2 Забазпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 681.3.06

ШПИОНСКИЕ ПРОГРАММЫ И НОВЕЙШИЕ МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Николай Красноступ, Денис Кудин
ООО "Центр информационной безопасности"

Аннотация: **Обзор посвящен проблеме защиты от несанкционированных методов перехвата информации пользователей персональных компьютеров с использованием программных и аппаратных средств для скрытого мониторинга нажимаемых клавиш на клавиатуре.**
Summary: **This survey deals with the problem of protection against unauthorized capturing of information from users' PCs by means of hardware devices and software tools for surreptitious monitoring of key strokes.**
Ключевые слова: **Защита информации, кейлоггер, мониторинг, слежение, перехват.**

I Введение

Программное обеспечение и аппаратные устройства, предназначенные для скрытого слежения за деятельностью пользователей персональных компьютеров, получили в последнее время самое широкое распространение. В мировой сети Интернет можно найти много ресурсов и документов, посвященных различным аспектам данной проблемы (юридическим, техническим, политическим и т. д.).

Особую опасность представляют мониторинговые программные продукты и аппаратные устройства, которые могут быть скрытно и несанкционированно (как правило, дистанционно) установлены без ведома владельца (администратора безопасности) автоматизированной системы или без ведома владельца конкретного персонального компьютера. Данная категория мониторинговых продуктов далее в статье будет именоваться как "программы-шпионы" или "продукты-шпионы".

Санкционированные же мониторинговые программные продукты используется администратором безопасности вычислительной системы (службой информационной безопасности предприятия или организации) для обеспечения ее наблюдаемости – "свойства вычислительной системы, позволяющего фиксировать деятельность пользователей и процессов, использование пассивных объектов, а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и/или обеспечения ответственности за определенные действия" [1]. Именно это свойство в зависимости от качества его реализации позволяет в той или иной мере контролировать соблюдение сотрудниками предприятия установленных правил безопасной работы на компьютерах и политики безопасности.

Между мониторинговыми продуктами для обеспечения наблюдаемости и продуктами-шпионами очень тонкая грань – это грань между управлением безопасностью и нарушением безопасности. При этом наличие в программе таких специальных функций как возможность предварительной конфигурации модуля (клиента, агента и т. п.) мониторинга и получение "скомплектованного" исполнимого файла, который при инсталляции не выводит никаких сообщений и не создает окон на экране, встроенные средства доставки и дистанционной установки сконфигурированного модуля на компьютер пользователя – способствует и содействует превращению продукта для мониторинга и наблюдаемости в продукт-шпион.

Напротив, наличие в программе следующих требований: возможность инсталляции и конфигурации модуля мониторинга только при непосредственном физическом доступе к компьютеру пользователя, обязательное наличие прав администратора для инсталляции и конфигурации программы – зачастую делает продукт малопригодным для шпионских целей и несанкционированного применения. Исключение составляют случаи, когда, например, злоумышленником является сам администратор.

Отметим, что законность/незаконность использования мониторинговых (и шпионских) программ зависит от законодательства каждой конкретной страны (или административной единицы), а также от соблюдения правил использования этих программ, установленных законодательством.

Для чего используются мониторинговые программы?

Их применение позволяет специалисту, ответственному за информационную безопасность

предприятия:

- определить (локализовать) все случаи попыток несанкционированного доступа к конфиденциальной информации с точным указанием времени и сетевого рабочего места, с которого такая попытка осуществлялась;
- определить факты несанкционированной установки программного обеспечения;
- проконтролировать возможность использования персональных компьютеров в нерабочее время и выявить цель такого использования;
- определить все случаи несанкционированного использования модемов в локальной сети путем анализа фактов запуска несанкционированно установленных специализированных приложений;
- определить все случаи набора на клавиатуре критичных слов и словосочетаний, подготовки каких-либо критичных документов, передача которых третьим лицам приведет к материальному ущербу;
- определить факты нецелевого использования персональных компьютеров;
- получить достоверную информацию, на основании которой будет разрабатываться политика информационной безопасности предприятия;
- контролировать доступ к серверам и персональным компьютерам;
- контролировать контакты собственных детей при серфинге в сети Интернет;
- проводить информационный аудит;
- исследовать и расследовать компьютерные инциденты;
- проводить научные исследования, связанные с определением точности, оперативности и адекватности реагирования персонала на внешние воздействия;
- определить загрузку компьютерных рабочих мест предприятия;
- восстановить критическую информацию после сбоев компьютерных систем и т. д.

