Итоги 2013: угрозы и эксплуатация Windows

Мировой ландшафт угроз становится насыщеннее и активнее с каждым годом, каждый день появляется множество модификаций вредоносных программ, а также новые вредоносные программы и иные инструменты для кибератак. Ушедший год только закрепил основной тренд разделения вредоносных программ на два вида: используемые злоумышленниками для извлечения личной материальной выгоды и используемые для направленных атак, watering hole с целью компрометации определенной компании, отрасли индустрии или региона земного шара.

Несмотря на то, что Remote Code Execution уязвимости в популярном ПО (браузерах) играют существенную роль для удаленной доставки вредоносного контента, в котором заинтересованы атакующие (основной тренд drive-by), они часто прибегают к гораздо более простым методам установки вредоносных объектов в систему, используя человеческий фактор. Использование двойных расширений файлов, убедительное фишинговое сообщение, нацеленность на определенных людей (с учетом проведенной разведки), поддельные иконки файлов, документы с убедительным содержанием – все это составляет арсенал атакующих, которые заинтересованы в установке вредоносного кода в систему предполагаемой жертвы.

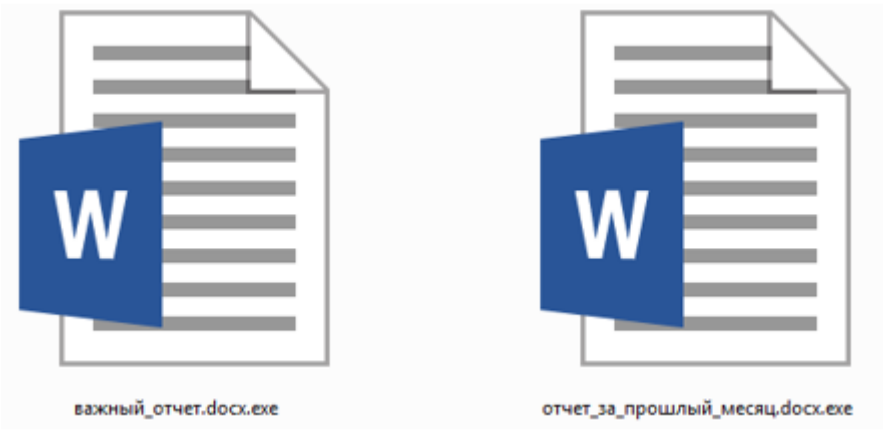


Рис. Типичный пример использования двойного расширения в имени файла с вставленной в исполняемый файл иконкой документа MS Word. Надежный способ ввести жертву в заблуждение, поскольку в настройках по умолчанию Windows Explorer скрывает расширение известных ему файлов

Как показал опыт злоумышленников из группы APT1 и иных групп атакующих, которые занимались промышленным шпионажем, первоначально необходимо провести минимальную разведку для идентификации предполагаемой жертвы и получения информации о ней, например e-mail-адрес. В дальнейшем, на этот адрес будет выслано убедительное фишинговое сообщение.

Date: Tue, 22 Dec 2013 09:05:40

From: Company Manager <cmanager@gmail.com>

Subject: Information for Press-Release

<text>

Company Manager

Рис. Пример фишингового сообщения, которое может быть отправлено на корпоративный почтовый ящик пользователя, с целью компрометации корпоративной информации. Первое, что бросается в глаза, это использование менеджером компании почтового аккаунта gmail вместо корпоративного

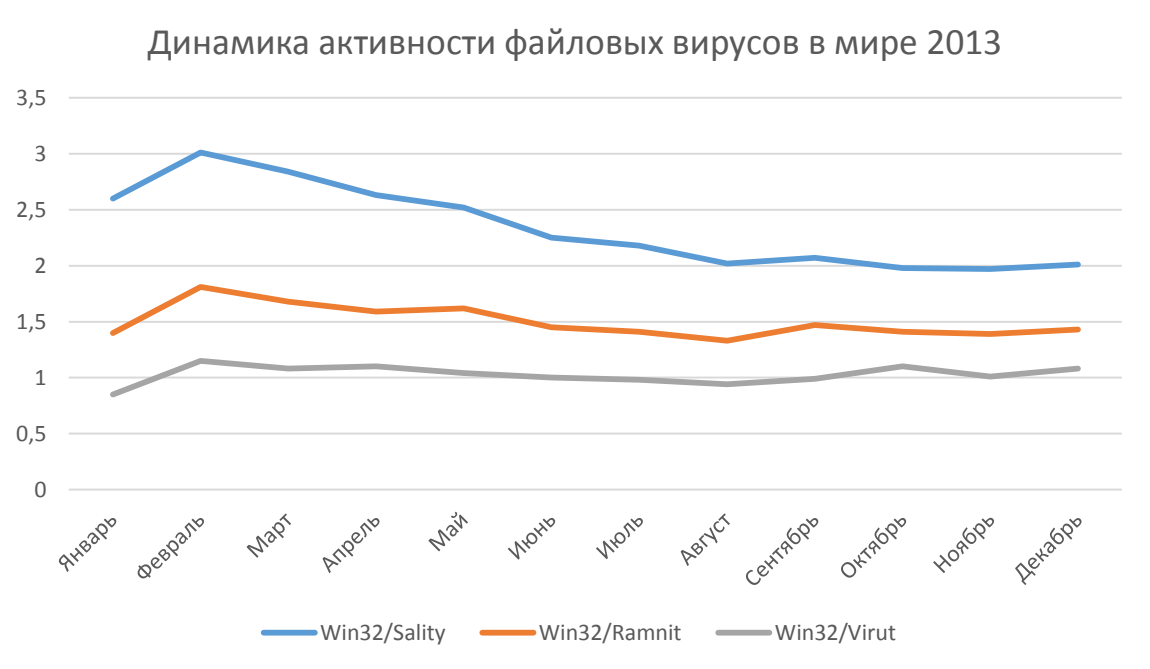
Подобный вид атаки может использоваться не только для промышленного шпионажа, но и в более локальных атаках на конкретную компанию, например, с целью получения у конкурентов важной информации с использованием вредоносного кода.

Угрозы Windows

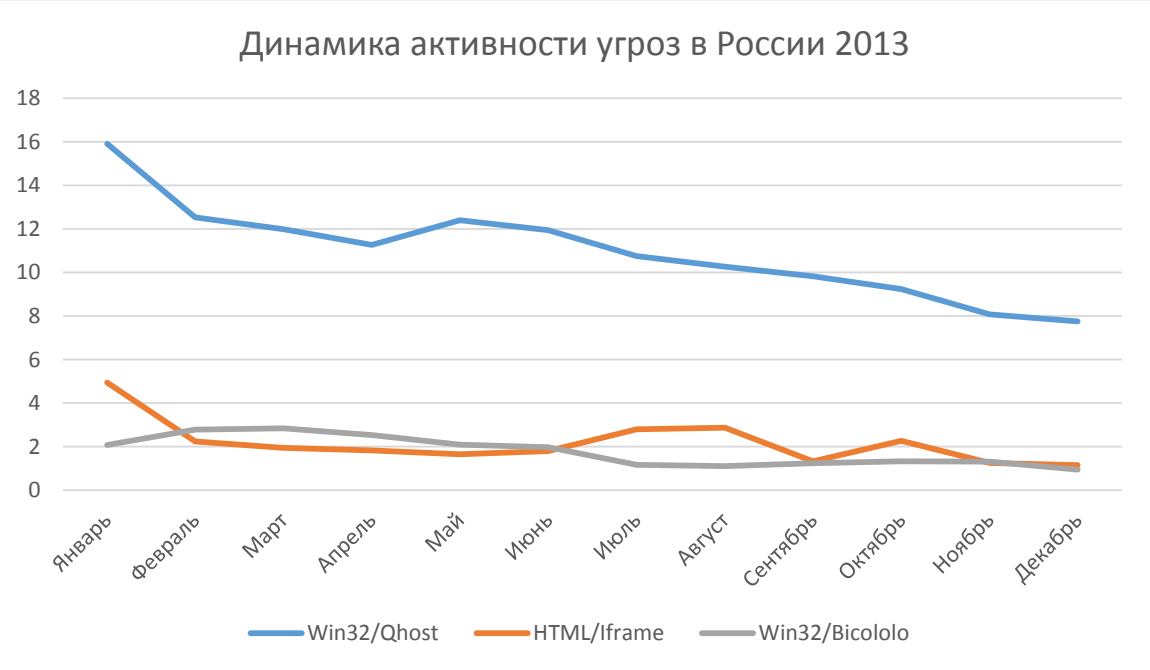
Нельзя сказать, что ушедший год принес для Windows что-то принципиально новое. Включение компьютера в ботнет, кража данных аккаунтов и данных онлайн-банкинга, получение удаленного доступа к компьютеру (бэкдор), блокирование компьютера с целью получения выкупа (вымогатель) являются основными целями киберпреступников, которые заинтересованы в извлечении материальной выгоды от скомпрометированных пользователей. Ниже мы приводим статистику по некоторым семействам вредоносного кода, которые были активны в прошедшем году.

