УДК 65.012:34(477)

В.В. Кальченко, М.В. Цуранов

Харьковский национальный университет внутренних дел, Харьков

ИСПОЛЬЗОВАНИЕ ПРОГРАММ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ ДЛЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Рассмотрены методы несанкционированного доступа злоумышленника в информационную систему при помощи программ удаленного администрирования. Приведена классификация угроз удаленного доступа, проведен анализ возможных ошибок при установке программ удаленного администрирования. Рассматриваются способы скрытой инсталляции программ удаленного администрирования и методы противодействия данной угрозе.

Ключевые слова: *программы удаленного доступа, несанкционированный доступ, удаленное администрирование, угрозы информации.*

Введение

В настоящее время компьютеры прочно вошли в повседневную жизнь, каждый день в мире обрабатывается и передается огромное количество информации. Для получения информации хакеры используют широкий набор программных средств, с которыми можно бороться при помощи специального программного обеспечения (ПО): антивирусов и брандмауэров, а также правильно настроив компьютер. Каждый день происходит совершенствование алгоритмов вредоносных программ и методов их проникновения на персональный компьютер. Как правило, антивирусы их обнаруживают, предотвращают запуск и выполнение деструктивных операций [1].

Основным недостатком вирусов, с точки зрения злоумышленника, является их быстрое обнаружение. При широком распространении определенного вида вируса, его сигнатуры в кратчайшие сроки добавляются в антивирусные базы. Также новые эвристические алгоритмы позволяют обнаружить возможную угрозу, при этом они имеют высокую вероятность ложного срабатывания. Всё вышеперечисленное затрудняет действия злоумышленника по проникновению в компьютер и получению конфиденциальной информации.

Следует отметить, что эксперты в области информационной безопасности мало обращают внимание на опасность исходящую от ПО, которое санкционировано установлено и регулярно используется, т.е. от тех программ, которые не идентифицируются как вредоносные, в программном коде которых присутствуют следующие недоработки:

- непреднамеренные ошибки, приводящие к утечке информации;

- «черные ходы» (люки);
- модули удаленного администрирования;
- отсутствие системы обнаружения изменения системных файлов.

Рассматривая проблему несанкционированного доступа (НСД), стоит также упомянуть о таком явлении как работа с конфиденциальной информацией на домашних компьютерах. Проникновение и совершение противоправных действий, в данном случае, значительно проще. Это связано с тем, что пользователи крайне редко защищают свои домашние компьютеры. Поэтому рассматриваемая проблема актуальна не только для администраторов и специалистов в области информационной безопасности, но и для любого пользователя, чей компьютер подключен к сети.

Организация несанкционированного доступа с использованием программ удаленного администрирования

Рассмотрим возможность НСД с использованием программ удаленного администрирования (ПУА). Среди которых можно выделить наиболее популярные: Radmin, Symantec pcAnywhere, UltraVNC и др. [2]. Также к этому классу необходимо отнести встроенное ПО: удаленный рабочий стол Windows и утилиту telnet [3]. Предназначение данных программных продуктов (ПП) – облегчение работы системного администратора по настройке, управлению и администрированию компьютеров в корпоративных и иных сетях. Кроме того, обычные пользователи используют их для связи со своим рабочим компьютером. Использование ПУА обусловлено значительной экономией времени, материальных ресурсов и удобством выполнения работы [3].

НСД к информационной системе с использованием ПУА может осуществляться целенаправленно (на строго определенный компьютер), либо массово (с целью получения доступа к максимально возможному числу компьютеров).

Даже при санкционированной установке ПУА возможны ошибки, которые могут привести к проникновению злоумышленника в систему [5]:

- применение «простых» или коротких паролей;
- использование первоначального, установленного разработчиками, пароля;
- использование одного пароля для доступа ко всем компьютерам в сети;
- отсутствие периодической смены пароля.

Всё это может привести к тому, что, получив тем или иным образом пароль к ПУА, работа сети становится подконтрольной злоумышленнику.

С точки зрения злоумышленника ПУА имеют ряд преимуществ по сравнению с вирусами [6 – 8]:

- не обнаруживаются антивирусным ПО;
- как правило, не блокируется брандмауэром;
- большинство пользователей даже при включенном брандмауэре разрешают сетевую активность ПУА;
- необходимость значительно меньшего уровня знаний и временных затрат на создание и внедрение вредоносной программы на компьютер жертвы;
- осуществление доступа ко всем программным и аппаратным ресурсам жертвы;
- отслеживание действий пользователя и получение информации в режиме реального времени и её модификация (в зависимости от программы);
- возможность конфигурирования политик безопасности;
- настройка работы ПО безопасности;
- внедрение вредоносного ПО для получения хранящихся паролей, логов программ, журналов аудита и их последующая модификации;
- скрытое использование компьютера жертвы для сетевых атак;
- доступ к ресурсам сети, в которую входит компьютер жертвы и атака на них;
- уничтожение операционной системы и возможность сокрытия самого факта проникновения;
- осуществление мошеннических финансовых операций.