Для чего используются несанкционированно устанавливаемые мониторинговые программы, т. е. программы-шпионы?

Их применение позволяет злоумышленнику:

- несанкционированно перехватывать чужую информацию;
- осуществлять экономический шпионаж;
- осуществлять политический шпионаж;
- получить несанкционированный доступ к системам "банк-клиент";
- получить несанкционированный доступ к системам криптографии пользователя персонального компьютера – открытым и закрытым ключам, парольным фразам;
- получить несанкционированный доступ к авторизационным данным кредитных карточек и т. д.

Продукты-шпионы представляют серьезную опасность защите отдельных и соединенных в сеть компьютерных систем.

Одна из наиболее опасных особенностей всех программ-шпионов и аппаратных устройств – кейлоггеров – регистрация нажатий клавиш, сделанных пользователем, с целью контроля компьютерной активности. Когда пользователь набирает на клавиатуре пароль и данные своей кредитной карточки, возможно, в этот момент записывается каждое нажатие клавиши. Кроме этого, современные программы-шпионы позволяют захватывать текст из окон приложений и делать снимки (скриншоты) экрана и отдельных окон. Другими словами, программа-шпион может перехватить текст из документа, даже если пользователь его не набирал с клавиатуры, а просто открыл и просмотрел файл.

Ниже мы постараемся более детально осветить вопрос, что же собой представляют продукты-шпионы, которые могут быть использованы для скрытого съема информации с персонального компьютера, и какие существуют сегодня средства для защиты конфиденциальной/секретной информации, хранимой на жестком диске персонального компьютера, от описанных выше угроз.

II Программные кейлоггеры, предназначенные для контроля информации, вводимой пользователем персонального компьютера

Программные кейлоггеры (keyloggers, key loggers, keystroke loggers, key recorders, key trappers, key capture programs и множество других вариантов названия) принадлежат к той группе программных продуктов, которые осуществляют контроль за деятельностью пользователя персонального компьютера. Первоначально программные продукты этого типа предназначались исключительно для записи информации о нажатиях клавиш клавиатуры, в том числе и системных, в специализированный журнал регистрации (Log-файл), который впоследствии изучался человеком, установившим эту программу. Log-файл может отправляться по сети на сетевой диск, ftp сервер в сети Интернет, по Email и др. В последнее время программные продукты, имеющие данное название, выполняют много дополнительных функций – это перехват информации из окон, перехват кликов мыши, "фотографирование" снимков экрана и

активных окон, ведение учета всех полученных и отправленных Email, мониторинг файловой активности, мониторинг системного реестра, мониторинг очереди заданий, отправленных на принтер, перехват звука с микрофона и видео-изображения с веб-камеры, подключенных к компьютеру и др.

Кейлоггеры могут быть встроены в коммерческие, бесплатные и условно-бесплатные программы, троянские программы, вирусы и черви. В качестве примера можно привести недавнюю нашумевшую эпидемию червя Mydoom, который содержал в себе кейлоггер. Эта эпидемия вызвала целую волну публикаций, показывающих особую актуальность проблемы защиты от программ-шпионов. Лишь некоторые ссылки приведены ниже:

