КОНТРОЛЬ ПРОРЫВА АДРЕСНОГО ПРОСТРАНСТВА ПРОЦЕССОВ

М.П. Ревотюк, Ю.М. Ревотюк

Внедрение вредоносного кода в исполняемый процесс в среде Windows NT/2000/XP/2003/Vista базируется на прорыве адресного пространства процесса посредством подключения к процессу динамической подключаемой библиотеки (DLL). Механизм внедрения, например, посредством удаленного порождения потоков не нуждается в наличии на рабочей станции средств отладки, а возможность управляемого подключения к процессу DLL позволяет скрыть любой код.

Однако факт создания потока может быть зарегистрирован, например, на уровне драйвера или даже прикладного процесса. Выявление момента создания потока, причем непосредственно перед активизацией кода его функции, возможно посредством обработки событий DLL_THREAD_ATTACH и DLL_THREAD_DETACH, о которых уведомлена факультативная для любой DLL функция DllEntryPoint.

Используя доступность информации о файле внедряемой DLL, несложно создать для защищаемого процесса агент контроля попыток порождения нерегламентированных потоков. Такой агент, исполняемый в отдельном потоке с максимальным приоритетом и с нулевыми масками доступа, должен создавать слой проверок и установок условий безопасности процесса, а также порождать события аудита. Тело функции агента может быть представлено в отдельной DLL, играющей роль сенсора потоков.

Представленная схема защиты, тем не менее, уязвима к угрозам подключения отладчика на нулевом шаге создания процесса, а также к внедрению DLL через асинхронный вызов процедур (APC) без порождения потоков. Предлагается обнаруживать факт замораживания потоков при отладке динамической системой, образуемой, по меньшей мере, триадой однородных потоков. Любой из потоков должен перевести память процесса в состояние, не подлежащее интерпретации внешнему наблюдателю. Запуск такой системы должен выполняться с секретными параметрами пользователя синхронно с процедурами авторизации и аутентификации.