

VIRUS: ETAT DES LIEUX

OSSIR – Groupe Sécurité Windows – 8 juillet 2002

François PAGET

McAfee A.V.E.R.T

francois_paget@avertlabs.com

<http://www.avertlabs.com>

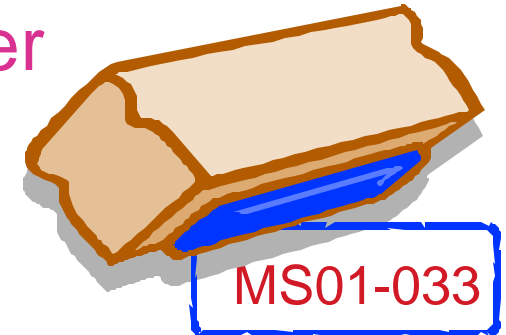
COPYRIGHT

Copyright (c) 2002 Network Ass. Tous droits réservés. Cette présentation ne peut en aucun cas, même partiellement, être reproduite, diffusée, transcrite, stockée dans un système de récupération ou traduite dans quelque langue que ce soit, de quelque manière ou par quelque moyen que ce soit, sans la permission écrite de Network Ass., et de son auteur.

VIRUS: ETAT DES LIEUX

- 2001: L'APOGEE (?) DES VIRUS COMMUNIQUANTS,
- EVOLUTION ET PERSPECTIVE,
- L'OBSERVATOIRE VIRUS,
- QUELQUES CONSEILS.

En 2000 et 2001, les principaux virus furent ceux qui exploitaient les outils de messagerie, INTERNET ou le réseau pour se propager



17 juillet 2001: **W32/CodeRed.A**

Un exemple de propagation rapide.

- Uniquement en mémoire dans sa version initiale, il doit être détecté dans le flux HTTP.
- Cible les serveurs IIS, infecte W2K & XP par le port TCP/IP 80
- Autonome, le virus s'active et se joint aux autres pour rechercher d'autres cibles (scan IP) tout en causant des ralentissements et des arrêts système sporadiques.
- Attaque DDoS sur www.whitehouse.gov
- 250.000 machines sont infectées en moins de 9 heures

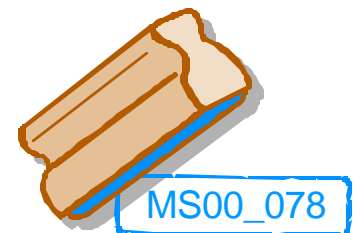
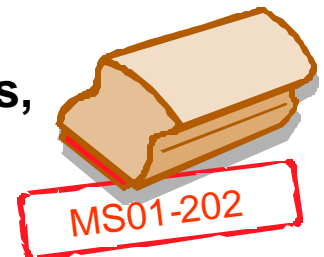
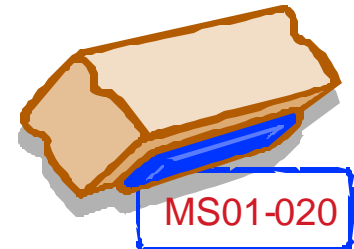
Panorama de la Cyber-criminalité, année 2001 - CLUSIF

En 2000 et 2001, les principaux virus furent ceux qui exploitaient les outils de messagerie, INTERNET ou le réseau pour se propager

18 septembre 2001: **W32/Nimda@mm**

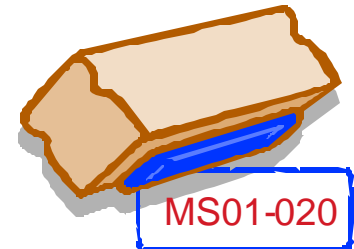
Un exemple de virus multi-facettes

- Propagation par e-mails,
- Propagation à travers des serveurs Microsoft IIS vulnérables,
- Propagation à travers les partages réseaux du système,
- Propagation à travers des consultations web,
- Propagation à travers des fichiers exécutables.
- Propagation lors de l'ouverture de fichiers RTF



Panorama de la Cyber-criminalité, année 2001 - CLUSIF

En 2000 et 2001, les principaux virus furent ceux qui exploitaient les outils de messagerie, INTERNET ou le réseau pour se propager



24 novembre 2001: W32/Badtrans @mm

Un exemple de virus communiquant...

- Il ré-expédie le résultat de ses recherches (autres exemples: W32/Magistr @mm, W32/Klez.h @mm),
- Il porte atteinte à la confidentialité et intéresse le FBI...



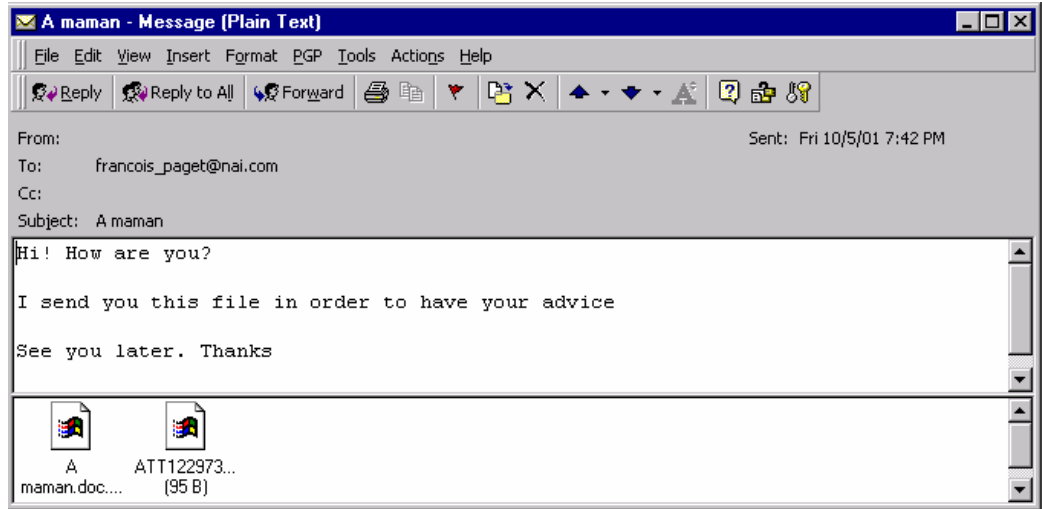
....logpassrem
conternet....