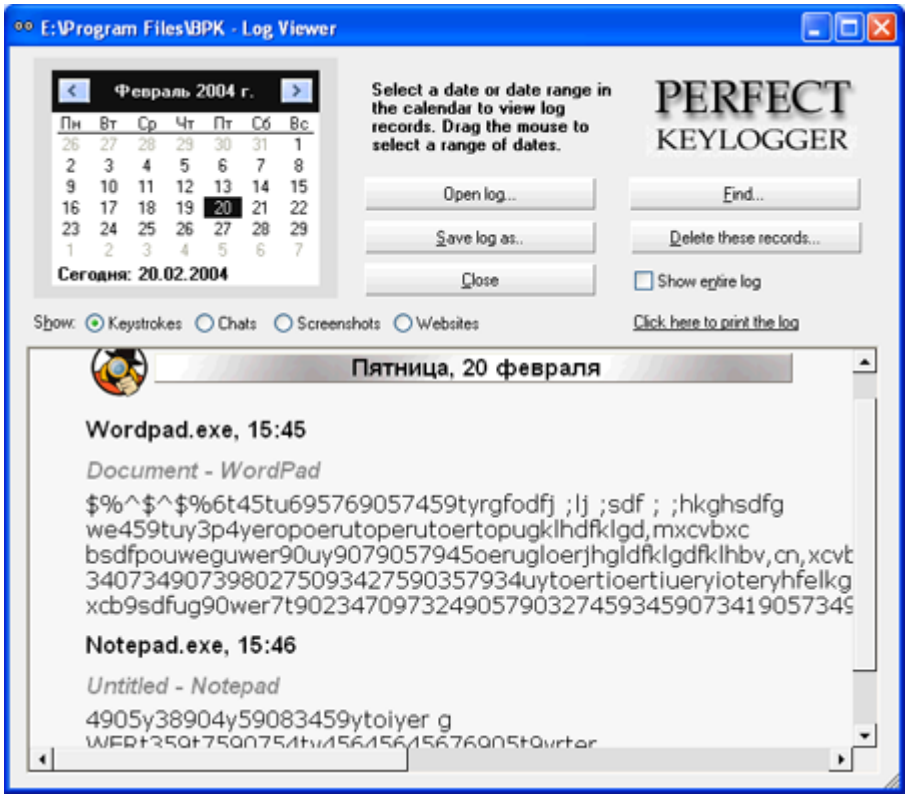
MYDOOM - worst yet to come
The Age
... So far, the damage is minimal. But the pre-eminent danger is that one
virus strain has a keylogger." Faulkner said it is possible ...
http://www.theage.com.au/articles/2004/01/29/1075088122616.html
CI Host CEO Monitors Computer Virus Epidemic Effects: ...
Yahoo News (press release)
... One in every dozen e-mails carries the virus. So far, the damage is
minimal. But the preeminent danger is that one virus strain has a keylogger." ...
http://biz.yahoo.com/prnews/040128/flw020_1.html
MYDOOM virus delivers gloom
Press of Atlantic City
... Infected computers still will have a backdoor in them, as well
as a key logger that records every keystroke. "A backdoor ...
http://www.pressofatlanticcity.com/news/newjersey/012804MYDOOM_J27.html
SCO offers $250000 reward for arrest of Mydoom worm author
ComputerWorld
... According to Symantec, the worm also installs a "key logger" that can
capture anything that is entered, including passwords and credit card
numbers, and will ...
http://www.computerworld.com/securitytopics/security/virus/story/0,10801,89470,00.html
NEW, fast-spreading worm spells Doom
InfoWorld
... The worm will install a "key logger" that can capture anything that
is entered, including passwords and credit card numbers, Ruckman said...
http://www.infoworld.com/article/04/01/27/HNdoomworm_1.html
NO move to stop email bounce messages yet, says Telecom
Computerworld New Zealand
... Symantec also claims the worm will install a "key logger" that can
capture anything that is entered, including passwords and credit card
numbers ...
http://www.computerworld.co.nz/news.nsf/UNID/23A51A1010B535FCCC256E280012F960?OpenDocument
WEB virus beats defence
Melbourne Herald Sun
... Anti-virus company Symantec warned the virus could install a "key logger"
program on to computers, allowing hackers access to every keystroke, including ...
http://www.heraldsun.news.com.au/common/story_page/0,5478,8513866%255E421,00.html
GLOBAL Hauri Offers Quick Fix to the Latest Cyber Threat
Market Wire (press release)
... spread by email. With the infections MyDoom also installs a key logger
and backdoor server on the infected computer. A new feature ...
http://www.marketwire.com/mw/release_html_b1?release_id=62255
INVESTOR Scammed By Keylogger Spyware
Emediawire (press release)
... In reality what was in their download was a keylogger that
captured & recorded the usernames and passwords to online accounts ...
http://www.emediawire.com/releases/2004/1/emw100583.htm

