, Канада, Германия, Великобритания и Франция – в лидерах по доле Windows 8.1. Эти четыре страны – единственные из первой десятки, где самая актуальная система набрала больше 10%. Значительно меньше своих соседей по Европе (8,1%) набрала Италия. В «середнячках» – Мексика и Бразилия. В аутсайдерах – Россия (5,14%) и Индия, набравшая меньше 3%.

Примечательно, что доля предыдущей версии системы - Windows 8 - на территориях стран - лидеров чарта не намного больше Windows 8.1: в США в июне она составляла 12,48%, в Канаде – 10,93%. В совокупности доля систем Windows 8.x в этих странах в июне составляет 28,75% и 24,45% соответственно, т. е. в обоих случаях – около четверти общего объема пользователей операционных систем Windows, «видимых» «Лаборатории Касперского» на конкретных рынках. В Германии совокупная доля Windows 8 и 8.1 в июне составляла 17,24%, в Великобритании – 17,91%. Для систем, существующих на рынке в совокупности чуть более полутора лет и имеющих такого сильного «конкурента», как проверенная и привычная Windows 7, результат как минимум неплохой, особенно в сравнении с общемировой долей двух ОС.

Таков портрет новейшей операционной системы Microsoft чуть больше чем через полгода после ее появления. Далее мы рассмотрим ситуацию еще с одной операционной системой, судьба которой была особенно интересна в последние полгода, – Windows XP.

Windows XP и ее поразительная живучесть

Операционная система Windows XP как коммерческий продукт стартовала более 12 лет назад, в 2001 году. Ее продажи в любом виде (как розничные, так и в виде предустановки на новые компьютеры) завершились к 2010 году. Примерно в то же время прекратилась стандартная техническая поддержка потребительских версий этой системы, а в апреле этого года – и расширенная поддержка. По признанию самой Microsoft, Windows XP оказалась наиболее долго живущей системой за всю историю компании.

Это вполне подтверждается данными «Лаборатории Касперского». В июне 2013 года на долю этой операционной системы приходилось 25,42% пользователей. Другими словами, еще год назад примерно каждый четвертый владелец Windows-компьютера в пользовался XP, а в июне 2012 года – более трети (35,64%) всех пользователей отдавали предпочтение этой системе, в июне 2011 года – 47,86%. В июне 2014 года доля таких пользователей сократилось до 16,37%.

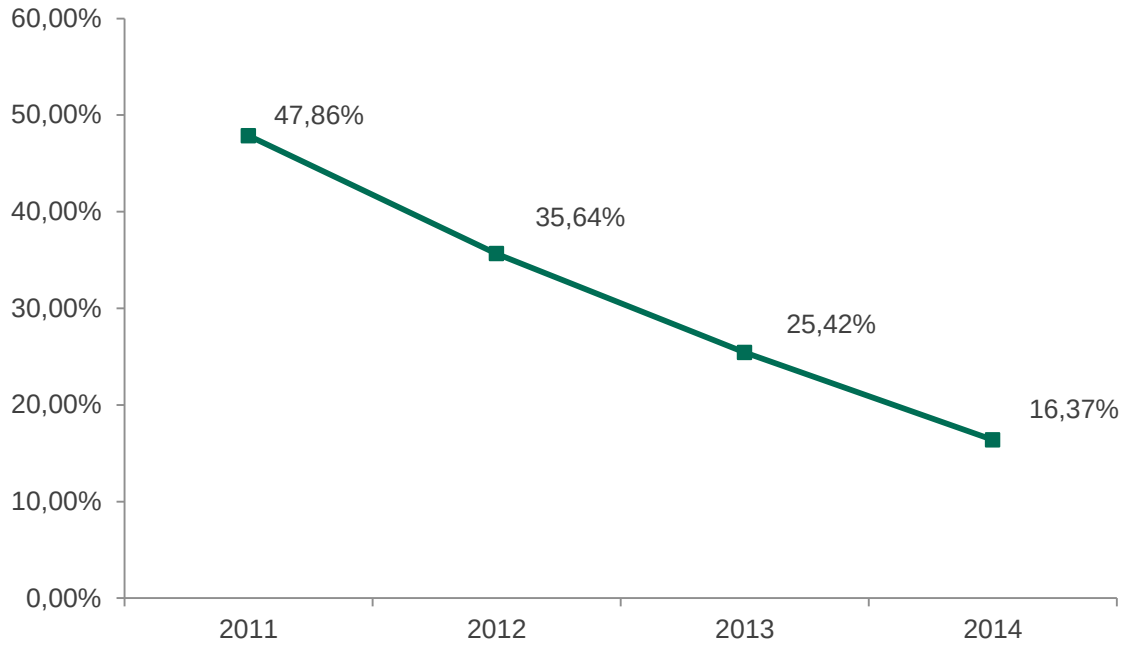


Рис. 8: Популярность XP с 2011 по 2014 годы

Как можно легко вычислить, в течение последних трех лет доля XP сокращалась со средней скоростью чуть более 10 процентных пунктов в год. При этом сокращение постоянно замедлялось. Так, если за 12 месяцев, прошедших с мая 2011 по май 2012 года доля этой система сократилась на 12,22% п.п., то по итогам аналогичного периода с июня 2012 по июнь-2013 года уменьшение составило уже 10,22 п.п. , а к концу июня 2014 года оно замедлилось до 9,05 п.п..

