Histoire des virus informatique
Chronologie

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

8 août 2006

1971
- Le virus CREEPER fait son apparition sur ARPANET. Il est capable d'accéder seul à un système distant via un modem et de s'y copier. Les systèmes infectés affichent le message : "I'm the creeper : catch me if you can."[1]

1974
- Le virus RABBIT se propage de machines en machines. Il a été appellé ainsi en raison de sa rapidité de propagation.

1982
- ELK CLONER, écrit pour le système Apple II, est connu pour être le premier virus informatique "In the Wild". C'est à dire, le premier virus trouvé en dehors des laboratoires ou de l'ordinateur sur lequel il a été créé.

1986
- (C)BRAIN, premier virus écrit pour IBM PC. Il se répand dans le monde entier en quelques mois. C'est un virus de boot d'origine pakistanaise.
- Ralf Burger, un programmeur allemand, publie un "proof of concept" VIRDEM. Il s'agit du premier virus conçu pour infecter par ajout dans les fichiers .com .

1987
- (C)BRAIN est découvert à l'université de Delaware ;
- LEHIGH est découvert dans l'université américaine du même nom ;
- JÉRUSALEM est découvert dans une université israélienne ;
- Le virus STONED est découvert dans l'université de Wellington en Nouvelle Zélande ;
- VIENNA est découvert dans une université viennoise en Autriche ;
- IBM CHRISTMAS TREE se propage sur le réseau américain BITNET et paralyse le réseau de messagerie privée VNET ;

1988
- PING PONG est découvert dans l'université de Turin en Italie ;
- DEN ZUK est écris par Denny Yanuar Ramdhani à Bandung en Indonésie. Ce virus détecte et détruit le virus (C)BRAIN ;
- CASCADE est découvert en Allemagne ;

[1] Que l'on peut traduire part : *"Je me faufile partout, attrape moi si tu peux"*.

- Le vendredi 13 mai, le virus JERUSALEM infecte plusieurs sites dans le monde : l'université de Londres, l'hôpital royal de Glasgow, le centre informatique de la British Rail à Derby. Le virus détruit tous les programmes fonctionnant ce jour là[1, Cf. la rubrique Malware history].
- Le 2 novembre 1988, le ver MORRIS infecte, en moins de cinq heures, l'université de Stanford, le MIT, les universités du Maryland et de Berkeley. L'institut de recherche de la NASA d'Ames, le laboratoire national de Lawrence Livermore et plus de 6 000 systèmes informatiques aux USA sont aussi touchés. Les pertes globales sont estimées à 96 millions de dollars américains ;

1989

- 30 virus sont répertoriés "In the wild" ;
- En janvier, un jeune bulgare se faisant appellé Dark Avenger[2] développe le virus DARKAVENGER. Ce virus est représentatif de l'escalade dans la lutte virus versus antivirus. C'est un infecteur rapide, une fois en mémoire, il infecte les fichiers auxquels le système accède. Paradoxalement, un simple scan antivirus accélère la propagation du virus.
- du 13 octobre au 31 décembre, le virus DATACRIME est actif. Ce virus, découvert en mars de la même année, effectue un formatage bas niveau du premier cylindre du disque dur. Il suscite une grande inquiétude dans le monde entier. Finalement peu d'ordinateurs seront infectés.
- Le 16 octobre, le ver WANK[3] apparaît sur les ordinateurs VAX/VMS[4] du réseau SPAN. Le ver se propage via le protocole DecNET et remplace les messages système par : "WORMS AGAINST NUCLEAR KILLERS"[5]. Enfin, le ver remplace les mots de passe système par des séquences de caractères aléatoires qu'il envoie ensuite à un utilisateur nommé GEMPAK.

1990

- La population des virus informatiques continue de croître, on en répertorie 300 environ.
- Naissance des premiers virus polymorphes. À partir des caractéristiques du virus CASCADE et s'inspirant du livre de Burger sur le virus VIENNA, Mark Washburn développe les virus de la famille Chameleon (de V2P1 à V2P6). Le code de ces derniers n'est pas simplement chiffré, il change à chaque infection. Ainsi la détection par simple signature devient inefficace.
- Durant le deuxième trimestre 1990, deux virus innovants font leur apparition, il s'agit de FRODO et de WHALE. WHALE est un virus très gros (9 Ko) et très complexe. Il comporte de nombreuses techniques de protection contre le désassemblage ce qui en fait le premier virus défensif. Quand à FRODO, il s'agit du premier virus totalement furtif. Ces deux virus fonctionnent mal et ne se propagent pratiquement pas. Cependant les techniques mises en œuvre dans leur code présentent un grand intérêt.
- En septembre 1990, un virus très visuel émerge. En effet, FLIP (alias OMICRON), pivote de 180 degrés l'affichage de l'écran des ordinateurs qu'il infecte.
- Émergence des premiers virus russes : PETERBURG, VORONEZH et LOVECHILD.