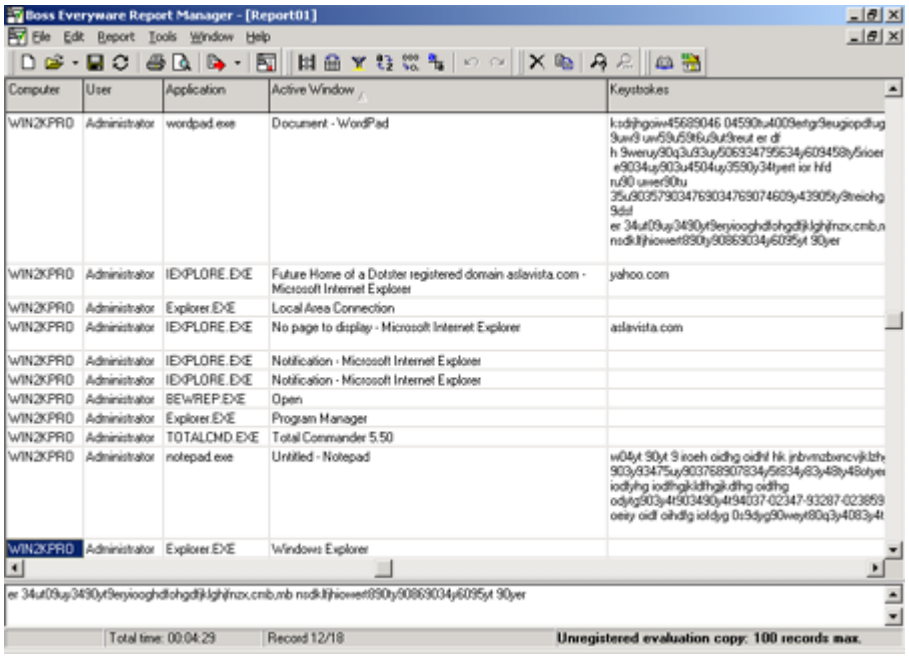
Mydoom – не единственный пример. Многие серьезные и наиболее опасные предшественники Mydoom также содержали кейлоггеры. При этом нередко для распространения червей использовалась широко известная уязвимость IFrame браузера Microsoft Internet Explorer, которая позволяла запустить произвольный код на компьютере пользователя при простом просмотре HTML документа в браузере или почтовом клиенте Outlook. И хотя она была "залатана" еще в 2001 году (http://www.microsoft.com/technet/security/bulletin/MS01-020.asp), широкомасштабные вирусные эпидемии в недавнем прошлом еще раз показали, что многие пользователи до сих пор работают на устаревших системах без обновлений и патчей, несмотря на регулярные предупреждения антивирусных компаний. Кроме того, компания Microsoft регулярно выпускает патчи, закрывающие новые уязвимости, позволяющие злоумышленнику выполнять произвольный код на компьютере пользователя.

Примерами известных программных кейлоггеров являются Activity Logger, Boss Everyware, Ghost

Keylogger, HookDump, IamBigBrother, Invisible KeyLogger Stealth, iOpus STARR, iSpyNOW, KeyCopy, KeyKeeper, KeyKey, KeyLog, KeySpy, Keystroke Reporter, PC Spy, Perfect Keylogger, ProBot, Realtime Spy, Spector Pro, SpyAgent, SpyBuddy, WinWhatWhere Investigator. В мире на сегодняшний день существуют сотни подобных продуктов, отличающихся друг от друга функциональностью, удобством работы, информативностью отчетов, возможностями по невидимости и защите от обнаружения/удаления.

Образцы внешнего вида анализаторов Log-файла программ Perfect Keylogger и Boss Everyware приведены ниже.





III Аппаратные кейлоггеры, предназначенные для контроля информации, вводимой пользователем персонального компьютера с клавиатуры

Аппаратные кейлоггеры (keystroke recording device, hardware keylogger и пр.) представляют собой миниатюрные приспособления, которые могут быть прикреплены между клавиатурой и компьютером или встроены в саму клавиатуру. Они регистрируют все нажатия клавиш, сделанные на клавиатуре. Процесс регистрации абсолютно невидим для конечного пользователя. Аппаратные кейлоггеры не требуют установки какой-либо программы на компьютере интересующего объекта, чтобы успешно перехватывать все нажатия клавиш. Такое устройство может быть тайно прикреплено к ПК объекта кем угодно – коллегой, уборщицей, посетителем и т. д.. Когда аппаратный кейлоггер прикрепляется, абсолютно не имеет значения, в каком состоянии находится компьютер – включенном или выключенном.

