УДК 004

РУТКИТЫ И ЗАЩИТА ОТ НИХ

Е.В. Вишнякова, А.Р. Орлова, студентки 2 курса экономического факультета
Руководитель – Е.А. Ильдутов, ассистент
ФГБОУ ВПО «Ульяновская государственная сельскохозяйственная академия»

Ключевые слова: *рутките, вирусы, утилиты, суперпользователь, компьютер*

Статья посвящена знакомству с вредоносной программой – рутките и методами борьбы с ним, которая скрывает следы присутствия злоумышленника или вредоносного кода в операционной системе. При изучении данного вируса было установлено, что рутките можно обнаружить только с помощью специализированных программ Sophos Anti-Rootkit, Rootkit Buster.

В нашу уже почти кибернетическую эпоху, при столь обширном и массовом распространении компьютерной техники, и общей автоматизации, Мы наблюдаем удручающую картину: несмотря на то, что Антивирусные программы, и программы защиты постоянно обновляются, уже даже ежедневно, наши с Вами компьютеры продолжают атаковать и пытаться заразить вредоносные программы из интернета. Особенно учитывая увеличение в геометрических степенях скорости доступа в интернет.

Не самую последнюю роль в этом кибер - безобразии играют рутките. Это те вредоносные коды микропрограмм, ввиду популярности которых и написана данная статья, несущая собой цель – познакомить Вас с этими программами.

Первый признак, на который стоит обращать внимание: компьютер ведет себя как-то не так. В автозагрузке чисто, процессы в порядке, антивирус ничего не находит, однако у Вас есть подозрение, что система не в порядке. В лучшем случае, Вы видите присутствие вирусов воочию, в худшем – визуально ничего не заметите, кроме странного поведения, либо подтормаживания. При всем этом подозрительном спокойствии, Вы и не заметите, как с вашего ПК рассылается спам, крадутся пароли от сайтов или почты, происходят атаки на сайты или делаются другие,

не особо приятные другим пользователям сети интернет вещи.

Как же получается так, что вирус не опознается антивирусной программой, и спокойно находится в операционной системе? В некоторых случаях это вредоносные программы особого рода – руткиты.

Итак, руткит (rootkit) – это программа (набор программ) для скрытия следов присутствия злоумышленника или вредоносного кода в операционной системе. Установив руткит на ваш компьютер, хакер получает над ним полный контроль, может удаленно управлять компьютером и загружать на него другие вредоносные программы. Он пользуется различными командами, утилитами.

Более того, основная задача руткита – не допустить обнаружения действий вирусов хозяином компьютера, скрыть от пользователя присутствие хакера и изменений в системе. Руткит прячет от ваших глаз вредоносные процессы, системные службы, драйвера, сетевые соединения, ключи реестра и записи автозагрузки, модули, папки, файлы и, конечно же, прячет сам себя. В общем, ситуация не приятная, и ваш компьютер при этом могут использовать в любых не добрых целях.

Сам термин «руткит» берет свое начало из операционных систем семейства Unix. Именно для них были написаны руткиты, которые хакеры устанавливали на компьютеры сразу после получения прав суперпользователя (root-а, отсюда и название rootkit). Суперпользователь в Unix – это то же самое, что Администратор в Windows. Руткиты были необходимы, так как все действия в Unix системах, а ныне в современном Linux, выполнялись не от имени обычного пользователя, не имеющего прав на какое-либо критическое изменение параметров системы, а только от имени суперадминистратора - ROOT. Таким образом, руткит позволял злоумышленнику полностью завладеть ОС и полноправно властвовать над системой.

В конце прошлого века появились руткиты и под операционную систему Windows. Поскольку на момент их адаптации к среде WINDOWS ни один антивирус их не опознавал, перед руткитами открывалось много перспектив. Однако в скором времени они были обнаружены и крупные антивирусные компании и производители систем защиты начали добавлять функционал по обнаружению кодов руткитов в свои продукты.