Несмотря на то, что стандартная поддержка и продажи системы закончились более чем за три года до мая 2014 года, доля пользователей этой ОС остается довольно значительной. При этом внешние события, которые могли бы ускорить уменьшение популярности этой системы (такие, как выпуск Windows 8.1 в октябре прошлого года или прекращение расширенной поддержки XP в апреле этого года), не слишком отразились на изменении доли пользователей XP (см. график ниже).

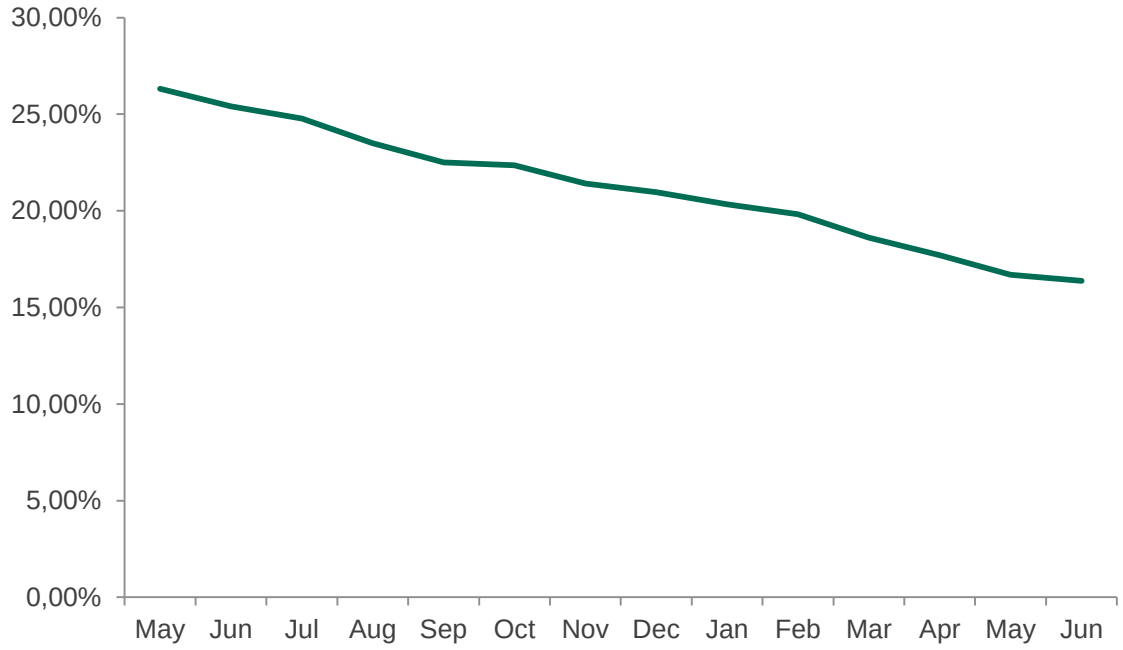


Рис. 9: Сокращение доли XP 2013-2014

При неизменной динамике к июню 2015 года доля пользователей этой системы уменьшится до 5-7%, а для условно полного исчезновения XP из списка наиболее популярных должно пройти еще около полугода.

Причины такой «упорности» XP очевидны: после череды не во всем удачных систем Windows 98, 2000 и Windows ME, операционная система XP, базирующаяся на ядре NT (в то время как семейство Windows 9x/ME базировалось на DOS) стала несомненной удачей благодаря своему быстродействию и сравнительной стабильности. Вышедшую в ноябре 2006 г. Windows Vista многие расценили как шаг назад, на эту систему обрушился шквал критики, и надежная и экономичная XP стала спасительной гаванью, в которую возвращались некоторые пользователи, познакомившиеся с Vista.

В результате к дебюту следующей системы Windows 7 в 2009 году, которая, к слову, сумела вернуть Microsoft репутацию производителя качественных и быстрых программных продуктов, сильно устаревшая уже даже к тому времени XP фактически стала синонимом «качественной операционной системы».

Не исключено, что именно столь позитивная репутация повлияла на неохотный переход пользователей XP на следующие версии ОС. Еще один фактор – неофициальные версии и сборки. С момента появления системы прошло достаточно времени, чтобы энтузиасты научились делать собственные вариации на тему XP. Таких модификаций только в базе Kaspersky Security Network более 160, из которых официальных версий, выпущенных Microsoft, лишь около десятка. Разумеется, большинство подобных сборок распространялись и распространяются бесплатно, и это еще один сильный фактор, обеспечивающий завидную живучесть XP.

