МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
ФАКУЛЬТЕТ РАДИОТЕХНИКИ И КИБЕРНЕТИКИ

ЭССЕ ПО КУРСУ: ЗАЩИТА ИНФОРМАЦИИ

Вирусы и антивирусы в мобильных устройствах

Выполнил студент 314 группы
Доронина Светлана

2007

1 Введение

Первый вирус для смартфонов был создан в июне 2004 года. Вирус «называет себя» Cabir, функционирует на базе операционной системы Symbian и распространяется при помощи технологии беспроводной передачи данных Bluetooth. Автором вируса являлась международная группа вирусописателей 29A. Эта группа ставила своей целью создание новых, концептуальных вирусов для нестандартных операционных систем и приложений. Ее участники как бы демонстрировали антивирусным компаниям и другим вирусописателям, что существуют новые направления атаки. В этот раз целью было создание вредоносной программы для смартфонов. Для размножения червя был выбран нестандартный способ. Обычно черви распространяются по электронной почте, однако червь Cabir распространяется при помощи Bluetooth.

В качестве среды функционирования червя используется операционная система Symbian. На сегодняшний день данная операционная система является лидером среди ОС мобильных телефонов. Именно поэтому большинство мобильных вирусов написано именно под операционную систему Symbian. К тому же Symbian содержит несколько серьезных ошибок «by design» в системе работы с файлами и сервисами, что также создает большое поле деятельности для вирусописателей. В случае с Cabir ошибки не были использованы, однако в большинстве современных троянцев для смартфонов они использованы в полной мере.

Оригинальный экземпляр Worm.SymbOS.Cabir был разослан в антивирусные компании по поручению самого автора, однако позже исходные коды червя появились в интернете, что повлекло за собой создание большого количества новых модификаций данной вредоносной программы. Фактически, после публикации исходных кодов Cabir начал самостоятельно «бродить» по мобильным телефонам во всем мире.

2 Существующие виды мобильных вирусов

В настоящее время выделяют три основных вида мобильных вирусов:

- черви, распространяющиеся через специфические для смартфонов протоколы и сервисы;
- троянцы-вандалы, использующие ошибки Symbian для установки в систему;
- троянцы, ориентированные на нанесение финансового ущерба пользователю.

Современные мобильные вирусы умеют практически все то же самое, что и компьютерные вирусы:

- Распространяются через Bluetooth, MMS
- Посылают SMS
- Заражают файлы
- Дают возможность удаленно управлять смартфоном
- Изменяют иконки, системные приложения
- Устанавливают «ложные» или некорректные шрифты, приложения
- Борются с антивирусами
- Устанавливают другие вредоносные программы
- Блокируют работу карт памяти
- Воруют информацию

Как подчеркивают специалисты «лаборатории Касперского», мобильные вирусы прошли тот же путь развития, что и компьютерные вирусы, но в 10 раз быстрее: за 2 года вместо 20! Таким образом, мобильные вирусы - одна из самых динамичных и быстро развивающихся областей вредоносных программ, причем очевидно, что до пика своего

развития ей еще очень далеко. Существует огромное многообразие форм и видов вирусов. В настоящий момент «Лаборатория Касперского» учитывает 31 семейство вредоносных программ для мобильных телефонов.

Однако, несмотря на обилие мобильных семейств, существует крайне ограниченное число действительно оригинальных вирусов, выделяют три основных мобильных вируса, которые, по мнению специалистов, и послужили основой для дальнейшего развития мобильных вирусов. Это:

- Cabir
- Comwar
- Skuller.gen

2.1 Cabir

Cabir не только породил несколько своих вариантов, отличающихся лишь именами файлов и составом своего инсталляционного sis-файла. На основе этого червя были созданы такие самостоятельные и на первый взгляд непохожие друг на друга семейства, как StealWar, Lasco и Pbstealer.

2.2 Lasco

Lasco стал первым вирусом, который помимо функций червя обладает способностью заражения файлов на телефоне. К счастью, идея заражения файлов не получила дальнейшего распространения среди вирусописателей, даже несмотря на то, что автор этого вируса опубликовал исходные коды своего творения на собственном сайте.

2.3 Pbstealer

Pbstealer - первый троянец-шпион для Symbian От Cabir была взята все та же функция рассылки файлов через Bluetooth. Однако авторы троянца внесли одно, но значительное изменение в оригинальный код. Троянец ищет адресную книгу телефона и отсылает данные из этой книги через Bluetooth на первое из найденных устройств. Отсюда и его название Pbstealer — «Phonebook Stealer». До сих пор для кражи подобной информации злоумышленники использовали различные уязвимости в самом протоколе Bluetooth, например BlueSnarf. С появлением этого троянца возможности преступников значительно расширились.

