

Борьба со скрытыми каналами взаимодействия с информационной сетью.

Программы-шпионы

В. А. Комарова, менеджер по PR
и маркетинговым коммуникациям
Компания Aladdin

Выражение «читать между строк» по своей сути означает «улавливать скрытое», «понимать недосказанное». Однако с точки зрения сокрытия какой-либо информации у него есть и прямой смысл. Допустим, нам нужно отослать письмо адресату, причем так, чтоб прочесть наше послание и понять его истинную суть смог лишь тот, кому оно предназначается. Мы знаем, что письмо будет проверяться неким «цензором», а, значит, нам надо замаскировать его содержимое. Простейшим способом для реализации нехитрой шифровки будет написание текста в обычном режиме черным по белому, но при этом между черных строк мы впишем строки белыми буквами. Не видно? Не видно. Возможно, наша затея и удастся. Ведь, по сути, мы применили метод стеганографии – скрытой передачи данных.

Естественно, с развитием компьютерных и информационных технологий само понятие скрытого канала нашло новую форму реализации. На сегодняшний день подобные технологии наносят серьезный ущерб компаниям и отдельным лицам, зачастую не подозревающим о том, что данные, хранящиеся и обрабатываемые на их компьютерах, уже давно являются не только их личным достоянием...

Известно множество способов организации побочных каналов утечки информации, связанных с электромагнитным излучением, которое может содержать информацию об обрабатываемых на компьютере данных. Еще в 1985 году голландский инженер, специалист в области компьютерных технологий Вим ван Эйк опубликовал в журнале *Computers & Security* памятную для многих ученых и инженеров того времени статью «Electro-magnetic radiation from video display units: an eavesdropping risk?», сопроводив описываемые разработки последующей демонстрацией своей технологии. В передаче BBC «Мир завтрашнего дня»

ван Эйк показал как с помощью телевизора, антенны и настраиваемого генератора синхроимпульсов можно дистанционно ретранслировать изображение с другого экрана.

В дальнейшем работа коллег Ван Эка, таких как Маркус Кун и др., с побочными электромагнитными излучениями и наводками (ПЭМИН) привела к развитию технологии Soft Tempest, обеспечивающей скрытую передачу данных по каналу ПЭМИН с помощью программных средств. Интересно, что до 1980 года само понятие «tempest» означало кодовое название всего, что связано с экранированием и защитой аппаратуры от компрометирую-

щих утечек, а также добычей разведанных по каналам ПЭМИН. Естественно, под грифом «top secret».

По сути, Soft Tempest – атака, впервые показанная Куном, позволяет с использованием специальной программы-закладки, внедряемой на компьютер жертвы с помощью вредоносного ПО (троянских программ, сетевых червей и др.) отсортировать необходимую информацию и передавать ее путем модуляции изображения монитора. Принимая побочные излучения монитора, можно выделить полезный сигнал и передать содержащиеся в нем приватные или корпоративные данные заинтересованной стороне [1].

Фактически, работа злоумышленника в этом случае сводится к трем основным задачам: установить шпиона, доставить перехваченную информацию условному заказчику и скрыть следы преступления, то есть сам факт того, что на компьютере жертвы была (или присутствует) какая-либо активность, помимо тех процессов, что запущены самим хозяином ПК. Понятно, что чем больше «вес» шпиона или объем передаваемых с его помощью данных, тем выше риск быть обнаруженным. Когда с компьютера секретаря с невероятной скоростью будут передаваться пакеты данных с недетектируемым содержимым, секретарь может удивиться, но не придать этому значения. А вот системный администратор, обнаружив подобную аномалию, скорее всего, максимально быстро ликвидирует этот канал передачи данных. Таким образом, злоумышленник сталкивается с необходимостью скрывать свою деятельность, для чего им широко используются методы скрытной передачи данных, в том числе и упомянутой здесь стеганографии.

Скрытые каналы

Впервые понятие скрытого канала было введено в работе Лэмпсона «A Note of the Confinement Problem» в 1973 году. Канал является скрытым, если он не проектировался, не предполагался для передачи информации в электронной системе обработки данных. Иными словами, это

некий способ скрытой (замаскированной) несанкционированной передачи информации стороннему лицу, нарушающий системную политику безопасности. При этом для организации передачи данных могут использоваться атрибуты, не предназначенные для этого: задержки между регистрируемыми событиями, порядок следования сообщений, длины передаваемых блоков данных и т. п.

