Introduction à la virologie informatique

Eric Filiol

ESIEA
Laboratoire de virologie et de cryptologie opérationnelles

11 février 2009

Plan

- Introduction
- Historique
- Définitions – Généralités
- Les différents types d'infection
- Les modes de propagation
- La lutte anti virale
- Conclusion

Microsoft TechDays 09
L'innovation avance avec vous

Introduction

- Risque récent : 30 ans
- Volonté maligne : les pirates informatiques
- La défense évolue moins vite que l'attaque

Microsoft TechDays 09
L'innovation avance avec vous

Introduction

- Risque récent : 30 ans

Vulnerability/Exploit	Value	Source
"Some exploits"	$200,000 - $250,000	Gov't official referring to what "some people" pay [9]
Significant, reliable exploit	$125,000	Adriel Desautels, SNOSoft [11, 22, 13]
Internet Explorer	$60,000 - $120,000	H.D. Moore [22]
Vista exploit	$50,000	Raimund Genes, Trend Micro [24]
"Weaponized exploit"	$20,000-$30,000	David Maynor, SecureWorks [18]
ZDI, iDefense purchases	$2,000-$10,000	David Maynor, SecureWorks [18]
WMF exploit	$4000	Alexander Gostev, Kaspersky [26]
Microsoft Excel	$\geq$ $1200	Ebay auction site [21, 25]
Mozilla	$500	Mozilla bug bounty program [4]

Table 1: Estimates on exploit values.

- Logiciels ;
- Utilisateurs.

Microsoft TechDays 09 L'innovation avance avec vous

Plan

- **Introduction**
- **Historique**
- Définitions – Généralités
- Les différents types d'infection
- Les modes de propagation
- Conclusion

Microsoft TechDays 09 L'innovation avance avec vous

Historique : apparition des virus

- 1983 : Premi
- 198 virus" et les vers quittent les laboratoires :
  - *Jerusalem/PLO*
  - *Internet* infecte 6000 machines

TOUS LES SYSTEMES D'EXPLOITATION SONT CONCERNES !

Microsoft TechDays 09
L'innovation avance avec vous

Historique : l'explosion

- 1990s : moteurs de mutation
- 1991 : générateurs de virus
- 1995 : virus de document (*Concept*)
- 1999 : ver *Melissa* (macro-ver)
- 2000 : ver *I LOVE YOU* (ver d'e-mail)
- 2001 : ver pour Palm Pilot
- 2002-2003 : intensification des attaques
- 2004 : portab
- … et ça

TOUS LES ENVIRONNEMENTS CAPABLES D'EXECUTION SONT CONCERNES !

Sécurité : 1 million de virus en 2008 !

03-04-2008
Par la rédaction

Selon F-Secure, le cap du million de virus sera franchi d'ici la fin 2008 avec l'émergence de la menace sur les mobiles et le retour de rootkit MBR...

"Le nombre de nouvelles menaces n'a jamais été aussi haut", constatent les ingénieurs des laboratoires de F-Secure qui reçoivent environ 25.000 nouvelles menaces chaque jour, sept jours sur sept.

Bilan des courses, si cette tendance se poursuit, le nombre total de virus et de Trojans dépassera le million d'ici la fin 2008.

Il existe une nouvelle tendance au sein de la cybercriminalité. A savoir contourner par tous les moyens les systèmes de défense des antivirus, pare-feu et autres solutions. Pour cela, les malfaiteurs de la Toile utilisent la technique dite du "drive-by download" (pages qui tentent d'exploiter les visiteurs en installant et en exécutant automatiquement des programmes malveillants.)

Ces attaques commencent souvent avec un spam par email, mais dans lequel la pièce jointe a été remplacée par un lien Web, qui attire l'utilisateur vers le site malveillant. Ainsi, au lieu d'être infecté par SMTP, vous êtes infecté via HTTP.