И хотя время и конкуренция со стороны более современных родственных систем все же берут свое и глобальная доля XP неумолимо стремится к единицам процентов, в мире остается много стран, где эта система еще долго будет занимать значительную долю.

Windows XP: география лидеров

Если страны, где самый большой процент более новых и более современных версий операционных систем (Windows 8 и Windows 8.1) в общем объеме используемых ОС Windows, - это в основном страны Северной Америки и Европы, то в случае с XP картина совсем иная.

Как и с Windows 8.1, для того чтобы определить страны-лидеры, мы сначала отобрали страны с наибольшим абсолютным числом пользователей Windows XP, а затем – проанализировали, какую долю в этих странах занимает XP. В результате десятка стран с наибольшим числом пользователей XP выглядит следующим образом:

Russian Federation
Vietnam
India
Germany
Italy
United States
Algeria
China
France
Spain

В совокупности на 10 этих стран в июне приходилось более чем 65% всех пользователей продуктов «Лаборатории Касперского», использующих на XP. Рейтинг популярности XP в этих странах таков:

Vietnam	**38,8%**
China	**27,3%**
India	**26,8%**
Algeria	**24,2%**
Italy	**20,3%**
Spain	**19,2%**
Russian Federation	**17,4%**
France	**12%**
Germany	**8,5%**
United States	**4,5%**

Как видно, Вьетнам – в абсолютных лидерах с 38,79% пользователей, которые все еще предпочитают работать на Windows XP. Более четверти пользователей в Китае (27,35%) Индии (26,88%), и почти четверть (24,25%) в Алжире также предпочитают легендарную систему. На XP работает каждый пятый компьютер, защищенный продуктами «Лаборатории Касперского», находящийся в Италии (20,31%) и в Испании (19,26%). Меньше всего пользователей XP осталось в США – 4,52%. При этом почти 60% копий XP, все еще работающих в США, – это Windows XP Professional, версия системы для корпоративных пользователей.

Эта же версия системы доминирует и на территории лидера данного чарта – Вьетнама. Около 99,72% пользователей XP этой страны работают с версией Professional.

Использование устаревшей версии операционной системы чревато рисками, связанными с кибератаками, в которых задействованы эксплойты – специальные программы, использующие уязвимости в легальном программном обеспечении для заражения компьютера другим опасным вредоносным ПО. Об этом – в следующей части исследования.

Часть 2: Уязвимости и эксплойты

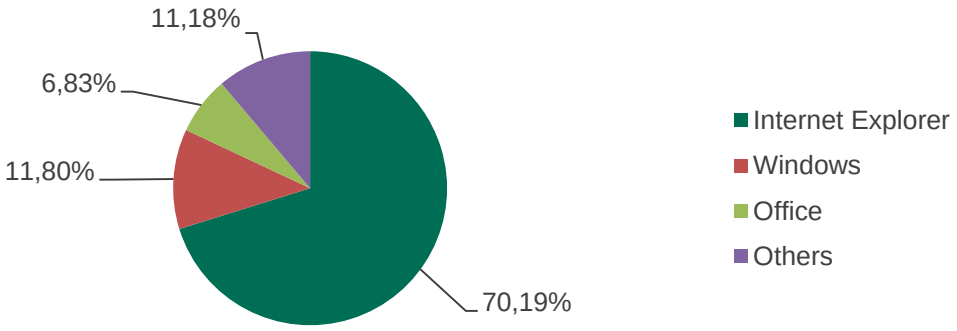
Эксплойты являются одним из самых эффективных инструментов для незаметной для пользователя доставки на компьютеры жертв «полезной нагрузки» - дополнительного вредоносного ПО с различными вредоносными функциями. Как показало прошлогоднее исследование «Лаборатории Касперского» Java under attack — the evolution of exploits in 2012-2013 , эксплойты под популярную программную среду Java занимают лидирующую позицию среди прочих. В том числе это обусловлено распространенностью данной платформы в мире (по официальным данным, ПО Java установлено на более чем 3 миллиарда устройств), а кроме того – обилием серьезных уязвимостей, обнаруженных за год.

Операционная система Windows вместе с офисным пакетом Microsoft Office, браузером Internet Explorer и некоторым другим ПО – один из немногих программных продуктов, сопоставимых с Java по охвату аудитории. Кроме того, в ПО от Microsoft регулярно находят уязвимости, что теоретически может указывать на то, что и среди киберпреступников эксплойты под Windows и другие продукты Microsoft пользуются популярностью.

Так ли это на самом деле станет ясно далее.

Уязвимости в продуктах Microsoft

По собственным данным «Лаборатории Касперского» и данным из открытых источников[3], за первые полгода 2014 года в 377 программных продуктах Microsoft была обнаружена 161 уязвимость. Из этого объема большая часть (113) уязвимостей пришлось на браузер Internet Explorer. На уязвимости в версиях ОС Windows[4] – 19 уязвимостей, на Office (включая Office Web App) – 11.