В докладе И. М. Тулупова «Скрытые каналы», сделанного в рамках научно-исследовательского семинара «Защита информации: аспекты теории и вопросы практических приложений», проводимого Кафедрой информационной безопасности МГТУ им. Баумана совместно с Ассоциацией «РусКрипто», приведена следующая классификация скрытых каналов:

- передача информации в именах файлов (примером является возможность показа на низком уровне названий и атрибутов директорий и файлов, созданных на верхнем уровне);
- передача информации в настройках общих ресурсов (кодирование информации в сохраняемых настройках каких-либо ресурсов общего пользования субъектов высокого и низкого уровней, когда настройки, произведенные на высоком уровне, доступны наблюдению на низком уровне и, следовательно, могут нести информацию, выраженную заранее условленным кодом.

При этом особо выделяются «потайные» каналы (subliminal channels) – нестандартные способы передачи информации по легальным каналам, например, электронной почте. Например, в систему может быть встроен нестандартный алгоритм электронной подписи, оставляющий место для тайных сообщений, не препятствующих проверке аутентичности ЭЦП.

Автор указывает, что двунаправленные потайные каналы обеспечивают взаимодействие с «троянскими» программами, когда необходимо не только получать информацию, но и осуществлять управление программой.

Для организации «скрытых каналов» используется как штатное программное обеспечение, так и специально созданное вредоносное ПО. Создателем скрытого канала может выступать как злоумышленник, находящийся вне организации и реализующий атаку удаленно, так и инсайдер. Администратор также может быть соучастником в организации подобной атаки, поскольку кто как не он знает все слабые места и уязвимости в защите сети. Лучшего соучастника трудно себе представить.

Допустим, системный администратор, работающий в крупной корпорации со строгим разграничением прав доступа и внедренной политикой информационной безопасности может не иметь доступа к информации о клиентах, суммах контрактов или стратегическим планам развития компании. Однако, занимаясь проектированием или оптимизацией определенных участков сети, он в состоянии предусмотреть способ получения интересующих его сведений, создав закладки или оставив специальные «пробелы» – уязвимости сети, которыми при случае он сможет воспользоваться, сведя риск быть обнаруженным к минимуму.

Находясь внутри системы, программа-шпион способна скрытым способом установить связь со своим автором и передавать ему требуемые сведения. Атаки с использованием скрытых каналов всегда приводят к нарушениям конфиденциальности информации, и крайне редко кто-либо пойдет на этот шаг ради удовлетворения личных амбиций. Чаще всего, это заказные, адресные и тщательно подготовленные мероприятия.

Используя скрытые каналы передачи данных, «удаленный» злоумышленник может преследовать цель организовать управление информационной сетью извне, превратив ее в бот. Все те, кто так или иначе связан с ИТ и информационной безопасностью, прекрасно знают о том, что производители софта достаточно часто сами используют «программные закладки», о чем красноречиво свидетельствует немалое число скандалов в прессе по обвинению разработчиков во встраивании руткит-

технологий. При этом даже применение всех известных мер защиты межсетевого экранирования не мешает внешнему нарушителю использовать эти уязвимости, маскируя свои действия при помощи «скрытых каналов».

Находка для «шпиона»

В тесной связи с развитием информационных технологий не менее активными темпами развиваются разнообразные ИТ-угрозы. А когда они становятся коммерчески оправданы и востребованы, проявляется некое подобие теневого рынка, где есть свои заказчики, «промежуточные» звенья и исполнители. В Интернете в изобилии представлены различные утилиты для формирования скрытых каналов (стего-программы). Заказать шпиона тоже не представляет особой сложности, если кому-то очень нужно добиться цели. Единственная задача — остаться неузнанным. А для этого шпиону необходимо закамуфлировать себя под легальный файл или программу, например, «дописав» свой код в конец файла-жертвы.

Многие помнят информационный шум вокруг новости о том, что в Рунете появился первый русскоязычный компьютерный вирус под названием Agent. Вредоносная программа маскировалась под обычные графические файлы формата bmp и была создана специально для атаки русской версии Windows 2000 — на других версиях этой операционной системы вредоносный код не работал. По мнению многочисленных комментаторов инцидента, этот факт косвенно указывал на Россию и страны СНГ как наиболее вероятные территории происхождения вируса.