Атакующий может снять устройство в любой удобный момент, а его содержимое (записанные нажатия клавиш) скачать, когда ему это будет удобно. Объемы внутренней энергонезависимой памяти данных устройств позволяют записывать до 10 миллионов нажатий клавиш. Фотографии, приведенные ниже, наглядно иллюстрирует, насколько легко прикрепить данное устройство к компьютеру пользователя. Данные устройства могут быть выполнены в любом виде, так что даже специалист не в состоянии иногда определить их наличие при проведении информационного аудита.

Аппаратные кейлоггеры подразделяются на внешние и внутренние; их отличительные особенности описаны ниже.

Внешние аппаратные кейлоггеры

Наружные аппаратные кейлоггеры подключаются между обычной клавиатурой ПК и компьютером и регистрируют каждое нажатие клавиш. Для работы им не нужны батареи, установленные программы, они могут работать на любом ПК. Вы можете подключить их к одному компьютеру, чтобы записать информацию, а затем, при необходимости, подключить к другому, чтобы воспроизвести ее.

Современные аппаратные кейлоггеры представляют собой встроенные приспособления, которые выглядят, как оборудование для ПК.

Внутренние аппаратные кейлоггеры

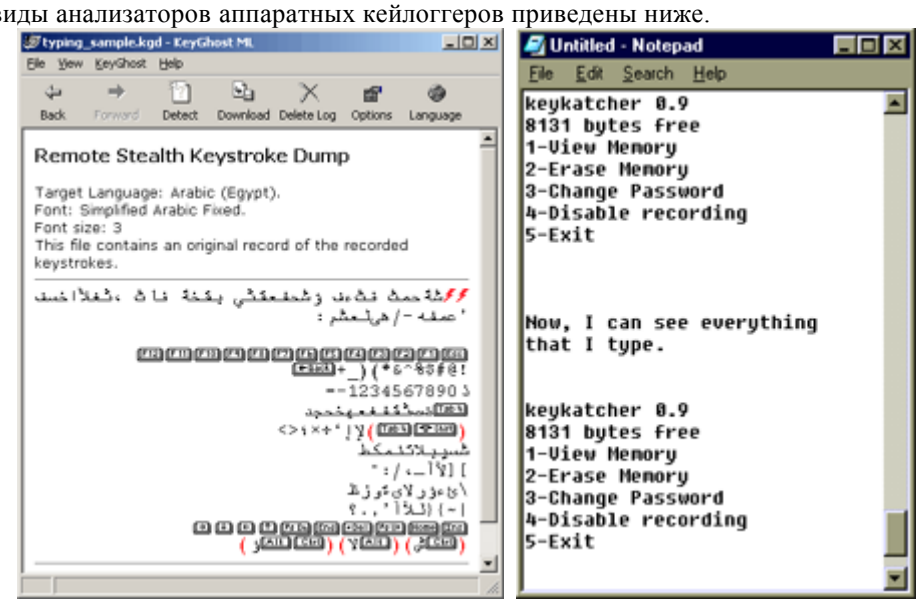
Сложнее всего обнаружить (и обезвредить) внутренний аппаратный кейлоггер, у которого аппаратный модуль перехвата нажатий клавиш встроен в корпус клавиатуры.

Современный внутренний аппаратный кейлоггер представляет собой встроенное приспособление, которое выглядит, как клавиатура ПК.

Небольшое устройство, внедренное в разрыв шнура клавиатуры и покрытое теплоизоляционным материалом.

Особо известны на рынке следующие аппаратные кейлоггеры - KeyKatcher, KeyGhost, MicroGuard, Hardware KeyLogger, производителями которых являются компании Allen Concepts Inc., Amecisco, KeyGhost Ltd., MicroSpy Ltd.

Внешние виды анализаторов аппаратных кейлоггеров приведены ниже.



