# МЕТОДЫ СКРЫТОЙ ПЕРЕДАЧИ ПРИВАТНОЙ ИНФОРМАЦИИ ЧЕРЕЗ КОМПЬЮТЕРНУЮ СЕТЬ И ПОСТРОЕНИЕ ЗАЩИТЫ

Барабаш А.А., Вороной С.М.
Донецкий государственный институт искусственного интеллекта

В этом докладе рассказывается о методах скрытой передачи информации в компьютерную сеть. Главной целью является раскрытие и анализ методик скрытой передачи информации с целью построения требований к системе защиты.

Существует категория программ, называемых файрволами. Среди функций которых есть задача учета и контроля доступа в сеть процессов, запущенных на компьютере [1].

Для злоумышленника представлять интерес на чужом компьютере могут:

- файлы, в которых храниться личная финансовая информация;
- персональные pin-номера;
- электронные копии налоговых деклараций (если они готовились с помощью приложений по созданию налоговых отчетов);
- номера кредитных карт;
- рабочая информация, которая может быть ценна для конкурента;
- возможность запуска атаки "распределенный отказ от обслуживания" против других компьютеров в Интернете и Web-сайтов.

Как правило, для контроля доступа в сеть существует два списка: список разрешенных процессов и список запрещенных процессов. Существует два основных принципа, т.н. политики безопасности. Первая: разрешать доступ всем процессам, которых нет в списке запрещенных, вторая запрещать доступ процессам, которых нет в списке разрешенных. Вторая политика является более надежной, т.к. количество процессов, которым доступ в сеть разрешен, будет ограничено. Процессы в списке идентифицируются по полному пути запускаемого исполняемого файла.

Существуют методики передачи данных через сеть в обход средств защиты информации, использующие описанные ниже принципы работы [2].

1. Подмена исполняемых файлов доверенных программ. При таком подходе вредоносная программа переименовывается в имя доверенной программы и переписывается в ее каталог.
2. Внедрение в адресное пространство выполняющейся доверенной программы стороннего кода. Внедренный код начинает исполняться на правах взломанного процесса, получая, в частности, доступ в Интернет;
3. Внедрение сторонней dll-библиотеки. Код из библиотеки получает права доверенного.
4. Запуск доверенной программы или системного сервиса с передачей параметров для сетевого запроса в командной строке или иным способом.

Общим у этих методов является участие в передаче доверенного процесса. Как правило, если используется политика безопасности, то в списке разрешенных процессов находится Web-браузер и программа почтовый клиент.

Для тестирования средств защиты существуют программы-тесты, которые реализуют описанные выше методы скрытой передачи информации [2]. На сегодняшний день наиболее популярными являются: AWFT, CopyCat, DNStester, FireHole, Ghost, LeakTest, Mbtest, Outbound, pcAudit, Surfer, Termite, Tooleaky, WallBreaker, Yalta.

Знание этих методик позволяет описать функциональные требования к системам защиты. Система защиты должна осуществлять:

- контроль аутентичности исполняемых файлов программ и библиотек, осуществляющих доступ в сеть;
- контроль загрузки библиотек;
- контроль внедрения кода;
- контроль целостности родительских процессов для доверенных программ.

Для контроля аутентичности программных компонентов целесообразно вести базу данных, которая будет содержать:

- список исполняемых файлов, процессы которых могут осуществлять доступ в сеть;
- для каждого исполняемого файла список загружаемых библиотек, а также ссылку на элемент, соответствующий родительскому процессу;
- для каждого элемента базы (процесса или библиотеки) значение ключа, однозначно соответствующего конкретному содержанию файла (в простейшем случае может быть контрольная сумма или CRC, но более предпочтительным является использование криптографических хэш-функций).

Алгоритм работы с такой базой для выявления попыток передачи данных подмененными приложениями следующий:

- при запуске процесса устанавливается ссылка на родительский элемент; если произошел первый запуск процесса, вычисляется значение ключа и заносится в базу;
- при загрузке библиотеки в адресное пространство процесса вычисляется значение ключа и добавляется элемент в список библиотек процесса;
- при попытке приложений передавать данные заново вычислять значение ключей исполняемых файлов, процесса, родительских процессов, а также файлов библиотек;
- в случае несовпадения значений ключей или появления новых библиотек с списке, информировать о ситуации пользователя, т.к. несовпадение значений может быть вызвано обновлением программ, о чем пользователь наверняка знает, и спрашивать разрешение на передачу данных.

**Литература**

[1] Джерри Ли Форд. *Персональная защита от хакеров:* Пер. с англ. - М: Кудиц-образ, 2002.

[2] Александр Красоткин *Методы тестирования брандмауэров* http://www.compdoc.ru/secur/soft/methods_of_firewall_testing/