Если пользователь запускал вложенный bmp-файл, шпион связывался с удаленным сервером и загружал с него на компьютер пользователя троянскую программу Throd. Однако данный шпион обладал относительно спокойным нравом — он был создан для кражи адресов электронной почты, из чего логичнее всего заключить, что его заказчиком являлась компания, занимающаяся рассылкой спама.

Вирусы скрываются и под видом mp3-файлов (MP3Concept) и даже под видом собственно антивирусов (Skull.L рассылался под видом антивируса Mobile Anti Virus от F-Secure) и обнаружить их домашними антивирусами бывает достаточно сложно, особенно если счастливый обладатель персонального компьютера не искушен в вопросах вирусологии и не так внимателен к требованиям обновления.

В статье «Скрытая утечка информации. Часть 2», опубликованной в отечественном журнале СЮ, автор приводит более сложный вариант маскировки вирусов. В качестве примера рассматривается вредоносный код Win95.CIH. Вирус внедряется в *.exe файл, используя особенности формата PE (Portable Executable), принятого в системе Windows, начиная с Windows 95. Windows-исполнимый файл *.exe может содержать не только код, но и многочисленные дополнительные данные: пиктограммы, различные служебные данные и дополнительная информация, например, об экспортируемых и импортируемых функциях. Каждый вид данных, содержащихся в файле формата PE — это отдельный объект, хранящийся в специальной секции фиксированного размера. Если объект не занимает всего объема секции, какая-то ее часть остается пустующей. Соответственно, эту «пустоту» можно заполнить любым другим кодом, в том числе и вредоносным. При этом размер файла не изменится и его работоспособность не нарушится.

Бороться и найти...

Несмотря на пугающие масштабы современных угроз и постоянно расширяющийся инструментарий злоумышленников, бороться с вредоносным программным обеспечением и кражей приватных данных можно и нужно. В масштабе корпорации этот аспект защиты должен быть закреплен в политике информационной безопасности, представляющей собой свод норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информа-

ции. Создание скрытых информационных потоков является строгим нарушением политики информационной безопасности, в связи с чем необходимо проводить регулярный анализ всей сетевой активности. Инспектирование должно предполагать решение следующих задач:

- выявление скрытых каналов;
- оценка пропускной способности скрытых каналов;
- оценка рисков, связанных с функционированием скрытых каналов;
- выделение сигнала и типа информации, передаваемой по скрытым каналам;
- противодействие функционированию скрытого канала вплоть до его уничтожения.

Для поддержки политики безопасности помимо механизмов защиты, препятствующих ее нарушению, должна проводиться перманентная работа с персоналом. Особенно актуальна проблема утечки для компаний, обладающих территориально распределенной филиальной сетью, а также компаний, сотрудники которых часто работают с ее информационными ресурсами (в том числе и с содержащими конфиденциальные данные) удаленно.

Грамотно организованная архитектура сети, защита которой построена на принципе эшелонирования, представляет собой серьезный барьер для злоумышленника. Лучшей практикой является построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование технологий защиты от вредоносного программного обеспечения и нежелательной корреспонденции на уровнях:

- входа в корпоративную сеть (gateway);
- сервера корпоративной сети;
- конечного устройства пользователя.

Самым сложным в этой и любой другой градации по уровням является организация защиты на уровне шлюза. Использование надежных гибко настроенных фильтров, блокирующих «шпионов» на сетевом шлюзе и позволяющих оперативно закрывать все возможные уязвимости в сети даже до выпуска официаль-

НОВОСТИ

ных патчей от вендоров, – это задача не из легких. И самым важным здесь как всегда остается вопрос о том, какое решение позволит это сделать. Ведь между всем известными spyware и adware есть множество других более сложно организованных кодов, селективно закрыть которые совсем не так просто. Не зря многие антивирусные вендоры опускают руки, если речь заходит об инспектировании графического контента или полной проверки HTML-кода.

Система контентной фильтрации на уровне шлюза должна удовлетворять следующим основным критериям:

- блокирование уязвимостей в программном обеспечении (эксплойтов) и атак, направленных на клиентские приложения;
- инспектирование 100 процентов HTTP/FTP-трафика в реальном времени;
- прозрачное блокирование для всех web-страниц (HTML) уязвимостей и атак 'driveby';
- многоуровневая защита от всех известных и неизвестных видов spyware, adware, «троянов», руткитов, перехватчиков нажатий на клавиши, вирусов и червей;
- предотвращение фишинговых атак как с известных и неизвестных фишинговых сайтов, так и с инфицированных хакерами доверенных сайтов;
- URL-фильтрация/родительский контроль с использованием постоянно обновляемой базы каталогизированных интернет-сайтов;
- прозрачное инспектирование на наличие спама и злонамеренных кодов почтовых протоколов POP3 и SMTP;
- неограниченная масштабируемость системы (с учетом роста компании);
- детализированные отчеты для каждого пользователя.