IV Методы противодействия программам-шпионам

Для обнаружения и удаления мониторинговых программных продуктов, которые могут быть установлены без ведома пользователя ПК, в настоящее время используются программы различных типов, обеспечивающие более или менее эффективную защиту исключительно только против ИЗВЕСТНЫХ программ-шпионов с помощью сигнатурного анализа. Для эффективной работы программ данного типа необходимо получить образец программы-шпиона, выделить из нее сигнатуру и включить данную сигнатуру в свою базу. При обновлении сигнатурной базы пользователи персонального компьютера получают возможность бороться с данным вариантом программы-шпиона. По данному принципу работают многие известные фирмы – производители антивирусного программного обеспечения.

Но есть и другая группа программ-шпионов, которая наиболее опасна для любых автоматизированных систем – это НЕИЗВЕСТНЫЕ программы-шпионы. Они подразделяются на программы пяти типов.

1. Программы-шпионы, разрабатываемые под эгидой правительственных организаций (как пример – продукт Magic Lantern, проект под названием Cyber Knight, США).

2. Программы-шпионы, которые могут создаваться разработчиками различных операционных систем и включаться ими в состав ядра операционной системы.

3. Программы-шпионы, которые разработаны в ограниченном количестве (часто только в одной или нескольких копиях) для решения конкретной задачи, связанной с похищением критической информации с компьютера пользователя (например, программы, применяемые хакерами-профессионалами). Данные программы могут представлять собой немного видоизмененные открытые исходные коды программ-шпионов, взятые из сети Интернет и скомпилированные самим хакером, что позволяет изменить сигнатуру программы-шпиона.

4. Коммерческие, особенно, корпоративные программные продукты, которые очень редко вносятся в сигнатурные базы, а если и вносятся, то только по политическим мотивам (как пример – программные продукты таких известных фирм, как WinWhatWhere Corporation, SpectorSoft Corporation, ExploreAnywhere Software LLC, Omniquad Ltd. и др.).

5. Программы-шпионы, представляющие собой keylogging модули, включаемые в состав программ-вирусов. До внесения сигнатурных данных в вирусную базу данные модули являются неизвестными. Пример – всемирно известные вирусы, натворившие много бед в последние годы, имеющие в своем составе модуль перехвата нажатий клавиатуры и отправки полученной информации в сеть Интернет. К ним, например, относятся:

- W32.Dumaru.Y@mm http://securityresponse.symantec.com/avcenter/venc/data/w32.dumaru.y@mm.html
- W32.Yaha.AB@mm http://securityresponse.symantec.com/avcenter/venc/data/w32.yaha.ab@mm.html

- W32.Bugbear.B@mm http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear.b@mm.html
- W32.HLLW.Fizzer@mm
http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.fizzer@mm.html
- W32.Badtrans.B@mm http://securityresponse.symantec.com/avcenter/venc/data/W32.Badtrans.B@mm.html

Информация о программах-шпионах первого и третьего типа, как правило (если не происходит утечек информации) нигде не опубликовывается, и, соответственно, их код не может быть внесен в сигнатурные базы, поэтому они не могут обнаруживаться никакими программными продуктами, использующими сигнатурный анализ.

Информация о программах-шпионах второго типа нигде не опубликовывается, данный код работает на уровне ядра операционной системы и, соответственно, они не могут обнаруживаться никакими приложениями.

Информация о программах-шпионах четвертого типа вносится в сигнатурные базы очень редко, так как это противоречит законодательству многих стран мира. Но даже если и внести такие программы в сигнатурные базы, то деактивировать, а, тем более, удалить их зачастую невозможно без разрушения операционной системы. Они не имеют своих процессов, а прячутся в виде потоков в системные процессы, они могут работать только с памятью компьютера и не работать с жестким диском, они имеют режимы контроля целостности и самовосстановления после сбоев.

Информация о программах-шпионах пятого типа вносится в сигнатурные базы через несколько часов или дней после начала соответствующей вирусной атаки. А за это время конфиденциальная информация пользователя персонального компьтера уже может быть украдена и отослана в сеть Интернет на заранее подготовленный вирусописателем адрес.

Что же может противопоставить пользователь персонального компьютера программам-шпионам?

