Неопасные вирусы в июле

Название	Даты активации	Описание
A2Space, семейство	x.7	**Неопасные резидентные вирусы**. При запуске поражают файлы C:\COMMAND.COM и \COMMAND.COM. Затем перехватывают INT 17h, 21h и записываются в конец COM- и EXE-файлов при их запуске. **В июле** по вторникам и четвергам при печати заменяют символы 'A' и 'a' на пробел. Содержат строку: C:\COMMAND.COM
Arcv.Ice.330	x.7	**Нерезидентные безобидные вирусы**. Ищут .COM-файл текущего каталога и записываются в его конец. "Arcv.Ice.250,330" шифруют себя. Вирусы содержат в себе текст "*.COM" и "Arcv.Ice.159" - [159] ICE-9 "Arcv.Ice.199" - [199] ICE-9 "Arcv.Ice.224" - [224] ICE-9 "Arcv.Ice.250" - [250] ICE-9 **В июле** "Arcv.Ice.330" выводит текст: "[330] by ICE-9".
Rawal.1378	x.7	**Неопасный нерезидентный вирус**. При запуске ищет командный процессор (COMMAND.COM), затем .COM-файлы и записывается в их конец. **В июле** расшифровывает и выводит текст: B I O - D A T A NAME : SANJAY RAWAL DOB : 24/11/1967 ADDRESS : 96, SATYA NIKETAN, NEW DELHI - 21 TELE : 675557 QUALS. : DIP. ELECTRICAL, SEC-A DIP. I.E.T.E.,POST DIP. : COMPUTER APPLICATIONS, SHORT COURSE FROM A.T.I.E.P.I. EXPRNCE : DBASE III+,CLIPPER,FOXPRO,ASSEMBLY 85/88, QBASIC,TURBO C : SINCE JAN. 1990 A N Y V A C A N C Y ???? Содержит также строки: *.com COMSPEC= S A N
CodeBreaker.431	1.7	**Неопасный нерезидентный вирус**. Ищет .COM-файлы и записывается в их конец. При заражении также записывает часть своего кода в середину файла. Для того, чтобы оставить файл работоспособным, вирус запоминает этот блок кода в своем теле и восстанавливает его перед возвратом управления зараженной программе. **1 июля** выводит текст: The temple bell stops, But the sound keeps coming Out of the flowers. Также содержит строки: [Basho] Sea4, CodeBreakers
HongKong.1997	1.7	**Неопасный резидентный зашифрованный вирус**. Записывается в начало COM-файлов (кроме COMMAND.COM), середину EXE-файлов и MBR винчестера. При запуске зараженного файла записывается в MBR, затем (также, как и при загрузке с зараженного

		винчестера) перехватывает INT 13h, 21h и заражает запускаемые файлы. При помощи перехвата INT 13h реализует стелс при чтении/записи зараженной MBR. При запуске зараженных файлов вирус проверяет командную строку. В зависимости от каких-то символов в этой строке (вирус использует двух-байтную китайскую кодировку) вирус либо лечит MBR, либо выводит текст: HONG KONG 1997 Это же сообщение выводится **1-го июля**. Вирус использует несколько приемов противодействия отладке и лечению: при заражении MBR зиписывает в Disk Partition Table такой код, что MS-DOS (включая DOS 7.0) записает при загрузке с системной дискеты (при этом вирус вполне нормально грузится с винчестера). В результате оказывается невозможным загрузить систему с дискеты, проверить диск и вылечить вирус при помощи расположенного на дискете антивируса. Второй прием заключается в том, что 90% кода вируса (ассемблерных команд) перемешано с одно-байтовым случайным мусором. Для того чтобы пропускать этот мусор при работе, вирус перехватывает INT 1 (трассировка) и при выполнении каждой команды своего кода вызывает процедуру, пропускающую байты мусора.