Естественно, обеспечить такую защиту в домашних условиях фактически невозможно. Не стоит забывать и о том, что злонамеренный код постоянно прогрессирует и становится все более «умным». Его создатели прекрасно понимают, что на данный момент в мире фактически нет компьютеров, на которых не ус-

тановлен антивирус. Соответственно, вредоносное программное обеспечение должно сначала заблокировать антивирус, чтобы проникнуть на персональный компьютер, и затем реализовать любую активность, начиная от сбора ценных сведений и заканчивая выводением из строя сети.

Наиболее адекватным выходом для защиты домашних компьютеров является использование их хозяевами провайдинг-сервиса доставки «чистого» контента, прошедшего фильтрацию на узле провайдера и, следовательно, освобожденного от 99 % вредоносного кода и спама. Подобные услуги уже достаточно широко распространены на Западе, и в России отдельные прогрессивные xSP-провайдеры уже начинают оценивать подобные сервисы в качестве новой рыночной ниши. Общая же масса относительно таких проектов пока настроена скептически. Еще бы, ведь помегобайтная система оплаты трафика не предполагает выявления вредного контента – пользователь платит за общий объем, независимо от того, сколько «мусора» в итоге осело на его машине. Однако вирусологи не дремлют, и кто знает, оправдает ли себя такой реактивный подход или уже пора задуматься о превентивной защите. ■

ЛИТЕРАТУРА

1. Овсянников В. Скрытая утечка информации. Часть 1–2 / Опубликовано 03.09.2003.
2. Тулунов И. М. «Скрытые каналы передачи информации» (доклад в рамках научно-исследовательского семинара «Защита информации: аспекты теории и вопросы практических приложений», организованного Кафедрой информационной безопасности Московского государственного технического университета им. Баумана совместно с Ассоциацией «Рус-Крипто»).
3. www.anti-malware.ru
4. Никольский А. Ю. Дипломная работа «Проблемы информационной безопасности банков», Государственный комитет Российской Федерации по высшему образованию, Финансовая академия при правительстве Российской Федерации. 1999 г.
5. Киви Берд. Волны компромата. Побочные каналы утечки информации при работе компьютеров // Компьютера. № 24, 2007.

Международная конференция «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2007)

В период с 13 по 15 сентября 2007 г. в Санкт-Петербурге будет проводиться один из ведущих международных форумов в области исследования фундаментальных и прикладных проблем защиты компьютерных сетей – четвертая международная конференция «Математические модели, методы и архитектуры для защиты компьютерных сетей» (MMM-ACNS-2007). Конференция организуется Санкт-Петербургским институтом информатики и автоматизации РАН и Университетом Бингхэмптона (США). Со-председатели конференции – В. И. Городецкий, И. В. Котенко и В. А. Скормин.

Предыдущие конференции, проведенные в 2001, 2003 и 2005 годах, продемонстрировали острый интерес исследовательских организаций и ученых всего мира к тематике использования формальных методов, моделей и построению перспективных архитектурных решений для обеспечения безопасности информационных ресурсов в компьютерных сетях.

В ходе подготовки к конференции было получено 60 докладов из 17 стран. Наибольшее количество статей поступило из России, США, Китая, Польши и Франции. В результате рецензирования международным программным комитетом было отобрано 32 лучших доклада, из которых 18 – для полных презентаций и 14 – для коротких.

Помимо этого, для участия в конференции персонально приглашены известные специалисты в области защиты информации. В частности, с докладами выступят А. Керомитис (Колумбийский университет, США), К. Колберг (Аризонский университет, США), П. Вериссимо (Лиссабонский университет, Португалия) и др. Труды конференции будут опубликованы в издательстве Springer в серии Lecture Notes in Computer Science.

Желающие принять участие в конференции найдут необходимую информацию на сайте данного мероприятия: <http://www.comsec.spb.ru/mmm-acns07/>.