На сегодняшний день существует множество антивирусов и специализированных программ, позволяющих обнаружить и нейтрализовать руткиты.

В зависимости от того, с какой областью памяти работают руткиты, их можно подразделить на следующие виды:

• системы, работающие на уровне ядра (Kernel Level, или KLT);

• системы, функционирующие на пользовательском уровне (User Level).

Первый известный руткит для системы Windows, NT Rootkit, был написан в 1999 году экспертом в области безопасности Грегом Хоглундом в виде драйвера уровня ядра. Он скрывал все файлы и процессы, в имени которых встречалось сочетание _root, перехватывал информацию, набираемую на клавиатуре, и использовал другие способы маскировки.

Далее рассмотрим наиболее популярные и эффективные утилиты для поиска и деактивации данного типа вирусов.

Sophos Anti-Rootkit

Небольшая утилита, умеющая бороться с руткитами, которая работает, в операционных системах Windows XP и Vista. SophosAnti-Rootkit сканирует реестр и критические каталоги системы и выявляет скрытые объекты, то есть следы творчества руткитов.

Программа обычным образом устанавливается на компьютер и обладает интуитивно понятным интерфейсом. Прежде всего, вам необходимо задать объекты, которые должна искать и обнаружить утилита.

В описании найденных объектов программа предложит вам свои рекомендации на счет их удаления. Для этого следует выделить найденный объект и удалить. Sophos Anti-Rootkit предупредит о возможных проблемах с операционной системой после удаления программ, которые не приносят никакого вреда системе.

Rootkit Buster

Также бесплатная утилита для извлечения руткитов из системы, работающая без предварительной установки в Windows XP.

Для того чтобы начать сканирование просто распакуйте архив и запустите файл Rootkit Buster.exe, затем в окне утилиты нажмите кнопку «Scan Now». При этом Rootkit Buster проверит загрузочную запись MBR и скрытые файлы, реестр, процессы и драйвера.

По завершении сканирования вы увидите список найденных объектов. Любой из них можно выделить и удалить нажатием кнопки «Delete Selected Items».

Мы рассмотрели специализированные утилиты, которые помогают выявлять и бороться с вирусами типа «руткит». В заключении стоит предупредить, о том, что даже используя описанные программы нет 100% гарантий полной защиты, как впрочем, и использование любых других антивирусных программ. Следует признать, что обезопасить компьютер от вирусов возможно, соблюдая так сказать гигиену в опе-

рационной системе, и программах используемых на компьютере. Стоит чаще делать резервные копии данных, если они для вас особо важны. При постоянной работе в интернет обязательно иметь установленную антивирусную программу с ежедневно обновляемыми антивирусными базами. И не переходить на незнакомые ссылки в интернете, чтобы избежать случайного заражения трояном, руткитом.

Библиографический список:

1 Rootkits под Windows. Теория и практика программирования «шапок-невидимок», позволяющих скрывать от системы данные, процессы, сетевые соединения, Д. Колисниченко, Наука и техника, 2006 г., 320 стр.

2 Руткиты. Внедрение в Ядро Windows, Г. Хоглунд, Дж. Батлер, 2006

3 http://www.cybersecurity.ru/manuals/crypto/law/5734.html

4 http://www.xakep.ru/post/40549/default.asp

ROOTKIT AND PROTECTION AGAINST THEM

E.V.Vishnyakova, A.R.Orlova, student 2 courses of economics department
The head – E.A.Ildutov, the assistant
FGBOU VPO «Ulyanovsk State Agricultural Academy of a name of P.A.Stolypin»

Keywords: rootkit, viruses, utilities, superuser, computer

Article is devoted to acquaintance to the harmful program – rootkit and methods of fight against it which hides traces of presence of the malefactor or a malicious code in an operating system. When studying this virus it was established that rootkit it is possible to find only by means of the specialized programs Sophos Anti-Rootkit, Rootkit Buster.