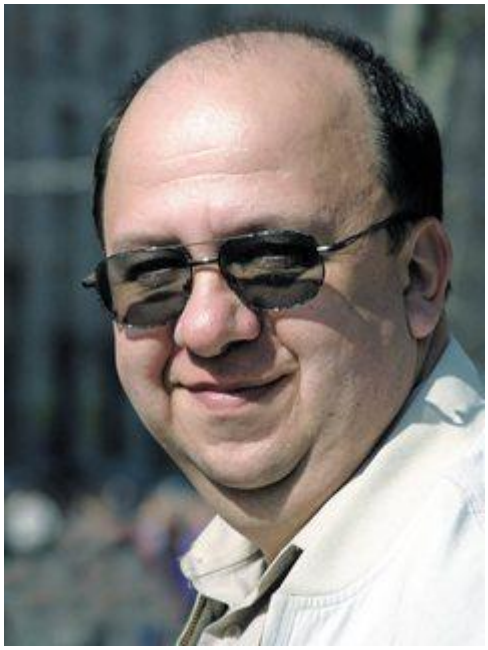
Эра Post PC

http://www.it-world.ru/tech4business/security/45016.html



Эксперты предсказывали наступление пост компьютерной эры в течение нескольких лет. Вопрос был простым: «Когда мы узнаем, что она наступила?» Ответ, безусловно, также прост. Мы знаем, что она наступила, потому что злоумышленники вышли за рамки ПК. Если судить по этому показателю, то в 2012 году мы вошли в послекомпьютерную эру, так как злоумышленники перешли в атаку на Android, социальные сети и компьютеры от Apple.

Целевые атаки продолжаются с ошеломляющей скоростью.

Как сообщают «Ведомости» со ссылкой на слова президента Ассоциации региональных банков «Россия» Анатолия Аксакова, практически 20% киберпреступлений в мире пришлось на Россию в 2012 году. Большинство инцидентов безопасности, связанных с банковскими картами, происходит из-за халатности их владельцев.

«Есть такая Ассоциация российских членов Europay (АРЧЕ), которая в различных формах дает информацию о киберпреступлениях, в том числе в сфере платежных карт. Они говорят о сумме примерно в $2,5 млрд. Причем отмечают, что в целом по миру объем таких мошеннических операций составляет приблизительно $13 млрд, то есть, если говорить о России, это довольно значительный вес — около 20%, что должно внушать нам обеспокоенность», — сказал Аксаков.

В 2012 году количество киберпреступлений в России выросло на 60%. Причем практически все атаки направлены на системы банков и силовых структур.

Наиболее важным в 2012 году можно назвать то, что ОС Android потребовалось менее трех лет, чтобы объем вредоносных угроз достиг того же уровня, что и для ПК за 14 лет.

В поиске уязвимостей для атак злоумышленники все чаще обращают внимание на Java. Именно в 2012 году Java вытеснила с первого места чистые Windows-угрозы.