Файловые вирусы все еще весьма активны. В этом году три семейства **Win32/Sality**, **Win32/Ramnit** и **Win32/Virut** стабильно попадали в десятку угроз по миру согласно

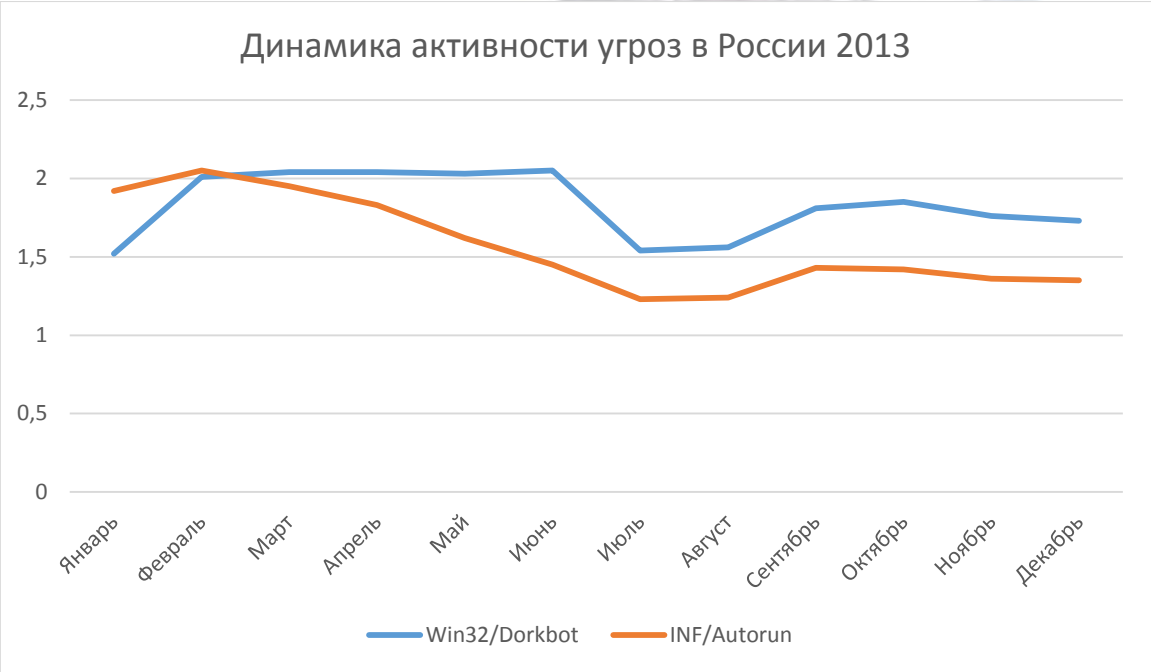
статистике нашей системы телеметрии ESET Live Grid. Вирусы подвергают компрометации исполняемые файлы на компьютере пользователя и нарушают их целостность, а также могут ставить под угрозу целую сеть предприятия, если на одном из компьютеров присутствует хотя бы один вредоносный файл, поскольку умеют заражать сетевые диски других компьютеров в сети.



Для России наиболее актуальной вредоносной программой является **Win32/Qhost**, кроме этого она сама по себе, в первую очередь, ориентирована на российских пользователей (см. географию распространения ниже), что явно намекает на ее отечественные корни. Сам код Qhost является довольно простым и выполняет модификацию системного hosts-файла для перенаправления пользователя на необходимые злоумышленникам фишинговые, рекламные и вредоносные ресурсы. Подобные перенаправления (клики) в последующем монетизируются и приносят злоумышленникам фактическую прибыль.



Общее обнаружение **HTML\IFrame** используется для идентификации вредоносных элементов веб-страниц. Часто вредоносные IFrame используются для перенаправления пользователя с легитимной веб-страницы на вредоносный контент или набор эксплойтов.



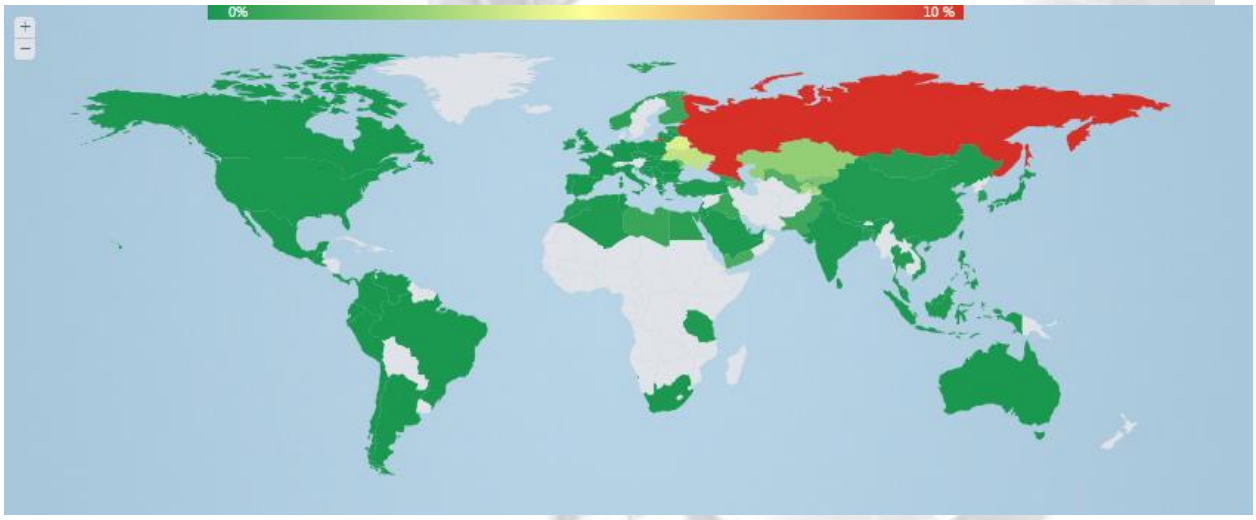


Рис. География распространения Qhost. Россия является наиболее пораженным регионом

Как видно на диаграмме выше, в России (и в мире) все еще высока активность вредоносных программ, которые используют INF-файлы для обеспечения своего запуска как со съемных носителей, так и локально в системе. Антивирусные продукты ESET обнаруживают эти вредоносные файлы под общим семейством INF/Autorun. Такой механизм автозапуска особенно актуален для устаревших ОС, поскольку они имеют по умолчанию включенный механизм автозапуска со съемных носителей через Autorun-файлы. Более подробно об отключении автозапуска с использованием файлов Autorun на таких ОС см. KB967715.

В таблице ниже приведены уязвимости (0day на момент эксплуатации), с помощью которых злоумышленники доставляли вредоносный код. Ушедший 2013 год по праву можно назвать годом направленных атак и атак watering hole, для многих из них

злоумышленники специально осуществляли поиск той или иной уязвимости и использовали ее эксклюзивно для атаки на конкретный регион или конкретную компанию. В частности, watering hole использовался для компрометации веб-сайтов, которые активно посещались предполагаемыми жертвами в различных регионах мира. Мы полагаем, что в 2014 году такой тренд получит еще большее распространение.

Уязвимость in-the-wild	Обнаружение	Месяц (добавлен/обнаружение эксплуатации)	Направленная атака*
CVE-2013-0422	Java/Exploit.CVE-2013-0422	Январь	Нет (Java 0day через наборы эксплойтов)
CVE-2013-0640	JS/Exploit.Pdfka.QCV	Февраль	Да (Adobe Reader & Acrobat 0day)
CVE-2013-1347	JS/Exploit.CVE-2013-1347	Май	Watering hole (см. ниже)
CVE-2013-3660	Win32/Exploit.CVE-2013-3660	Июнь	Нет (см. ниже)
CVE-2013-3163	SWF/Exploit.CVE-2013-3163	Июль	-
CVE-2013-3893	Win32/Exploit.CVE-2013-3893	Сентябрь	DeputyDog (см. ниже)
CVE-2013-3897	Win32/Exploit.CVE-2013-3897	Октябрь	Да (см. ниже)
CVE-2013-3918	Win32/Exploit.CVE-2013-3918	Ноябрь	Watering hole (см. ниже)
CVE-2013-5065	PDF/Exploit.CVE-2013-5065	Ноябрь	-
CVE-2013-3906	Win32/Exploit.CVE-2013-3906	Ноябрь	Да

(*) – первоначальное обнаружение эксплойта в направленной атаке или watering hole, прочерк – нет данных

В этом году мы неоднократно писали про атаки на популярные мессенжеры мгновенных сообщений типа Skype и Gtalk, а также социальные сети, например, Facebook или Vkontakte. Не будем повторяться, а только отметим, что атакующие используют преимущество убедительных фишинговых сообщений, якобы доверенные домены, в которых присутствует описка на несколько букв и сервисы сокращения ссылок для заманивания пользователей к переходу по вредоносной ссылке. Для организации масштабной спам-рассылки злоумышленникам нужно создать вспомогательные поддельные аккаунты в том или ином сервисе, использовать для рассылки сообщений аккаунты пользователей с пониженными настройками безопасности, а также вредоносный код с возможностью инъекции своего кода в мессенжеры (**Win32/Rodpicom.C**). Поскольку количество пользователей всех этих сервисов только увеличивается, мы полагаем, что можно ожидать подобного рода атак и в будем году.

