УДК 517.929

© Рыжов Б.С., Зорин Э.Ф.
Ryzhov B., Zorin E.

МЕТОДИКА ИСКЛЮЧЕНИЯ ФАЙЛОВ ВИРУСНОЙ ПРОГРАММЫ С ФУНКЦИЯМИ УДАЛЕННОГО ДОСТУПА, МАСКИРУЮЩЕЙСЯ ПОД АНТИВИРУСНОЕ СРЕДСТВО ЗАЩИТЫ

TECHNIQUE OF ELIMINATION OF FILES OF THE VIRUS PROGRAM WITH FUNCTIONS OF THE REMOTE ACCESS, MASKING UNDER THE ANTI-VIRUS SECURITY FEATURE

Аннотация. *В статье рассматривается методика исключения файлов вирусного кода из операционной системы и даны рекомендации для предупреждения подобных нештатных ситуаций в процессе эксплуатации автоматизированного рабочего места.*

Annotation. *In paper the technique of elimination of files of the virus code from an operating system is considered, and recommendations for the warning of similar supernumerary situations of while in service automated workplace are made.*

Ключевые слова. *Автоматизированное рабочее место, вирусный код, программное обеспечение, поиск, удаление вируса.*

Key words. *Workstation viral code, software, search, virus removal.*

Актуальность статьи вызвана необходимостью поддержания автоматизированного рабочего места (АРМ) специального назначения, размещенного в составе критически важного информационного сегмента (КВИС) и выполняющего задачу по сбору и обработке информации, в работоспособном состоянии.

При передаче информации в территориально-распределенной сети вследствие использования разнородного программно-аппаратного обеспечения существенно возрастает возможность несанкционированного доступа (НСД) потенциальным нарушителем к информации. Одним из актуальных способов осуществления НСД является заражение папок и файлов, находящихся в открытом доступе сети, компьютерными вирусами с функциями удаленного доступа.

Использование таких функций потенциальным нарушителем позволяет получать все необходимые данные с требуемого компьютера по технологии удаленного доступа. Наибольшую опасность с точки зрения заражения работоспособности АРМ представляет вредоносный код, замаскированный под «оригинальный» антивирус. Заражение таким вирусом приводит не только к утечке данных с компьютера, но и к потере работоспособности АРМ. Последнее в свою очередь влияет на КВИС и может привести к невыполнению поставленной задачи и в целом к неприемлемому ущербу [1–4].

На основании вышеизложенного справедлива следующая постановка задачи. Дано:

1. АРМ оператора с операционной системой (ОС) «Windows XP», зараженный ПО, замаскированным под легальное антивирусное ПО. На АРМ присутствует: подключение к глобальной информационной системе (ГИС) «Интернет», антивирусное ПО (Kaspesky WorkStation 6.0), интернет браузер (например, Opera.exe).

2. Дополнительный АРМ с выходом в ГИС «Интернет».

3. ПО для поиска и удаления вирусов с функциями удаленного доступа.

4. Внешний носитель, с которого можно осуществить загрузку (LIVE-CD).

5. Установочный диск с ОС «Windows XP».

Требуется: восстановить работоспособность АРМ при условии полного сохранения данных.

Зорин Эдуард Фёдорович – кандидат технических наук, старший научный сотрудник, ведущий научный сотрудник, 4 ЦНИИ Минобороны России, тел. (495) 515-64-28;
Рыжов Борис Сергеевич – кандидат технических наук, старший научный сотрудник, 4 ЦНИИ Минобороны России, тел. (495) 544-26-24;

Zorin Eduard – Cnd.Sci.Tech., the senior scientific employee, the senior scientific employee, 4 Central Scientific Research Institute Ministry of Defence of Russia, tel. (495) 515-64-28;
Ryzhov Boris – Cnd.Sci.Tech., high scientific employee, 4 Central Scientific Research Institute Ministry of Defence of Russia, tel. (495) 544-26-24.