Panorama de la Cyber-criminalité, année 2001 - CLUSIF

W32/Badtrans@mm

L'atteinte à la confidentialité...



```

022240 .....
022280 .....G.....Times New Roma
0222C0 n.....Symbol.. ....Arial.....Times New Roman...
022300           Maman..Déja 15 ans que tu es partie.pourquoi
022340 n'est tu pas resté parmi nous.J'ai souvent l'idée d'aller te rej
022380 oindre depuis quelque temps.Sauf que mes enfants m'en empeches.T
0223C0 u as 5 petit enfants et un 6 en route.Dont deux qui son a moi :X
022400 XXXXXX et YYYYYYY.Je ne suis plus avec leurs pere.De toute facon
022440 s'étais peine perdu..J'ai rencontrer un autre jeune homme.Il a
022480 28 ans,il s'appelle ZZZZ.Il adore les enfants.Sauf qu'il y a que
0224C0 lque chose qui ne clique pas entre nous.Je serais tellement bien
022500 avec.Il est tellement gentil,affectueux,doux avec les enfants.J
022540 e ne sais meme plus quoi penser face a lui.J'aimerais tellement
022580 qu'il m'aime juste un peu.Maman aide moi a voir plus clair je ne
0225C0 sais plus quoi faire ...           Ta fille qui s'ennuie.
022600           YYYYYY xxx.           écrit le 10 octobre 2000.....
022640 .....
022680 .....
    
```

Les virus communicants...

Certains d'entre eux utilisent INTERNET pour se mettre à jour (exemples: W32/Babylonia@mm, W32/Hybris@mm).

```
From: Use-Author-Address-Header@[127.1]
Subject: i_rz D[CZ CzSjaLenCO
Newsgroups: alt.comp.virus
View: (This is the only article in this thread) | Original Format
Date: 2000-12-10 23:13:40 PST
```

```
IMGDDNFKFBKCHDMJILRGJGIGHFDJKIPHGOHGFFMHGJNBIPPEIMPMPQHEL CBROHKIOQN
GNINOZNMDEIJPEIOIDQLHBQBMZFHDZCEJBRJEHNPDHJLIKFGGDKFZCKJCOFPDMIGP
HGQJHJCGFFHBQKJMONHIFNDILMLJKZPGFJLMIKHGEZIBFIGOROPPHICZONRJEEOCGZ
MJPZCJMJLMOIPFFZCJPD LGCONHLGOMKDOKIHQDIPOZHICZDEGDPHPZRB FEDJPEEDFL
FJNKENROQJGCNZGNJKJGIPHPCDKZKNOLFGE BPHEZLOPDOIQZMERJFGFFKOIHCLCFMD
[continues]....
[more coded lines]
GNCMRENJDFJZNNGJMBREKOINQPM
****
```

Google Search:
group:alt.comp.virus
author:Use-Author-Address-Header@[127.1]

VER, VIRUS => PROPAGATION

Le ver est généralement considéré comme un sous-ensemble dans la famille des virus

SUFFIXE '@m'

Le suffixe "@m" est dédié aux virus/vers qui ciblent une seule boîte à lettres à chacune de leur activation.

W32/Ska@m (janvier 1999)
W95/Fix.A@m (septembre 1999)
JS/Kak.A@m (octobre 1999)
W32/Babylonia@m (décembre 1999)
VBS/San@m (février 2001)

SUFFIXE '@mm'

Le suffixe "@mm" est dédié aux virus/vers qui ciblent plusieurs boîtes à lettres à chacune de leur activation.

W97M/Melissa.A@mm (mars 1999)
VBS/Loveletter.A@mm (mai 2000)
W32/Magitr.A@mm (mars 2001)
W32/Sircam@mm (juillet 2001)
W32/Klez.h@mm (avril 2002)

Un risque « Medium » et une extension '@mm' indique un danger majeur potentiel pour une entreprise.

SUFFIXES '@m' et '@mm'

Janvier 1999

W32/Ska@m → Un destinataire à chaque activation.
Le virus met plus de 6 mois pour inonder la planète...

Mars 1999

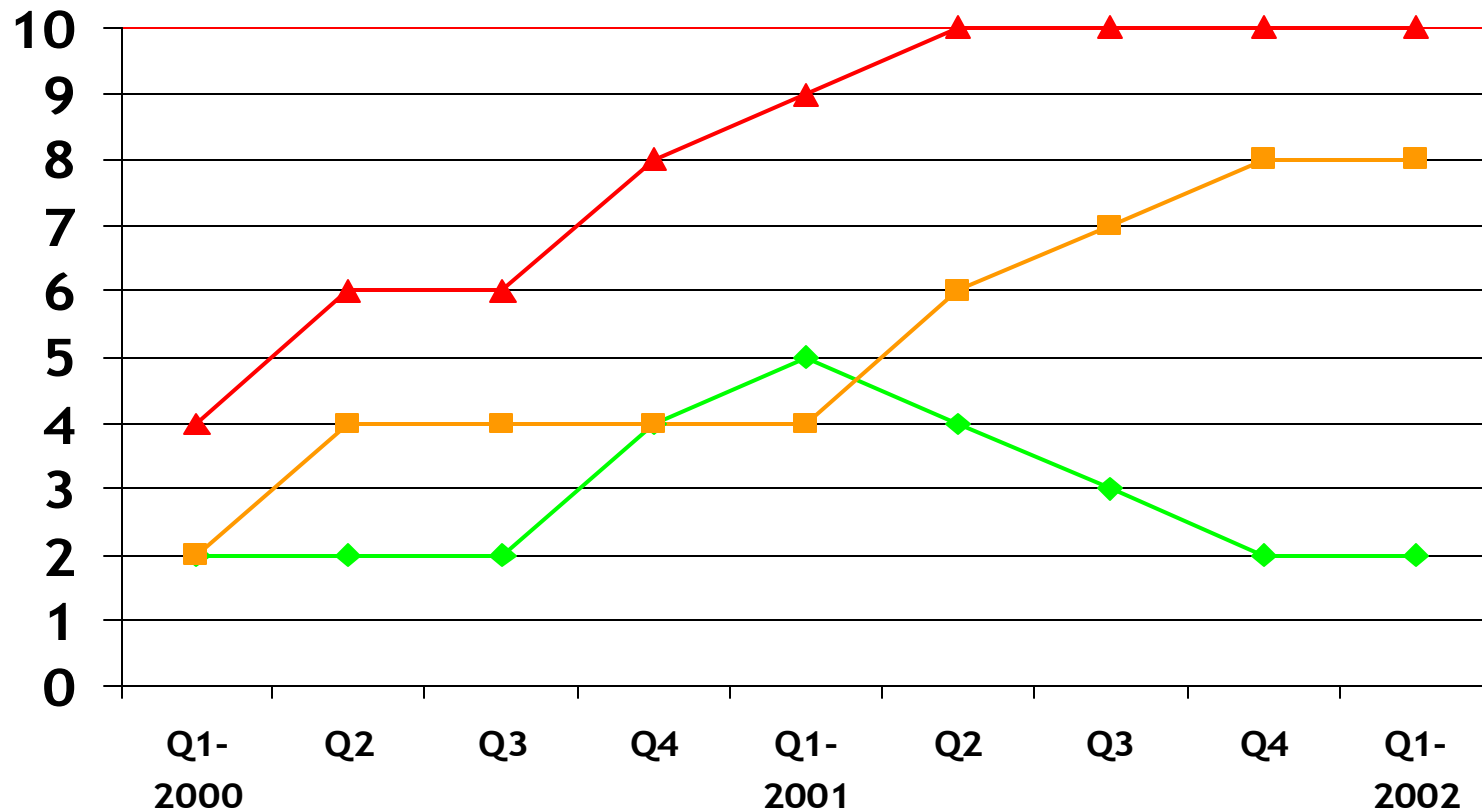
W97M/Melissa.A@mm → 50 personnes dans chaque carnet d'adresses.
Le virus met 2 jours pour se propager à grande échelle...