Тренды для Windows

- Злоумышленники все чаще прибегают к использованию возможностей анонимной сети Tor для работы с удаленными C&C-серверами. В этом году появилось несколько новых угроз с такими возможностями. Например, **Win32/Atrax.A**, **Win32/Agent.PTA**, **Win32/Napolar**. Использование Tor позволяет злоумышленника быть более незаметными, поскольку позволяет скрывать информацию о C&C (IP-адрес или домен). Это особенно полезно для сокрытия информации от систем анализа трафика, которые собирают информацию о входящем/исходящем трафике в сети того или иного предприятия. Через такие логи служба безопасности может быстро обнаружить истинный вредоносный URL.
- Использование распределенной архитектуры в вымогателях-шифровальщиках. На примере Cryptolocker (**Win32/Filecoder.BQ**) стало очевидно, что если использовать

алгоритм шифрования с открытым ключом типа RSA для файлов (для шифрования ключа симметричного алгоритма, которым зашифрованы файлы), то у пользователя не будет другой возможности как платить злоумышленникам за выкуп, либо потерять свои файлы. В декабре мы сообщали об обнаружении его новой модификации, которая называется «Cryptolocker 2.0» (**MSIL/Filecoder.D**, **MSIL/Filecoder.E**), см. таблицу ниже. Кроме этого, в начале этого года появилась информация о новом шифровальщике, который использует схожий подход и называется Prison Locker (Power Locker), об этом сообщили в блоге malwaremustdie.

- Наиболее востребованным вредоносным кодом у злоумышленников являются инструменты, которые используются для похищения различной конфиденциальной информации аккаунтов онлайн-сервисов, а также информации онлайн-банкинга. Мы называем подобные вредоносные программы инструментами, поскольку они содержат в себе несколько компонентов, например, мобильный, который используется для обхода двухфакторной аутентификации в виде кодов подтверждения SMS (mTAN). Такие инструменты являются профессиональным средством похищения денежных средств у пользователей. К ним относятся, например, **Win32/Qadars** и **Win32/Spy.Hesperbot**.
- Сложные вредоносные программы как способ извлечения большой прибыли. Пример печально известного семейства ZeroAccess (**Win32/Sirefef**, **Win64/Sirefef**) показывает, что скрывая свой код глубоко в системе, применяя нестандартные подходы к заражению файлов и ориентирование на платформу x64, которая все больше вытесняет x32, позволяет добиться извлечения максимально возможной материальной выгоды для злоумышленников. По подсчетам Microsoft Digital Crimes Unit, которые занимались получением контроля над этим ботнетом, ZeroAccess заражены около 2 млн. компьютеров с предполагаемой ежемесячной прибылью злоумышленников $2,7 млн.
- 64-битные угрозы. В этом году была обнаружена модификация широко известного файлового вируса Expiro, которая умеет заражать 64-битные файлы (**Win64/Expiro.A** и **Win64/Expiro.B**). Win64/Expiro обладает переносимым кроссплатформенным телом (x32-x64) и способен заражать как 32-битные так и 64-битные файлы. Кроме этого, многие вредоносные программы уже имеют в своем составе 64-битную полезную нагрузку. Очевидно, что киберпреступники руководствуются весьма практическими целями, поскольку 64-битных ОС в мире становится все больше.

Более подробная информация об обнаруженных модификациях Cryptolocker приведена ниже в таблице.

Свойство	Cryptolocker	Cryptolocker 2.0
Обнаружение ESET	Win32/Filecoder.BQ	MSIL/Filecoder.D, MSIL/Filecoder.E
Язык программирования	C++	C#
Оплата через	Moneypak, Ukash, cashU, Bitcoin	Bitcoin
Алгоритм шифрования файла	AES	3DES
Алгоритм шифрования ключа	RSA-2048	RSA-1024
Зашифрованный ключ хранится в	Конец зашифрованного файла	Отдельный файл %filename%.%fileext%.k
Шифрование при работе с C&C	RSA	AES
Адреса C&C	Hardcoded, DGA	Hardcoded

Мобильные угрозы – главный тренд уходящего года

В нашем прошлогоднем отчете, который назывался «Обзор основных угроз и тенденций 2012 года» ESET указывала на стремительное распространение вредоносного ПО для Android. Например, в 2012 г. по сравнению с 2011 количество обнаруживаемых нами вредоносных объектов выросло в 17 раз. Мы также прогнозировали стремительный рост новых угроз в 2013 г. Подобное предсказание действительно оправдалось и в этом году мы зафиксировали появление большого количества вредоносных программ для этой платформы.

Не секрет, что Android является самой распространенной платформой для мобильных устройств. Статистика, приводимая Gartner за вторую четверть 2013-го года показывает, что Android еще больше укрепил свои позиции на рынке мобильных устройств почти достигнув отметки 80%.

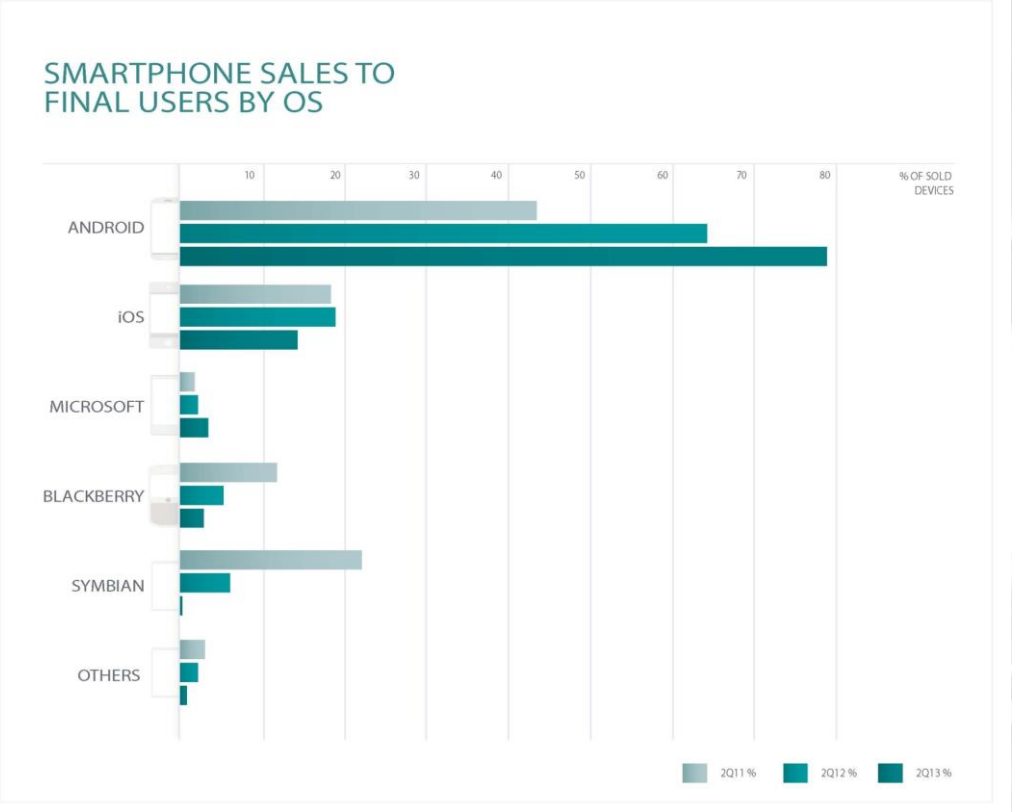
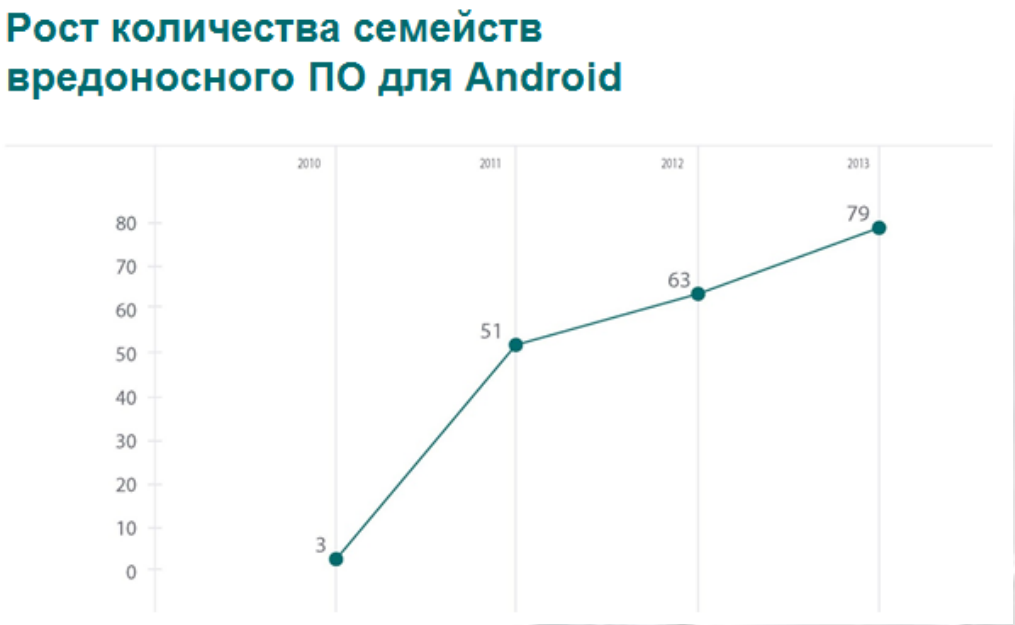


Рис. Процентное соотношение мобильных ОС, проданных с соответствующими устройствами во втором квартале 2011, 2012 и 2013 гг. (данные Gartner)

Что касается относительно новых мобильных платформ компании Microsoft – Windows RT (основана на Windows 8, напр., Surface 2) и Windows Phone 8 (основана на Windows NT/Windows 8, напр., Nokia Lumia), которые используются на ряде смартфонов и их флагманском планшете Surface, то злоумышленникам, пожалуй, нет смысла создавать такой узкоспециализированный вредоносный код, при том что рынок устройств под управлением этих ОС весьма и весьма невелик. То же самое касается и iOS, но в этом случае злоумышленникам гораздо сложнее дистрибуцировать вредоносное ПО, ввиду ограничений, накладываемых центром цифровой дистрибуции App Store для iOS. Ни одно приложение не может быть загружено в App Store без строгой предварительной проверки.