[3] Для исследования использовались данные с сайта http://www.cvedetails.com/ объединяющего всю доступную публично информацию об известных уязвимостях в популярном ПО
[4] Под уязвимостями в ОС в данном случае понимаются уязвимости в ядре и в реализации различных технологий, сервисов и протоколов, являющихся неотъемлемыми частями конкретных версий Windows;

Рис. 10: Уязвимости в продуктах Microsoft в первой половине 2014 года (данные CVE details)

Примечательно, что за аналогичный период 2013 года Internet Explorer набрал 55 уязвимостей, Windows – 66, а Office - всего 3.

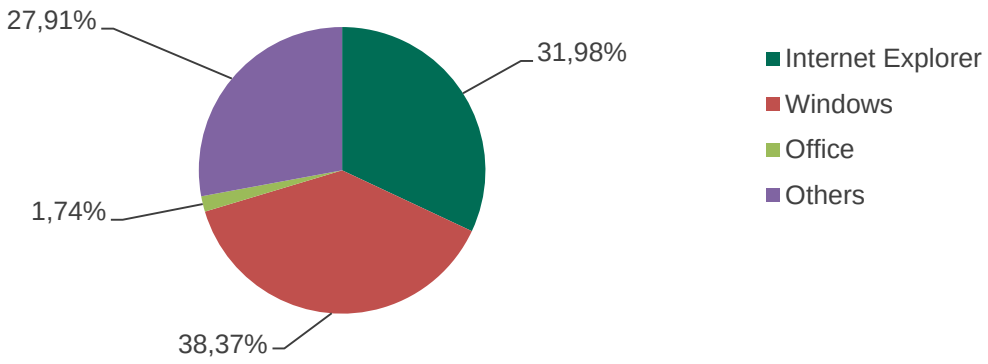


Рис. 11: Уязвимости в продуктах Microsoft в первой половине 2013 года

За год, как видно, изменилось многое. При примерно одинаковом совокупном количестве уязвимостей (172 в первой половине 2013 года, против 161 в первом полугодии 2014) распределение количества уязвимостей между ключевым продуктами Microsoft существенно изменилось. Так, более чем вдвое увеличилось количество уязвимостей в различных версиях браузера Internet Explorer, а количество уязвимостей в ОС и ее компонентах – наоборот, упало почти втрое. Это падение преимущественно произошло из-за Windows XP. Если год назад исследователи информационной безопасности активно тестировали систему и за первые 6 месяцев 2013 года обнаружили 46 уязвимостей, то за аналогичный период 2014 года – всего 6. Такое сокращение, впрочем, едва ли означает, что в Windows XP кончились уязвимости. Просто абсолютное большинство сообщений об уязвимостях в Windows и других продуктах Microsoft публикует сама Microsoft, а прекращение технической поддержки системы, в том числе означает и прекращение тестирований на безопасность.

Всего за все время существования этой ОС, в ней было обнаружено 727 различных уязвимостей. Это абсолютный рекорд среди операционных систем Microsoft. Для сравнения, в вышедшей через пять лет после XP системе Windows Vista к текущему моменту было обнаружено 467 уязвимостей, в Windows Server 2008 – 465, Windows 7 – 338, в Windows 8 – 78 уязвимостей, в Windows 8.1 – 22 уязвимости.

Впрочем, большое количество уязвимостей еще не говорит о том, что все они используются для атак . Злоумышленники создают эксплойты только либо под уязвимости, эксплуатация которых не требует специальных условий, либо под самые

опасные уязвимости, те, что позволяют исполнять на компьютере атакованного пользователя вредоносную нагрузку - как правило, вредоносное ПО для похищения конфиденциальных данных, денег и других нелегальных действий.

Эксплойты под уязвимости в Windows: далеко от лидеров

Всего с ноября 2013 по июнь 2014 годов «Лаборатории Касперского» зафиксировала 15,06 миллиона срабатываний защитных продуктов на идентифицированные эксплойты[5], зафиксированные на 3,64 миллионах компьютеров под управлением различных версий Windows. Ожидаемо большинство из этих срабатываний (52,85%) пришлось на эксплойты, написанные под программную среду Java. Эксплойты под различные продукты Microsoft (Office, WMA, Visio, Silverlight) распространены в гораздо меньшей степени: 1,67% срабатываний пришлось на вредоносные программы под эти продукты.

Хотя за исследуемый период системы детектирования «Лаборатории Касперского» точно идентифицировали использование эксплойтов под более чем 40 уязвимостей в продуктах Microsoft, основную «лепту» в количество атак внесли всего четыре из них.