Решение поставленной задачи предполагает выполнение следующего алгоритма (см. рисунок):

Порядок выполнения мероприятий в методике исключения файлов вирусной программы с функциями удаленного доступа, маскирующейся под антивирусное средство защиты может быть представлен в виде следующих операций:

1. Проверка содержимого системного раздела на наличие и содержание системных файлов и метафайлов с использованием другой ОС. Например, в «Windows XP» содержатся системные файлы: boot.ini, ntldr, bootfont. bin, ntdetect.com и метафайлы: $MFT, $MFTMirr, $LogFile, $Volume, $AttDef, $Bitmap, $Boot, $Badclus, $Secure, Upcase, $Extend.

2. Удаление подозрительных файлов, не имеющих отношения к ОС (предварительно необходимо сохранить системный раздел на другой раздел жесткого диска).

3. Запуск ОС на компьютере в штатном режиме.

4. При условии, если операции 1–2 дали приемлемый результат требуется выполнить операцию 5, в противном случае выполняется пункт 6.

5. Вывод сообщения о том, что файлы вирусной программы с функцией удаленного доступа исключены из ОС.

6. Запуск интернет браузера и ввод ссылки //trojan-killer.net/download/explorer.exe. Сохранение приложения на жестком диске.

7. Выполнение загрузки ОС с внешнего носителя (например, LIVE-CD).

8. Установка программного обеспечения для обнаружения и удаления вредоносного кода на жесткий диск исследуемого компьютера через виртуальную операционную систему.

9. Сканирование зараженного компьютера программным обеспечением для обнаружения и удаления вирусов.