Microsoft использует для Windows Store и Windows Phone Store схожий с Apple подход к безопасности цифрового контента. Windows Store используется как платформа цифровой дистрибуции приложений для Windows 8/8.1, а Windows Phone Store для Windows Phone 7 и 8. Размещаемые там приложения должны соответствовать определенным правилам безопасности и проходить предварительную проверку. Таким образом пользователи этих платформ являются более защищенными в виду ее новизны и правил безопасности.



Согласно данным на диаграмме выше, в этом году антивирусной лабораторией ESET был зафиксирован значительный рост семейств вредоносных программ для Android, достигнув отметки 79 семейств. Семейство вредоносных программ представляет собой совокупность различных модификаций вредоносного ПО, которое можно соотнести в одну группу по каким-либо общим признакам кодовой базы и поведению. Мы также зафиксировали, что странами с наибольшим ростом угроз являются Иран, Китай и Россия.

Нужно отметить, что для Android велик процент так называемого потенциально нежелательного ПО (PUA или greyware). Причем абсолютное большинство этих приложений находится в сторонних магазинах приложений. Подобное ПО не представляется возможным строго классифировать как malware, скорее оно просто подвергает пользователя определенной степени риска, так как содержит сомнительные функции, например, является рекламным ПО или шпионским (spyware). Магазины приложений Android пытаются оградить пользователей от вредоносных приложений

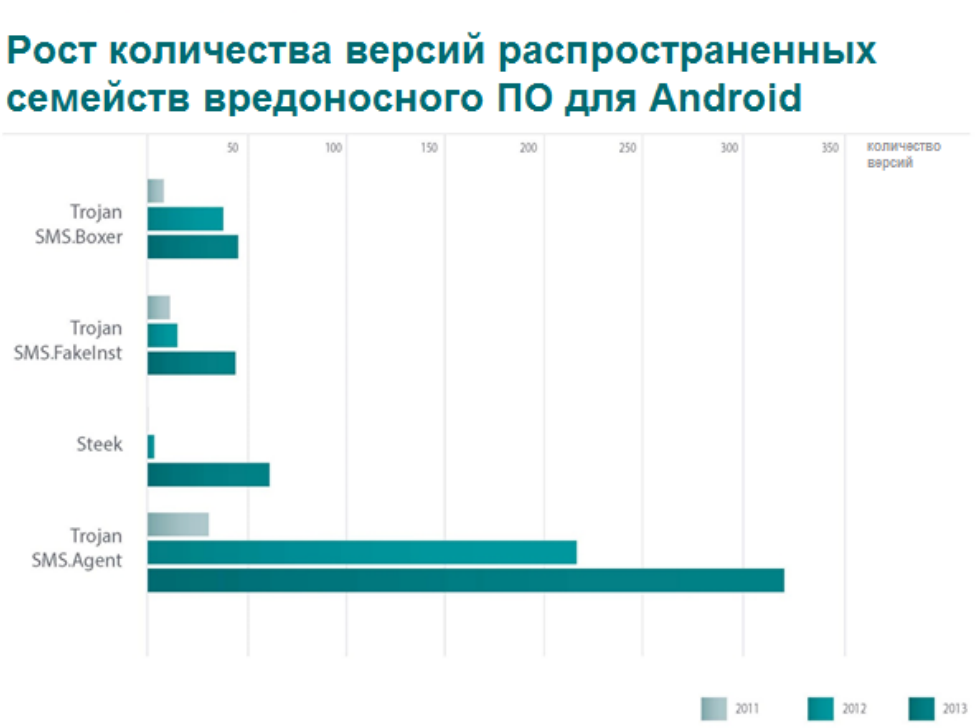
путем реализации специальных правил и фильтрации или удалением таких приложений по поступающим жалобам. Тем не менее некоторые вредоносные программы могут избегать подобных проверок и обеспечивать свое присутствие в списках приложений того или иного магазина.

Прошедший год отметился появлением новых видов вредоносных программ для Android. Прежде такие угрозы были характерны для персональных компьютеров, но теперь мы наблюдаем их и на мобильных устройствах. Некоторые из них обнаруживались и раньше, но не проявляли высокой активности как в этом году.

- Загрузчик (даунлоадер): пытается загрузить из интернета файлы других вредоносных программ и установить их на устройство.
- Дроппер: устанавливает другие угрозы на устройство при своем запуске, угрозы находятся в файле самого дроппера.
- Кликер: предназначен для генерации трафика на сайты через искусственное увеличение количества кликов, полученных на зараженных устройствах.
- Банковское вредоносное ПО: специализируется на краже конфиденциальной информации пользователя, которая используется для проведения операций, связанных с онлайн-банкингом.

Мы прогнозируем увеличение количества модификаций угроз для каждого из этих типов в будущем. Особенно это касается банковского вредоносного ПО, которое все больше стало проявлять свою активность из-за возможностей проведения финансовых операций пользователя прямо через устройство с использованием специальных приложений для работы с системой онлайн-банкинга. Пользователи могут осуществлять подобные операции через браузер, который может быть скомпрометирован вредоносным кодом. В результате злоумышленники могут иметь доступ к вводимым в формы данным.

В этом году мы наблюдали появление банковской троянской программы Hesperbot, которая использует компрометацию мобильного устройства пользователя с целью получения доступа к SMS-подтверждениям (mTAN), которые представляют собой механизм двухфакторной аутентифиации, проводимых пользователем операций. Hesperbot выполняет заражение компьютера пользователя, но в случае присутствия двухфакторной аутентификации при работе с системой онлайн-банкинга, его методы получения средств будут бесполезными. Поэтому злоумышленники привлекают для этих целей мобильный компонент.



Выше на графике показана статистика роста количества версий или модификаций распространенных семейств вредоносного ПО для Android. По прежнему самым актуальным семейством является троянская программа SMS.Agent, злоумышленники используют ее для скрытной отправки платных SMS-сообщений и для подписывания пользователя на платные услуги. В 2013 году это семейство претерпело значительный рост версий, при этом всего было зафиксировано 324 версии. Для сравнения, в 2012 г. было обнаружено 214 ее версий. Доминирующим семейством по появлению новых версий также является семейство Steek.

Удаленное исполнение кода как наиболее эффективный метод доставки вредоносного ПО

В прошлом году компания Microsoft исправила большое количество уязвимостей для ОС Windows и ее компонентов, а также для Office. Некоторые из этих уязвимостей использовались злоумышленниками для доставки вредоносного кода еще до выхода исправления (0day). Как правило большинство из них были ориентированы на те или иные иъяны в браузере Internet Explorer.

Уходящий год отметился появлением 0day уязвимостей, которые, в первую очередь, использовались в направленных атаках. Это своего рода тренд ушедшего года, злоумышленники осуществляют разработку эксплойтов не для спонтанного распространения вредоносного кода, а используют их в атаках на конкретных пользователей, преследуя при этом определенное цели.

Ниже показана статистика по исправленным Microsoft уязвимостям в рамках patch tuesday за прошедший год.