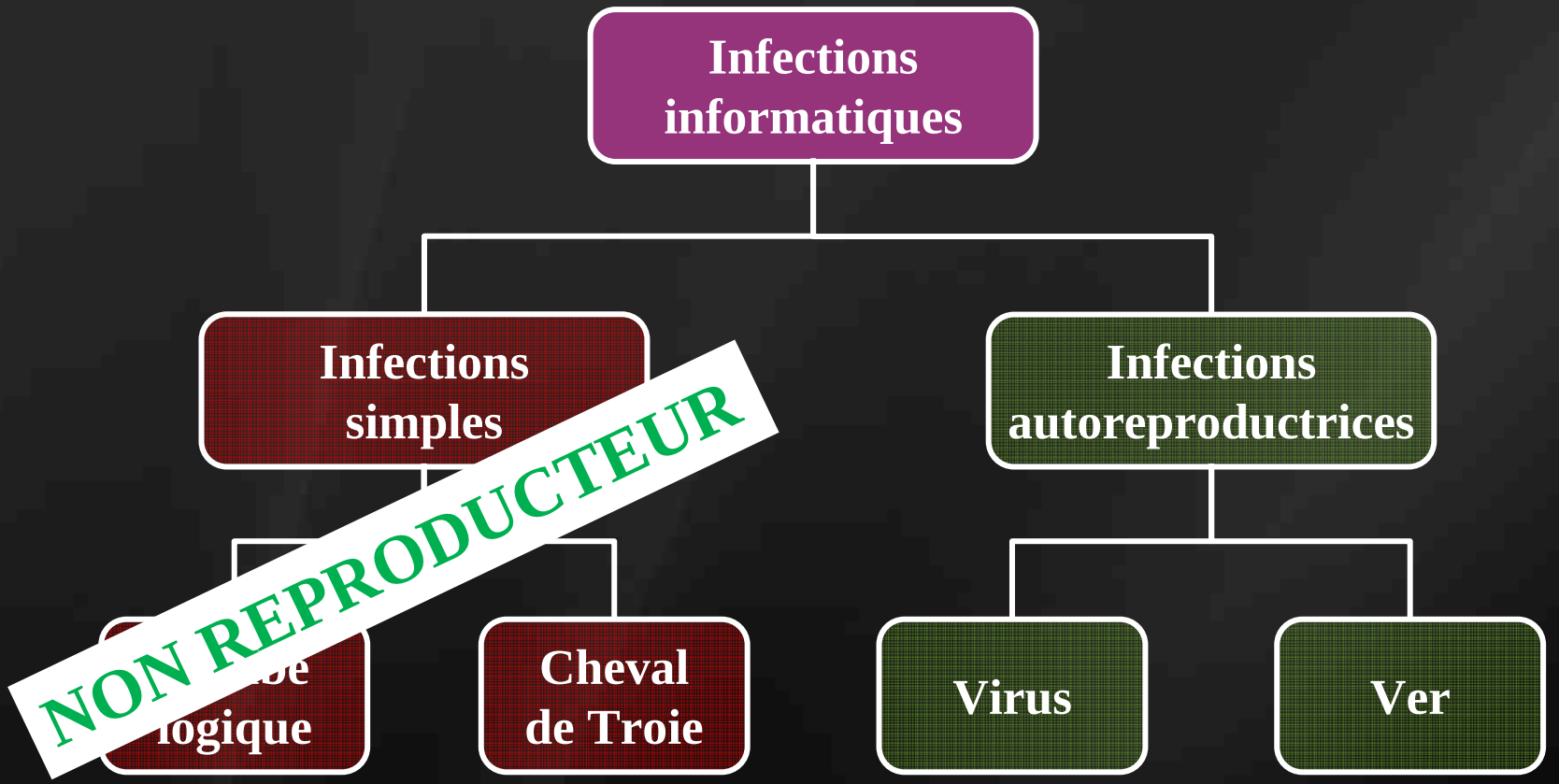
Pla
n

- **Introduction**
- **Historique**
- **Définitions – Généralités**
- Les différents types d’infection
- Les modes de propagation
- Conclusion

Microsoft TechDays 09
L’innovation avance avec vous

Les infections informatiques

Classification d'Adleman



Microsoft TechDays 09
L'innovation avance avec vous

Définitions

- Deux grandes catégories :
  - **Les programmes simples :**

    programmes s'installant dans le système pour mener leur action sans se reproduire.
  - **Les programmes autoreproducteurs :**

    programmes se propageant en recopiant leur code.

