УДК:004.491.22:004.45

СКЛЕИВАНИЕ ВИРУСОВ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Куликов П.А., Соловьев А.С., Крюков С.И.
КГТУ им. И. Раззаков

В статье разбирается вариант "склеивания" злоумышленником компьютерного вируса с интернет браузером Google Chrome для получения доступа к компьютеру "жертвы".

Добавлением вирусов в программное обеспечение пользуются многие злоумышленники, под привычной установкой программ мы зачастую не замечаем, что же происходит по ту сторону установки. На данный момент злоумышленник может «склеить» вирус с любым программным обеспечением, последствия могут быть разными как простая шутка, так и кража личных данных и выведение компьютера из строя. И так, «склеивание» вирусов и программ осуществляется многими способами, рассмотрим самый обычный способ. Для начала поставим цель: кража информации из директории «Мои документы». Изначально у нас есть вирус и определенное программное обеспечение, например всем известный браузер Google Chrome. Чтобы спрятать вирус от антивирусов используются разные компиляторы которые придадут нашему вирусу расширение как и у обычной программы, но вирус по сути своей не будет являться программой а всего лишь её установщиком. Дело в том что на данный момент во многих антивирусных программах используется функция блокировки дочернего запуска программ или антивирус выдаёт оповещение о том что была запущенна неизвестная программа. Исходя из вышенаписанного мы создадим свой собственный загрузчик который сначала будет исполнять код вируса, который длится не более пяти секунд а затем начнет установку программы. При этом все действия выполняемые вирусом будут происходить в скрытом режиме и пользователь не увидит, что происходит ему будет показано что устанавливается программа. После установки Google Chrome все запланированные нами операции по копированию информации из папки «Мои документы» будет завершена, но основной проблемой такого метода является размер копируемой информации, так как она может быть разных размеров, для устранения этой проблемы используется архивирование файлов а затем их копирование. Существует еще один вариант по «склеиванию» вируса и программы который осуществляется не подменой установщика программы, а непосредственное заражение самой программы, путём создание дополнительных библиотек самой программы, этот метод в отличие от первого требует знания программирования на языках высокого уровня. На данный момент защиты от такого рода «Хакерских» действий не существует, но есть определенные функции в самой операционной системе windows которые не дадут запуститься этому вредоносному коду. Опыты показали, что при использовании методов операционной системы установка таких приложении блокируется, но слегка переделанный нами код позволяет операционной системе самой его запускать тем самым считая его системным файлом, на который не действуют ограничения. В конечном итоге мы получим информацию которую можно скопировать на флэш карту или отправить по интернету без ведома пользователя. Возможности этого метода не имеют граней, они использую все функции операционной системы, позволяя тем самым нагружать компьютер до его полного отказа в работе, открывать средства удаленного доступа и администрирования о котором мы поговорим далее. Рассмотрев отрицательные функции данного вредоносного кода перейдем к его положительным возможностям. Как говорилось выше, возможности этого вируса неограниченны и благодаря этому мы создали свой код который отключает такие функции как удаленный реестр (с помощью которого производятся атаки на сервера крупных компаний через их клиентов), включает и отключает брандмауэр (с помощью которого производится фильтрация входящего и исходящего трафика) эти две функции в руках злоумышленников являются очень эффективным средством для взлома сайтов компаний, зомбирования компьютеров для объединения их в так называемую бот сеть с целью проведения Ddos атак. Помимо закрытия уязвимостей в операционных системах к положительным функциям можно отнести и заведомо-ложное инфицирование мелких вирусов таких как компьютерные черви.

Возьмём например распространенный вирус, который скрывает папки на flash карте и заражает компьютер и все флэшки подключаемые к нему. Принцип действия этого вируса заключается в копировании самого вируса в автозагрузку операционной системы, тем самым вирус автоматически запускается при загрузке операционной системы. Копирование на flash карту происходит автоматически и запуск самого вируса непосредственно на съемном носителе. Антивирусные программы не реагируют на данный вирус, но при их регулярном обновлении антивирусы все-таки находят вирус и удаляют его. Принцип работы этого вируса очень хорошо продуман. Разобрав данный вирус мы нашли в нем уязвимость которая может изменить сам вредоносный код и вместо того чтобы скрывать папки, он просто на просто распространяется по flash картам но не скрывает папки. За основу этой идеи был взят обычный метод лечения человеческих вирусных заболеваний, штамм вируса инфицируется и вирус теряет своё «нехорошее» значение и используется как антивирус «лекарство».