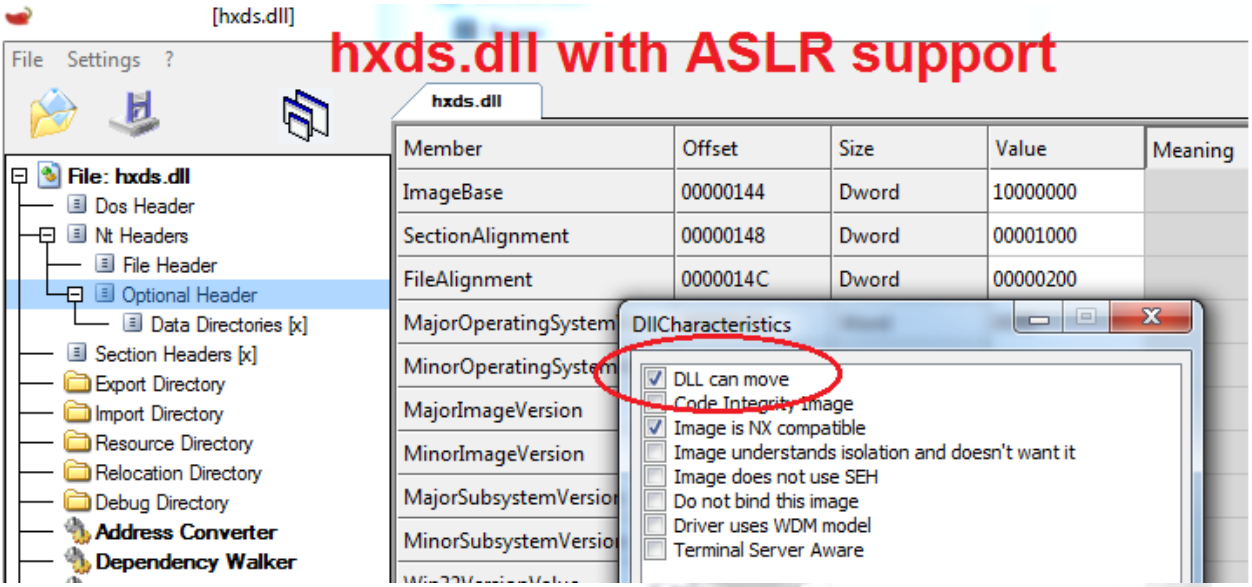
Component	Bulletin	Type	Vulnerability
Internet Explorer	MS13-008, MS13-009, MS13-010, MS13-021, MS13-028, MS13-037, MS13-038, MS13-047, MS13-055, MS13-059, MS13-069, MS13-080, MS13-088, MS13-090, MS13-097	Remote Code Execution(15), Elevation of Privilege(1)	**CVE-2012-4792**, CVE-2013-0015, CVE-2013-0018, CVE-2013-0019, CVE-2013-0020, CVE-2013-0021, CVE-2013-0022, CVE-2013-0023, CVE-2013-0024, CVE-2013-0025, CVE-2013-0026, CVE-2013-0027, CVE-2013-0028, CVE-2013-0029, **CVE-2013-0030**, CVE-2013-0087, CVE-2013-0088, CVE-2013-0089, CVE-2013-0090, CVE-2013-0091, CVE-2013-0092, CVE-2013-0093, CVE-2013-0094, CVE-2013-1288, CVE-2013-1303, CVE-2013-1304, CVE-2013-1338, CVE-2013-0811, CVE-2013-1297, CVE-2013-1306, CVE-2013-1307, CVE-2013-1308, CVE-2013-1309, CVE-2013-1310, CVE-2013-1311, CVE-2013-1312, CVE-2013-2551, CVE-2013-3140, **CVE-2013-1347**, CVE-2013-3110, CVE-2013-3111, CVE-2013-3112, CVE-2013-3113, CVE-2013-3114, CVE-2013-3116, CVE-2013-3117, CVE-2013-3118, CVE-2013-3119, CVE-2013-3120, CVE-2013-3121, CVE-2013-3122, CVE-2013-3123, CVE-2013-3124, CVE-2013-3125, CVE-2013-3139, CVE-2013-3141, CVE-2013-3142, CVE-2013-3166, CVE-2013-3115, CVE-2013-3143, CVE-2013-3144, CVE-2013-3145, CVE-2013-3146, CVE-2013-3147, CVE-2013-3148, CVE-2013-3149, CVE-2013-3150, CVE-2013-3151, CVE-2013-3152, CVE-2013-3153, CVE-2013-3161, CVE-2013-3162, **CVE-2013-3163**, CVE-2013-3164, CVE-2013-3184, CVE-2013-3186, CVE-2013-3187, CVE-2013-3188, CVE-2013-3189, CVE-2013-3190, CVE-2013-3191, CVE-2013-3192, CVE-2013-3193, CVE-2013-3194, CVE-2013-3199, CVE-2013-3201, CVE-2013-3202, CVE-2013-3203, CVE-2013-3204, CVE-2013-3205, CVE-2013-3206, CVE-2013-3207, CVE-2013-3208, CVE-2013-3209, CVE-2013-3845, CVE-2013-3871, CVE-2013-3872, CVE-2013-3873, CVE-2013-3874, CVE-2013-3875, CVE-2013-3882, CVE-2013-3885, CVE-2013-3886, **CVE-2013-3893**, **CVE-2013-3897**, CVE-2013-3908, CVE-2013-3909, CVE-2013-3871, CVE-2013-3910, CVE-2013-3911, CVE-2013-3912, CVE-2013-3914, CVE-2013-3915, CVE-2013-3916, CVE-2013-3917, **CVE-2013-3918**, CVE-2013-5045, CVE-2013-5046, CVE-2013-5047, CVE-2013-5048, CVE-2013-5049, CVE-2013-5051, CVE-2013-5052
Win32k	MS13-005, MS13-016, MS13-036, MS13-046, MS13-053, MS13-076, MS13-081, MS13-101	Elevation of Privilege(8), Remote Code Execution, Denial of Service(2)	CVE-2013-0008, CVE-2013-1248, CVE-2013-1249, CVE-2013-1250, CVE-2013-1251, CVE-2013-1252, CVE-2013-1253, CVE-2013-1254, CVE-2013-1255, CVE-2013-1256, CVE-2013-1257, CVE-2013-1258, CVE-2013-1259, CVE-2013-1260, CVE-2013-1261, CVE-2013-1262, CVE-2013-1263, CVE-2013-1264, CVE-2013-1265, CVE-2013-1266, CVE-2013-1267, CVE-2013-1268, CVE-2013-1269, CVE-2013-1270, CVE-2013-1271, CVE-2013-1272, CVE-2013-1273, CVE-2013-1274, CVE-2013-1275, CVE-2013-1276, CVE-2013-1277, CVE-2013-1283, CVE-2013-1291, CVE-2013-1292, CVE-2013-1333, CVE-2013-1334, CVE-2013-1300, CVE-2013-1340, CVE-2013-1345, CVE-2013-3129, CVE-2013-3167, CVE-2013-3172, CVE-2013-3173, **CVE-2013-3660**, CVE-2013-1341, CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, CVE-2013-3864, CVE-2013-3865, CVE-2013-3866, CVE-2013-3879, CVE-2013-3881, CVE-2013-3899, CVE-2013-3902, CVE-2013-5058
KM drivers (tcpip.sys, http.sys, usb, dxgkrnl.sys, afd.sys, portcls.sys)	MS13-018, MS13-049, MS13-039, MS13-027, MS13-046, MS13-064, MS13-065, MS13-081, MS13-093, MS13-101	Denial of Service(5), Elevation of Privilege(4), Information Disclosure	CVE-2013-0075, CVE-2013-3138, CVE-2013-1305, CVE-2013-1285, CVE-2013-1286, CVE-2013-1287, CVE-2013-1332, CVE-2013-3182, CVE-2013-3183, CVE-2013-3200, CVE-2013-3888, CVE-2013-3887, CVE-2013-3907
.NET Framework	MS13-004, MS13-015, MS13-040, MS13-052, MS13-082	Elevation of Privilege(3), Information Disclosure, Spoofing, Remote Code Execution(2), Denial of Service	CVE-2013-0001, CVE-2013-0002, CVE-2013-0003, CVE-2013-0004, CVE-2013-0073, CVE-2013-1336, CVE-2013-1337, CVE-2013-3129, CVE-2013-3131, CVE-2013-3132, CVE-2013-3133, CVE-2013-3134, CVE-2013-3171, CVE-2013-3128, CVE-2013-3860, CVE-2013-3861
NTOS	MS13-017, MS13-031, MS13-048, MS13-063, MS13-092 (Hyper-V), MS13-101	Elevation of Privilege(4), Information Disclosure, Denial of Service	CVE-2013-1278, CVE-2013-1279, CVE-2013-1280, CVE-2013-1284, CVE-2013-1294, CVE-2013-3136, CVE-2013-2556, CVE-2013-3196, CVE-2013-3197, CVE-2013-3198, CVE-2013-3898, CVE-2013-3903
CSRSS (csrss.exe), SCM (services.exe), GDI	MS13-019, MS13-033, MS13-077, MS13-089	Elevation of Privilege(3), Remote Code Execution	CVE-2013-0076, CVE-2013-1295, CVE-2013-3862, CVE-2013-3940
Print Spooler	MS13-001, MS13-050	Remote Code Execution, Elevation of privilege	CVE-2013-0011, CVE-2013-1339
Silverlight	MS13-022, MS13-052, MS13-087	Remote Code Execution(2), Information Disclosure	CVE-2013-0074, CVE-2013-3129, CVE-2013-3131, CVE-2013-3178, CVE-2013-3896

Красным шрифтом помечены эксплуатируемые на момент закрытия уязвимости.

Ниже в таблице дается более подробная информация об уязвимостях, которые эксплуатировались in-the-wild в ушедшем году (до выхода соответствующего исправления, 0day).