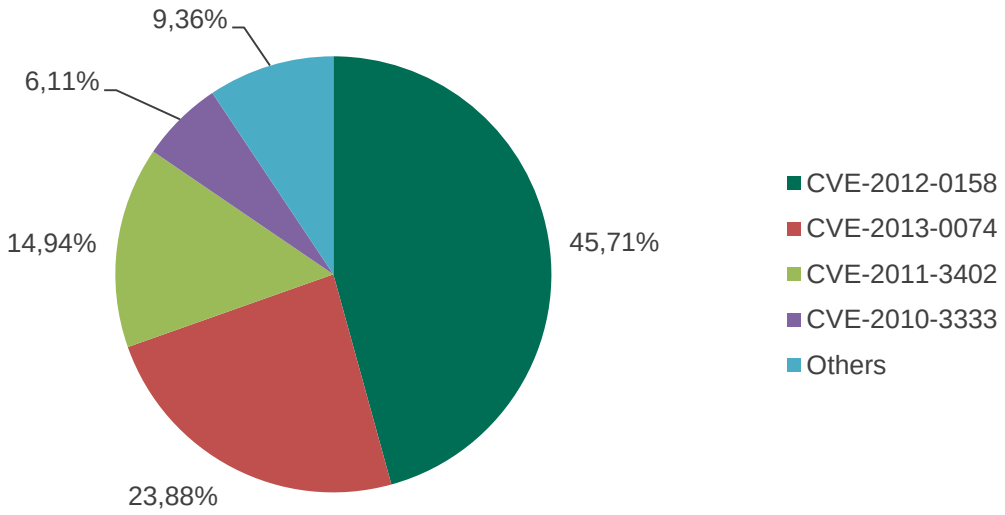


Рис. 12: Срабатывания продуктов «Лаборатории Касперского» на эксплойты под уязвимости в продуктах Microsoft в период с ноября 2013 года по июнь 2014 года

[5] Под идентифицированными эксплойтами в данном случае понимается эксплойты, при детектировании которых была идентифицирована программная платформа, под которую они были написаны. В силу технических особенностей, часть детектирований продуктами «Лаборатории Касперского» осуществляется с помощью общих эвристик. Такие эвристики покрывают различные типы эксплойтов, но не позволяют точно определить платформу, на которую нацелен эксплойт. Данные о таких срабатываниях в данном исследовании не учитывались.

Как видно на графике, подавляющее большинство срабатываний приходится на уязвимость в Microsoft Word CVE-2012-0158. Впервые о ней стало известно в октябре 2012 года, а в начале 2013 года эксперты «Лаборатории Касперского» сообщили, что эксплойт под эту уязвимость использовался операторами Red October. Позже эксплойт под эту уязвимость был замечен экспертами «Лаборатории Касперского» в еще одной кампании кибершпионажа – Nettraveller и многих других атаках. Кстати, 6,11% в общем количестве срабатываний на эксплойты под продукты Microsoft пришлось на CVE-2010-3333, еще одну довольно старую уязвимость в Word, которая использовалась в паре с CVE-2012-0158 и в Red October, и в Nettraveller.

Вторыми по популярности за исследуемый период стали эксплойты под уязвимость CVE-2013-0074, содержавшуюся в Microsoft Silverlight –приложении для отображения мультимедийного контента. Хотя технология, которую Microsoft позиционировала как собственного конкурента Adobe Flash, так и не обрела широкой распространенности, эксплойты под эту уязвимость использовались киберпреступниками. В частности, осенью 2013 года, более чем полгода спустя после того, как Microsoft выпустила обновление безопасности, закрывающую эту уязвимость, эксплойт под нее был обнаружен в составе эксплойт-пака Angler и использовался вплоть до конца исследуемого периода.

На третьем месте CVE-2011-3402 с 14,94% срабатываний – уязвимость в модуле обработки шрифтов TrueType, затрагивающая целый ряд версий Windows (от XP до Windows 7, включая Windows Server 2003/2008). Она была обнаружена в сентябре 2011 года. Вредоносные программы для ее эксплуатации, в том числе, использовались для распространения опасной шпионского троянца Duqu, который, среди прочего, имеет «родственные» связи с печально известным червем Stuxnet. Он, кстати, тесно связан с пятой уязвимостью, с эксплойтами для которой, часто сталкиваются пользователи продуктов «Лаборатории Касперского».

Эхо Stuxnet

Летом 2010 года стало известно о существовании Stuxnet, компьютерного червя, который – как выяснилось впоследствии – был создан специально для саботажа процесса обогащения урана на нескольких предприятиях в Иране. Stuxnet стал настоящей бомбой, продемонстрировавшей, на что способно вредоносное ПО, если предельно сузить его цели и тщательно подготовиться. Для распространения червь использовал эксплойт под уязвимость CVE-2010-2568. Она представляет собой ошибку в обработке ярлыков в ОС Windows, позволяющая загружать произвольную динамическую библиотеку без ведома пользователей. Уязвимость затронула системы Windows XP, Vista, 7, а также Windows Server 2003 и 2008.

