Новое время, новые угрозы. Готовы ли вы?

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

С приходом смартфонов и планшетов наш мир изменился. Появилось новое пространство для приложения усилий злоумышленников. Вместе с тем стоит отметить, что большинство пользователей, да и не только пользователей, и ИТ в том числе, на мой взгляд еще недостаточно осознают степень угрозы со стороны смартфонов.

Почему? Да прежде всего потому что смартфоны и планшеты, на мой взгляд, первые компьютерные устройства, которые вначале проникли на пользовательский рынок, а уж потом становятся корпоративными устройствами. А информационная безопасность, так уж повелось, развивается наоборот, от защиты бизнеса к защите интересов конкретных пользователей.

Стоит признать, что пользователи, в большинстве своем, не осознают степень угрозы, а раз так, не хотят, да и не умеют защищаться.

Что сегодня происходит на рынке безопасности смартфонов и планшетов?

Давайте обратимся к отчетам антивирусных компаний.

Общая статистика

По сведениям специалистов «Лаборатории Касперского», за 2011 год количество вредоносных программ для мобильных устройств выросло в 6(!) раз. Только в декабре 2011 годв а антивирусные базы «Лаборатория Касперского» добавила больше образцов мобильного вредоносного ПО, чем за предыдущие 7(!) лет.

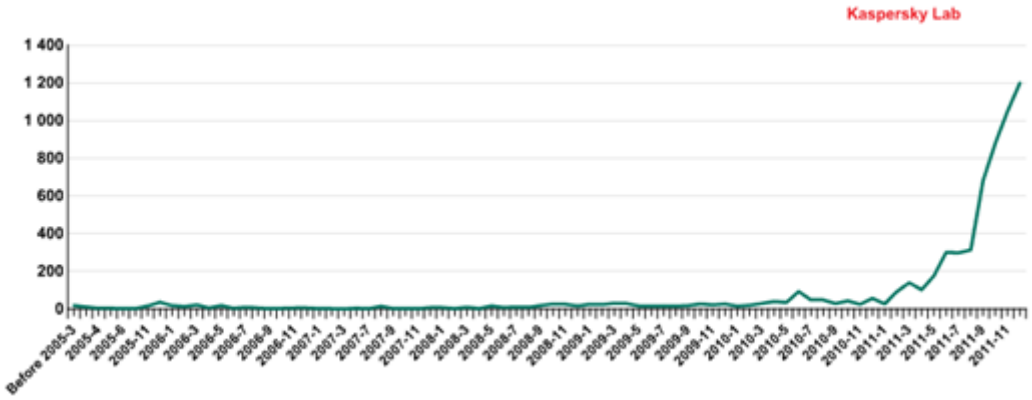

Рисунок 1 Число новых модификаций мобильных вредоносных программ по месяцам (2004–2011 гг.)

Таблица 1 **Количество новых мобильных зловредов в 2011 и начале 2012 гг.**

месяц	всего	Android	J2ME	Symbian	Windows Mobileидр. (iOS, Python, Blackberry
2011-1	27	4	22	0	1
2011-2	96	14	75	2	5
2011-3	134	33	92	7	2
2011-4	106	12	80	11	3
2011-5	186	36	141	8	1
2011-6	322	133	185	3	1
2011-7	296	212	68	7	9
2011-8	315	162	148	5	0
2011-9	681	562	111	8	0
2011-10	973	876	86	10	1
2011-11	1465	1420	38	7	0
2011-12	1393	1361	31	1	0
2012-1	1048	1026	21	1	0
2012-2	1955	1909	44	2	0

По данным «Лаборатории Касперского» (http://www.securelist.com/ru/analysis/208050757/Razvitie_informatsionnykh_ugroz_v_pervom_kvartale_2012_goda) за первый квартал 2012 года обнаружено более 5 000 (5444) вредоносных программ для платформы Android. Стоит отметить, что за последнее полугодие количество всех вредоносных программ под OS Android увеличилось в 9 раз. При этом график роста выглядит следующим образом (рис. 2).