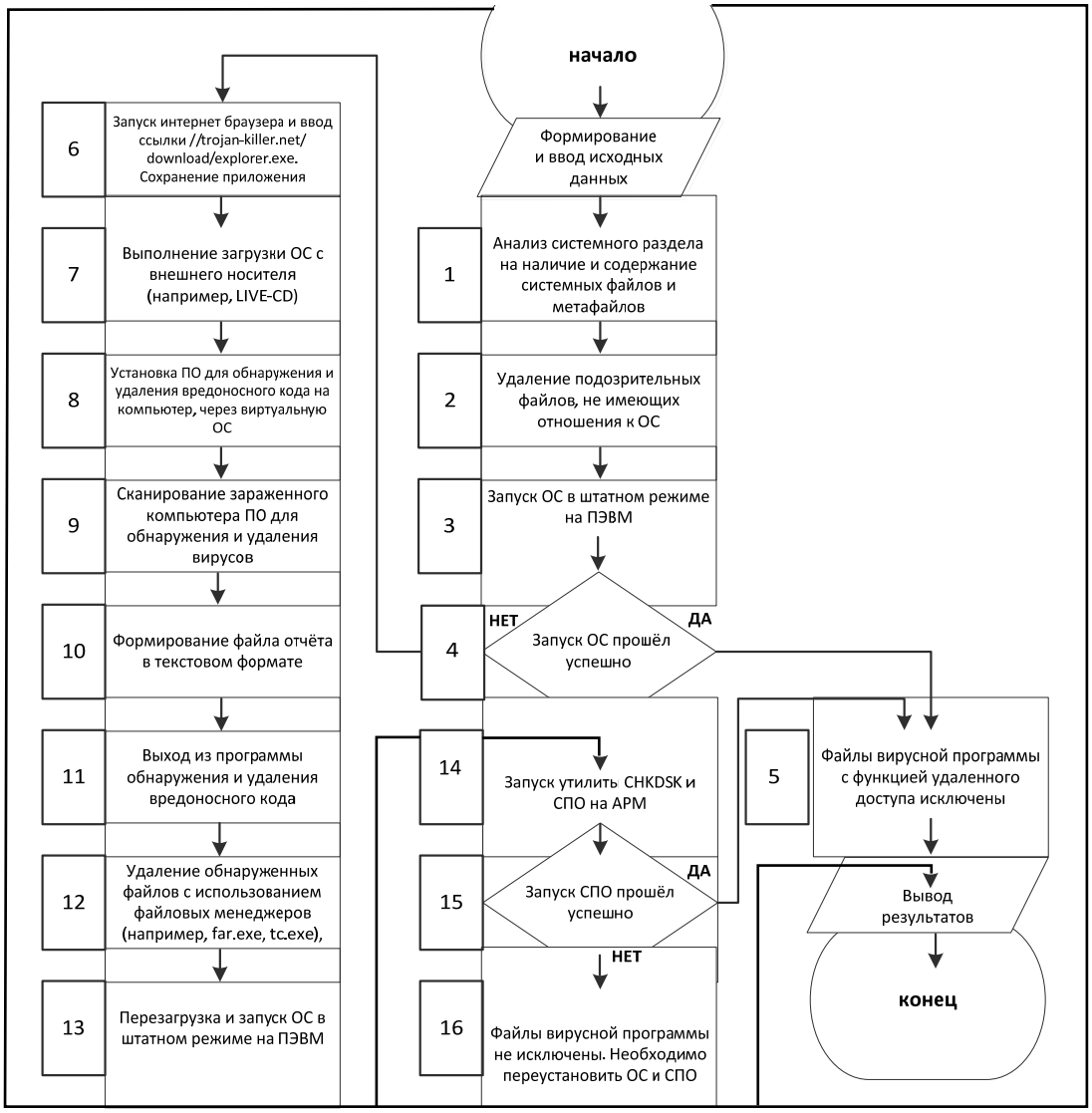

Рис.1. Алгоритм исключения файлов вирусной программы с функциями удаленного доступа, маскирующейся под антивирусное средство защиты

10. Формирование файла отчёта в текстовом формате (или любом другом удобном для чтения).

11. Выход из программы обнаружения и удаления вредоносного кода.

12. Удаление обнаруженных файлов с использованием файловых менеджеров (например, far.exe, tc.exe), которые, как правило, входят в комплект LIVE-CD.

13. Перезагрузка компьютера и запуск его в штатном режиме.

14. Запуск утилиты CHKDSK с ключом r в ОС «Windows XP» и СПО на ПЭВМ.

15. Проверка условия исключения вирусного кода из ОС. В случае штатного запуска СПО требуется выполнить пункт 5, в противном случае выполнить пункт 16.

16. Вывод сообщения о том, что файлы вирусной программы с функцией удаленного доступа не исключены из ОС. Необходимо переустановить ОС и СПО.

Рассмотрим в качестве примера типовую ситуацию поражения АРМ вирусом «Essential Cleaner». При поражении ОС данным вирусом происходит блокирование запуска всех программ, имеющих расширение exe. Операцию по устранению вируса рассмотрим с пункта 6, потому что, как правило, ручное удаление файлов вируса не приводит к положительному результату - это связано с отсутствием знаний у оператора о расположении файлов тела вредоносной программы.

Далее, в соответствии с проводимыми операциями, производится загрузка интернет браузера «opera» по ссылке //trojan-killer.net/download/explorer.exe. В появившемся меню выбирается опция «сохранить». После сохранения файла на диске АРМ необходимо запустить файл «explorer.exe». После запуска данной программы вирусный код будет заблокирован, что позволит оператору выполнить требуемые действия. На следующем этапе устранения вредоносного кода необходимо запустить ПО для поиска и удаления вирусов, например, «GridinSoft Trojan Killer v.2.0.9.4». Запуск данного ПО производится из ОС с внешнего носителя (USB или CD-ROM). По окончании работы «GridinSoft Trojan Killer v.2.0.9.4» необходимо сохранить отчет о обнаруженных вирусах в log файле и закрыть ПО. Это связано с тем, что, незарегистрированная программа не может произвести удаление. Рассмотрим пример log файла программы trojankiller:

GridinSoft Trojan Killer v.2.0.9.4

Report file date: 23.05.2011 19:22:54

Scanning for 376966 virus strains and unwanted programs

Windows version: Microsoft Windows XP (version 5.1)

Username: SYSTEM

Computer name: WINPE

Starting the file scan:

C:\Documents and Settings\All Users\Application Data\oD26400KcDkC26400\oD26400KcDkC26400.exe

C:\System Volume Information_restore{4B09D5B3-D7D9-4C4D-AB03 - 066F7AD3AF01}\RP311\A0115175.exe

C:\System Volume Information_restore{4B09D5B3-D7D9-4C4D-AB03-066F7AD3AF01}\RP311\A0115176.exe

C:\System Volume Information_restore{4B09D5B3-D7D9-4C4D-AB03-066F7AD3AF01}\RP311\A0115177.exe

C:\System Volume Information_restore{4B09D5B3-D7D9-4C4D-AB03-066F7AD3AF01}\RP311\A0115178.