Впервые вредоносные программы, эксплуатирующие эту уязвимость, были замечены в июле 2010 года. В частности, червь Sality использовал ее для распространения собственного кода: червь генерирует уязвимые ярлыки и распространяет их в локальной сети. Стоит пользователю открыть папку, содержащую такой ярлык, как тут

же начнется запуск зловредной программы. После Sality и Stuxnet эту же уязвимость использовали известные шпионские программы Flame и Gauss

Microsoft выпустила обновление безопасности, закрывающее эту уязвимость еще осенью 2010 года. Не смотря на это, системы детектирования «Лаборатории Касперского» до сих пор регистрируют десятки миллионов срабатываний на эксплойты, использующие CVE-2010-2568. Если конкретно, то за исследуемый период было зафиксировано более 50 миллионов срабатываний на более чем 19 миллионах компьютеров по всему миру.

Намеренно мы не стали учитывать статистику этих срабатываний, поскольку из-за особенностей использования этой уязвимости, невозможно точно определить, в каких случаях продукты «Лаборатории Касперского» защищали от реальных атак с помощью эксплойтов под CVE-2010-2568, а в каких – просто детектировали автоматически созданные тем или иным червем уязвимые ярлыки.

Тем не менее, статистика KSN все же позволяет сделать некоторые выводы. К примеру, на следующем графике видна динамика срабатываний продуктов «Лаборатории Касперского» на эксплойты под уязвимость CVE-2010-2568 и вирус Sality.

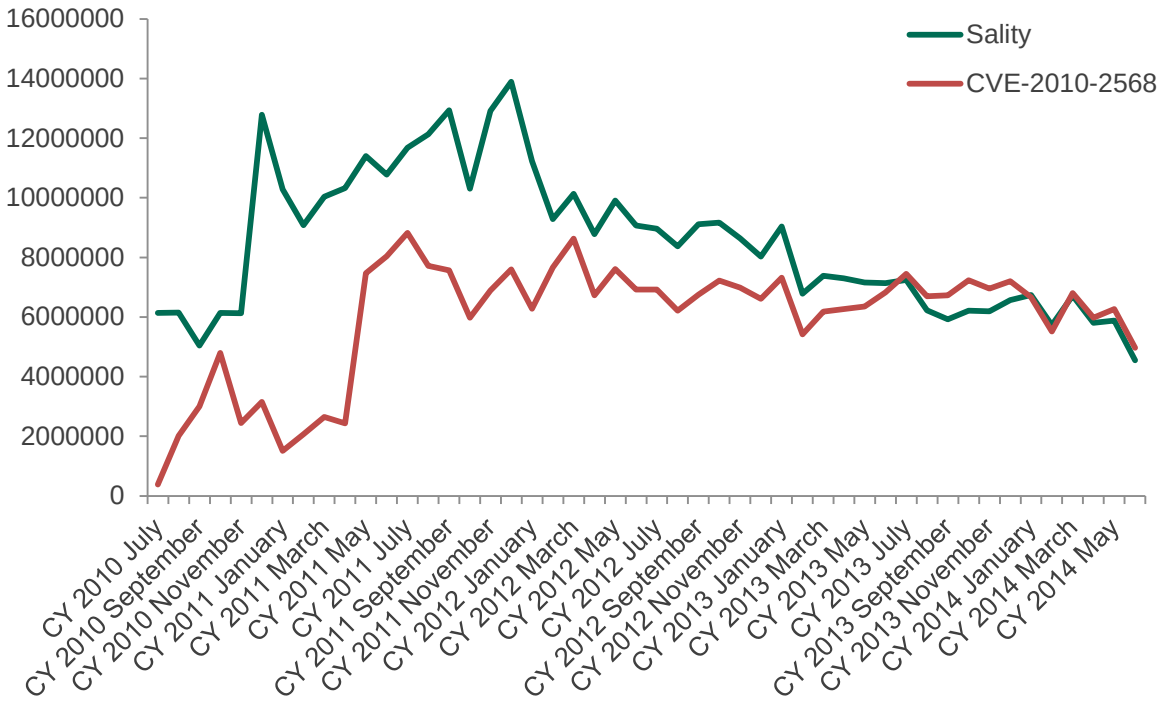


Рис. 13: Срабатывания продуктов «Лаборатории Касперского» на червь Sality в соотношении со срабатываниями на эксплойты под уязвимость CVE-2010-2568

Как видно на графике, «дружба» двух вредоносных программ продолжается уже много лет. Сокращение между количеством срабатываний на два семейства вредоносных программ объясняется, прежде всего, сокращением количества модификаций Sality. Очевидно, что с января 2014 года количество срабатываний на Sality и на CVE-2010-2568 практически синхронизировались – свидетельство того, что активными в этот период остались лишь версии, работающие в паре с CVE-2010-2568. В то время как ранее широкое распространение имело множество других версий зловреда.