Рисунок 2 Количество обнаруженных модификаций вредоносного ПО для Android OS

По данным компании F-Secure, приведенным в отчете за первый квартал 2012 года число вредоносного ПО для смартфонов под управлением Android с 2011 года по настоящее время увеличилось в 4 (!) раза. В 1 квартале 2011 года было обнаружено 10 вредоносных семейств, аза 1 квартал 2012 года это число составило 37 семейств, т.е. за год прирост составил 270%.

Если же сравнивать количество вредоносных пакетов (APKs) то рост получается еще более ошеломляющий. Со 139 в 1 квартале 2011 года до 3063 в 1 квартале 2012 года.

Вместе с тем стоит отметить, что 34 из 37 обнаруженных семейств были ориентированы на кражу денег у пользователей зараженных смартфонов.

Согласно отчета Juniper Networks Mobile Threat Center (http://conference.auscert.org.au/conf2012/Juniper%20brochure.pdf) распределение вредоносного ПО по мобильным платформам в 2010/2011 году выглядело следующим образом (рис.3).

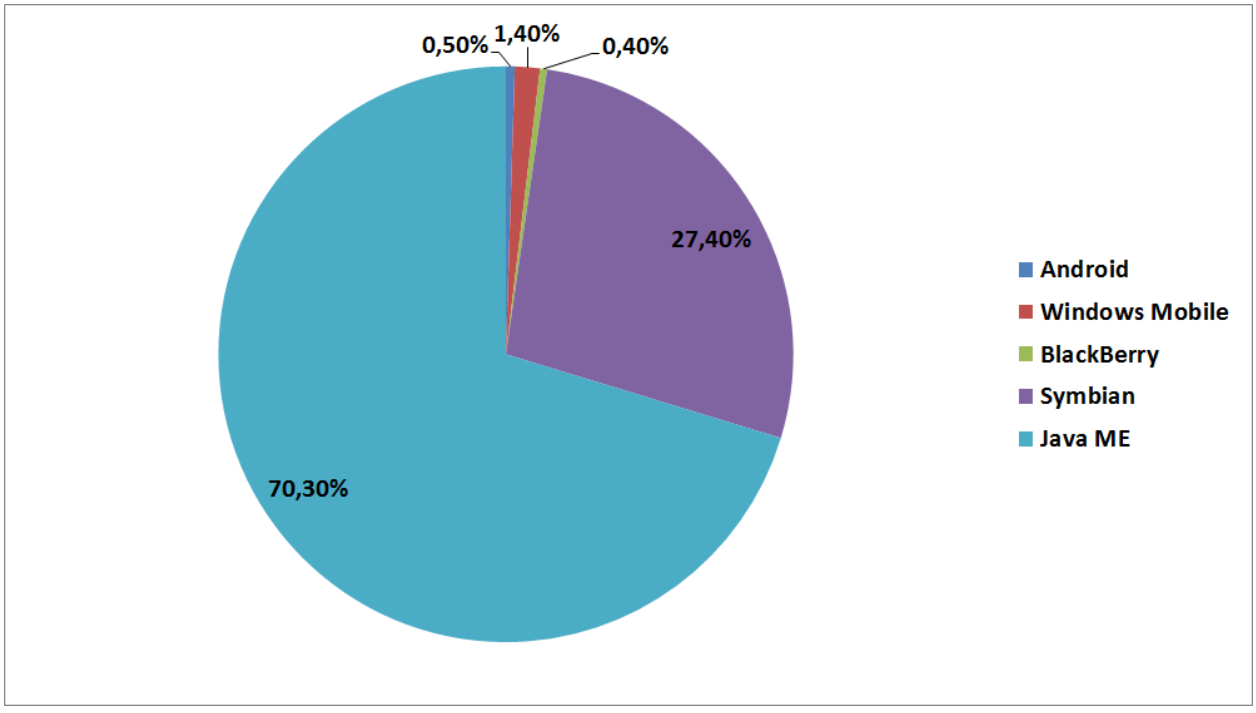

Рисунок 3 Распределение вредоносного ПО в 2010 году

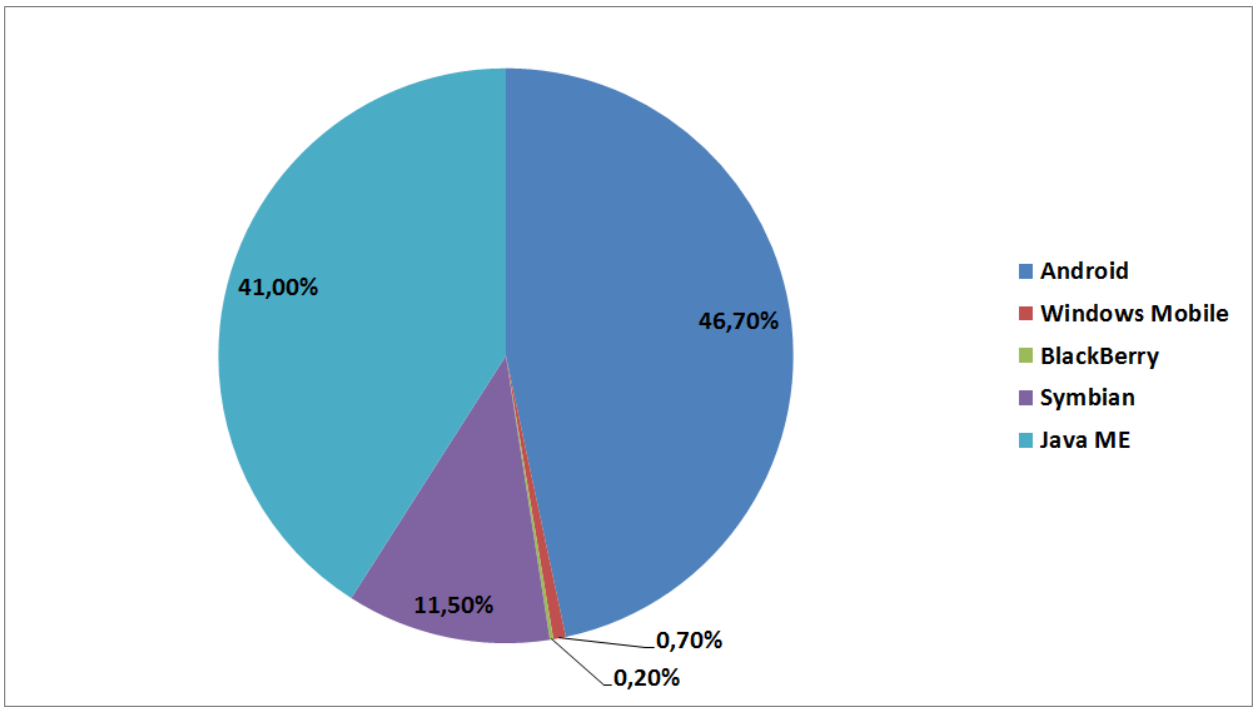

Рисунок 4 Распределение вредоносного ПО в 2011 году

Более наглядно это видно на рис.5

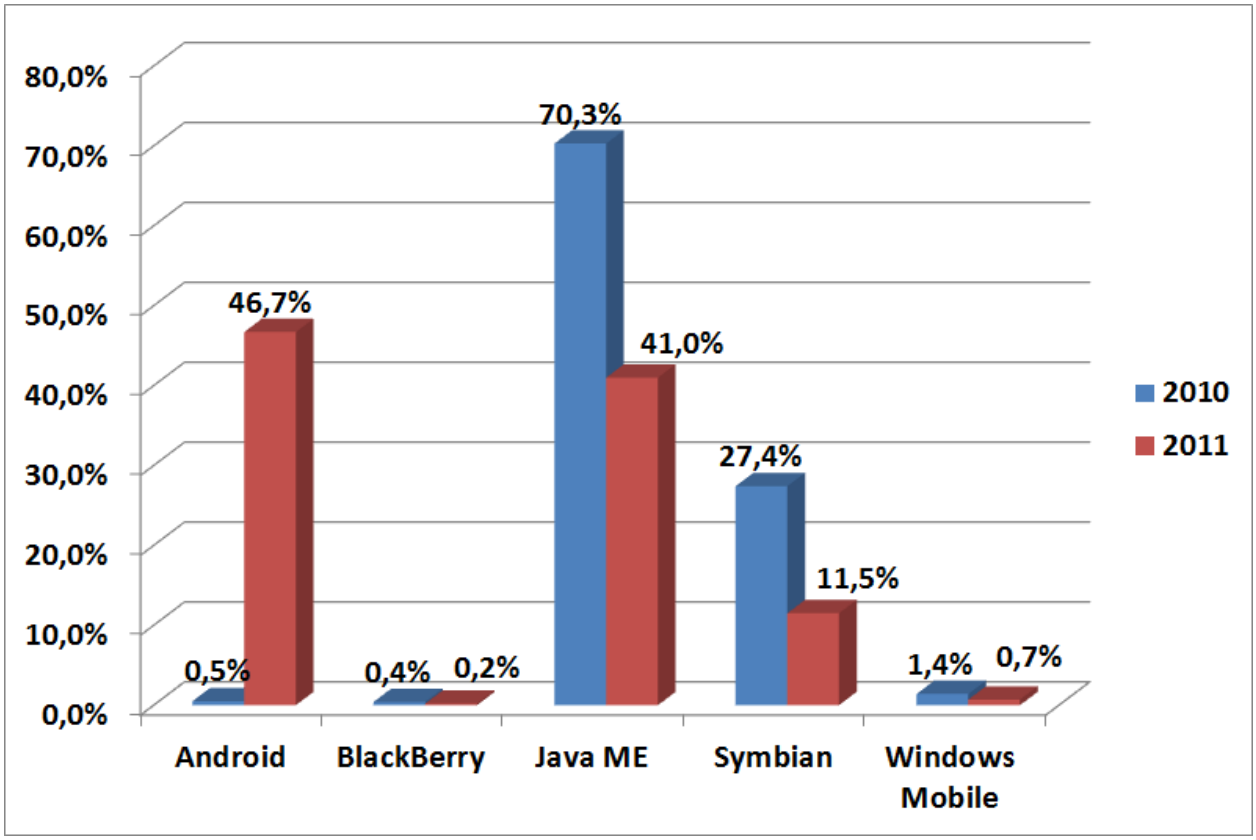

Рисунок 5 Распределение вредоносного ПО по платформам 2010/2011 год

Если же сравнивать общее количество экземпляров, то согласно того же отчета в 2010 году было зарегистрировано 11 138 экземпляров, а на конец 2011 года – 28 472. Рост составил почти 160%.

Таким образом, не сложно сделать вывод о том, что основной рост вредоносного программного обеспечения в ближайшее время придется на вредоносное ПО, рассчитанное на смартфоны и планшеты под управлением ОС Android.

Вместе с тем стоит отметить, что основным направлением вредоносного ПО сегодня (а я уверен что эта тенденция сохранится и в ближайшем будущем) станут не СМС-трояны, а вредоносное ПО, направленное на хищение банковских и персональных данных. Почему? На мой взгляд, на то есть несколько причин:

1. Срок жизни СМС-трояна не велик, а значит суммы, которые можно украсть с его помощью также будут не очень велики, либо нужно заразить уж совсем фантастическое количество смартфонов.
2. Все большее количество смартфонов и планшетов используется при проведении онлайн платежей
3. Все больше планшетов, которые не обладают свойствами смартфонов (не умеют звонить) появляется на рынке, а прости таких устройств СМС-трояны бессильны.