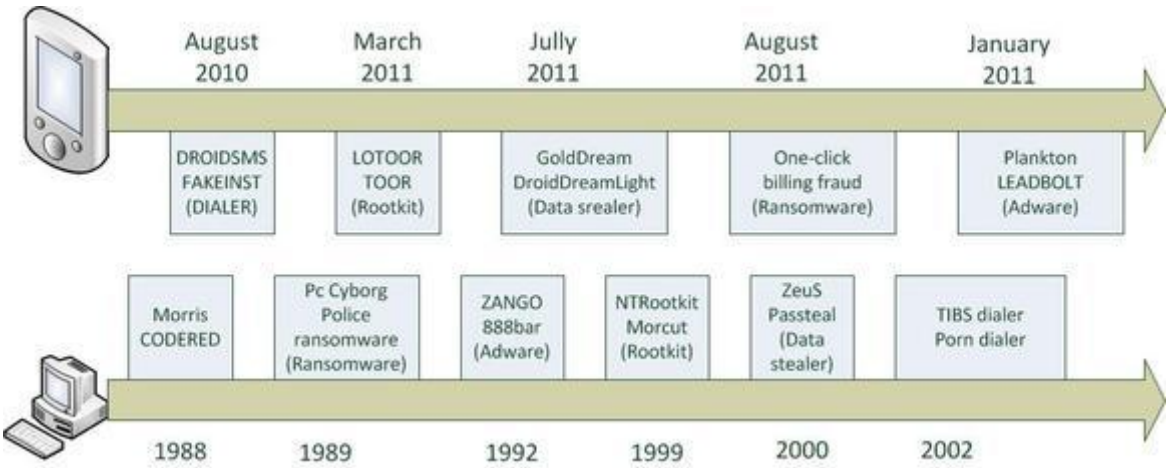


Рис. 1. Сравнение злонамеренного ПО под PC и Android

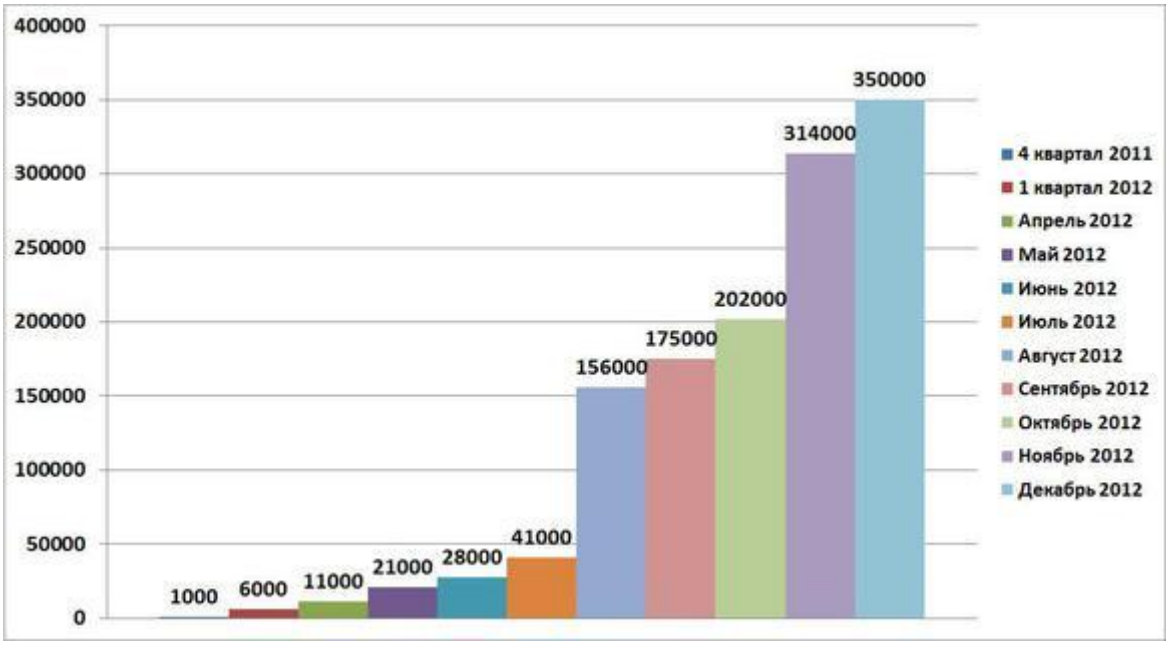


Рис. 2. Рост числа вредоносного ПО под Android (по версии Trend Micro)

Распределение вредоносного ПО по типам угроз (по версии Trend Micro) представлено на рис. 3.