Party, семейство	1.7	**Неопасные нерезидентные вирусы**. Ищут .COM-файлы и записываются в их конец. **1-го июля** выводят текст: This is Weeding Party 1.0 virus by Dark Judge in Tainan, Taiwan <R.O.C>
Macro.Word97.Calendar	1.7 4.7	Содержит 7 макросов: AutoOpen, AutoClose, ToolsMacro, FileSaveAs, FileTemplates, Calendar, ViewVBCode. При открытии файла выключает опцию VirusProtection, заражение происходит при открытии, закрытии и сохранении с другим именем документов (AutoOpen, FileClose, FileSaveAs). При вызове меню Tools/Macro выдается MessageBox: Microsoft Word You do not have permission to do this По праздникам выдаются поздравительные MessageBoxes: 1 января "New Year's Day", 20 января "Martin Luther King Jr. Day", 12 февраля "President Lincoln's Birthday and Ash Wednesday", 14 февраля "Valentine's Day", 17 февраля "Presidents Day", 22 февраля "President Washington's Birthday", 17 марта "St. Patrick's Day", 23 марта "Palm Sunday", 28 марта "Good Friday", 30 марта "Easter", 22 апреля "Passover", 9 мая "Calendar, coded by DarkChasm [SLAM]", 11 мая "Mother's Day", 17 мая "Armed Forces Day", 19 мая "Victoria Day", 26 мая "Memorial Day Observed", 30 мая "Traditional Memorial Day", 15 июня "Father's Day", **1 июля** "Canada Day", **4 июля** "Independence Day", 2 октября "Rosh Hashonah", 11 октября "Yom Kippur", 12 октября "Columbus Day", 13 октября "Columbus Day Observed", 16 октября "Happy Birthday DarkChasm", 24 октября "United Nations Day", 31 октября "Halloween", 4 ноября "Election Day",

		11 ноября "Veteran's Day", 27 ноября "ThanksGiving Day", 21 декабря "Happy Birthday Christy", 24 декабря "Christmas Eve and Hanukkah", 25 декабря "Christmas", 31 декабря "New Year's Eve".
Macro.Word97.Ethan	2.7	Макро-вирусы семейства содержат одну процедуру "Document_Close" в модуле "ThisDocument". Заражение системной области макросов происходит при закрытии зараженного документа. Другие документы заражаются также при их закрытии. При заражении вирус выключает встроенную защиту от вирусов MS Word (опцию VirusProtection) и предупреждение о изменении файла NORMAL.DOT. При инсталляции в систему вирус создает в корне диска C: файл ETHAN.___ и записывает туда код всех процедур текущего модуля (включая невирусные, если таковые присутствуют). Этот файл используется вирусом при заражении документов вирус: он копирует в них свой код, сохраненный в этом файле. Вирус удаляет файл C:\CLASS.SYS, который содержит экспортированный код вируса "Macro.Word97.Class". В зависимости от системного счетчика случайных чисел вирус изменяет служебные поля документов: Title: Ethan Frome Author: EW/LN/CB Keywords: Ethan ***Ethan.d*** В первый рабочий день каждого месяца 1999 года при открытии документов до полудня вирус выдает на экран одно из сообщений: 1 апреля 1999 г.: Y2K! Spread the word This is not an April fools joke. I wish it were! The year 2000 is fast approaching, and the word still needs to be spread about the implications and dangers of the millennium bug commonly referred to as the Y2K bug. The virus that has infected this word document was written to help spread the word about the Y2K bug, and educate you so you can prepare yourself and your family for Saturday January 1, 2000. Today until January 1, 2000, on the first business day of each month, I will give you a lesson in Y2K preparation. Spread the word. Knowledge is power! 3 мая 1999 г.: Hello again! Lets start our first lesson to help prepare you for the millennium bug. Although I don't personally believe there will be food shortages, power shortages, gas shortages as a result of a computer bug, there will be food, power and gas shortages by hoarding nitwits that fear the millennium bug. As a result, I highly recommend that you begin to stockpile bottled water (1-month supply), canned food (1-month supply), and as much gas as you can store (keep your vehicle gas tank always topped up starting December 1st). That's it for this month. See you next month! 1 июня 1999 г.: How's the weather? Right now it's pretty warm out, so you are probably not thinking much about the winter. But remember the millennium bug is expected to hit in the middle of winter. If you're in a northern climate, like the Great White North (Canada), I suggest you consider purchasing a good airtight wood stove, and at least a face cord of wood. Even if there are no disruptions in natural gas, or oil, or electricity, the wood stove is a great way of reducing your heating bills. And if there is a problem, you will be comfortable in your own heated home, unlike your unprepared neighbors (remember the Canadian ice storm last year!) That's it for this month. See you next month!