Давайте посмотрим, а что же говорится на эту тему в отчетах ИТ-компаний.

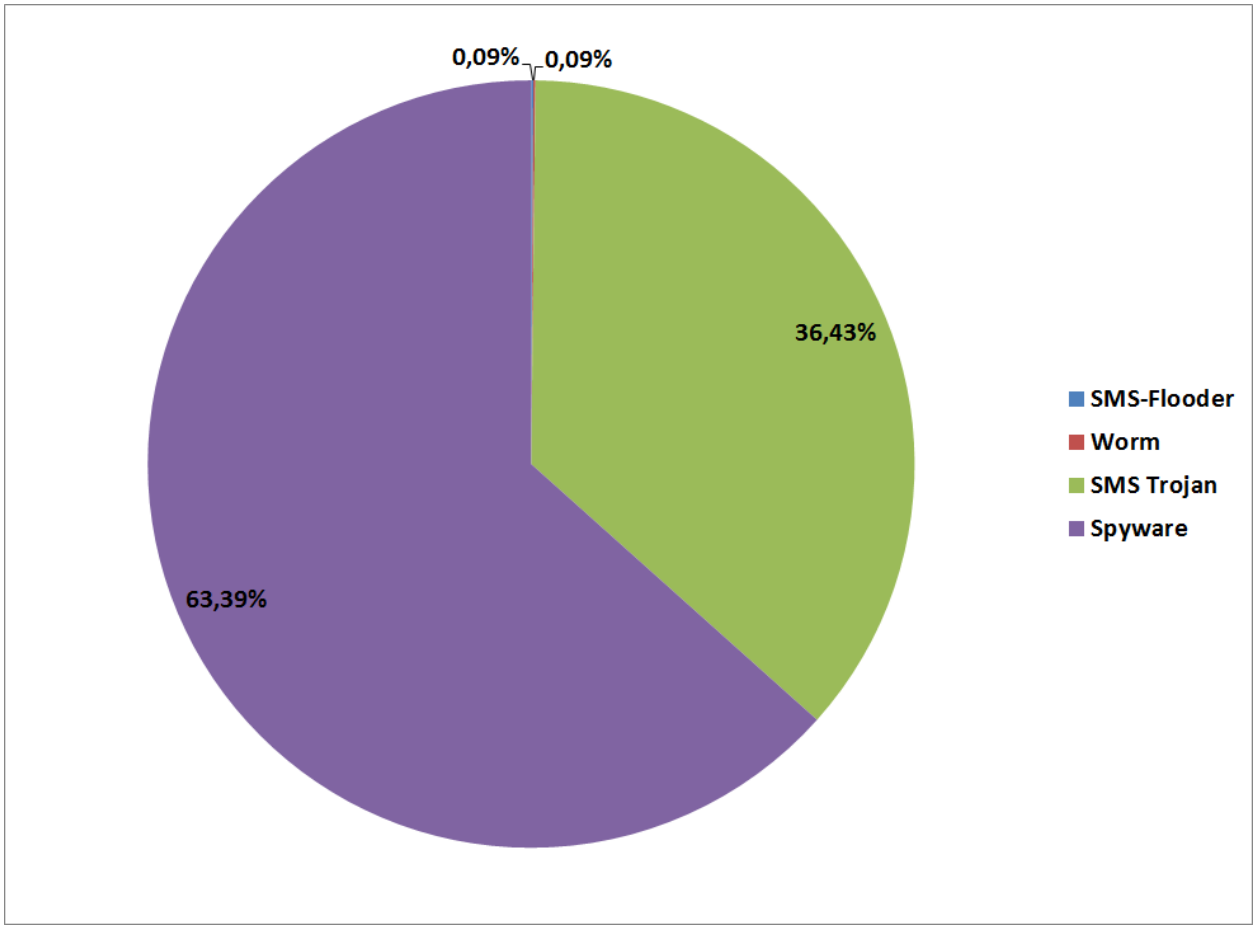

Рисунок 6 Распределение вредоносного ПО по версии Juniper Network

Spyware

Согласно отчета Juniper – Spyware доминировало среди вредоносных программ под ОС Android. Всего было выявлено более 63% такого типа вредоносного ПО. Программы-шпионы прежде всего предназначались для захвата и передачи данных таких как:

- GPS-координаты;
- Тексты, вводимые с клавиатуры;
- Список посещенных web-страниц;
- Другие данные, которые могут быть использованы для получения финансовой выгоды атакующим либо для хищения персональных данных владельцев смартфонов.

SMS Trojan

Согласно отчету Juniper, на данный вид вредоносного ПО приходится порядка 36% всего вредоносного ПО в 2011 году. Данное ПО предназначено для тайной отправки SMS на платные номера, принадлежащие злоумышленнику. После отправки деньги, как правило, не могут быть возвращены, а владельцы таких платных номеров, как правило, анонимны.

Другое

Вместе с тем хотелось бы отметить рост числа вредоносных программ, направленных на хищение информации или денег у жертв, а также рост числа приложений, направленных на хищение персональных данных.

- 30% приложений могут получать информацию я устройства без явного согласия пользователя;
- 14,7% запрашивают разрешения, однако это может привести к телефонным звонкам без согласия (и без оповещения) пользователя
- 6% просят возможность просмотра всех учетных записей на устройстве, в том числе электронной почты и сайтов социальных сетей
- 4,8% могут отправить SMS без уведомления пользователя.

По данным специалистов «Лаборатории Касперского» среди обнаруженных вредоносных программ лидировали SMS Trojan, однако их доля падает и по итогам 2011 составила 36.6% Второе место Backdoors (позволяют удаленно контролировать устройство). Данный тип вредоносного ПО практически не использовался в 2010 году, практически подавляющее число программ такого типа ориентировано на ОС Android. Всего их число составило 24,18%. На третьем месте Spyware, предназначенные для хищения персональной информации и/или данных о зараженном мобильном устройстве(20,61%). Остальные типы поведения заняли 18,62%