И, конечно же, Cabir стал излюбленным «носителем» для всевозможных других троянцев. Более половины различных Skuller, Appdisabler, Locknut, Cardtrap и прочих «вандалов» содержат в себе Cabir, измененный так, чтобы он рассылал не только себя, но и весь троянский «пакет».

2.4 Comwar

Вторым этапом в развитии мобильных вирусов стал Comwar. Это первый червь, распространяющийся через MMS. Как и Cabir, он способен рассылаться через Bluetooth, однако именно MMS является его основным способом размножения, и, если учитывать его масштаб, наиболее опасным из всех возможных.

Радиус действия Bluetooth составляет 10-15 метров, и заражению могут быть подвержены другие устройства только в этих пределах. MMS границ не имеет и способен мгновенно пересылаться на телефоны даже в другие страны.

В настоящий момент известно 7 модификаций данного червя, из которых четыре являются «авторскими».

В варианте Comwar.g автор червя впервые применил возможность заражения файлов. Червь ищет на телефоне другие sis-файлы и дописывает себя в них. Таким образом, он получает еще один способ распространения, помимо традиционных MMS и Bluetooth.

Пока еще Comwar не стал «родителем» множества других семейств, и это напрямую связано с недоступностью его исходного кода. Его используют в качестве «носителя» для других троянских программ, точно так же, как и Cabir. Пожалуй, единственной из всех вредоносных программ, использующих Comwar в своих целях, на статус родоначальника самостоятельного семейства претендует только StealWar. Это червь, в котором объединены Cabir, Comwar и троянец Pbstealer. Подобный «комбайн» имеет повышенную опасность и способность к размножению.

Однако сам принцип MMS-рассылок неминуемо станет превалирующим среди других способов размножения мобильных вирусов.

Говоря о том, что еще привнес Comwar в мобильные вирусы, следует отметить, что именно в нем (вариант .c) впервые была применена технология, которую можно считать руткитом. Червь скрывает себя в списке процессов и не виден в стандартном списке запущенных приложений. Это возможно из-за того, что он устанавливает тип своего процесса как «системный». Конечно, при помощи других программ, позволяющих просматривать списки запущенных процессов, он может быть легко обнаружен. В настоящее время подобный способ маскировки используют и некоторые другие вредоносные программы для Symbian.

2.5 Skuller

Skuller представляет самое многочисленное семейство мобильных троянцев — на 1 сентября 2006 года лабораторией Касперского классифицирован 31 вариант. Создать подобного троянца под силу любому человеку, умеющему пользоваться утилитой для создания sis-файлов. Все остальное сделают уязвимости Symbian: возможность перезаписи любых файлов, включая системные, и крайняя неустойчивость системы при ее столкновении с неожиданными (нестандартными для данного дистрибутива либо поврежденными) файлами.

В основе большинства вариантов Skuller лежат два файла. Их называют Skuller.gen, и именно они имеют особенности, отличающие это семейство от похожих по функционалу (например, Doombot или Skudoo):

- файл с именем подменяемого приложения и расширением «aif», размером 1601 байт. Это файл-иконка с изображением черепа. Файл также содержит в себе текстовую строку «↑Skulls↑Skulls»;
- файл с именем подменяемого приложения и расширением «app», размером 4796 байт. Это приложение EPOC, файл-«пустышка», который не содержит никакого функционала.

Троянец Skuller.a

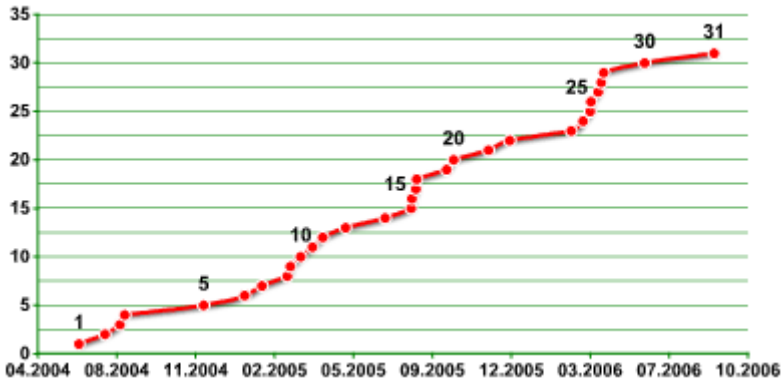
В данной таблице можно увидеть основные черты каждого из этих семейств.