Microsoft TechDays 09
L'innovation avance avec vous

ccusés par un virus

MONDE | 24.10.03 | 13h21

mment deux pères de familles britanniques ont vu leurs vies brisées par l'intrusion de rus dissimulant des photos pédophiles dans leur ordinateur.

squ'à l'automne 2000, Karl Schofield, 36 ans, originaire de Reading, près de Londres, se nsidérait comme un homme comblé. Consultant pour des grandes entreprises de télécoms, il gnait beaucoup d'argent et dirigeait sa propre société. Il avait travaillé aux Pays-Bas, en abie saoudite, puis à Chypre, où il avait rencontré sa seconde épouse, une Russe de 23 ans. puis peu, le couple habitait Reading, dans une grande maison où vivaient également les rents de Karl : *"C'était la belle vie, parfois nous allions passer le week-end à New York... est bien fini tout ça."*

matin d'octobre 2000, alors qu'il vient d'arriver au bureau, sa femme l'appelle : des poli- rs sont chez eux et demandent à le voir. Karl Schofield rentre aussitôt, pour trouver sept quêteurs dans son salon. *"Ils m'ont posé des tas de questions sur mon PC de bureau, mon rtable, mes CD-ROM, mes mots de passe,* se souvient-il. *Je leur ai dit que j'avais peut-être s copies pirates de jeux vidéo, mais je ne voyais pas où ils voulaient en venir."* Ils lui an- ncent alors qu'ils cherchent des images pédophiles : *"Je ne les ai pas crus, ça me semblait lirant. Ma femme a ri, pour elle c'était forcément une erreur. Elle me connaît bien de ce té-là."* La perquisition ne donne rien, mais les policiers emportent les ordinateurs.

Cheval de Troie Mac OS X : des versions mutantes se développent

09-11-2007
Par La rédaction

Après la découverte la semaine dernière d'un cheval de Troie affectant les systèmes Mac, les experts en ont identifié au moins 32 variantes.

Les auteurs des attaques par cheval de Troie qui ont affecté les systèmes Mac OS X la semaine dernière continuent à frapper, à en croire les experts en sécurité. Mikko Hyppönen, directeur de recherche chez F-Secure, a déclaré dans un blog officiel de l'éditeur que le cheval de Troie avait d'ores et déjà été modifié pour donner naissance à au moins 32 variantes. *"Le groupe qui en est à l'origine semble déterminé à viser aussi bien les utilisateurs de Mac que de Windows"*, écrit-il. *"Et cela n'est pas près de s'achever"*

Le cheval de Troie sous Mac a été découvert la semaine dernière par des chercheurs d'Intego, éditeur de solutions de sécurité pour Internet. Le programme se dissimule dans un fichier codec nécessaire pour visionner les vidéos. Si l'on pensait au départ que le code était hébergé uniquement sur des pages de films pour adultes, il a été en réalité rapidement découvert sur un certain nombre de faux sites diffusant des "codec" et, dans certains cas, il a été propagé avec des programmes malveillants pour Windows.

Alors que F-Secure met en garde les utilisateurs contre la menace de ce cheval de Troie, un autre expert en sécurité tente d'apaiser les craintes. Alex Eckelberry, président de Sunbelt Software, a assuré dans un blog que la charge utile du cheval de Troie n'était pas aussi inquiétante que certains le prétendent.

Le malware, appelé DNSchanger, modifie le serveur DNS cible pour permettre au pirate de réacheminer les requêtes du site Web. Intego a indiqué qu'un cheval de Troie pouvait permettre à un pirate de détourner et de rediriger les requêtes Web pour des sites tels que PayPal ou eBay vers des sites de phishing.

mails avaient été envoyés à des députés et des employés du Parlement et ont été

Los Angeles botmaster pleads guilty, faces 60 years in prison, $1.75 million fine

Frank Washkuch Jr.
November 12 2007

A California man is facing a maximum of 60 years in prison and a $1.75 million fine after agreeing to plead guilty to using botnets to steal PC users' personal and financial information.

John Schiefer, 26, of Los Angeles has agreed to plead guilty to one felony count each of accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud.

Schiefer is the first guilty plea for a violation of federal wiretapping statutes in relation to botnet use, Thom Mrozek, a spokesman for the U.S. Attorney's Office for the Central District of California, told SCMagazineUS.com today.

Schiefer used his army of bot computers to defraud a Dutch advertising company not identified by the U.S. Department of Justice (DOJ).

Schiefer also mined usernames and passwords of PayPal users whose PCs had been infected with malware. He and associates then accessed bank accounts to make fraudulent purchases, Schiefer acknowledged in a criminal information and plea agreement filed Friday in U.S. District Court in Los Angeles.

Une question :

Pourquoi sommes-nous concernés ?

- Réseaux cloisonnés
- Système de SAS (stations de décontamination)

… et pourtant…

Microsoft TechDays 09
L'innovation avance avec vous

Généralités : les ministères de la défense aussi !