C:\System Volume Information_restore{4B09D5B3-D7D9-4C4D-AB03-066F7AD3AF01}\RP311\A0115179.dll

D:\System Volume Information_restore{1922AB70-70A7-4FFC-A8F4-2D9BD1F8904C}\RP38\A0003520.exe

D:\Программы\Принтеры -SOFT\HP-3500\program files\Hewlett-Packard\3500\AltPdfs\hbr.pdf

Каждый из инфицированных файлов в отчете содержит конкретную информацию, например: General Mal/Packer!se5 – название вирусного файла;

ProdVer: 3, 1, 0, 2 – версия продукта;

FileVer: 3, 1, 0, 2 – версия файла;

Name–: Audio Recorder Pro – название вирусного файла;

Company: EZ SoftMagic

NAC: F64CBC0108D7F691848363A8806658B2:30 – управление доступом в сеть (network access control);

MD5: BC3E0278110B18368AF9F6902EE7E605:398157 – алгоритм шифрования и хэшсумма;

RIC: 575978C4AF32C3AF5E33614BD2B51D8D:22384 – преобразователь канала Ethernet в другие каналы;

EP: 87 25 10 81 56 00 61 94 55 A4 B6 80 FF 13 73 F9 33 C9 FF 13 73 16 33 C0 FF 13 73 1F B6 80 41 B0 10 FF 13 12 C0 73 FA 75 3A AA EB E0 FF 53 08 02 F6 83 D9 01 75 0E FF 53 04 EB 24 AC D1 E8 74 2D 13 – точка входа в программу.

Удаление файлов, обнаруженных ПО «GridinSoft Trojan Killer v.2.0.9.4», производится в ручном режиме с использованием файлового менеджера (например, far.exe, tc.exe).

На следующем этапе необходимо подправить реестр ОС с целью полного удаления следов вируса и невозможности его восстановления. В приведенном примере необходимо изменить следующие ключи реестра ОС «Windows XP»:

HKEY_CLASSES_ROOT\PersonalSS.

DocHostUIHandler

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download «RunInvalidSignatures» = «1»

HKEY_CURRENT_USER\Software\Microsoft\

Windows\CurrentVersion\Internet Settings «ProxyServer» = «http=127.0.0.1»

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run «Essential Cleaner»

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options «Debugger» = «svchost.exe»

После проведения процедуры удаления программного вируса необходимо запустить системную утилиту CHKDSK с ключом r для восстановления поверхности жесткого диска, который мог быть поврежден в результате работы вирусной программы (запуск утилиты осуществляется при помощи установочного диска с ОС «Windows XP»).

На основании вышеизложенного можно сделать выводы, представляющие собой рекомендации оператору при эксплуатации АРМ:

• постоянно проводить резервное копирование файлов как системы, так и данных, необходимых для работы оператора АРМ;

• иметь установленное антивирусное ПО на АРМ (сертифицированное СЗИ);

• постоянно (регулярно) обновлять БД антивирусного ПО;

• не использовать неучтенные (посторонние) носители информации, потому что через них может проникнуть вредоносное ПО на АРМ;

• отключать автоматический запуск программ;

• проверять системный диск на наличие посторонних файлов, они могут служить источниками распространения вирусов;

• иметь в наличии системный диск для запуска с внешнего носителя (LIVE-CD);

• внимательно следить за тем, что именно необходимо скачивать, потому что, как правило, название и расширение файла могут не соответствовать его содержимому или могут быть специально скрыты от оператора злоумышленником.

Вывод: Применение разработанной методики позволяет исключить вредоносный код из применяемого в территориально-распределенной сети специального программного обеспечения и тем самым обеспечить решение целевых задач автоматизированных рабочих мест с требуемыми оперативно-техническими характеристиками.

Литература

1. Петраков А.В. Основы практической защиты информации. - М: Радио и связь, 2001.

2. Герасименко В.А. Защита информации в информационных системах обработки данных - М: Энергоатомиздат, 1994.

3. Гультяев А.К. Восстановление данных. - Спб.: Питер, 2006. – 379 с.

4. Кэрриэ Б. Криминалистический анализ файловых систем. - Спб.: Питер, 2007. – 480 с.

Материал поступил в редакцию 29. 11. 2011 г.