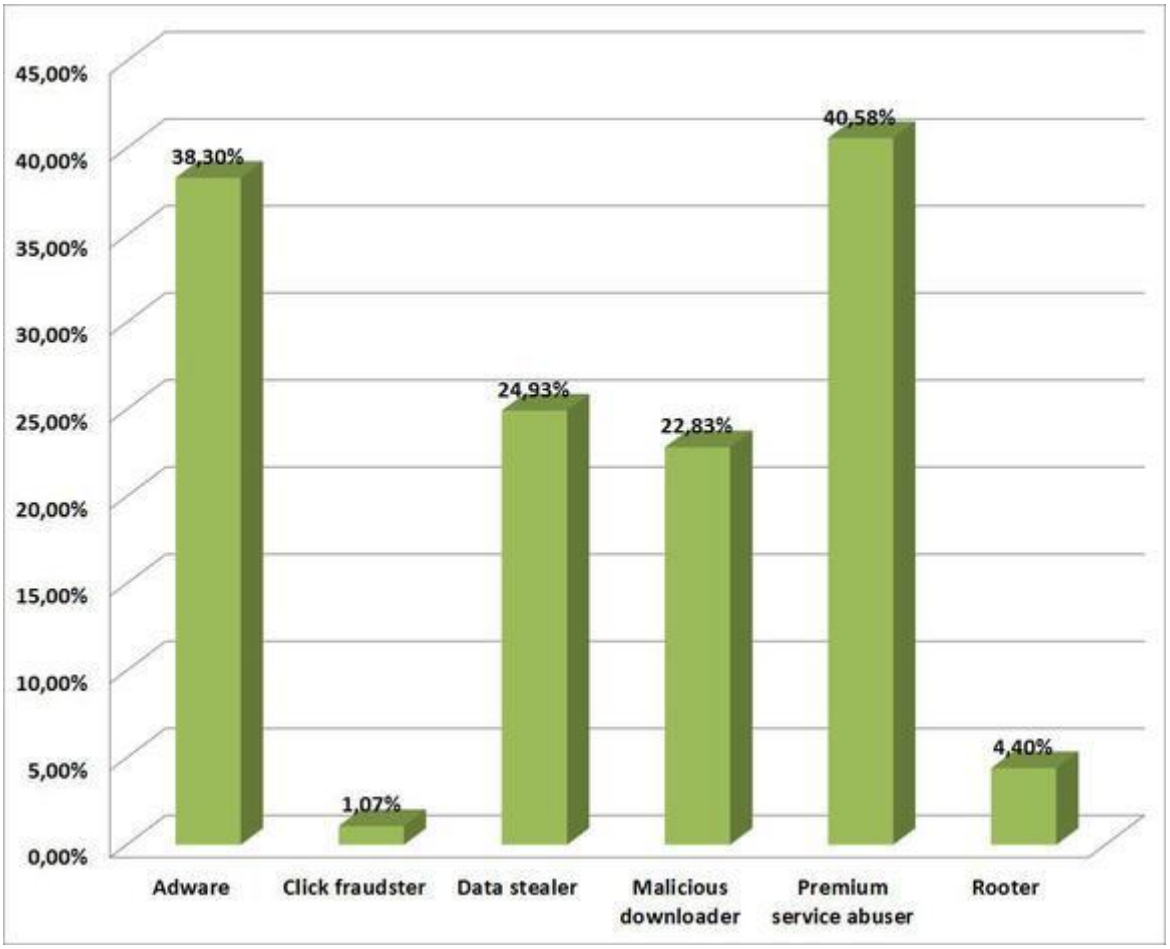


Рис. 3. Распределение вредоносного ПО по типам угроз (согласно отчета Trend Micro)

ТОП-10 стран, в которых загружалось вредоносное ПО:

1	Нигерия
2	Перу
3	Индия
4	Италия
5	Кувейт
6	Россия
7	Бразилия
8	Австрия

10	Филиппины

Если обратиться к статистике «Лаборатории Касперского», то мы получим не менее ужасающую картину:

· На январь 2013 года зарегистрировано 5 916 926 вредоносных приложений под Android.

· За последние три месяца, по данным Kaspersky Security Network, предотвращена установка 104 000 вредоносных приложений.

· В среднем ежедневно взламывают более 35 сайтов и устанавливают на них ссылки на мобильные вредоносные программы.

· За 84% всех заражений мобильных устройств в России (по данным KSN) отвечают четыре самые популярные троянские программы (HEUR:Trojan-SMS.AndroidOS.FakeInst.a, HEUR:Trojan-SMS.AndroidOS.Opfake.a, HEUR:Trojan-SMS.AndroidOS.Agent.u, HEUR:Trojan-SMS.AndroidOS.Opfake.bo)

Таблица 2. Распределение мобильных вредоносных программ по платформам

Платформа	Количество модификаций	Количество семейств	%
Android	44321	270	94,07
J2ME	2262	64	4,8
SymbOS	381	107	0,81
WinCE	85	27	0,18
Python	64	6	0,14
IPhone	15	5	0.03
Sgold	5	3	0.01
BlackBerry	8	2	0.02