Весьма красноречиво и распределение операционных систем компьютеров, на которых были зафиксированы срабатывания на эксплойт под LNK-уязвимость. Львиная доля срабатываний (64,19%) за последние восемь месяцев пришлось на XP и только 27,99% - на Windows 7. Продукты «Лаборатории Касперского», защищающие серверные операционные системы Windows Server 2003 и 2008 также регулярно рапортуют об обнаружении подобных эксплойтов – 1,58% и 3,99% срабатываний соответственно. Большое количество срабатываний, приходящих от пользователей XP свидетельствует о том, что на большинстве этих компьютеров либо не установлено защитное решение, либо используется уязвимая версия Windows, либо сочетаются два фактора. Срабатывания, приходящие от серверных систем – это свидетельство наличия вредоносных ярлыков, эксплуатирующих уязвимость CVE-2010-2568, на сетевых папках с открытым доступом.

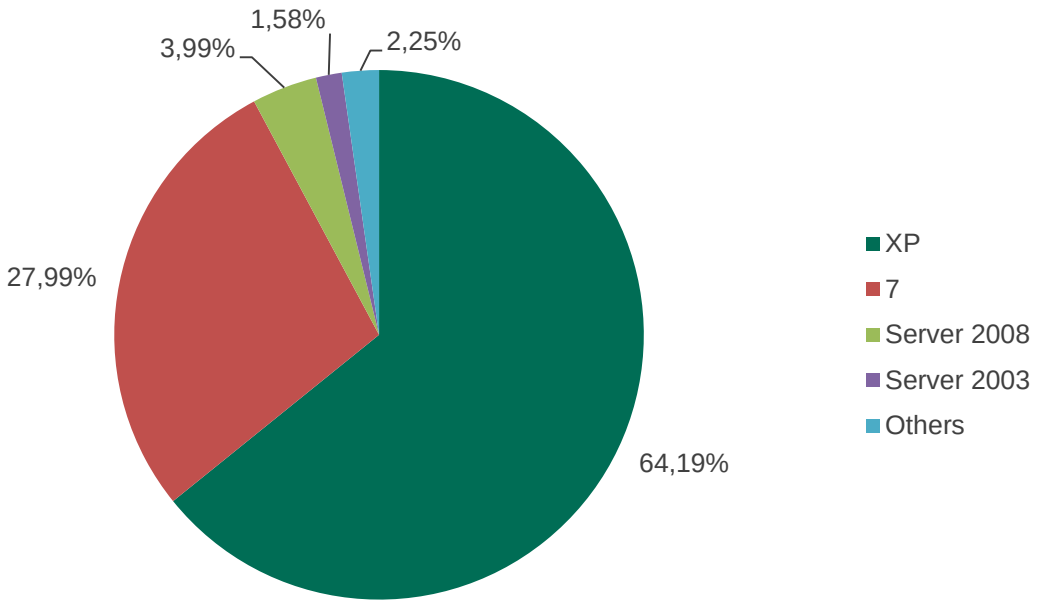


Рис. 14: Распределение операционных систем компьютеров, на которых были зарегистрированы срабатывания продуктов «Лаборатории Касперского» на эксплойты под уязвимость CVE-2010-2568 в период с ноября 2013 года по июнь 2014 года.

Интересно и географическое распределение всех зафиксированных срабатываний на CVE-2010-2568.