Mai 2000

VBS/LoveLetter.A@mm → Ensemble des adresses.
Le virus met 3 heures pour son tour du monde...

**Un risque
« Medium » et
une extension
'@mm' indique
un danger
majeur
potentiel pour
une entreprise.**

EVOLUTION DU NOMBRE DES « MASS-MAILERS » DANS LE TOP10 TRIMESTRIEL DU CLUSIF

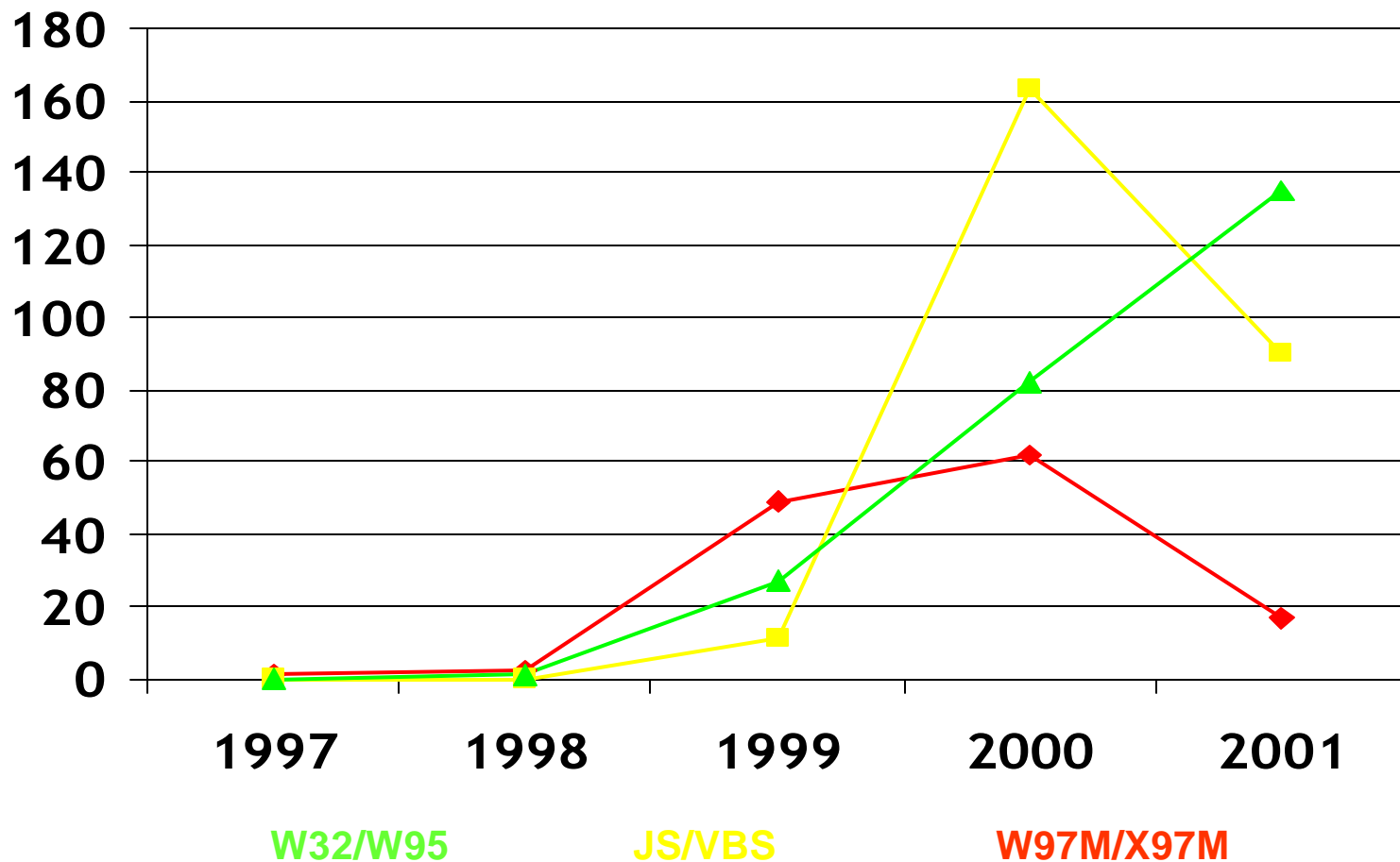


@M + @MM

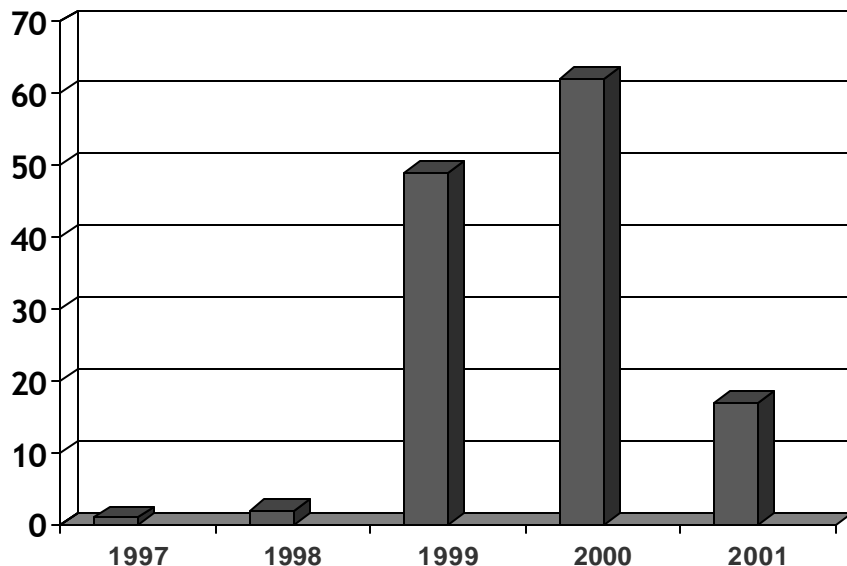
@MM

@M

EVOLUTION GLOBALE DES « MASS-MAILERS » PAR PLATEFORME



EVOLUTION DES « MASS-MAILERS » PAR PLATEFORME



**Les macro virus sont
de moins en moins
répandus.**

La mode est passée.