CVE	Тип	Компонент	Уязвимость	Исправлен	Обход DEP&ASLR, иное
CVE-2012-4792	Remote Code Execution	Internet Explorer 6-8	use-after-free	MS13-008	non-ASLR-msvcr71.dll/ROP
CVE-2013-0030	Remote Code Execution	Internet Explorer 6-10	memory-corruption	MS13-010	-
CVE-2013-1347	Remote Code Execution	Internet Explorer 8	use-after-free	MS13-038	non-ASLR-msvcrt.dll/ROP
CVE-2013-3163	Remote Code Execution	Internet Explorer 8-10	use-after-free	MS13-055	heap-spray/ROP
CVE-2013-3893	Remote Code Execution	Internet Explorer 6-11	use-after-free	MS13-080	non-ASLR-hxds.dll/ROP
CVE-2013-3897	Remote Code Execution	Internet Explorer 6-11	use-after-free	MS13-080	heap-spray/ROP
CVE-2013-3918	Remote Code Execution	Windows XP SP3 – 8.1 (ActiveX, icardie.dll)	memory-corruption	MS13-090	msvcrt.dll ROP
CVE-2013-3660	Elevation of Privileges	Windows XP SP3 – 8.1 (Win32k.sys)	memory-corruption	MS13-053	win32k!EPATHOBJ::pprFlattenRec bug (Ormandy, PowerLoader)
CVE-2013-5065	Elevation of Privileges	Windows XP SP3 – Server 2003 (NDProxy.sys)	memory-corruption	MS14-002	ndproxy.sys bug
CVE-2013-3906	Remote Code Execution	Office 2003-2010 (TIFF codec)	memory-corruption	MS13-096	heap-spray/ROP

Как мы видим, злоумышленники могут использовать некоторые системные библиотеки, скомпилированные без поддержки ASLR для построения стабильных ROP гаджетов и обхода ASLR. Одним из таких примеров является библиотека Office 2007-2010 hxds.dll, которая скомпилирована без поддержки ASLR. В рамках декабрьского patch tuesday компания закрыла эту оплошность (которая называется Security Feature Bypass) с помощью MS13-106, обеспечивая пользователей Windows, которые работают с этой версией Office, должным уровнем защиты.



Список выпущенных в прошедшем году рекомендаций по безопасности (Security Advisory).

SA	Уязвимость	Месяц	Описание
2794220	CVE-2012-4792	Декабрь ('12)	Internet Explorer 6-8 RCE
2798897	-	Январь	Отзыв цифровых сертификатов
2819682	CVE-2013-1299	Март	Обновление для Windows Store
2820197	-	Май	Пакет обновлений для ActiveX Kill Bits
2846338	CVE-2013-1346	Май	Malware Protection Engine RCE
2847140	CVE-2013-1347	Май	Internet Explorer 8 RCE
2719662	-	Июль	Windows Gadgets RCE
2876146		Август	Раскрытие информации через Wireless PEAP-MS-CHAPv2 (Windows Phone 8)
2861855	-	Август	Обновления для системы сетевой аутентификаци в RDP
2862973	-	Октябрь	Обновление для Windows, которое ограничивает использование MD5 в качестве доверенного алгоритма для применения в цифровых сертификатах из Microsoft root certificate program.
2887505	CVE-2013-3893	Октябрь	Internet Explorer 6-11 RCE
2854544	-	Ноябрь	Обновления для сервисов криптографии и обработки цифровых сертификатов
2862152	CVE-2013-3876	Ноябрь	Обновление для Windows, которое устраняет недоработку типа Security Feature Bypass в сервисах DirectAccess и IPSec
2868725	-	Ноябрь	Отключает использование RC4 в Windows 7+
2880823	-	Ноябрь	Запрещает корневым центрам сертификации (CA) выдавать сертификаты типа X.509 с использованием алгоритма SHA-1 (сертификаты для SSL и подписания программ) после 1 января 2016 г.
2914486	CVE-2013-5065	Ноябрь	LPE через ndproxy.sys на Windows XP
2755801	CVE-2013-5331 CVE-2013-5332 (Adobe SA, APSB13-28)	Декабрь	Обновление Adobe Flash Player в Internet Explorer 10+
2871690	-	Декабрь	Обновление отзывает информацию о цифровых подписях девяти UEFI-модулей (отказ в доверии)
2896666	CVE-2013-3906	Декабрь	Office 2003-2010 (TIFF codec) RCE
2905247	-	Декабрь	Обновление для ASP.NET (Elevation of Privilege)
2916652	-	Декабрь	Отзыв цифровых сертификатов
2915720	-	Декабрь	Обновление для компонента проверки цифровых подписей (Authenticode)

Ниже показан рейтинг наиболее исправляемых компонентов в Windows за 2013 г. Отметим, что на текущий момент поддерживаемыми MS версиями ОС являются Windows от XP SP3 / x64 XP SP2 до Windows 8.1 / RT 8.1.

То же самое в сравнение с Office (2003 – 2013 для Windows).

Drive-by download – основной метод скрытной доставки вредоносного кода через перенаправление пользователя на страницы наборов эксплойтов.

Local Privelege Escalation (LPE, Elevation of Privelege) – метод получения максимальных системных привилегий, как правило, связанный с запуском кода режима ядра минуя ограничения ОС накладываемые на исполнение кода в пользовательском режиме (user-mode restrictions escape).

Remote Code Execution (RCE) – удаленное исполнение кода, используемое, например, в drive-by, но в данном случае может активироваться не только через веб-страницу.

Тренд по выпущенным обновлениям показывает, что такие продукты как браузер Internet Explorer, компоненты .NET и плагин к браузеру Silverlight используются злоумышленниками для удаленного исполнения кода, причем в большинстве случаев это может происходить через браузер. Атакующие используют специальным образом подготовленную веб-страницу с вредоносным содержимым для установки на компьютер пользователя того или иного вредоносного кода. При данном сценарии использования Internet Explorer применение технологии «Защищенного режима» работы браузера, а также технологии sandboxing «Расширенный защищенный режим» является важным условием обеспечения своей безопасности для работы в сети.

Мы отмечаем, что использование технологий типа sandboxing для браузеров уже давно является обязательным требованием обеспечения соответствующего уровня безопасности для пользователей. Обойти подобный режим работы браузера крайне сложно и заставляет атакующих применять иные методы повышения своих прав в системе. Под иными методами имеется в виду разработка LPE-эксплойтов, которые будут работать в связке с эксплойтом, вызывающим удаленное исполнение кода. Такой подход необходим злоумышленникам ввиду того, что попав в браузер через RCE-уязвимость шелл-код остается бесправным в исполнении каких-либо системных функций, так как процесс браузера работает на низком Integrity Level и со множеством запрещенных привилегий. Хорошим примером такой практики является продемонстрированный способ эксплуатации Google Chrome компанией MWR Labs на Pwn2Own 2013 с обходом ограничений режима sandbox через уязвимость в win32k.sys.

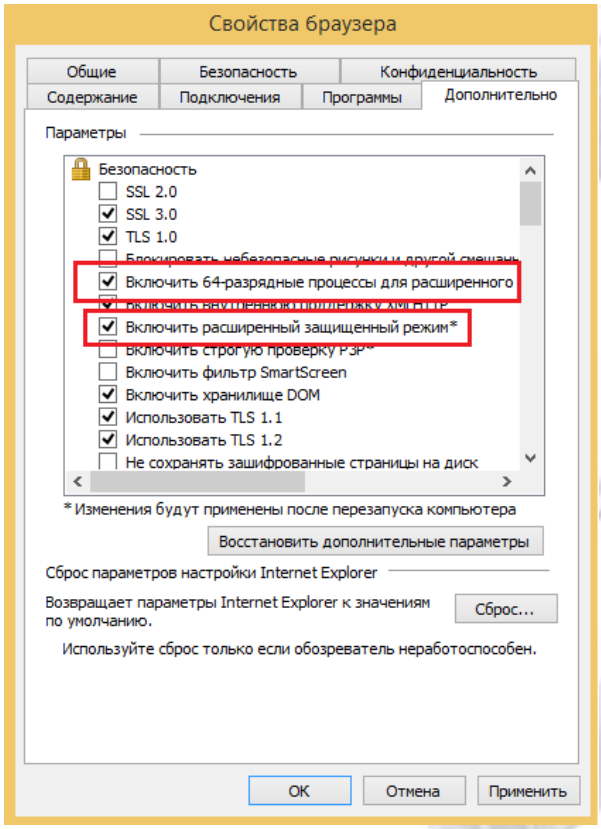
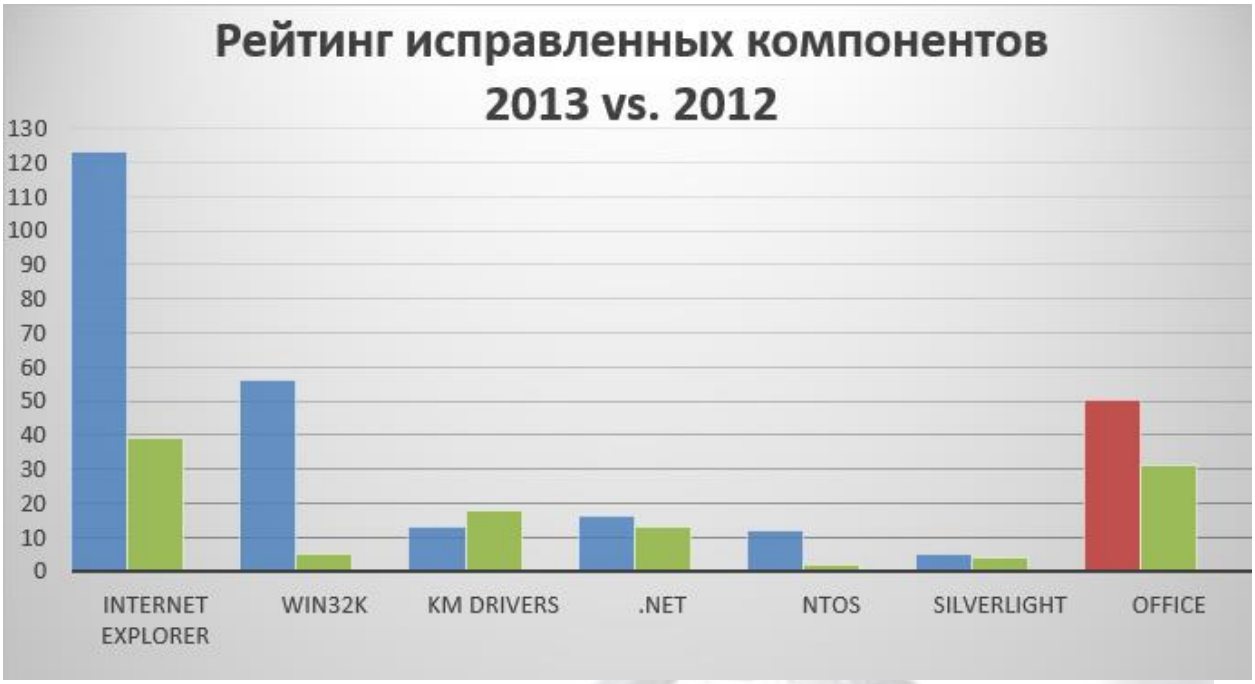