Перечень данных угроз не является полным, но позволяет примерно оценить степень рисков, исходящих от ПУА. При установке ПО, мало кто задумывается о том, что в процессе инсталляции кроме устанавливаемой программы может быть осуществлена скрытая установка как вирусов, так и программ удаленного доступа.

Существует два варианта реализации угроз проникновения в информационную систему с использованием ПУА:

- внедрение программы только на один, строго определенный, компьютер;
- массовое внедрение программы на все компьютеры выбранной группы пользователей.

Суть проникновения заключается в том, чтобы вместе с полезной (для потенциальной жертвы) программой внедрить на его компьютер ПУА, которая будет несанкционированно использована злоумышленником. Для его реализации необходимо установить диалог с пользователем (того компьютера, в который нужно проникнуть), в процессе общения выяснить названия повседневно используемых программных средств.

Применяя методы социальной инженерии [9], возможно получить не только технические детали компьютера жертвы (наименование антивируса, брандмауэра их версию, настройки безопасности, перечень повседневно используемых программ), но и осуществить целенаправленное внедрение. Для этого используются методы претексинга, дорожного

яблока, фишинга и прочие.

Используя претексинг, можно заставить пользователя выполнять необходимые (для злоумышленника) действия. Метод позволяет получить данные персонализации.

Метод дорожного яблока заключается в подбрасывании носителя информации, на котором содержится вредоносная программа.

Фишинг используется для получения некой ключевой конфиденциальной информации (пароля доступа, пин-кода кредитной карты и т.д.).

Есть еще один способ проникновения – создать такие условия, при которых пользователь сам обратиться к злоумышленнику и попросит о помощи. Это достигается путем создания незначительной неполадки на компьютере жертвы, с предварительным размещением объявления об устранении неполадок компьютеров [9].

После чего злоумышленник ищет подходящий ПП, добавляет в него ПУА и тем или иным способом заставляет пользователя осуществить инсталляцию этого измененного ПП.

Алгоритм действия злоумышленника по созданию вредоносного пакета программ может выглядеть так:

- выбор необходимого ПО удаленного администрирования либо же использование встроенного в операционную систему;
- выделение из пакета ПУА серверной части или конфигурация встроенной в ОС ПУА;
- конфигурирование серверной части под требуемые задачи: настройка параметров доступа и соединения, удаление графической оболочки т.д.;
- основываясь на предпочтениях пользователя, осуществляется поиск необходимого «полезного» ПО (игры, офисные программы, макросы и т.д.);
- создание инсталлятора, включающего в себя как полезную программу, так и серверную часть ПУА или формирование списка команд для активации встроенного ПО;
- проверка работоспособности пакета программ;
- пересылка данного пакета на компьютер жертвы.

Для реализации последнего пункта возможно применение методов социальной инженерии.

Если же говорить о массовом внедрении, то технические данные не играют роли, т.к. главная задача – это заражение как можно большего количества компьютеров.

Когда необходимо массово внедрить ПУА, то действия злоумышленника могут быть такими:

- поиск наиболее популярных приложений (среди выбранной группы пользователей);
- создание пакета инсталляции, который будет включать не только популярное приложение, но и ПУА;
- размещение данного пакета на файлообменных серверах;
- размещение ссылки на данный пакет на популярных сайтах;
- мониторинг скачиваний (с целью определения ip-адресов потенциальных жертв);

Противодействие программам удаленного доступа

Методы предотвращения внедрения и использования ПУА аналогичны общепринятым рекомендациям по борьбе с вирусами и шпионскими приложениями [10], среди которых необходимо сделать акцент на следующих рекомендациях:

- необходимо определить список повседневно используемых приложений и запретить установку/удаление любого другого ПО;
- постараться отказаться от использования нелицензионного ПО;
- по возможности заменить нелицензионное ПО на лицензионное, или использовать бесплатные версии программ;
- максимально ограничить перечень открытых сетевых портов;
- при легальном использовании ПУА использовать нестандартный номер сетевого порта и стойкий (к методу прямого перебора) пароль;
- использовать и правильно настроить брандмауэр (по крайней мере, настроить стандартный брандмауэр Windows);
- постоянно обновлять антивирусные базы;
- использовать специализированное ПО, предназначенное для защиты информации;
- осуществлять периодическую проверку компьютеров на предмет изменения параметров безопасности, перечня разрешенных программ, открытых сетевых портов;
- настройка политики безопасности ОС;
- периодическое проведение инструктажа персонала по правилам сетевой безопасности и контроль знаний.