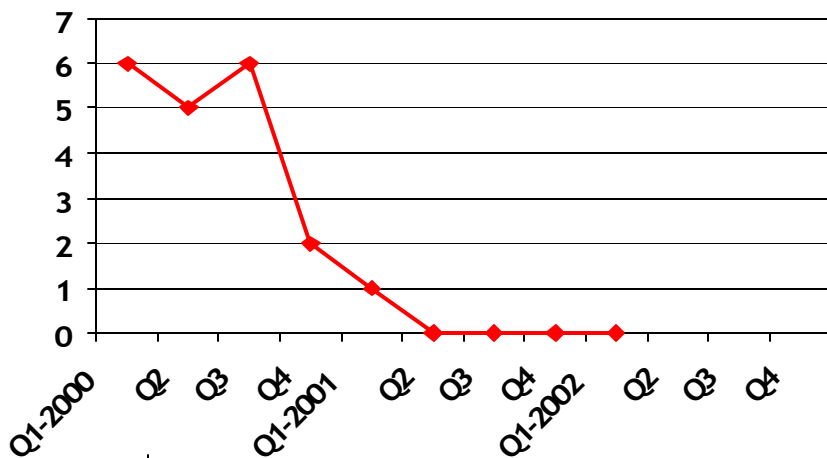
1997	1
1998	2
1999	49
2000	62
2001	17

W97M

X97M

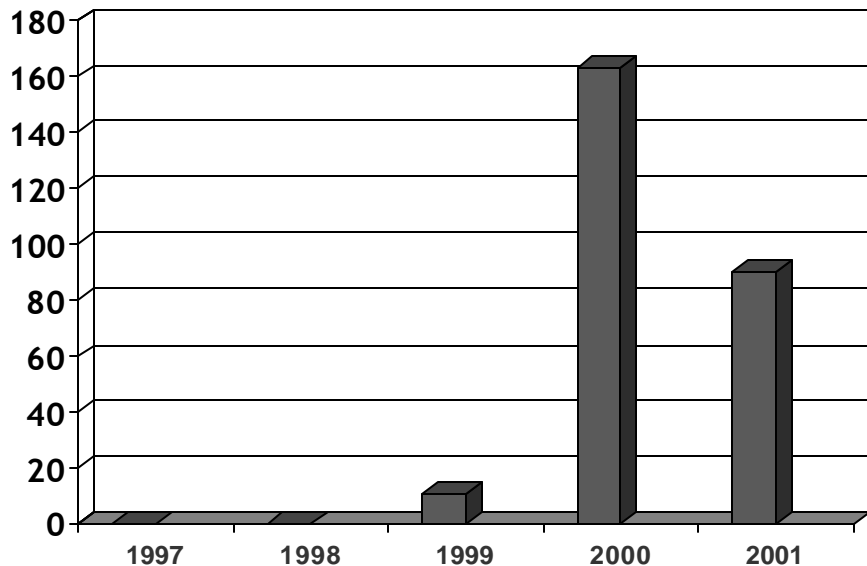
O97M

.....



Nombre de macro-virus dans le TOP 10 de
l'observatoire virus du CLUSIF

EVOLUTION DES « MASS-MAILERS » PAR PLATEFORME



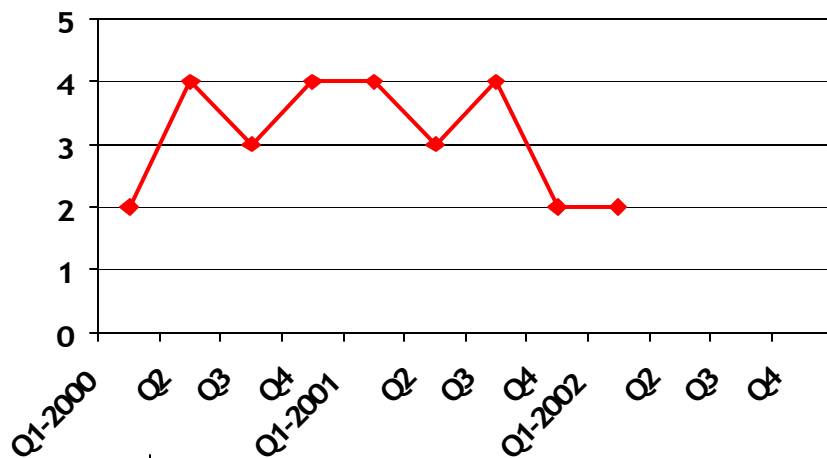
Le nombre de virus JScript & VBScript n'augmente plus.

La mode passe...

JS
VBS

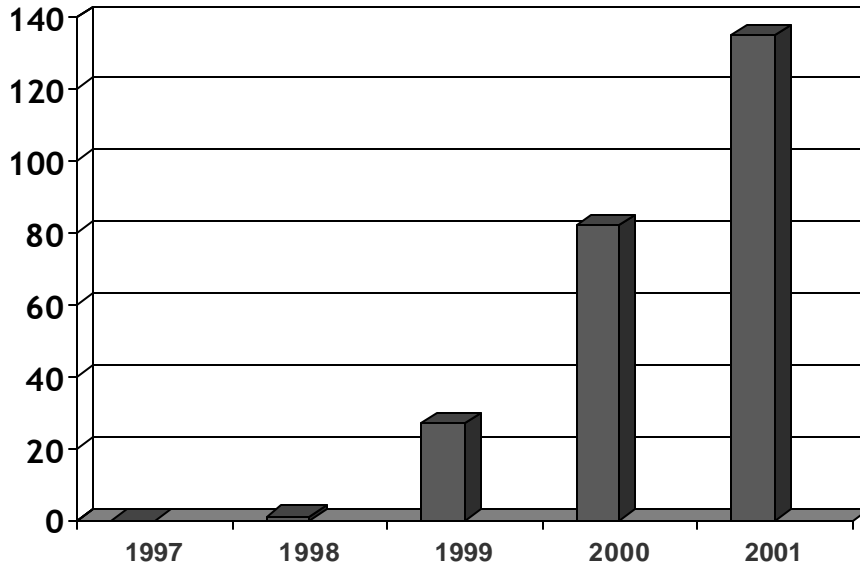
1997	0
1998	0
1999	11
2000	163
2001	90

.....