Решение данной проблемы возможно только при использовании комплекса программных продуктов:

- программный продукт N1 – это продукт, который использует эвристические механизмы защиты против программ-шпионов, созданных специалистами, имеющими больший опыт борьбы с программами-шпионами; он оказывает защиту непрерывно и не использует никакие сигнатурные базы;
- программный продукт N2 – это антивирусный программный продукт, использующий постоянно обновляемые сигнатурные базы;
- программный продукт N3 – это персональный Firewall, контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь.

Такая последовательность выбрана неспроста.

Антивирусный программный продукт успевает отреагировать на проникновение вируса с keylogging модулем, когда уже осуществлен перехват информации, т. к. вирусная база еще не успела пополниться новой информацией, а, соответственно, и обновиться на компьютере пользователя.

Персональный Firewall задает много вопросов, на которые даже очень хорошо подготовленный пользователь может ответить некорректно, тем самым неправильно его сконфигурировав. Например, некоторые коммерческие мониторинговые программы используют процессы программных продуктов, которым заведомо разрешен выход в Интернет (браузеры, почтовые клиенты и т. д.). Как правило, пользователь обязан разрешить им выход в Интернет. А это приводит к тому, что та информация, которая была уже украдена при полном бездействии антивирусной программы, спокойно будет передана в сеть Интернет на заранее подготовленный хакером (или кем-то иным) интернет-адрес.

И только программный продукт первого типа работает молча, не задавая ненужных вопросов пользователю, и осуществляет свою работу непрерывно в фоновом режиме.

Антивирусных программных продуктов, использующих постоянно обновляемые сигнатурные базы, в мире создано великое множество (AVP, Dr.Web, Panda Antivirus, Norton Antivirus и многие другие). Персональных межсетевых экранов создано еще больше (Norton Internet Security, BlackICE Defender, GuardianPro Firewall, Tiny Personal Firewall и многие другие). Защитные программные продукты первого типа представлены на сегодняшний день всего лишь одним продуктом, не имеющим аналогов в мире. Этот продукт называется PrivacyKeyboard™.

PrivacyKeyboard™ блокирует работу программ-шпионов без использования сигнатурных баз. Это стало возможным благодаря тому, что были найдены решения и разработаны алгоритмы, которые позволили отличить работу программы-шпиона от любого иного приложения, установленного в системе.

PrivacyKeyboard™ имеет в своем составе модули, обеспечивающие защиту от:

- перехвата нажатий клавиш клавиатуры;
- перехвата текста из окон;
- снятия изображения рабочего стола;
- снятия изображения активных окон.

Для собственной защиты от внешнего разрушительного воздействия программ-шпионов программный продукт PrivacyKeyboard™ имеет систему контроля целостности и другие защитные функции.

V Методы противодействия аппаратным кейлоггерам

Никакие программные продукты не в состоянии определить наличие установленных аппаратных устройств, которые обеспечивают перехват нажатий клавиатуры пользователем персонального компьютера.

Сегодня существует только два метода противодействия аппаратным кейлоггерам при работе на стандартном персональном компьютере:

физический поиск и устранение аппаратного кейлоггера;

использование виртуальных клавиатур для ввода особо важной информации (логины, пароли, коды доступа, PIN коды кредитных карт и т. д.).

Остановимся детальнее на втором пункте.

Программный продукт PrivacyKeyboard™ имеет в своем составе модуль защиты от аппаратных кейлоггеров, выполненный в виде виртуальной экранной клавиатуры, которая вызывается пользователем в случае необходимости.

Раскладка виртуальной клавиатуры переключается автоматически при переключении раскладки основной клавиатуры персонального компьютера и поддерживает все языки и раскладки, которые установлены в операционной системе Microsoft Windows NT/2000/XP.

VI Механизм функционирования PrivacyKeyboard™

Структурная схема и краткое описание механизма функционирования программы PrivacyKeyboard™ представлены ниже.

Модуль блокирования программных кейлоггеров является активным по умолчанию, обеспечивая постоянную и прозрачную защиту "на лету" от различных типов программных кейлоггеров. Его можно легко выключить/включить одиночным щелчком левой клавиши мыши на иконке PrivacyKeyboard™ в системном трее. Когда модуль блокирования программных кейлоггеров включен, PrivacyKeyboard™ подавляет любые кейлоггеры, которые могут быть включены в состав коммерческих, бесплатных и условно бесплатных продуктов, а также "троянских коней" и вирусов, использующих самые разные принципы функционирования и основанных на модулях пользовательского уровня либо уровня ядра системы – dll, exe, sys и др., которые создают лог-файлы на жестком диске, в памяти, реестре, на сетевых дисках, либо пересылают лог-файлы на заранее указанные адреса по протоколам SMTP, FTP, HTTP и др.