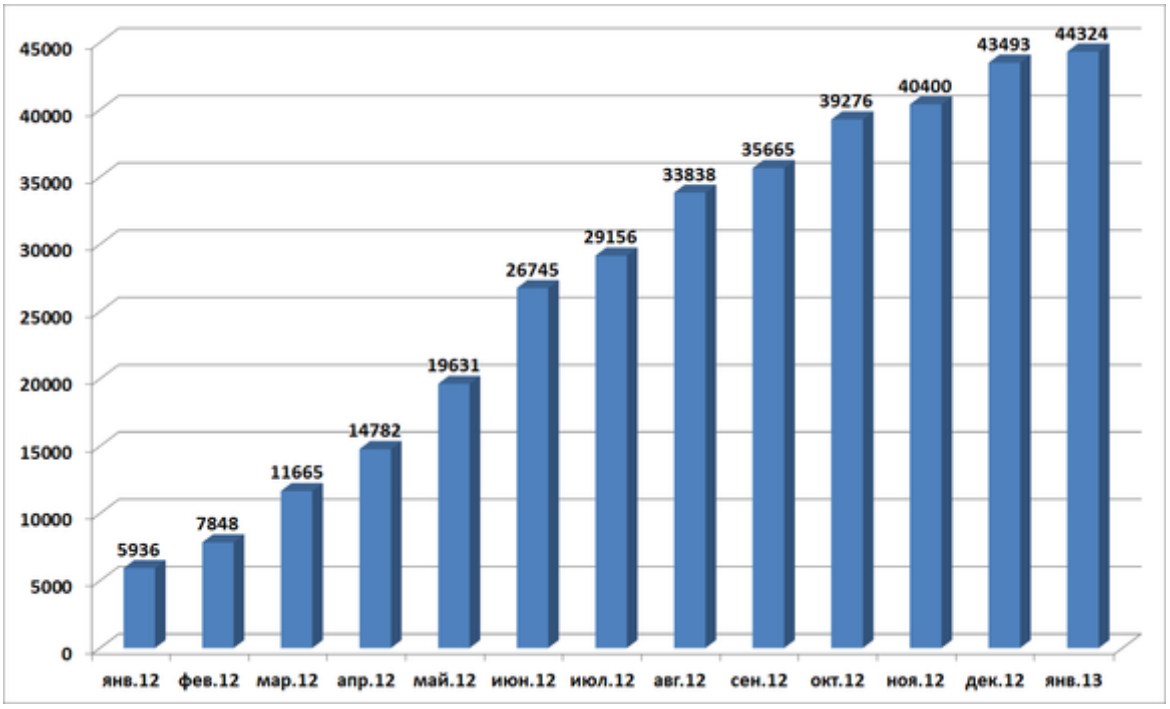


Рис. 5. Количество модификаций вредоносного ПО под ОС Android на начало месяца (согласно данным Лаборатории Касперского)

Вместе с тем мы имеем поразительное благодушие пользователей.

Сегодня пользователи весьма слабо информированы об опасностях, угрожающих им в связи с развитием современных информационных технологий. Около 80% пользователей смартфонов, как утверждает Говинд Раммурти, генеральный директор компании eScan MicroWorld, эксперт в области информационной безопасности, в принципе ничего не знает о существовании киберугроз.

В то же время борьба с вредоносным ПО становится приоритетом не только для предприятий, но и для домашних пользователей.

Мобильные технологии получают все большее распространение. Прошедшие в 2012 году летние Олимпийские игры привлекли свыше 40% пользователей мобильных устройств. 80% владельцев Apple iPad применяют свои планшеты, чтобы просматривать веб-страницы, более 600 млн человек используют мобильные платформы, чтобы заходить в социальную сеть Facebook. С 2010 гколичество мобильных интернет-пользователей в Китае выросло на 192%.

Все это, без сомнения, приведет к тому, что в ближайшее время мы будем наблюдать рост атак на эти устройства.

По статистике, под управлением ОС Google Android работают свыше 75% смартфонов, что делает эту операционную систему наиболее популярной для различных атак вирусописателей: только за последние два месяца огромное число (около 200 тыс.!) подозрительных программ было размещено в различных магазинах приложений данной платформы. Даже сервис Google Play содержал вредоносные программы под Android. Все чаще вредоносное ПО маскируется под

легитимные приложения, а пользователи нередко не в состоянии увидеть разницу между вредоносным и легитимным ПО.

Вместе с тем, несмотря на важность контроля над правами, предоставляемым приложениям, более 95% пользователей Android упускают из виду необходимость проверить тип доступа, который программа запрашивает перед установкой.

По статистике, только 15% пользователей ОС Google Android устанавливают антивирусное ПО.

Необходимо также отметить, что пользователи, загружающие приложения с официального Google Play, имеют меньше шансов заразить свой смартфон (планшет) вредоносным ПО, поскольку Google достаточно быстро детектирует вредоносные приложения.

Тем не менее даже эти пользователи рискуют. Однако куда больше рискуют те пользователи, которые для загрузки контента используют магазины приложений третьей стороны, чтобы не платить за приложения (первое место по числу пользователей, предпочитающих сторонние магазины, занимает Китай).