Nombre de virus de script dans le TOP 10 de l'observatoire virus du CLUSIF

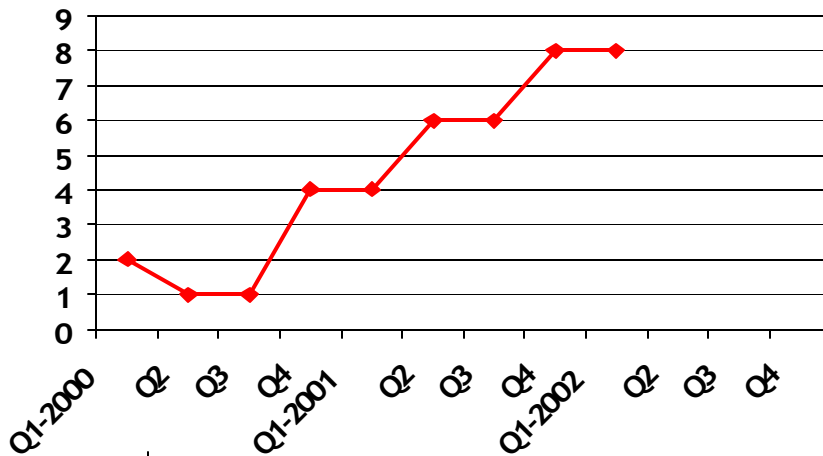
EVOLUTION DES « MASS-MAILERS » PAR PLATEFORME



**Les virus 32bits sont en augmentation.
Les virus programmes reviennent à la mode.**

1997	0
1998	1
1999	27
2000	82
2001	135

W32
W95
W2K
.....



Nombre de virus programmes dans le TOP 10 de l'observatoire virus du CLUSIF

L'OBSERVATOIRE VIRUS

Chaque mois, les membres du CLUSIF qui le souhaitent nous remontent leurs statistiques d'alertes virales. Vous pouvez participer à ce travail collectif en nous faisant part de votre expérience. La compilation de ces données nous permet d'établir une table de prévalence trimestrielle qui regroupe les virus les plus communément rencontrés en France

(<https://www.clusif.asso.fr/index.asp> - choix INFOVIRUS).

	ANNEE 2001	TYPE
01	W32/Sircam@mm	File
02	W32/Badtrans.B@mm	File
03	W32/Magistr.B@mm	File
04	VBS/VBSWG.X@mm (alias Homepage)	Script
05	W32/Magistr.A@mm (et .dam)	File
06	JS/Kak@m	Script
07	W32/Hybris.D@mm	File
08	VBS/Tam.A@mm	Script
09	W32/Navidad.B@m	File
10	W32/Badtrans.A@mm	File

	ANNEE 2001	TYPE
11	W32/Hybris.M@mm	File
12	W32/Hybris.B@mm	File
13	W32/Goner@mm	File
14	W32/MTX.A@m	File
15	VBS/VBSWG.J@mm (alias A. KOURNIKOVA)	Script
16	VBS/Stages.A@mm	Script
17	O97M/Tristate	Macro
18	W32/Navidad.A@m	File
19	W97M/Ethan.A	Macro
20	VBS/LoveLetter.AS@mm	Macro
21	W97M/Marker	Macro

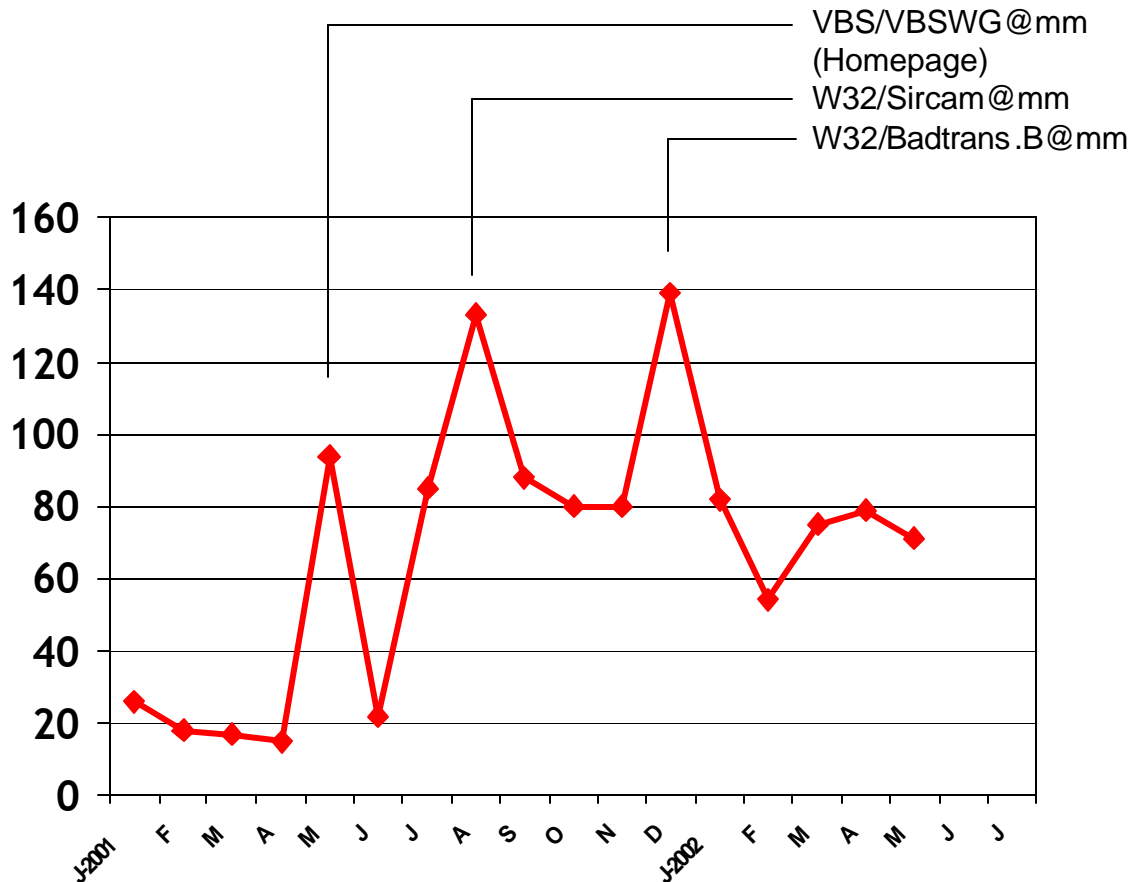
Plus de 50000 alertes
Entre 20000 et 50000 alertes
Entre 10000 et 20000 alertes
Entre 5000 et 10000 alertes
Entre 1000 et 5000 alertes
Moins de 1000 alertes

L'OBSERVATOIRE VIRUS

(<https://www.clusif.asso.fr/index.asp> - choix INFOVIRUS).

