БРЕШЬ В ЗАЩИТЕ ПРОГРАММНОЙ СИСТЕМЫ SECUDESCTOP2000

В. В. Сташин, *к.т.н., доцент кафедры «Электроника и защита информации» Московского Государственного Университета Путей Сообщения (МГУ ПС), (МИИТ)*
А. В. Ладиков, *студент 5-ого курса специальности «Компьютерная безопасность» кафедры «Электроника и защита информации» МГУ ПС (МИИТ)*
Д. В. Павлинов, *студент 5-ого курса специальности «Компьютерная безопасность» кафедры «Электроника и защита информации» МГУ ПС (МИИТ)*

Достаточно широкое распространение в организациях РФ, озабоченных проблемой защиты информации от несанкционированного доступа (НСД), получил программно-аппаратный комплекс средств защиты корпорации SecuGen. В частности, программа SecuDesctop2000 корпорации SecuGen, которая является программной частью комплекса защиты информации, использующего для аутентификации и идентификации пользователей биометрические особенности человека, в том числе отпечатков его пальцев. Продукт состоит из нескольких компонентов, предназначенных для управления рабочими станциями ЛВС и защитой информации в них.

Программа SecuFolder предназначена для шифрования и дешифрации каталогов пользователя. После процедуры шифрования доступ к файлам каталога и к каталогу в целом возможен только при условии корректной идентификации пользователя по его отпечатку пальца. При использовании данной программы была найдена недоработка, позволяющая получить доступ к зашифрованным файлам пользователя с других станций локальной сети. А именно, если каталог, который будет подвержен шифрованию, является каталогом общего доступа в локальной сети, то после процедуры шифрования программой SecuFolder все файлы в нем также будут доступны другим пользователям локальной сети. Рассмотрим следующий алгоритм получения доступа нелегального пользователя к файлу, зашифрованному SecuFolder.

Пусть в системе имеется легальный пользователь P_1, использующий рабочую станцию PC_1, подключенную к локальной сети. Пусть пользователь P_2 использует рабочую станцию PC_2; причем пользователь не обязательно является легальным. Тогда:

1. Пользователь P_1 шифрует некоторый каталог K, хранящийся на рабочей станции PC_1, причем к каталогу K был разрешен общесетевой доступ до процедуры шифрования.
2. Пользователь P_2, используя рабочую станцию PC_2 входит в локальную сеть, находит в ней станцию PC_1, и находит на ней каталог K, разрешенный для общего доступа.
3. Пользователь P_2 открывает данный каталог со своей рабочей станции, но не находит в нем ни одного файла.
4. После чего пользователь P_2 ждет активности пользователя P_1.
5. Пользователь P_1 заходит в систему со своей рабочей станции PC_1, идентифицируя на ней себя как легального пользователя при помощи программ SecuDesctop2000.
6. Желая произвести работу над своими персональными данными, хранящимися в каталоге K, пользователь P_1 идентифицирует себя как легального пользователя каталога K, получает доступ к файлам данного каталога и открывает некоторый файл k_i из каталога K.
7. В этот момент пользователь P_2 вновь открывает каталог K со своей рабочей станции PC_2 и находит в нем файл k_i.
8. После чего P_2 копирует файл k_i на свою рабочую станцию PC_2, получая тем самым доступ к персональным данным пользователя .

Очевидно, что если пользователь P_2 является злоумышленником, то он может создать вредоносную программу, которая будет устанавливать общесетевой доступ на каталог, подвергающийся шифрованию с помощью программы SecuFolder, получая при этом возможность постоянного НСД к конфиденциальной информации с любой рабочей станции локальной сети.

Стоит заметить, что в ответ на наше сообщение о найденной недоработке корпорация SecuGen отказалась вносить изменения в программный продукт, сообщив следующее:

«I am well aware that ALL commercial software is vulnerable. Microsoft is shown to have security problems on almost a daily basis. So far they are still one of the largest companies in the world», [Я осознаю, что ВСЕ коммерческое программное обеспечение является уязвимым. Microsoft имеет проблемы с безопасностью едва ли не ежедневно. Однако они остаются крупнейшей корпорацией в мире]. Ответ подписан: *From: «JeffBrown» <jbrown@secugen.com> To: Ладиков Андрей <andreynot@mail.ru> Date Wed, 20 Sep 2006 14:02:51-0700 Subject: RE: RE: SecuDesctop 2000.*

Данной публикацией мы хотим предупредить всех российских пользователей программного продукта SecuFolder корпорации SecuGen о том, что данный продукт уязвим для НСД, то есть имеет канал утечки информации. И этот канал, как мы показали, может быть создан относительно простыми средствами. Средства блокирования данного канала утечки не могут быть опубликованы в открытой печати. Тем, кто осознал уровень угрозы своим информационным ресурсам, мы рекомендуем обращаться к авторам статьи.