Название	Дата	ОС	Функционал	Технологическая основа	Количество вариантов
Worm.SymbOS.Cabir	Июнь 2004	Symbian	Распространение по Bluetooth	Bluetooth	15
Virus.WinCE.Duts	Июль 2004	Windows CE	Заражение файлов	(File API)	1
Backdoor.WinCE.Brador	Август 2004	Windows CE	Предоставление удаленного доступа по сети	(Network API)	2
Trojan.SymbOS.Mosquit	Август 2004	Symbian	Рассылка SMS	SMS	1
Trojan.SymbOS.Skuller	Ноябрь 2004	Symbian	Подмена файлов иконок, подмена системных приложений	Уязвимость ОС	31
Worm.SymbOS.Lasco	Январь 2005	Symbian	Распространение по Bluetooth, заражение файлов	Bluetooth, File API	1
Trojan.SymbOS.Locknut	Февраль 2005	Symbian	Инсталляция поврежденных приложений	Уязвимость ОС	2
Trojan.SymbOS.Dampig	Март 2005	Symbian	Подмена системных приложений	Уязвимость ОС	1
Worm.SymbOS.ComWar	Март 2005	Symbian	Распространение по Bluetooth и MMS, заражение файлов	Bluetooth, MMS, File API	7
Trojan.SymbOS.Drever	Март 2005	Symbian	Подмена загрузчиков приложений-антивирусов	Уязвимость ОС	4
Trojan.SymbOS.Fontal	Апрель 2005	Symbian	Подмена файлов шрифтов	Уязвимость ОС	8
Trojan.SymbOS.Hobble	Апрель 2005	Symbian	Подмена системных приложений	Уязвимость ОС	1
Trojan.SymbOS.Appdisabler	Май 2005	Symbian	Подмена	Уязвимость ОС	6

			системных приложений		
Trojan.SymbOS.Doombot	Июнь 2005	Symbian	Подмена системных приложений, инсталляция Comwar	Уязвимость ОС	17
Trojan.SymbOS.Blankfont	Июль 2005	Symbian	Подмена файлов шрифтов	Уязвимость ОС	1
Trojan.SymbOS.Skudoo	Август 2005	Symbian	Инсталляция поврежденных приложений, установка Cabir, Skuller, Doombor	Уязвимость ОС	3
Trojan.SymbOS.Singlejump	Август 2005	Symbian	Отключение системных функций, подмена иконок	Уязвимость ОС	5
Trojan.SymbOS.Bootton	Август 2005	Symbian	Инсталляция поврежденных приложений, установка Cabir	Уязвимость ОС	2
Trojan.SymbOS.Cardtrap	Сентябрь 2005	Symbian	Удаление файлов антивирусов, подмена системных приложений, установка Win32 Malware на карту памяти	Уязвимость ОС	26
Trojan.SymbOS.Cardblock	Октябрь 2005	Symbian	Блокировка работы карты памяти, удаление каталогов	Уязвимость ОС, File API	1
Trojan.SymbOS.Pbstealer	Ноябрь 2005	Symbian	Кража информации	Bluetooth, File API	5
Trojan-Dropper.SymbOS.Agent	Декабрь 2005	Symbian	Установка других вредоносных программ	Уязвимость ОС	3
Trojan-SMS.J2ME.RedBrowser	Февраль 2006	J2ME	Рассылка SMS	Java, SMS	2
Worm.MSIL.Cxover	Март 2006	Windows Mobile/ .NET	Удаление файлов, копирование своего тела на другие устройства	File (API), NetWork (API)	1
Worm.SymbOS.StealWar	Март 2006	Symbian	Кража информации, распространение по Bluetooth и MMS	Bluetooth, MMS, File (API)	5
Email-Worm.MSIL.Letum	Март 2006	Windows Mobile/ .NET	Распространение по электронной почте	Email, File (API)	3
Trojan-Spy.SymbOS.Flexispy	Апрель 2006	Symbian	Кража информации	—	2

Trojan.SymbOS.Rommwar	Апрель 2006	Symbian	Подмена системных приложений	Уязвимость ОС	4
Trojan.SymbOS.Arifat	Апрель 2006	Symbian	—	—	1
Trojan.SymbOS.Romride	Июнь 2006	Symbian	Подмена системных приложений	Уязвимость ОС	8
Worm.SymbOS.Mobler.a	Август 2006	Symbian	Удаление файлов антивирусов, подмена системных приложений, размножение через карту памяти	Уязвимость ОС	1
31 семейство, 170 вариантов					

Полный список известных семейств мобильных вирусов по классификации «Лаборатории Касперского» (по состоянию на 30 августа 2006 года).



Увеличение количества известных семейств мобильных вирусов

3 Средства защиты от мобильных вирусов

В настоящий момент существует несколько программных решений для защиты мобильных устройств от вирусов. В «Лаборатории Касперского» разработаны версии антивируса для Windows CE (Pocket PC, Windows Mobile), Symbian (6, 7, 8 версий и UIQ), а также для Palm OS. Подобные продукты предлагаются как известными производителями PC-антивирусов (TrendMicro, Network Associates, F-Secure), так и молодыми компаниями, специализирующимися непосредственно на разработке мобильных антивирусных решений (Airscanner, Simworks).

В случае с MMS-червями для мобильных телефонов оптимальной представляется защита на стороне оператора, при которой весь MMS-трафик проходит через интернет-сервер с установленным на нем антивирусным продуктом.