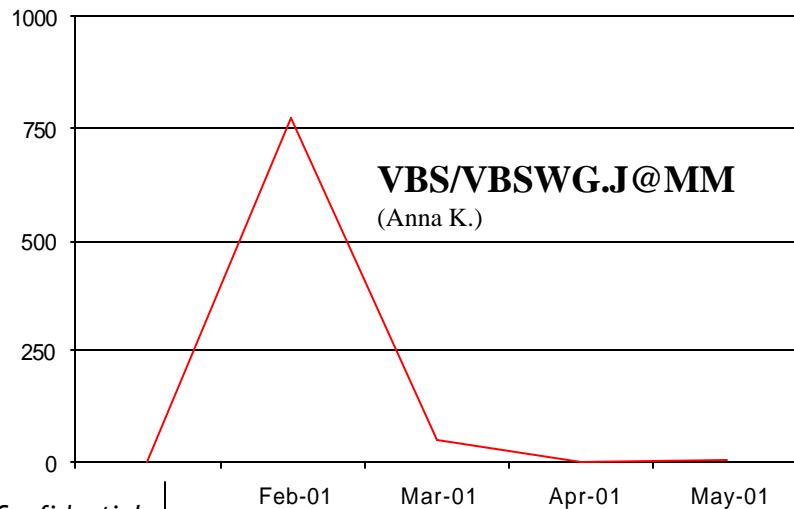
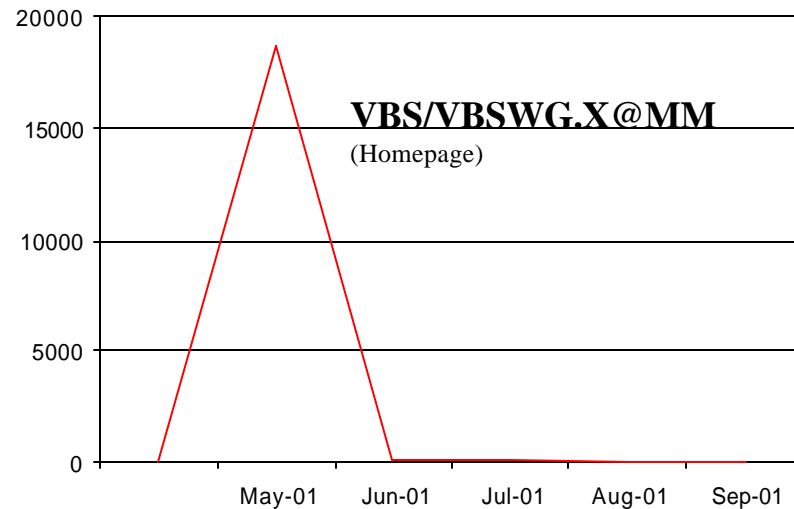
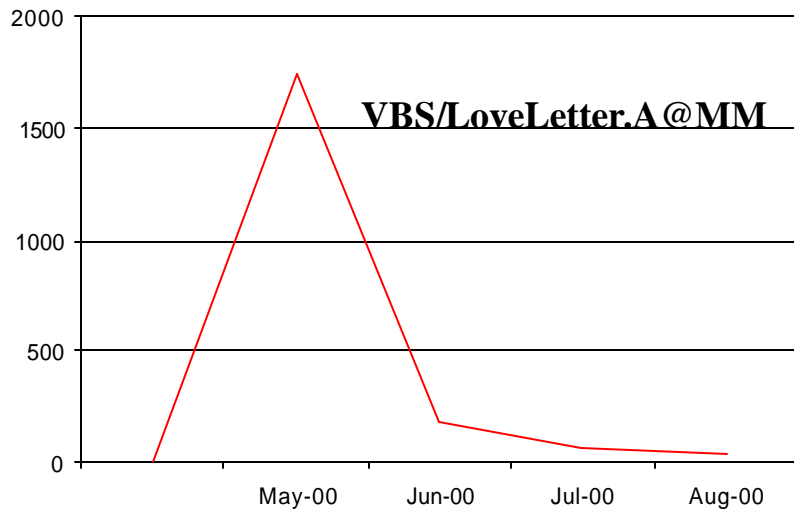
	Q1 ANNEE 2002	TYPE
01	W32/Sircam@mm	File
02	W32/Magistr.B@mm	File
03	W32/Badtrans.B@mm	File
04	W32/Klez.E@mm	File
05	W32/MyParty.A@mm	File
06	W32/Hybris@mm	File
07	W32/Goner@mm	File
08	VBS/Tam.A@mm	Script
09	JS/Kak@m	Script
10	W32/Badtrans.A@mm	File

Plus de 10000 alertes
Entre 1000 et 10000 alertes
Entre 500 et 1000 alertes
Entre 100 et 500 alertes
Entre 100 et 10 alertes
Moins de 10 alertes



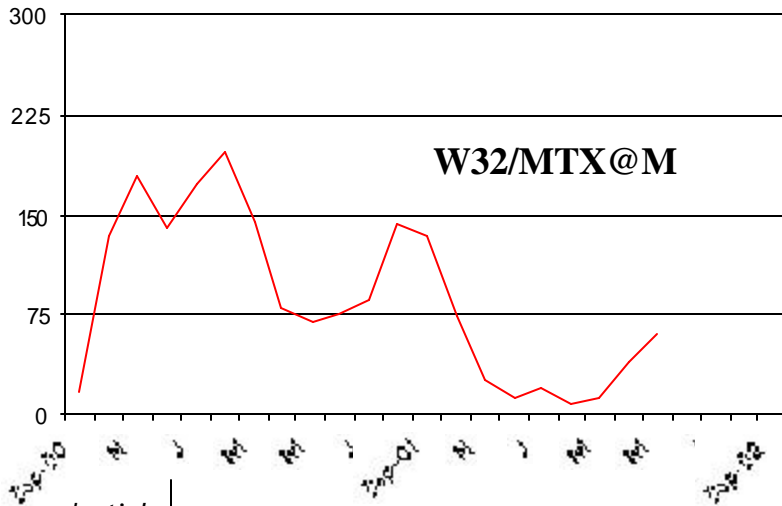
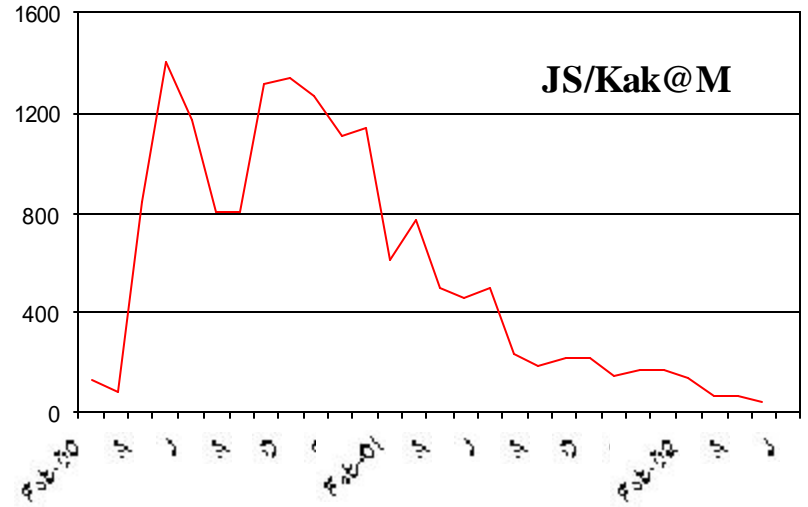
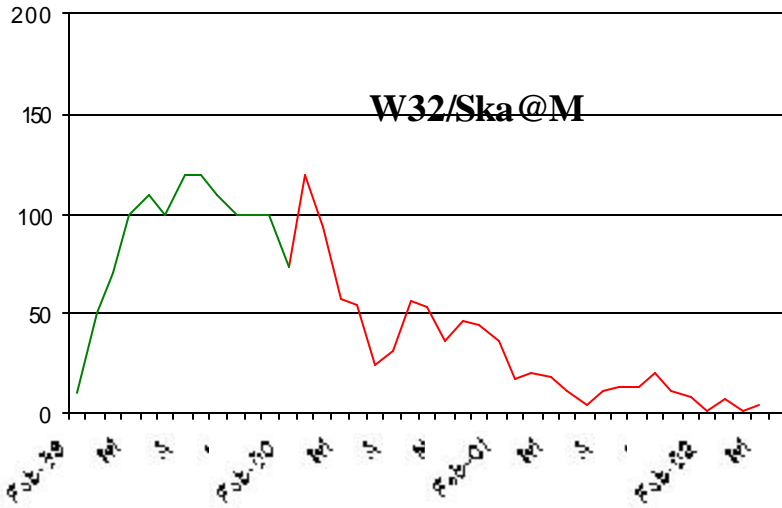
Pour 10000 mails: nombre de mails infectés