Модуль блокирования аппаратных кейлоггеров можно активировать путем нажатия правой клавиши мыши на иконке PrivacyKeyboard™ в системном трее и выбора опции “Показать модуль блокирования аппаратных кейлоггеров”. При этом на экране появится виртуальная клавиатура. Она поддерживает различные раскладки клавиатуры и языки, установленные в системе. При работе с виртуальной

клавиатурой в целях безопасности стандартная клавиатура блокируется.

VII Выводы

Проблема перехвата информации с помощью кейлоггеров стоит довольно остро. В мире существуют сотни подобных программ, которые могут быть несанкционированно установлены без ведома пользователя ПК. Многие вирусы и троянские программы имеют в своем составе модули для перехвата с клавиатуры. По итогам обзора можно сделать вывод, что существует комплексный подход, который позволит защитить персональные компьютеры от угроз данного вида. PrivacyKeyboard™ обеспечивает защиту от продуктов-шпионов большинства типов, причем делает это эффективнее других программ, которые используют сигнатурные базы для анализа.

Разработчиком программы PrivacyKeyboard™ является ООО "Центр информационной безопасности" (г. Запорожье, Украина). Доступна бесплатная версия для ознакомления, скачать которую можно по адресу: http://www.bezpeka.biz/download.html.

*Литература: **1**. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999. **2**. «2001 AMA Survey: Workplace Monitoring & Surveillance: Summary of Key Findings» American Management Association http://www.amanet.org/research/pdfs/ems_short2001.pdf. **3**. «Computer And Internet Surveillance in the Workplace: Rough Notes». Andrew Schulman, Chief Researcher, Privacy Foundation, US, 2001-2002 http://www.sonic.net/~undoc/survtech.htm. **4**. «The Extent of Systematic Monitoring of Employee E-mail and Internet Use» Andrew Schulman, Chief Researcher, Privacy Foundation, US, 2001-2002 http://www.sonic.net/~undoc/extent.htm.*

УДК 638.235.231

МОДЕЛЬ УГРОЗ, РЕАЛИЗУЕМЫХ АППАРАТНЫМИ РЕСУРСАМИ КОМПЬЮТЕРНЫХ СИСТЕМ

Валерий Горбачёв, Владимир Степаненко, Тарас Гриценко
Харьковский Национальный технический университет радиоэлектроники

Аннотация: **Предлагается модель компьютерной системы, учитывающая угрозы реализуемые аппаратными ресурсами компьютерных систем.**
Summary: **In this clause the model of computer system which is taking into account threats sold hardware resources of computer systems is offered.**
Ключевые слова: **Информация, компьютерная безопасность, доступ.**

Введение

В теории компьютерной безопасности формальное моделирование политики безопасности (ПБ) является одним из методов, который позволяет описывать различные аспекты безопасности и обеспечивать средства защиты формально подтвержденной алгоритмической базой.

Успешная разработка модели безопасности зависит от качества модели самой компьютерной системы (КС), от того, насколько полно удалось учесть все архитектурные особенности последней, а также угрозы компьютерной безопасности.

В работе предлагается субъектно-объектная модель аппаратных ресурсов КС [1, 2], охватывающая такой класс угроз, как аппаратные закладки (АЗ) [3].

I Основная часть

Определим АЗ как электронный компонент в интегральном исполнении, встроенный в интегральную схему при её проектировании и производстве, или выполненный в виде отдельной интегральной схемы и создающий угрозу безопасности информации своими не специфицированными функциями. В первом случае закладка является частью стандартного электронного компонента и изменяет его предполагаемые структуру и функции, во втором – сама является не специфицированным компонентом КС и изменяет предполагаемые структуру и функции самой КС. В работе будут рассмотрены АЗ, которые используют штатные каналы КС для передачи информации. В работе не будут рассматриваться все виды АЗ,