		2 июля 1999 г.: Did you get the stove? Last month I recommend purchasing a gas stove to help heat your home in the event that your supply of electricity, gas, or oil was interrupted. This month I would like to suggest that you purchase a portable generator and enough gas cans to store gas to power the generator. The generator can be used to power lighting and small electrical appliances should the power be disrupted. That's it for this month. See you next month! 2 августа 1999 г.: Getting back to basics In this installment, I would like to suggest that you consider purchasing candles, matches, flashlights, and batteries. These items will be invaluable during those cold, dark nights should the power companies fail in their Y2K conversion. Don't plan on relying on the banks or credit/debit cards. Start each month, and stash away enough money to last you at least 2 months. This money should include enough money to pay the rent/mortgage, utilities, FOOD, etc. Remember cold hard cash is accept EVERYWHERE. That's it for this month. See you next month! 1 сентября 1999 г.: A Limerick The millennium 's not far away Get onto your coding today Fix it or fudge it The boss won't begrudge it If everything works on the day! That's it for this month. See you next month! 1 октября 1999 г.: Three months to go Getting nervous? If you've followed my advice over the past months, there should be nothing for you to worry about. We will survive the Y2K bug, but preparation will insure that if there is any Y2K crisis, it will only be small bump on the road, not a major pothole for you. That 's it for this month. See you next month! 1 ноября 1999 г.: Two months to go Personally, I don't believe that there will be a major, global Y2K crisis. I trust the banks with my money, I trust MOST of the industrial sector, and I trust the power and water agencies to provide me with power and water over the infamous weekend. I even trust the Russians and there nuclear arms! BUT you can never be too careful. Take care. Be prepared. Use common sense. That 's it for this month. See you next month!" 1 декабря 1999 г.: Good Luck (30 days to go) Well, this will be the final installment in the Y2K preparation lessons. If you have followed my advice over the past few months, you will be in excellent shape to bring in the New Year. May the New Year bring you health and happiness. Best wishes. Bye!
Macro.Word.Ordo	2.7	Содержит всего 2 макроса: AutoOpen, ORDO. Размножается при открытии документов. Передается от файла к файлу не переписываясь в NORMAL.DOT - для этого открывает все документы из списка последних редактированных, заражает и затем закрывает. **2 июля** регистрирует в системе программу для сохранения экрана - \SYSTEM\MARQUEE.SCR, однако не создает этого файла на диске.
Glitter, семейство	4.7	**Неопасные нерезидентные зашифрованные вирусы.** Ищут COM- и .SYS-файлы и записываются в их конец. 8 мая, **4 июля**, 3 сентября и 5 ноября "Glitter.1462" выводит текст: □ Wish you a Happy Birthday □ Love Guess Who !! □? Вирусы также содержат строки: "Glitter.1207":

		□Glitter ver 1.0 , Coded by Siddharth.□ SID IS IN YOUR RAM CHIPS □ □Greetings From Siddharth Bombay-92□ "Glitter.1462": □Glitter ver 1.03 , Coded by DDISARTHH, □Hi Avi Guess Who?□ □Greetings From Siddharth, Mumbai 400 092□
Currar.1171	5.7	**Неопасный нерезидентный вирус**. При запуске ищет .COM-файлы и записывается в их конец. **5-го июля** выводит текст: Hoy me toca currar en tu ordenadoR Также содержит строки: *.COM CuR c:\command.com
OneMinute.2420	6.7	**Неопасный нерезидентный полиморфик –вирус**. При запуске ищет .COM- и .EXE-файлы (кроме COMMAND.COM), затем записывается в конец EXE-файлдов и начало COM-файлов. Уничтожает антивирусные базы данных: SMARTCHK.CPS, CHKLIST.CPS, CHKLIST.MS. 1-го января, **6-го июля**, 9-го сентября выводит текст: This day in the year 1976, [xx] China, had been left us for ever. Now, in order to express cherish the memory of this great man, let's observe One minute's silence... [yy] Thank you! Где [xx] является строкой: 1 января: Chou Enlai, Premier of the State Council of **6 июля**: Chu Te, Chief of the Standing Committee of the National People's Congress of 9 сентября: Mao Tsetung, Chairman of the Communist Party of и [yy] является счетчиком секунд - от "60" до "00".