EVOLUTION DES « MASS-MAILERS »



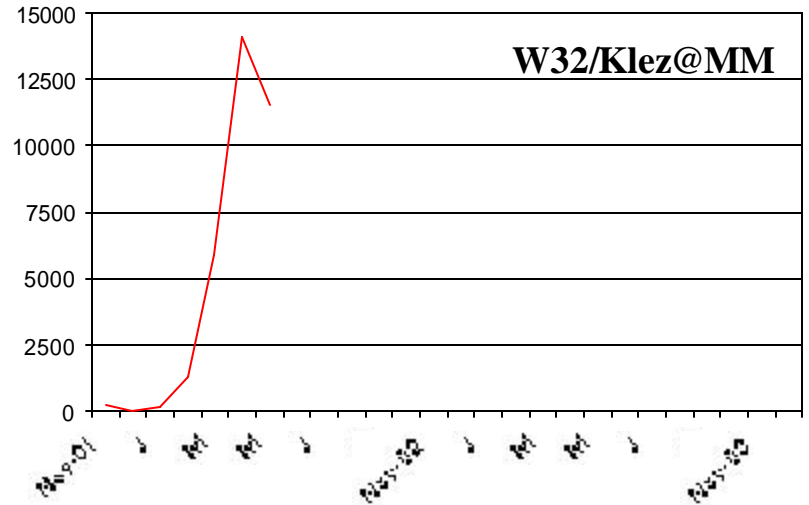
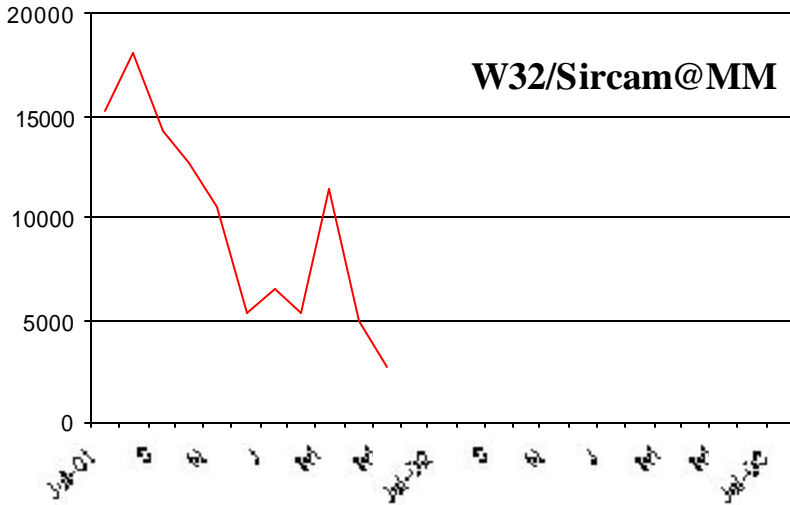
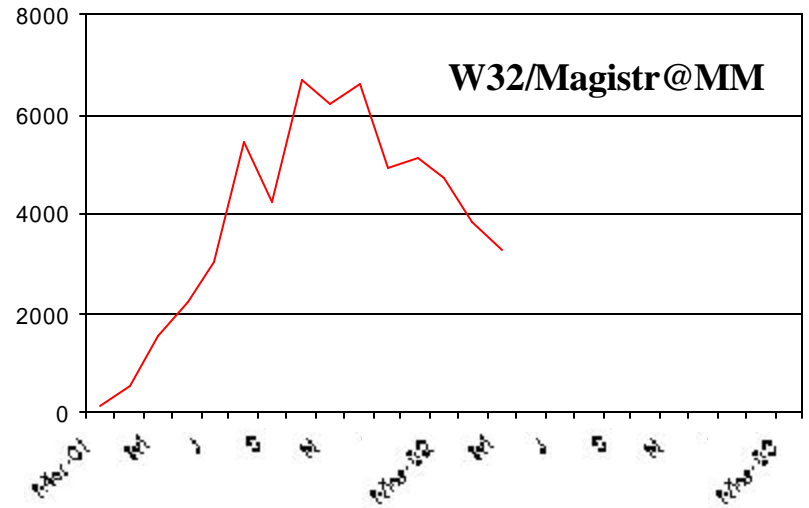
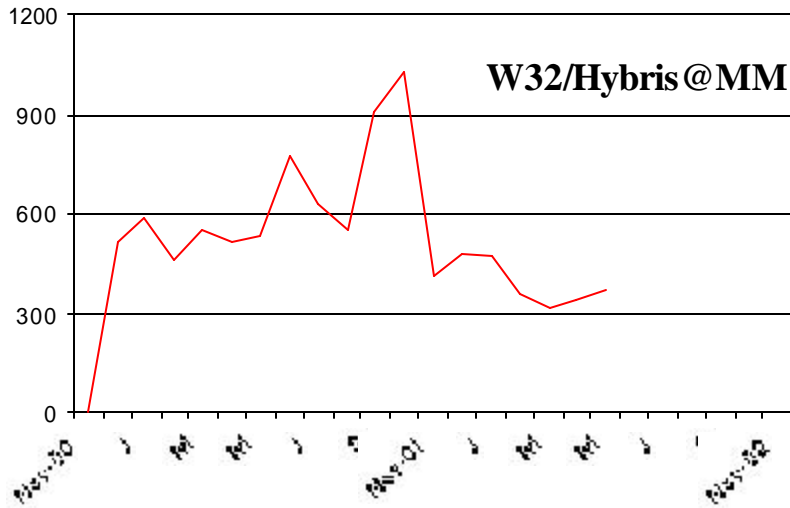
**Durée de vie:
3 mois**

EVOLUTION DES « MASS-MAILERS »



Durée de vie:
2 ans ?