1991

- La population des virus informatiques continue de croître, on en répertorie 1000 environ.
- En avril 1991, le virus TEQUILA est à l'origine d'une épidémie sérieuse. Développé par l'auteur présumé du virus FLIP, ce virus multipartite, partiellement furtif et hautement polymorphe, infecte le secteur d'amorçage et affiche aléatoirement une courbe fractale de Mandelbrot. Initialement TEQUILA est développé à des fins de recherche mais l'un des amis du développeur lui vole une copie du virus et la diffuse.

1992

[2] Le vengeur ténébreux

[3] http://www.cert.org/advisories/CA-1989-04.html

[4] Le VAX - Virtual Address eXtension - désigne désigne à la fois un processeur et l'architecture générale d'un ordinateur développé par la société Digital. VMS - Virtual Memory System - désigne le système d'exploitation pilotant les ordinateurs VAX.

[5] Les vers contre les tueurs nucléaires

- Découvert en Australie en 1991, le virus MICHELANGELO déclenche une épidémie en mars 1992. Programmé pour se déclencher le 6 mars[6], il écrase une zone d'environ 8 Mo sur les disques durs des ordinateurs infectés. À l'instar de DATACRIME en 1989, l'impact de Michelangelo est amplifié par les média : le chiffre de 5 millions de machines susceptibles d'être infectées est avancé. En fait, seulement quelques milliers d'ordinateurs seront touchés.

1995

- Au mois d'août le virus CONCEPT (alias PRANK[7]) s'attaque aux sytèmes utilisant Microsoft Word. Le virus contient une macro *AutoOpen*, il se lance donc automatiquement à l'ouverture d'un document infecté. Il fait le tour du monde en un mois seulement et occupe longtemps la première place dans le top ten des virus. À l'origine de l'épidémie, l'envoi accidentel du virus par Microsoft, sur un CD-ROM nommé "Microsoft windows 95 Software Compatibility Test", à des millers d'entreprise OEM. Un peu plus tard, la société Digital Equipment Corporation (DEC) distribue par accident des copies du virus CONCEPT aux participants d'une conférence organisée à Dublin. Il existe encore à l'heure actuelle plus d'une centaine de versions connues de ce virus.

1996

- En mars 1996, le virus WIN.TENTACLE provoque la première épidémie visant Windows 3.x. Ce virus infecte les systèmes informatiques de plusieurs sociétés françaises. Il est le premier virus, visant les systèmes Windows, trouver en dehors des cercles de chercheurs ou des forums spécialisés.
- En juillet 1996, le premier macro-virus pour Microsoft Excel, LAROUX, est détecté simultanément dans le réseau de deux compagnies de forage pétrolier situées respectivement en Alaska et en Afrique du Sud. Ce virus contient deux macro écrites en Visual Basic pour Application (VBA) : *auto_open* qui se lance à chaque ouverture d'un fichier infecté et *check_files* qui infecte tous les fichiers lors de leur création.

1998

- En juin 1998, le virus CIH[8] provoque une épidémie mondiale. Le nombre d'ordinateurs et de réseaux infectés se compte en milliers. Partie de Taiwan, l'épidémie s'étend jusqu'au États-Unis où le virus contamine des serveurs Web et s'introduit dans plusieurs programmes de jeu. En fonction du jour de l'infection le virus efface la mémoire BIOS Flash ou écrase une partie du disque dur. Il déclenche une nouvelle épidémie le 26 avril 1999, jour du 13ème anniversaire de la catastrophe de Chernobyl.[9] En mars 1999, des ordinateurs neufs Aptiva, vendus par IBM, colportent également le virus.
- Un grand nombre de chevaux de Troie programmés pour voler des mots de passe[10] et des utilitaires d'administration à distance voient le jour.

1999

- En janvier 1999, le virus[11] HAPPY99 - aussi connu sous le nom de SKA@M - déclenche, en 6 mois, une épidémie mondiale. Ce ver innove en se propageant via Outlook de Microsoft, devenu le client de messagerie standard dans les entreprises européennes et américaines. Il arrive sous la forme d'une pièce jointe et s'expédie de lui-même chaque fois qu'un courrier est émis vers un destinataire. Lorsque l'on double-clique sur la pièce jointe, une animation représentant un feu d'artifice s'affiche à l'écran.
- Le 26 mars, le premier macro-virus Word avec fonction de ver Internet, MELISSA, déclenche une autre épidémie mondiale.