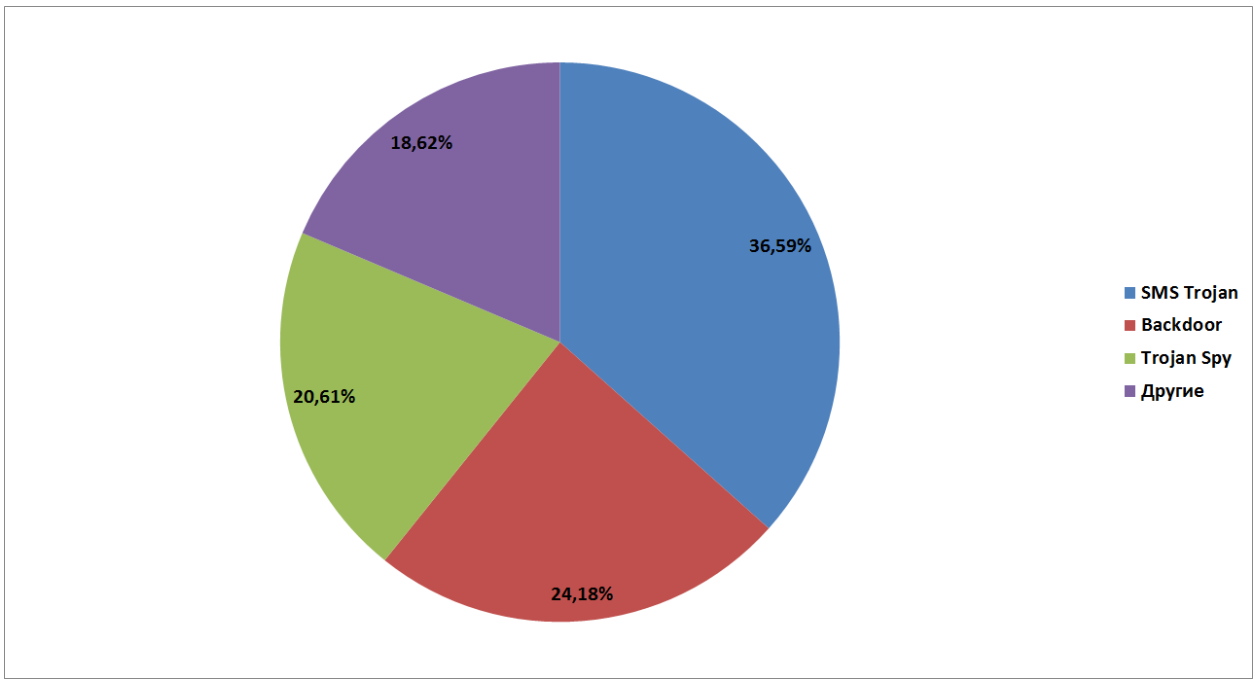

Рисунок 7 Распределение по поведениям мобильных вредоносных программ по итогам 2011г.

Android под прицелом

Другим весьма тревожным звонком, прозвучавшим в прошлом году стало то, что платформа J2ME перестала быть основной целью для вирусописателей. Причина в принципе очевидна – значительный рост популярности смартфонов под управлением ОС Android. В 2004-2006 ОС Symbian лидировала по популярности у вирусописателей. Однако позже ее вытеснила J2ME. Так как под управлением данной ОС работало куда больше мобильных устройств. Сегодня самой популярной ОС является Android, что несомненно сказывается на распределении вредоносного ПО.

Стремительный рост количества угроз для Android был зафиксирован во втором полугодии 2011 года. Примерно в середине лета количество вредоносного ПО для Android обогнало количество вредоносного ПО для Symbian, ну а осенью осталась позади и платформа J2ME. К концу года Android окончательно закрепился на позиции «любимой» платформы мобильных вирусописателей.

Все обнаруженные «Лабораторией Касперского» вредоносные программы для ОС Android можно разделить на две большие группы согласно поставленных задач:

- деньги или информацию (контакты, историю звонков, SMS-сообщения, GPS-координаты, фотографии и прочее).
- контролировать устройство (в результате заражения злоумышленник сможет удаленно осуществлять практически любые действия с зараженного устройства).

Вредоносное ПО в Google Play

Впервые вредоносное ПО зарегистрировано в Google Play (тогда еще Android Market) в начале марта 201 года, после чего вредоносное ПО появляется в онлайн магазине с завидной регулярностью.

Этому способствовали следующие факторы:

- Популярность Android;
- Простота разработки ПО;
- Возможность распространения через официальный источник;
- Неэффективный анализ новых приложений на предмет наличия вредоносного ПО.

Как результат - вредоносное ПО распространяется через Google Play на протяжении недель и даже месяцев.

Вывод

Думаю, читателей данной статьи удивило, а может даже и возмутило отсутствие в статье информации по телефонам под управлением iOS или Windows Phone 7 или Symbian. Но на самом деле основной упор сделан на ОС Android ввиду того, что основное внимание злоумышленников направлено именно на эту платформу.

Основной целью статьи было показать пользователям, что сегодня к выбору смартфона нужно подходить не только и не столько с точки зрения внешнего вида, объема памяти или количества мегапикселей в фотокамере. Сегодня уже пора думать о безопасности информации, хранимой на устройстве и более того, о вашей личной безопасности!

Очень хотелось бы, чтобы пользователи понимали, чем они рискуют и заранее задумывались, что важнее, дополнительные «рюшечки» в оформлении или ваша личная безопасность и сохранность ваших денег!

Думайте, уважаемые пользователи, думайте!!!