Argentina	9.7	**Резидентный неопасный вирус**, перехватывает INT 21h и записывается в начало стартующих .COM-файлов (кроме COMMAND.COM). При этом вирус создает файл MOM.MOM, записывает туда себя, затем добавляет заражаемый файл, удаляет его и переименовывает MOM.MOM в его имя. Если стартует COMMAND.COM вирус проверяет текущую дату и 25-го мая, 20 июня, **9 июля**, 17 августа выводит одно из сообщений: 25 de Mayo Declaracibn de la independencia Argentina 20 de Junio Dia de la bandera Argentina 9 de Julio Dia de la independencia Argentina 17 de Agosto Aniversario de la defuncibn del Gral. San Martin Затем выводит: Argentina Virus escrito por AfA - Virus benigno - ENET 35 Pulse una tecla para continuar... Также содержит строки: Argentina Virus 1.00 COMMANDCOM :MOM.MOM
Tucuman.828	9.7	**Резидентные вирусы**, перехватывают INT 21h и записываются в конец запускаемых EXE-файлов. "Tucuman.828" неопасен - **9-го июля** проявляется видео-эффектом. Содержит строки:

		"Tucuman.828": UTN-FRT Tucuman, Argentina by Mr. Bithead – 1995
Cumple.1249	11.7	**Неопасный резидентный вирус**. Перехватывает INT 21h и записывается в начало .COM-файлов (кроме COMMAND.COM) при их запуске. При заражении переименовывает файлы в MOM.MOM, заражает их, а затем переименовывает обратно. Выводит сообщения: 15-го ноября: Hoy es el cumpleaños de AэЯЯюю ... !!! **11-го июля**: Hoy es el cumpleaños de cЪЬIhЭ ... !! 28-го апреля: Hoy es el cumpleaños de KM чэ ... !!! Также содержит строки: COMMANDCOMMOM.MOM MrцsATT Activado . By \\prчMy and \\prЬIюЬэ ... :) Espere 2 min. para continuar :)
Macro.Word.PCW	15.7-30.7	Зашифрован, содержит два макроса: AutoOpen, DateiSpeichernUnter. Заражает систему при AutoOpen, записывается в файлы при DateiSpeichernUnter (FileSaveAs). Если номер текущего дня **>=15** и номер месяца **>=7** (**июль**), вирус выводит MessageBox: Happy Birthday Herzlichen Gl0ckwunsch Susanne B. aus E. zu deinem Geburtstag Ich liebe dich
Paradise.1400	17.7	**Неопасный резидентный полиморфик –вирус**. Трассирует и перехватывает INT 21h, затем записывается в конец COM- и EXE-файлов при обращениях к ним. При заражении переводит EXE-файлы в формат COM. **17-го июля** выводит одно из сообщений: LOST PARADISE GOTHIC SHADES OF GOD ICON Также содержит строки: PANTERA PARADISE LOST
Voices.1500	17.7	**Неопасный резидентный полиморфик-вирус**. Трассирует и перехватывает INT 21h, затем записывается в конец COM- и EXE-файлов при обращениях к ним. При вызовах DOS-функции FindFirst FCB (команда DIR) поражает файл COMMAND.COM. В зависимости от своего случайного счетчика заражает файлы повторно. **17-го июля** выводит текст: Hearing Voices, when I'm all Alone Hearing Voices, but there's nobody Home Также содержит строки: Discharge Sofia Command.com you keep this love tuturutki s.t. possessed SUICIDAL TENDENCIES
AntiEta.5315	21.7	**Неопасный резидентный полиморфик -вирус**. Записывается в конец COM- и EXE-файлов. Использует несколько уровней