Рис. Internet Explorer 11 с настройками режима sandboxing (оптимальное использование на Windows 8/8.1 x64)

Уязвимости в приложениях пакета программ Office также могут использоваться злоумышленниками для удаленной установки вредоносного кода. По выпущенным в этом году обновлениям для Office видно, что большинство из них были направлены на устранение уязвимостей типа Remote Code Execution. При таком сценарии злоумышленники формируют специальным образом подготовленный файл Office, например, .doc файл Word и отправляют его с фишинговым письмом на адрес жертвы. Сообщение должно быть убедительным, чтобы пользователь прочтя его перешел к вложению и открыл его. После открытия такого файла на уязвимой версии Office пользователю будет установлено вредоносное ПО.

Отметим, что новейшая версия Word 2013, а также Outlook 2013 при работе с Word (открытие вложений) используют стойкие механизмы sandboxing, которые запрезают приложению исполнять потенциально небезопасные функции. Например, Outlook запускает процесс Word на низком Integrity Level и с отключенными привилегиями, что позволяет ограничить потенциальный шелл-код от выполнения системных функций.

Компоненты ОС, которые работают в режиме ядра: драйвер подсистемы Windows – win32k.sys, системные драйверы (KM drivers) и само ядро ntoskrnl (NTOS), используются злоумышленниками для поднятия своих привилегий в системе, т. е. для исполнения кода в режиме ядра минуя ограничения ОС (user mode restrictions escape). В этом году особенно отличился драйвер win32k.sys, в котором было закрыто более пятидесяти уязвимостей.



Очевидно, что в 2013 г. компания закрыла гораздо больше уязвимостей чем в 2012. Наиболее четко эта тенденция очевидна для драйвера подсистемы Windows – Win32k.sys и браузера Internet Explorer. В октябре компания выпустила новую ОС Windows 8.1, а также браузер Internet Explorer 11.

Предотвращение эксплуатации на уровне ОС

Прошедший год показал, что Microsoft уделяла внимание защитным технологиям для противодействия эксплойтам. Три основных нововведения были нацелены на защиту от выделения памяти по нулевой странице, удаление указатателей на раличные функции ntdll из PEB (ASLR bypass mitigation) и запрещение предоставления информации об указателях на объекты ядра для недоверенных приложений на Windows 8.1 (KASLR bypass mitigations).

Технология	Реализована начиная с	Описание
NULL-page allocating	Windows 8 (Windows 7 **MS13-031**)	Запрещает выделять память на нулевой странице виртуальной памяти через *EPROCESS!LowVaAccessible*
***ntdll!LdrHotPatchRoutine* mitigation**	Windows 8 (Windows Vista+ **MS13-063**)	Удаляет из SharedUserData все адреса системных функций (перемещая их в *ntdll!LdrSystemDllInitBlock*)
Kernel ASLR bypass mitigation	Windows 8.1 (built-in)	Запрещает ядру предоставлять информацию об указателях на объекты ядра через системные функции ntoskrnl для приложений с Intergrity Level ниже среднего.

Выделение памяти по нулевой странице (с использованием *ZwAllocateVirtualMemory*) значительно облегчало жизнь атакующим, в т. ч., если они заинтересованы в повышении своих привилегий в системе. После выделения такого участка памяти нужен какой-либо уязвимый драйвер, который при передаче ему определенных параметров сможет исполнить код по этому адресу (баг).

Следующие возможности доступны в Internet Explorer как средства для защиты от эксплуатации. Последним пунктом указан тот факт, что все системные файлы, скомпилированные MS для Windows 8, поддерживают стойкий HEASLR.

Технология	Реализована начиная с	Поведение	Описание
Internet Explorer protected mode (защищенный режим)	Internet Explorer 7 (Windows Vista)	По умолчанию	Запускает процесс браузера на низком Integrity Level
Internet Explorer ForceASLR	Internet Explrorer 10 (Windows 8)	По умолчанию	Принудительно применяет ASLR для всех модулей, загружаемых в адресное пространство процесса.
Internet Explorer sandboxing (EPM)	Internet Explrorer 10 (Windows 8 x64)	Вручную	AppContainer для процессов вкладок
System executables (MS-compiled) HEASLR	Windows 8	Built-in	csrss, winlogon, services, svchost, etc.

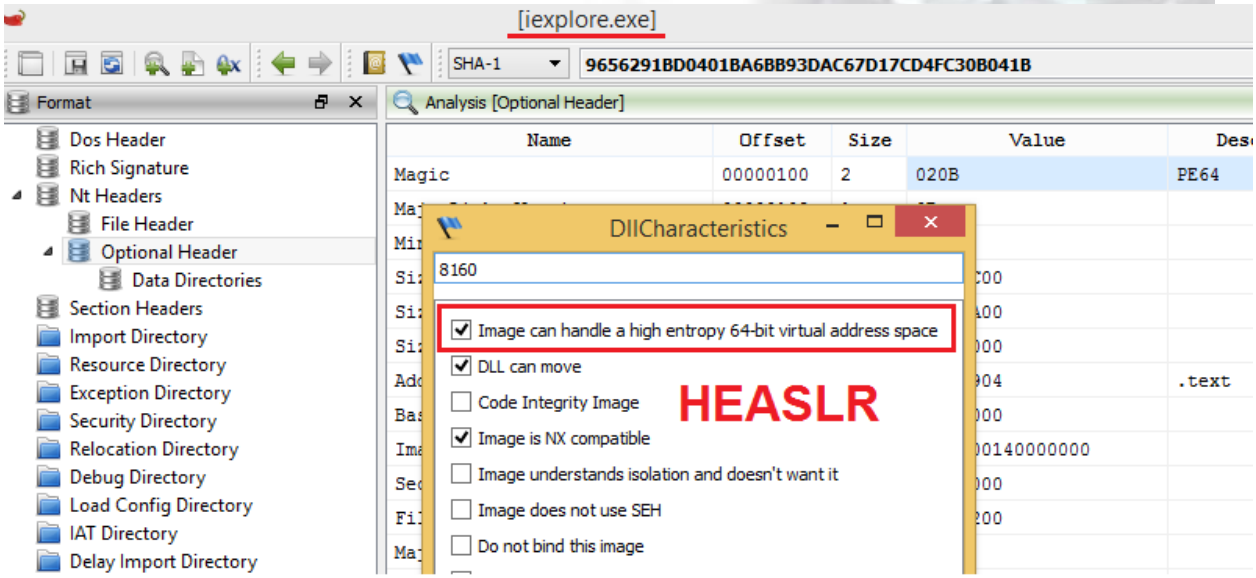


Рис. Системные файлы на Windows 8 x64+ скомпилированы с поддержкой усиленного ASLR – High Entropy ASLR, для максимально возможного снижения вероятности его обхода

Windows XP – последний аккорд

Ушедший год был последним, в котором Microsoft поддерживала последние выпуски Windows XP SP3 и Windows XP x64 SP2. Несмотря на рекомендации Microsoft и различных специалистов по безопасности, которые призывали пользователей уже давно отказаться от этой устаревшей и крайне небезопасной ОС, на сегодняшний день большое количество пользователей все еще используют ее. Согласно статистике компании Net Applications, Windows XP используется почти на 30% компьютеров.