Угроза внедрения ПУА оправдана не только для большого числа компьютера, но и для одного, конкретного ПК (если пользователь активно использует пиратское ПО). Данный метод позволяет получить полный контроль над компьютером, при достаточно низкой вероятности обнаружения вторжения. Стоит отметить, что данный метод проникновения возможно использовать для построения ботнет-сети [11].

Заключение

В приведенной статье рассматриваются методы несанкционированного доступа к информационным

ресурсам с использованием ПУА. Представлены методы скрытой установки ПУА или активизации встроенной в ОС, показаны варианты внедрения таких программ. Всё это позволяет получить информацию о работе пользователей, созданных ими документах и их содержимом. При таком виде проникновения существует большая вероятность того, что такой вид проникновения останется не обнаруженным.

Увеличение количества и качества программно-аппаратных средств защиты информации приводит к тому, что злоумышленнику проще получить конфиденциальную информацию путём обмана пользователей, которые имеют к ней доступ. Знание личностной психологии и изобретательность злоумышленников при атаках на информационные системы играют большую роль. Противодействие использованию ПУА для НСД к информационным ресурсам должно заключаться не только в использовании вышеописанных рекомендаций и применении программно-технических комплексов, но и постоянном обучении и контроле персонала.

Список литературы

1. *Лосэв М.Ю. Фільтрація пакетів в брандмауерах і вибір стратегії маршрутизації / М.Ю. Лосэв // Системи обробки інформації. Безпека та захист інформації в інформаційних системах. – Х.: ХУ ПС, 2009. – Вип. 7 (79). – С. 119-120.*
2. *Пахомов С. Программы удаленного доступа по локальной сети и через Интернет / С. Пахомов // КомпьютерПресс: журнал. – 2007. – № 9. – С. 23-24.*
3. *Когда RAdmin не нужен: удаленное администрирование встроенными средствами [Электронный ресурс]. – Режим доступа к документу: http://www.xakep.ru/post/37412/ default.asp.*
4. *Remote Administrator: сказка про военную тайну № 1 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.xakep.ru/post/22143/default.asp.*
5. *Кадер М. Типы сетевых атак, их описания и средства борьбы [Электрон.ресурс] / Михаил Кадер. – Режим доступа к документу: http://www.cnews.ru/reviews/free/oldcom/security/cisco_attacks.shtml.*
6. *Кузнецов С. Remote Office Manager – комплекс программ для удаленного управления и администрирования компьютеров [Электронный ресурс] / С. Кузнецов. – Режим доступа к документу: http://www.ixbt.com/soft/remote-office-manager.shtml.*
7. *RAdmin как веб-тулза – используем Remote Administrator в мирных целях // Спецвыпуск Хакер. – № 30. – С. 30-35.*
8. *Способы проникновения вредоносных программ в систему [Электронный ресурс]. – Режим доступа к ресурсу: http://www.securelist.com/ru/encyclopedia/objects?chapter=118. Социальная инженерия. [Электронный ресурс]. – Режим доступа к документу: http://ru.wikipedia.org/wiki/ Социальная_инженерия.*
9. *Азбука безопасности лаборатории Касперского [Электронный ресурс]. – Режим доступа к ресурсу: http://www.kaspersky.ru/threats_faq.*
10. *Информационная безопасность. Искусство обмана [Электронный ресурс]. – Режим доступа к ресурсу: http://moldova.cc/fraude.*

Поступила в редколлегию 24.03.2010

Рецензент: д-р техн. наук, проф. В.И. Долгов, Харьковский национальный университет радиоэлектроники, Харьков.

ВИКОРИСТАННЯ ПРОГРАМ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ ДЛЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

В.В. Кальченко, М.В. Цуранов

Розглянуто методи несанкціонованого доступу зловмисника в інформаційну систему за допомогою програм віддаленого адміністрування. Приведена класифікація загроз віддаленого доступу, проведено аналіз можливих помилок при установці програм віддаленого адміністрування. Розглядаються способи прихованої інсталяції програм віддаленого адміністрування та методи протидії даній загрозі.

Ключові слова: *програми віддаленого доступу, несанкціонований доступ, віддалене адміністрування, загрози інформації.*

USES PROGRAMS OF REMOTE ADMINISTRATION FOR UNAUTHORIZED ACCESS TO INFORMATION RESOURCES

V.V. Kalchenko, M.V. Tsuranov

The methods of intruders in an information system using software for remote administration. A classification of threats to remote access, an analysis of possible errors when installing programs for remote administration. Consider ways to install hidden programs for remote administration and methods to counter this threat.

Keywords: *program of remote access, unauthorized access, remote administration, the threat of information.*