Опасные вирусы в июле

Название	Даты активации	Описание
April1st.COM.b2	5.7	**Опасные резидентные вирусы.** Перехватывают INT 21h и заражают запускаемые файлы. При создании своей резидентной копии используют часть схемы вируса "Jerusalem". Записываются в начало .COM-файлов (кроме COMMAND.COM), запускаемых на выполнение. Опасны, так как не проверяют длину файлов. При заражении: - создают файл TMP$$TMP.COM; - записывают в него свою копию; - дописывают в него заражаемый файл; - уничтожают заражаемый файл; - переименовывают TMP$$TMP.COM в имя заражаемого файла. **5-го июля** "April1st.COM.b2" выводит: ENGLISH SUCKERS DIE IN BUENOS AIRES! Содержит строки: COMMAND.COM TMP$$TMP.COM и: "April1st.COM.b2": cOcK!sUcKrI MADE IN ARGENTINA91
Hanko.4167 aka Monica	7.7	**Опасный резидентный полиморфик -стелс -вирус**. Перехватывает INT 21h и записывается в конец COM- и EXE-файлов при их запуске или закрытии. При открытии, переименовании или отладке зараженных файлов вирус лечит их. Использует несколько уровней шифровки, при этом процедуры шифровки/расшифровки базируются на 64-битном алгоритме. В вирусе также встречаются антиотладочные и прочие приемы, затрудняющие его анализ. **7-го июля** в 7:07 вирус выводит текст и завешивает компьютер: My name is Monica. I'm your new virus. If you are a programmer, you can try to decode the author's info, that is encrypted somewhere in my body. The decryption routine is also implemented. You must only guess the key ... Good luck, friend. Now I stopped the computer. Press RESET, please. В теле вируса действительно присуствует строка текста, зашифрованная 64-битным крипто-алгоритмом с неизвестным ключом. После расшифровки этот текст выглядит следующим образом: Hi! You are really very good. So: My name is Michal Hanko, I'm from Czech Republic. I live in Letovice, Halasova street in Southern Moravia near Brno. My E-Mail is: hanko@math.muni.cz. Please, mail me that you've been succesful. Copyright (c) Majkl soft.
Macro.Word.Williamto	9.7	Зашифрованный Word макро-вирус, стелс, содержит 16 макросов: Halim, FileNew, AutoOpen, FileOpen, FileSave, FileClose, FilePrint, HelpAbout, Williamto, FileSaveAs, ToolsMacro, FormatStyle, JustifyPara, ViewToolBars, FileTemplates, ToolsCustomize. Записывается в область глобальных макросов при открытии зараженного документа (AutoOpen). Заражение документов происходит при их открытии, сохранении и сохранении с другим именем (FileOpen, FileSave, FileSaveAs). Стелс: подменяет системный диалог просмотра макросов на другой, который при нажатии на кнопки выдает MessageBox:

		WordBasic Err = 7 Not enough memory После открытия файлов выдает диалог: Williamto Virus Williamto WordBasic Virus Programmed by Williamto Halim Virus Research Laboratory Dedicated to Angelia Hadeli В случае ошибки при сохранении выдает MessageBox: Attention!!! Williamto Halim always lives in your computer При закрытии фалов выводит MessageBox: File Close Please close it later! Let's have fun! **9 июля** выдает поздравительный MessageBox: Nice Day Happy Birthday Amgelia Hadeli by Williamto Halim Подменяет About Microsoft Word на свой: About Microsoft Word Williamto WordBasic Virus Programmed by Williamto Halim Virus Research Laboratory Dedicated to Angelia Hadeli При печати стирается текст пользователя, а на печать выводится текст вируса: Welcome to Williamto Word Macro Virus I'm sorry about this but your computer has been infected by Williamto Word Macro Virus Please beware about this!!! This Virus will destroy your data in your disk!!! Copyright 1997 Virus Research Labs (Jakarta/Indonesia) При этом в строку состояния посимвольно выводится сообщение: [Welcome to Williamto Word Macro Virus - Programmed & Written by Williamto Halim the Hackers - Virus Research Laboratory] 11 ноября форматируется винчестер, перед этим выведя MessageBox: Attention!!! I will format your hard disk now, ha-ha-ha!
Macro.Word.Trash	24.7	Стелс макро-вирусы семейства "Trash" содержат три зашифрованных макроса: Документы NORMAL.DOT Save000 FileSaveAs,Save000 AutoOpen,Toolsmacro Toolsmacro Система заражается вирусом при открытии зараженного файла

		(AutoOpen). В документы вирусы записываются при сохранении документов с новым именем (FileSaveAs). **24 июля** стирает файлы C:\COMMAND.COM, C:\IO.SYS. В случае срабатывания макросов, если системное время - 55 секунд, вирус стирает файлы A:*.*, при значении времени менее 5 минут - заменяет слова на выражения: "hard" -> "fucking hard" "easy" -> "a piece of piss" "think" -> "fucking knows"
Minosse.3072	25.7	**Опасный резидентный полиморфик -вирус**. Перехватывает INT 21h и записывается в конец EXE-файлов при их запуске. **25-го июля** завешивает компьютер. Содержит строки: Minosse 1v5(c)93 WilliWonka □□□ CAMALEOCODE 4.1 by M.M.M. (c) 1993 □□□
Jobi	27.7	**Опасный резидентный загрузочный вирус**. Перехватывает INT 13h и записывается в boot-сектор диска C: и boot-сектора дискет. Сохраняет первоначальный boot-сектор в конце диска. **27-го июля** завешивает компьютер. Содержит строку: Ugly Jo's birthday
Wintermute.1052	26.7	**Опасный резидентный зашифрованный вирус**. Перехватывает INT 21h и записывается в конец COM- и EXE-файлов при их запуске. **26-го июля** при вызовах DOS-функций FindFirst/Next FCB и ASCII "показывает" у всех файлов длину 666 байт (это может привести к порче файлов при их копировании в архивы). Содержит строку: Apocalyptic by Wintermute/29ACOM
Koko.1780	29.7	**Опасный резидентный вирус**. Перехватывает INT 21h и записывается в конец COM- и EXE-файлов при их запуске. **29-го июля** и 15-го февраля выводит сообщение, после чего может стереть сектора дисков: Stop Keyboard Clicking KoKo is Sleeping in Your PC. ! To Scan & Clean Call, Adham Hammam Fax & Phone (20) 066 – 261841