Отдельно хотелось бы подчеркнуть масштабы угроз, связанных со смартфонами.

Корпорация Symantec сообщает о новой угрозе Android.Exprespam. Мошенники создают поддельные магазины приложений для платформы Android с целью получения персональных данных пользователей. Эксперты предполагают, что с помощью этой схемы злоумышленникам уже удалось похитить от 75 до 450 тысяч записей личных данных, и это только начало. Обезопасить себя можно, не переходя по подозрительным ссылкам от неизвестных отправителей.

Вредоносную программу Android.Exprespam обнаружили в начале января 2013 года, и таким образом она была активна всего пару недель, однако специалисты считают, что злоумышленникам уже удалось достигнуть успеха. Полученная в ходе исследования информация, указывает на то, что поддельный магазин Android-приложений, названный Android Express’s Play, собрал более 3000 посещений в период с 13 по 20 января.

Основываясь на информации из нескольких источников, эксперты Symantec подсчитали, что злоумышленникам предположительно удалось похитить от 75000 до 450000 записей личных данных.

Такая обманная схема появилась совсем недавно, а потому специалисты уверены, что это лишь начало и объемы собираемой злоумышленниками информации будут неуклонно расти.

Кроме того, эксперты сообщают, что обнаружили еще один интернет-домен, также зарегистрированный создателями Exprespam, где была размещена другая версия их поддельного магазина. На этот раз злоумышленники решили не давать магазину названия, так же как и не предоставлять имен тех, кто занимается его поддержкой. На данный момент магазин не активен, что может указывать на то, что злоумышленники дорабатывают его или же приберегают в качестве резервного, однако на данном сайте уже размещена последняя версия вредоносной программы.

«Злоумышленники постоянно совершенствуют тактику с целью повышения прибыльности своих афер. Эта деятельность не прекратится до тех пор, пока их не арестуют и не накажут, либо пока они сами не решат прекратить обманывать людей, что кажется крайне маловероятным, — отмечает Михаил Савушкин, технический специалист Symantec.— Надеюсь, что большинство пользователей уже достаточно хорошо осведомлено о подобного рода мошенничествах, чтобы не стать их жертвами».

Пользователи устройств под управлением Android могут обезопасить себя, просто не переходя по ссылкам в электронных письмах, полученных от неизвестных отправителей, взяв за правило скачивать приложения только с известных и заслуживающих доверия ресурсов.

Не стоит думать, что платформы iOS или Windows Phone более защищены и соответственно под них нет вредоносного ПО. Увы, это не так.

Не успела ОС Windows Phone 8 выйти на рынок, как уже в ноябре 2012 года, по сообщению SC Magazine (http://www.scmagazine.com.au/News/322844%2cwindows-phone-8-malware-developed.aspx), индийский хакер Shantanu Gawde заявил, что разработал первый образец вредоносного ПО под эту ОС. ПО предназначено для хищения личных данных пользователей, включая контакты и текстовые сообщения, загрузку фотографий. Кроме того, оно разработано таким образом, что может обойти проверку магазина приложений Microsoft Windows Phone 8.

Однако если вы думаете, что нынешние атаки ограничиваются только смартфонами, вы ошибаетесь!

Специалисты компании ReVuln опубликовали видеоролик, в котором наглядно продемонстрировали, как хакер может использовать уязвимости, обнаруженные им в Samsung Smart TV. В ролике демонстрировалось, как хакер получает удаленный доступ к файлам и другой конфиденциальной информации, включая параметры настройки телевизора, списки каналов, счета SecureStorage, список фильмов и т. д.

Уязвимости позволяют считывать информацию с USB-устройств, а также удаленно управлять телевизором.

==========

Советы пользователю:

· Регулярно проверяйте состояние вашего банковского счета, чтобы убедиться в отсутствии незаконных операций

· При проведении финансовых операций убедитесь, что в строке адреса содержится **https://**

· Не забудьте о необходимости использовать антивирусный пакет от известного производителя

· Обязательно устанавливайте последние обновления безопасности для вашего компьютера, смартфона, планшета

· Если можно, используйте автоматическое обновление

· Не используйте один и тот же пароль для различных приложений

· Не загружайте ПО из сомнительных источников

· Не переходите по ссылкам, полученным в письмах, отправителей которых вы не знаете

Автор: Владимир Безмалый, MVP Consumer Security, MicrosoftSecurityTrustedAdvisor