EVOLUTION DES « MASS-MAILERS »



Durée de vie:
3 ans max. ?

RECOMMANDATIONS

- Être à jour sur les patches de sécurité...
- Être protégé sur les 4 niveaux clés: postes, serveurs, messagerie et passerelle.
- Avoir une analyse HTTP native dans le flux (un port 80 est toujours ouvert... sinon pas d'INTERNET...).

W97M/Footprint



W97M/ATU.A



JS/Kak@m
VBS/Bubbleboy@mm



VBS/Davinia@mm



W32/Blebla.B@mm



MS98-008: Long File Name Security Issue

MS98-015: Untrusted Scripted Paste Issue in IE 4.01

MS98-018: Excel « call »

MS99-001: Exposure in Forms 2.0 TextBox Control that allows data to be read from user's Clipboard

MS99-002: Word 97 Template

MS99-014: Excel 97 Virus Warning

MS99-031: Virtual Machine Sandbox

MS99-032: Scriptlet typelib / Eyedog

MS99-044: Excel Sylk

MS00-034: Office 2000 UA Control Scripting

MS00-037: HTML Help File Code Execution

RECOMMANDATIONS

- Contrôler au niveau de chaque poste les applicatifs et les ports utilisés par ceux ci.
- Traquer le « tunneling HTTP ». Beaucoup d'entreprises limitent l'INTERNET à l'HTTP en désactivant le proxy SOCKS. Des sharewares sont disponibles pour permettre aux programmes de traverser les pare-feux sur n'importe quel numéro de port.

W32/CodeRed.C worm (Trojan) →

VBS/Loding.A@mm →

SunOS/BoxPoison worm (for replication) →

SunOS/BoxPoison worm (for payload) →

W32/Fever@m →

W32/Nimda.A@mm →

Goga/DUNpws.ik trojan →

MS00-052: « Relative Shell Path » Vulnerability

MS00-075: Microsoft VM ActiveX Component

CVE-1999-0977: Sun Security Bulletin #00191 / Solaris sadmind Buffer Overflow Vulnerability

MS00-078: Web Server Folder Traversal

MS01-020: Incorrect MIME Header CAN-2001-0154

MS01-027: Flaws in Web Server Certificate Validation Could Enable Spoofing

MS01-028: RTF document linked to template can run macros without warning

RECOMMANDATIONS

- Avoir un reporting évolué, une politique AV sans modifications utilisateurs et une possibilité de réaction immédiate à distance...
- Installer un firewall personnel sur les postes nomades.
- Apprenez comment restaurer des fichiers depuis les CD-ROM Microsoft.

W32/CodeRed.A worm →

MS01-033: Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise (superseded by MS01-044)

W32/Nimda.A@mm →

MS01-044: Cumulative Patch for IIS

JS/Exploit-Messenger →

MS02-005: Cumulative Patch for Internet Explorer

MS02-015: Cumulative Patch for Internet Explorer

W32/Sharpei@mm →

~~MS02-010~~

D'AUTRES VERS...

CIBLES	EXEMPLE...	DATE
INSTANT MESSAGING	W32/Hello.worm W32/Choke.worm	04/01 06/01
Applications IRC (mIRC & Pirch)	IRC/Acoragil W32/Azaco.cmp IRC/Theme.worm	12/97 11/99 09/01
Ver RESEAU (propagation au travers des réseaux locaux)	W32/AntiQFX VBS/Netlog W32/Qaz	01/00 02/00 09/00
Ver UNIX-like	UNIX/Admw0rm SUNOS/BoxPoison.worm	03/98 05/01
Ver serveur IIS	W32/CodeRed	07/01
WINDOWS-NT (voir nota)	WinNT/Remote Explorer	12/98
Via AUTORUN.INF	W32/Autoworm	09/99
Ver GNUTELLA	W32/Gnuman.worm	02/01
Ver KaZaa P2P	W32/Benjamin.worm	05/02
Ver SQL serveur	JS/SQLSpida.worm	05/02

Nota: La fonctionnalité « ver » (capacité de propagation par le réseau) est controversée par certains membres de notre profession.

CONCLUSION

- **Les virus utilisent les moyens de propagation de leur époque. Les disquettes ont laissé la place à la messagerie et aux réseaux,**
- **Alors qu'un individu ne pouvait envisager la diffusion simultanée de milliers de disquettes, un simple e-mail peut atteindre des milliers de destinataires en un instant.**
- **Les auteurs de virus cherchent clairement à utiliser les nouvelles fonctionnalités d'INTERNET. Une nouvelle ère s'ouvre pour les virus programmes. Avec l'arrivée de W32/Nimda @mm apparaît le véritable « virus INTERNET » imaginé en Février 1999...**

Janvier 1999	W32/Ska@m	Un mono-diffuseur (slow mass-mailer)
Mars 1999	W97M/Melissa@mm	Multi-diffuseur (fast MM) ciblant 50 destinataires en 1 seule activation
Décembre 1999	W32/Babylonia@mm	Multi-diffuseur à modules téléchargeables externes (plugin)
Mai 2000	VBS/LoveLetter@mm	Multi-diffuseur ciblant l'ensemble des destinataires
Août 2000	W32/MTX@m	Multi-diffuseur, virus programme conventionnel, propagation via des disques partagés, porte dérobée
Septembre 2001	W32/Nimda@mm	Multi-diffuseur, virus programme conventionnel, propagation via des disques partagés, porte dérobée, propagation via les serveurs IIS

CONCLUSION

- **La communauté anti-virale réagit de plus en plus rapidement,**
- **Pour se propager, un virus ne peut plus se contenter d'une propagation lente et discrète. L'auteur de virus doit tabler sur une propagation massive dans un délai le plus bref possible,**
- **La mise en place et l'activation des processus heuristiques et génériques minimisent les risques (mettez régulièrement à jour vos « moteurs »).**
- **LINUX devient un nouveau challenge pour les auteurs de virus.**