Histoire des virus informatique
Evolution des techniques virales

Michel Dubois
myshell.dubois@neuf.fr
http://vaccin.sourceforge.net

8 août 2006

ANNÉE	ÉVOLUTION	NOM
1961	Premiers organismes	DARWIN (CORE WAR)
1971	Premier ver	CREEPER
1974	Premier virus	RABBIT
1981	Premier virus pour Apple II	ELK CLONER
1984	Création du Club de la Sécurité des Systèmes d'Information Français.	CLUSIF
1985	Premier antivirus	CHK4BOMB
1986	Premier virus furtif - *en cas de tentative de lecture du secteur infecté, le virus affiche les données originales saines.*	BRAIN
1987	Premier virus crypté - *seuls restent en clair les 35 premiers octets dédiés au décryptage. Il est l'ancêtre des virus polymorphes.*	CASCADE
	Premier virus à endommager directement les données - *le virus détruit les informations sur les disques.*	LEHIGH
	Premier virus capable d'infecter les fichiers EXE.	SURIV-2
	Première épidémie mondiale	JERUSALEM (SURIV-4)
1988	Premier forum électronique dédié à la lutte antivirale	VIRUS-L (USENET)
	Création du Computer Emergency Response Team.	CERT
	Premier virus antivirus - *il détecte, supprime et immunise contre le virus (c)Brain.*	DEN ZUK
	IBM crée un laboratoire de recherche interne - *le High Integrity Computing Laboratory afin de développer un antivirus. Cet antivirus effectue une recherche par signature.*	IBM V SCAN
	Apparition du premier canular diffusé par Mike RoChennel.	A 'REALLY NASTY VIRUS'
1989	Premier virus "médiatique" - *ce virus suscite une vive réaction dans le monde entier, relayée et amplifiée par les média.*	DATACRIME
	Naissance de nouveaux logiciels antivirus.	F-PROT, -V, VIRUSSCAN
	Naissance d'une publication internationale sur la prévention, la détection et la suppression des virus informatiques.	VIRUS BULLETIN
	Premier virus infecteur rapide - *une fois en mémoire, il est à même d'infecter un fichier lors d'une manipulation simple (copie d'un répertoire vers un autre).*	DARK AVENGER.1800
	Création du Computer Threat Research Organisation - *cette association anglaise a pour objectif de faire des recherches sur les virus et chevaux de Troie.*	COTRA

ANNÉE	ÉVOLUTION	NOM
1990	Premier virus polymorphe	FAMILLE CHAMELEON
	Premiers virus Russes	PETERBURG, VORONEZH
	Premier virus totalement furtif	FRODO
	Premier BBS[1] d'échange de virus (créé par Dark Avenger)	VX BBS
	Premier virus multipartite - *il infecte à la fois les zones systèmes et les fichiers.*	FLIP (ALIAS OMICRON)
	Premier virus défensif - *ce virus utilise plusieurs techniques de protection contre le désassemblage.*	WHALE
	Premier virus compagnon	AIDS-II.8064
1991	Naissance de nouveaux logiciels antivirus.	NORTON ANTIVIRUS, CENTRAL POINT ANTIVIRUS
	Premier virus délocalisé	DIR-II
	Création du Computer Antivirus Research Organisation	CARO
	Création de l'European Institute for Computer Antivirus Research	EICAR
	Premier virus Netware	GP1
1992	Premier générateur de virus polymorphe	MTE
	Premier virus annihilant les antivirus - *il supprime la base de données du contrôleur de modification de Central Point AntiVirus.*	PEACH
	Premiers constructeurs de virus - *ils permettent de créer des virus en choisissant parmi un éventail de charges utiles malicieuses.*	VCL ET PS-MPC
	Premier virus pour Windows	WIN.VIR_1_4
	Premier virus pour la CMOS - *Il modifie la CMOS pour interdire le démarrage sur disquette.*	EXEBUG
	Premier virus infectant les fichiers .SYS	INVOL
	Premier virus de secteur de boot polymorphique	V-SIGN
1993	Naissance du logiciel antivirus de Microsoft	MSAV
	Premier virus compresseur - *il compacte les fichiers .com qu'il infecte.*	CRUNCHER
	Premier virus résidant en mémoire ciblant les fichiers de commandes (.bat).	BATMAN
	Premier virus pour les fichiers compressés.	ARJ-VIRUS
	Premier retro-virus.	TREMOR
	Première WILDList postée par Joe Wells. 47 virus *"in-the-Wild"* y sont référencés.	WILDLIST
1994	Premier virus infectant les fichiers OBJ	SHIFTER
	Premier virus infectant les codes C et Pascal	SCRVIR
	Premier virus à positionnement fragmenté - *une partie du code du virus est éparpillé en divers endroits du fichier infecté.*	ONE_HALF
	Premier virus s'attaquant aux routines BIOS du DOS.	3APA3A
1995	Création par McAfee du groupe : Antivirus Emergency Response Team	AVERT
	Premier virus de macro. *Dorénavant, les virus ne se propagent plus uniquement via un programme exécutable mais aussi à partir de simples fichiers de bureautiques. Ce virus est destiné à Word, il est écrit en Word Basic.*	WM/CONCEPT
	Premiers virus pour OS2.	OS2/DA ET OS2FIRST
	Premier virus rendant un PC totalement inaccessible depuis un environnement sain.	RAINBOW