[6] D'où son nom. En effet, Roger Riordan, qui a découvert le virus, propose de le nommer MICHELANGELO en référence à l'artiste Michel Ange né le 6 mars 1475.

[7] Nom choisi par Microsoft espérant ainsi diminuer l'importance de l'affaire de la diffusion du virus sur l'un de leur CD-ROM (Prank signifie escapade).

[8] Le nom du virus correspond aux initiales de son auteur : Chen Ing-Hau.

[9] Ce qui le fera surnommé Chernobyl.

[10] famille PSW

[11] Son auteur *Spanska* est français.

Découvert sur un NewsGroup à caractère sexuel, MELISSA se présente sous la forme d'un fichier *list.doc* supposé contenir une liste de mots de passe permettant d'atteindre gratuitement des sites à caractère pornographique.

Après avoir infecté un ordinateur, MELISSA balaie le carnet d'adresse d'Outlook et envoie sa propre copie aux 50 premières adresses qu'il trouve. MELISSA agit à l'insu de l'utilisateur mais les emails envoyés semblent provenir de ce dernier[12] accentuant ainsi les chances de propagation du virus.

MELISSA cause des dégats considérables obligeant des entreprises comme Microsoft, Intel ou encore Lockheed Martin à fermer leur serveur de messagerie. Les dégats estimés, se chiffrent en dizaine de millions de dollars.

- En novembre 1999, une nouvelle génération de virus se propage via courrier électronique. BUBBLEBOY le premier a faire parler de lui, n'a pas besoin de pièce jointe pour infecter l'ordinateur, la simple consultation du mail suffit. Il utilise une faille d'Internet Explorer[13] lui permettant de s'exécuter même si les options de sécurité du navigateur sont configurées au niveau élevé. Le ver KAKWORM, découvert en octobre 1999, utilise la même technique que BUBBLEBOY. Très vite, il le dépasse dans le top dix des virus et se répand dans le monde entier.

2000

- En novembre 1998, Eugène Kaspersky publie une étude révélant les menaces que représentent les virus écrit en Visual Basic dans de simples fichiers textes. A l'époque, il n'est pas pris au sérieux. Malheureusement, le virus LOVELETTER[14] lui donne raison.

  A 1h du matin dans la nuit du 4 au 5 mai 2000, le virus est détecté aux Philippines. Vers 10h00 le 5 mai, 4 500 000 mails infectés sont recensés en France. La rapidité de propagation[15] du virus prend de court les entreprises. Nombre d'entre elles ne mettant pas à jour régulièrement leur antivirus sont envahies et doivent arrêter leurs serveurs de messagerie.

  Les conséquences financières de LOVELETTER sont lourdes : 45 millions de mails infectés en 1 mois, le chiffre de 47 milliard de Francs de pertes fut avancé. Son auteur présumé, Onel de Guzman, est un étudiant en informatique philippin. Il est arrêté puis libéré en l'absence de loi locale interdisant le développement de ce type de programme. On compte actuellement environ 90 variantes de ce virus en circulation.

2001

- Le 19 janvier 2001, le virus RAMEN attaquent les systèmes fonctionnant sous Linux. Un grand nombre de réseaux d'entreprises sont ainsi infectés en quelques jours.
- Le 8 mai 2001, le ver SADMIND se développe en exploitant une faille des ordinateurs fonctionnant sous Solaris et une autre affectant les serveurs IIS.
- Le 13 juillet 2001, le ver CODERED scanne sur Internet les machines vulnérables[16] et les infecte. En 24 heures, il contamine 350 000 ordinateurs dans le monde.
- Le 4 août 2001, une nouvelle version de CODERED, CODERED II commence, à partir de la Chine, à se répandre dans le monde.
- Le 18 septembre 2001, NIMDA[17] est le premier ver à utiliser simultanément plusieurs modes de propagation. S'appuyant sur la vulnérabilité décrite dans MS01-044 et les backdoors laissées par les vers CODERED II et SADMIND , il infecte les systèmes informatiques en passant par les messageries, les serveurs IIS et les partages réseau.

[12] Le sujet du mail envoyé par MELISSA est *Important message from <nom>* ou <nom> était le nom complet de l'utilisateur qui était censé en être l'expéditeur.

[13] MS99-032 Scriplet.Typelib/Eyedog

[14] LOVELETTER est aussi connu sous le nom de I LOVE YOU ou de LOVE BUG.