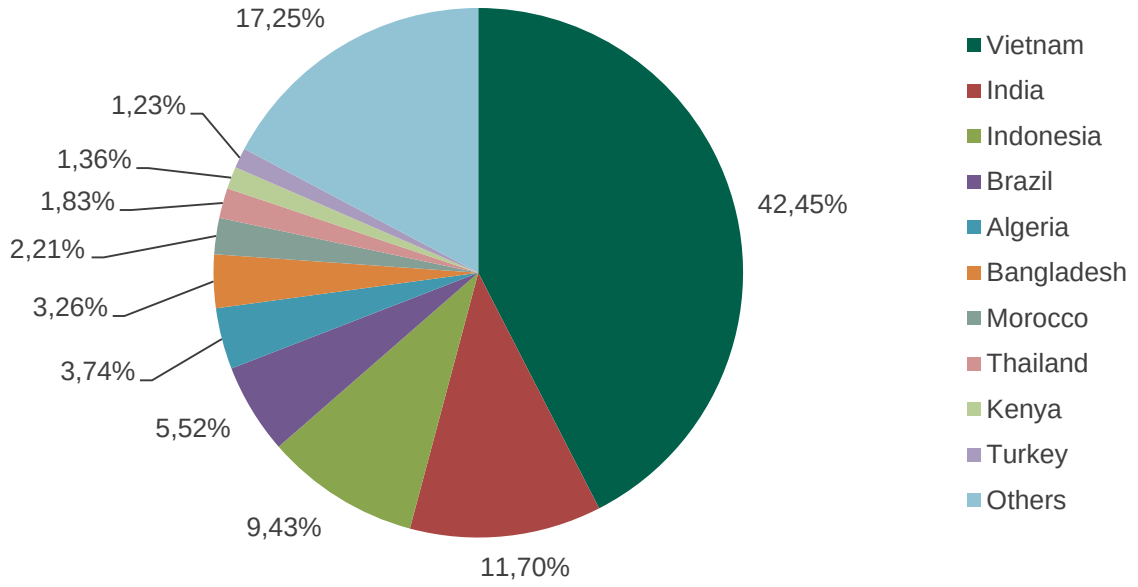


Рис. 15: Географическое распределение срабатываний продуктов «Лаборатории Касперского» на эксплойты под уязвимость CVE-2010-2568 в период с ноября 2013 года по июнь 2014 года.

Как видно, Вьетнам (42,45%) Индия (11,7%) и Алжир (5,52%) не только в числе лидеров по проценту использования устаревшей XP, но также и в топе по числу срабатываний защитных продуктов «Лаборатории Касперского» на одну из самых опасных уязвимостей в Windows из известных на сегодняшний день.

Отдельно стоит оговориться, что все эти цифры отнюдь не являются свидетельствами того, что пользователи стран, где чаще всего регистрируются срабатывания на CVE-2010-2568, сплошь используют уязвимые версии Windows. По техническим причинам в KSN нет возможности точно определить, на каких компьютерах какие обновления безопасности установлены, однако косвенные признаки, такие, как география срабатываний и распределение операционных систем, все же позволяют определить пользователям каких стран следует задуматься о безопасности своих компьютеров, прежде всего. Киберпреступники, как правило, расчетливы и не совершают действий, которые не возымеют эффект. Возможно, именно поэтому страны с небольшой долей компьютеров под управлением XP, такие как США, Германия, Великобритания, Канада и др., отсутствуют в чартах, демонстрирующих распространение эксплойтов под CVE-2010-2568 – просто потому, что использование этой уязвимости для распространения вредоносного ПО в сетях данных государств не будет эффективным.

Заключение и рекомендации

Один из основных выводов исследования: почти 13 лет спустя после запуска, Windows XP все еще работает на компьютерах значительного числа пользователей по всему миру, и это очевидно является большой угрозой безопасности пользователей.

Второй важный вывод – хотя эксплойты под Windows и другие популярные продукты Microsoft и не имеют широкого распространения (за исключением LNK-уязвимости CVE-2010-2568) в сравнении, например, с эксплойтами под уязвимости в Java, они, однако, представляют большую опасность – реальные примеры использования уязвимостей в Windows и Microsoft Office в рамках сложных кампаний кибершпионажа – тому подтверждение.

Третий вывод заключается в том, что когда речь заходит об уязвимостях в Windows и других продуктах Microsoft, злоумышленники не слишком стремятся «идти в ногу со временем» и создавать эксплойты под сравнительно новые уязвимости. Возможно, это происходит потому, что в ситуациях, когда они могут пригодиться, атакующим вполне хватает старых уязвимостей – большое число компьютеров с устаревшим ПО от Microsoft исправно льет воду на мельницу эффективности эксплойтов под давно известные уязвимости.

Чтобы избежать возможных инцидентов информационной безопасности, связанных с не обновленным ПО Microsoft и их последствий эксперты «Лаборатории Касперского» дают следующие советы:

Для пользователей домашних ПК:

- Используйте наиболее свежие версии операционной системы Windows и следите за сообщениями о появлении обновлений безопасности для нее и прочих продуктов Microsoft.
- К сожалению, даже сознательный пользователь не застрахован от ситуации, когда уязвимость существует, а исправление для нее – еще нет. Поэтому для обеспечения максимально возможного уровня защиты своих цифровых ценностей, используйте защитное решение, оснащенное технологиями для противодействия атакам с помощью эксплойтов.

Для корпоративных пользователей:

- Отраженная в последней части этого исследования ситуация с распространенностью эксплойтов LNK-уязвимость в Windows – это иллюстрация того факта, что администраторы многих сетей, в том числе корпоративных, не уделяют должного внимания находящимся в их управлении публичным серверам, в результате чего вредоносное ПО, такое, как Sality, годами самовоспроизводится в локальных сетях, угрожая пользователям, осуществляющим к ним доступ. Если в корпорации существуют ни чем не защищенные рабочие станции, работающие под управлением уязвимой версии

Windows, они могут стать входной точкой для организатора целевой атаки. Поэтому «Лаборатория Касперского» призывает компании тщательно следить за актуальностью ПО на корпоративных серверах и рабочих станций и не экономить на их защите от вредоносных атак

- В ситуации, когда переход на наиболее свежую версию операционной системы не возможен по техническим соображениям, необходимо использовать надежное защитное решение, оснащенное средствами для предотвращения атак с помощью эксплойтов, а кроме того – для поиска и оперативного устранения уязвимостей в корпоративном ПО.