ANNÉE	ÉVOLUTION	NOM
1996	Premier virus pour Windows95 - *Premier virus infectant les fichiers exécutables au format Portable Exécutable (PE).*	BOZA
	Premier virus pour GNU/Linux - *Premier virus infectant les fichiers exécutables au format Exécutable Linkable Format (ELF).*	STAOG
	Premier virus de macro pour Excel - *il est écrit en VBA.*	XM/LAROUX
1997	Naissance de Network Associates - *regroupement de McAfee Associates et de Network General.*	NAI
	Premier vers se propageant via le protocole FTP.	HOMER
	Premier virus crypté pour Windows.	WIN95.MAD
1998	Premier virus entièrement écrit en Visual Basic Script.	RABBIT
	Premier virus pour Access.	ACCESIV
	Premier virus de macro multiplateforme.	CROSS
	Premier module exécutable malicieux java.	JAVA.STRANGEBREW
	Premier virus HTML.	HTML.INTERNAL
	Premier virus pour Powerpoint.	ATTACH
	Premiers tests réguliers et indépendants contrôlant l'efficacité des antivirus. Projet lancé par le magazine Virus Bulletin.	VB 100%
1999	Premier virus utilisant la messagerie électronique pour se propager.	SKA - HAPPY99
	Premier virus à infecter des fichiers à l'aide de fichiers Windows HLP.	SK
	Premier virus de macro (Word) avec des fonctions de ver Internet.	MELISSA
	Premier virus pour CorelDraw - *entièrement programmé en Corel script.*	GALA
	Premiers vers se propageant via messagerie électronique sans pièce jointe.	KAK@M ET BUBBLEBOY
	Premier virus capable de se rajeunir à distance - *il se connecte régulièrement à un serveur au Japon afin de télécharger une liste de modules de virus. Si les virus sont plus récents que ceux de l'ordinateur infecté, ils sont alors téléchargés.*	BABYLONIA
2000	Premier virus pour PalmOS.	PALMOS/PHAGE
	Premier cheval de Troie pour les les Personal Digital Assistant sous PalmOS.	LIBERTY
	Premier virus pour les suites Autocad	STAR
	Premier virus capable de manipuler les Alternate Data Stream[2] de NTFS	STREAM
	Premier virus pour les fichiers PIF	FABLE
	Premier virus écrit en PHP	PIRUS
2001	Premiers vers sans fichier - *Ces vers sont capables de se reproduire et de fonctionner sur les machines infectées sans utiliser de fichiers : ils existent uniquement dans la mémoire RAM et se propagent sous la forme de paquets de données spécialement configurés.*	CODERED.WORM[3]
	Premier virus Internet - *il utilise plusieurs mode de propagation : la messagerie, les serveurs IIS[4], les partages réseaux et lors des consultations web.*	NIMDA@MM
	Premier ver pour les réseaux peer to peer	MANDRAGORE

ANNÉE	ÉVOLUTION	NOM
2002	Premiers vers pour l'environnement .NET.	LFM & DONUT
	Premiers vers de courrier électronique se propageant en se connectant directement aux serveurs SMTP intégrés des machines infectées.	LENTIN & KLETZ
	Premier virus pour les environnements Windows et Linux - *il infecte aussi bien les programmes au format ELF (Linux) que les programmes au format PE (Windows 32).*	LINUX.SIMILE
2003	Premier virus pour les documents MapInfo[5].	MBP.KYNEL
	Premiers chevaux de Troie proxy serveur - *Les machines sont d'abord infectées par un cheval de Troie qui va ensuite faciliter l'envoi massif de courriers électroniques. Ces chevaux de Troie permettent de créer des réseaux de machines zombies.*	WEBBER.A
2004	Premier ver ICQ.	BIZEX
	Premier virus pour Win64.	RUGRAT
2006	Premier ver pour Mac OS X - *Ce ver se répand via le système de messagerie iChat. Contenu dans un fichier appelé latestpics.tgz, il se rediffuse automatiquement vers la liste de contacts de l'ordinateur infecté.*	LEAP-A
	Premier virus ciblant les fichiers de scripts du désassembleur IDA Pro[6].	W32/GATT

[1]Bulletin Board System

[2]Les Alternate Data Stream permettent, dans un système de fichier NTFS, d'ajouter un flux de données additionnel à un fichier ou à un répertoire. Cette fonctionnalité a été ajoutée dans un souci de compatibilité avec HFS de Macintosh.

[3]CodeRed apparaît en juillet 2001. En 24 heures, il infecte 350 000 machines dans le monde.

[4]Internet Information Server, Serveur Web de Microsoft.

[5]MapInfo est une entreprise spécialisée dans les logiciels de Geographic Information System (GIS).

[6]IDA Pro : www.datarescue.com