[15] Alors que SKA@M avait eu besoin de 6 mois pour faire le tour du monde et 2 jours pour MELISSA, seulement quelques heures suffirent à LOVELETTER.

[16] Vulnérabilité MS01-033.

[17] Admin à l'envers.

2002

- Le ver KLEZ est détecté le 26 octobre 2002. À partir de cette date et j'usqu'à la fin de l'année 2002, 60% des infections enregistrées sont imputables à KLEZ.

2003

- En l'espace de quelque minutes, le 25 janvier 2003, le ver SLAMMER[18] infecte plusieurs centaines de milliers d'ordinateurs dans le monde et augmente le volume du trafic sur le réseau à un tel point que plusieurs tronçons d'Internet s'effondrent. Il utilise une vulnérabilité du serveur Microsoft SQL et de MSDE[19] décrite dans MS02-039 et MS02-061. Ces vulnérabilités et les patchs permettant de les corriger avaient été publiées près de 6 mois avant l'émergence du ver.
- Le 11 août 2003, BLASTER alias LOVESAN se répand dans le monde entier. Sa propagation est qualifiée d'explosive, la presque totalité des internautes est attaquée par ce ver. Il utilise une faille dans le service RPC DCOM de Windows 2000/XP.
- Le premier ver de la famille SOBIG est détecté en janvier 2003. Mais c'est la version F du ver qui restera dans l'histoire. Détecté le 18 août 2003, SOBIG.F infecte plusieurs millions d'ordinateurs dans le monde en une semaine. Les développeurs des vers de la famille SOBIG veulent créer un réseau de machines infectées afin de lancer des attaques par déni de services sur des sites choisis au hasard.
- Le ver WELCHIA est lui aussi détecté le 18 août 2003. Il tente de supprimer maladroitement, dans les ordinateurs infectés, le ver BLASTER et d'installer le patch Windows.
- D'autres vers comme DUMARU ou SWEN déclencheront des épidémies. Leur action est plus orientée vers les ordinateurs familiaux que vers les ordinateurs d'entreprise.

2004

- Le 26 janvier 2004, vers 19h00 (heure française) un nouveau ver est repéré se propageant essentiellement via la messagerie électronique et les réseaux Kazaa. Craig Schmugar, chercheur au sein du groupe AVERT[20], en décompilant le code du ver trouve la chaîne de caractères *mydomai*. Le nom du nouveau ver est trouvé : MYDOOM.

  Ce dernier se répand extrêmement rapidement. En une semaine, il contamine 20 200 000 mails et 1 064 000 ordinateurs[21]. Le 25 février 2004, se sont 54 millions d'emails qui sont infectés.

  A l'instar de ses prédécesseurs, MYDOOM se propage, entre autre, au travers d'un réseau de machines zombies[22] et il installe une backdoor sur les ordinateurs infectés. MYDOOM est programmé pour réaliser une attaque par déni de services sur le serveur Web de *sco.com* : chaque seconde, entre le 1er et le 12 février 2004 il tente de charger la page d'accueil du site.
- Février 2004, un nouveau ver émerge : NETSKY. Ce dernier tente de supprimer les vers concurrents MYDOOM, BAGLE et MIMAIL. Il est le point de départ d'une guerre entre les développeurs de virus qui, par le biais des codes sources des virus, vont échanger des insultes. Au temps fort de cette bataille, trois versions de chaque ver aparaît en l'espace d'une journée.
- En avril 2004, Sven Jaschan diffuse le ver qu'il vient de créer SASSER. À partir de la vulnérabilité LSASS de Windows, décrite dans MS04-01, SASSER se connecte directement sur les ordinateurs reliés à l'Internet. Il provoque une sérieuse épidémie en Europe. Il est intéressant de noter qu'il n'y a eu que deux jours de délai entre la publication de la vulnérabilité et l'émergence du ver.

2005

- Le 16 août 2005 le ver ZOTOB exploitant la vulnérabilité décrite dans MS05-039 est découvert. Ses effets sont exagérés en raison du nombre important de média en ligne américains infectés.

[18] Aussi connu sous le nom de SAPPHIRE.
[19] Microsoft SQL-server Desktop Edition.
[20] Antivirus Emergency Response Team
[21] D'après la société MessageLabs - http ://www.messagelabs.com/emailthreats/
[22] Les réseaux de machines zombies sont des réseaux d'ordinateurs contenant une backdoor permettant de les commander à distance.

Références

[1] MARTIN (H.). « Virus bulletin ». http://www.virusbtn.com, 2006.