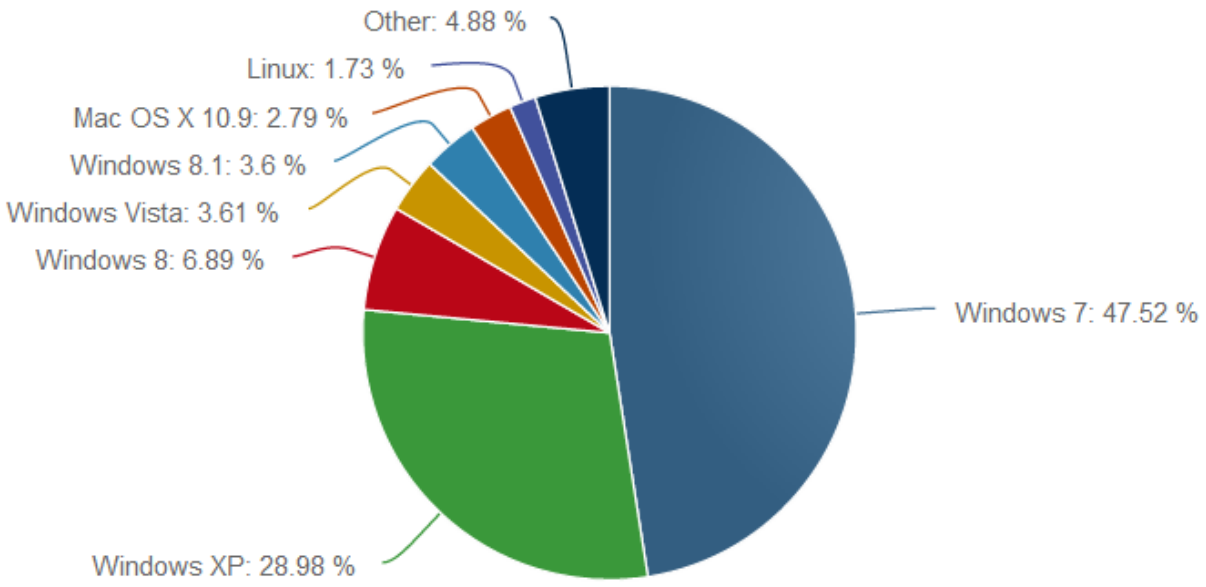


Рис. Статистика использования ОС на компьютерах по данным Net Applications

В апреле 2014 года компания откажется от поддержки Windows XP SP3 и Windows XP x64 SP2 (поддержка Windows XP & SP1 & SP2, Windows XP x64 & SP1 уже была завершена) и таким образом полностью закроет цикл поддержки кодовой базы и продуктов ОС, которые основаны на Windows XP. Для пользователей, в первую очередь, это будет означать тот факт, что они лишатся security и иных обновлений, которые Microsoft гарантированно выпускала каждый второй вторник месяца (т. н. patch tuesday) или внепланово, а также инструкций в Security Advisory (SA) или workaround в случае обнаружения эксплуатируемой атакующими уязвимости в ОС (компания оставляет за собой право публиковать или нет эту информацию).

Хорошим примером такой уязвимости для Windows XP, исправление которой компания отложила на 2014 год, является CVE-2013-5065. В силу поддержки Windows XP до апреля, Microsoft исправляет ее в январском наборе обновлений как Important обновление MS14-002 (в дальнейшем, после апреля, подобные уязвимости исправляться не будут).

Об CVE-2013-5065 стало известно в конце ноября из SA 2914486. Уязвимость присутствует в той версии драйвера ndproxy.sys, которая поставляется в составе Windows XP и Windows Server 2003, она позволяет злоумышленникам повысить свои привилегии до уровня системы и через обход ограничений пользовательского режима исполнить свой код в режиме ядра (Local Privilege Escalation, LPE) через отправку специально сформированного запроса (IOCTL) драйверу ndproxy.sys.

Для того чтобы обезопасить пользователей, которые все еще продолжают использовать Windows XP SP3, Microsoft выпускает бесплатный инструмент EMET (v 4.1 текущая верси). EMET помогает пользователю обезопасить ОС от различных действий эксплойтов, через которые атакующие пытаются компрометировать систему и запускать там вредоносный код. Применительно к Windows XP SP3, EMET поможет ввести следующие функции возможности, которые значительно повысят иммунитет системы.

- Включить ASLR.
- Принудительно включить DEP для всей системы.

- Включить возможность защиты от перезаписи указателей в SEH на уровне ОС – SEHOP.
- Использовать стандартные возможности EMET для защиты от эксплойтов.

Механизмы EMET применяются к процессам, поэтому пользователь волен выбрать конкретные процессы в списке, чтобы применить к ним возможности безопасности. По умолчанию он защищает следующие критические относительно удаленной эксплуатации процессы:

- Adobe Reader (от эксплуатации через PDF);
- MS Office (включая Excel, Word, Access, Outlook и др. от эксплуатации через вложения в электронной почте);
- Java (от эксплуатации через браузер);
- Браузер Internet Explorer.

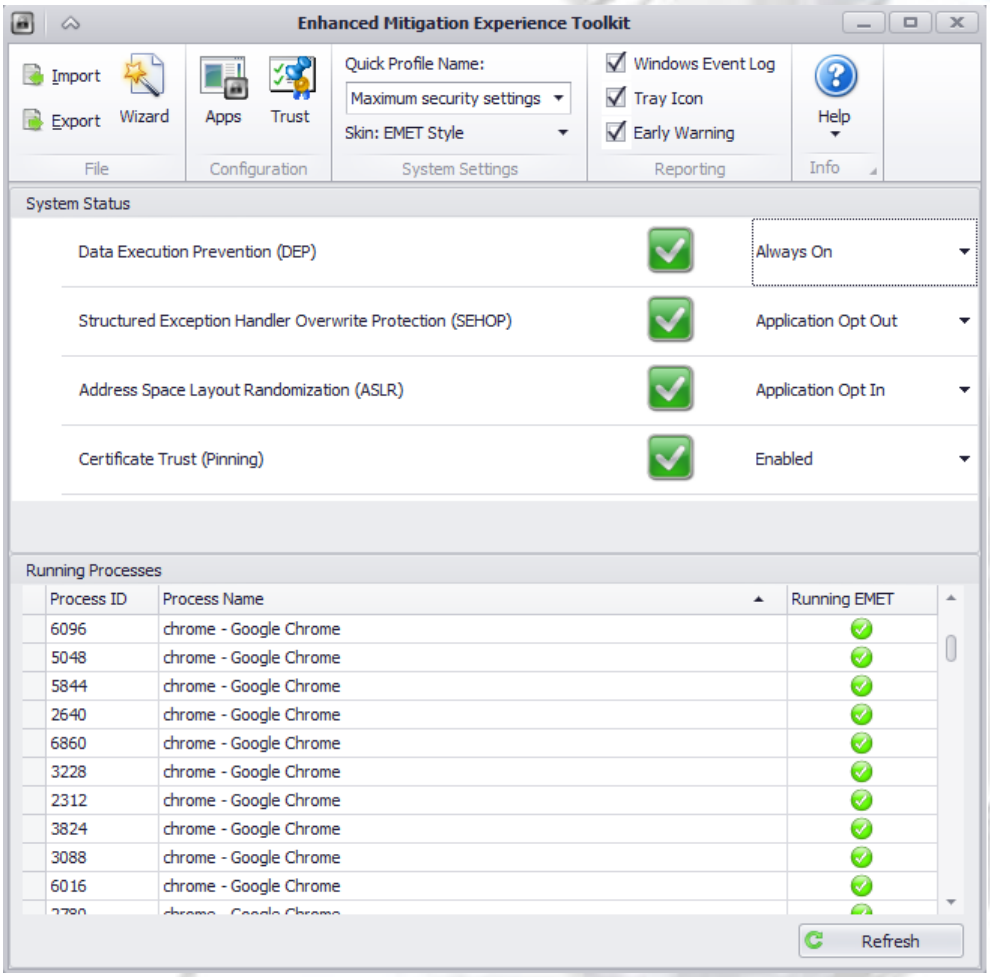


Рис. Главное окно EMET с максимальными настройками, в списке процессов браузер Google Chrome – как защищаемый

Рекомендации SA часто содержат отсылку к EMET и его опциям для быстрого исправления ситуации и защиты от той или иной уязвимости еще до выхода официального обновления. Большинство подобных настроек доступно из пользовательского интерфейса инструмента, но есть и те, которых там нет. Например, эксплойты часто используют технику heap spraying как средство обхода ASLR. При таком сценарии, атакующие знают какое значение может принять тот или иной регистр при ошибочной ситуации в исполнении кода (баг). Далее им остается только зарезервировать определенное количество блоков памяти, которые прилегают к этому адресу (spraying). В

дальнейшем, при провоцировании ситуации эксплуатации, ошибочный код сам передаст управление на один из адресов, который нужен атакующим. Список таких адресов перечислен в параметре реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EMET_settings_\{GUID}. Этот список является пополняемым согласно рекомендациям SA (напр., см. SA 2887505).

Заключение

Ушедший год показал высокую активность различного вредоносного кода и злоумышленников, которые его используют. Как мы упоминали выше, количество направленных атак в этом году только увеличилось и подобный способ распространения вредоносного кода является все более актуальным у злоумышленников. Удаленное исполнение кода через специально обнаруженные для конкретной атаки эксплойты также является существенным трендом прошлого года.