		самошифровки как в файлах, так и в своей TSR-копии. **21-го июля** выводит изображение ладони и текст: "ANTI-ETA". Содержит также строку: << ANTI-ETA ViRuS Bio.Coded By GriYo / 29A >> При запуске зараженного файла вирус перехватывает INT 21h и остается резидентно в памяти. Затем он при запуске и открытии файлов запоминает их имена и заражает их при закрытии или окончании работы программ. Не заражает файлы с именами: TBAV, SCAN, WIN and COMMAND.COM. При смене текущего каталога в зависимости от своего случайного счетчика создает зараженный COM-файл со случайным именем. Уничтожает антивирусные файлы данных: ANTI-VIR.DAT, CHKLIST.MS.
AntiGUS.1570	24.7	**Неопасный резидентный полиморфик -вирус.** Перехватывает INT 8, 21h и записывается в конец EXE-файлов при их запуске. **24-го июля** сообщает: Happy birthday to me! :-) В зависимости от своего внутреннего счетчика пишет какие-то данные в какие-то порты (выключает Gravis Ultra Sound card?). Вирус также содержит строки: E-VIRUS II aka Anti-GUS.12th December 1994.KL,Malaysia. @@@@@TM was here!@@@@@
Macro.Word97.Lulung	26.7	Содержит 23 макроса. При открытии зараженного документа код вируса переносится в NORMAL.DOT. Заражение документов происходит при открытии, закрыти и записи их на диск, а также при закрытии Word'a. Вирус отключает опцию VirusProtection, комбинации клавиш Alt-F8 и Alt-F11, прячет панель инструментов "Visual Basic" и меню "Tools/Macro...". **26 июля** выдает сообщение: Today Is My Wife's Birthday. Happy Birthday Honey! 8 февраля выдает сообщение: Today Is My Wedding's Day. Thank's God! 8 июня, а также при выборе некоторых пунктов меню показывает диалоговое окно с фотографией. Код вируса содержит комментарии: Welcome To My Listing Program ! Created and Programmed By. June 8, 1971 йApril, 1998 - Ciputat Sorry, If my program disturbs you ! It's not danger, I just want to be your friend !
Morgan.470	26.7	**Неопасный нерезидентный вирус**. Ищет .COM-файлы и записывается в их конец. **26-го июля** и 6-го декабря выводит текст: You have been infected by a living MORGANISM
Australian.482	27.7	**Неопасный резидентный вирус**. Перехватывает INT 21h и записывается в конец COM-файлов при их запуске или загрузке оверлеев. **27-го июля** выводит сообщение:

		The Hitcher virus. Hitchhiking through your system. Didn't your mum tell you not to pick up stray viruses. Также содержит строки: The Hitcher virus #1p by AP[AIH] HITCHER
Macro.Word.Nova	28.7	Зашифрован. Содержит 2 макроса: AutoExit, AutoClose, и заражает систему и документы при закрытии файлов. При выходе из Word **28 июля** выдает в StatusBar строки: + meu aniverscrio Parabцns para mim! По другим дням выводит: Nova Vэtima Fechando 2807M!
Macro.Word97.Nova.e	28.7	Содержит два авто-макроса: AutoClose и AutoExit. Заражение глобальных макросов и документов происходит при закрытии инфицированного документа. При выходе из Word **28-го июля** выдает сообщение: Meu aniversбrio Parabйns para mim! В другие дни: Nova Vнtima Fechando 2807M!