Badtrans.B, le méchant virus qui espionne votre clavier

Le ver Blaster se diffuse et prépare une attaque contre le site de Microsoft

Le ver exploite une vulnérabilité connue de Windows et se répand à grande

Le virus Bagle.AT s'attaque aux fonctions de sécurité de Windows

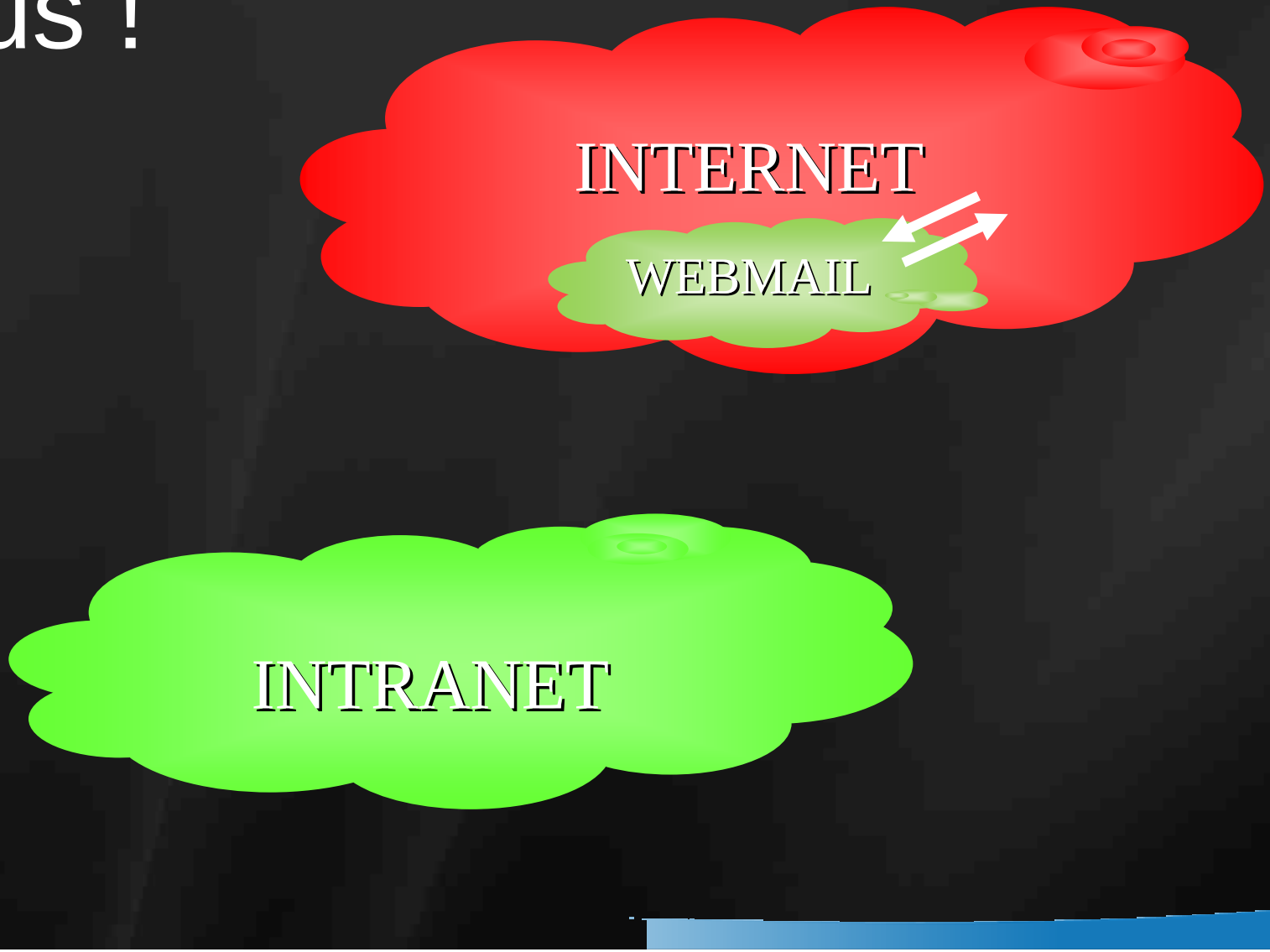
Cette nouvelle variante ouvre une porte de derrière sur le poste infecté, et désinstalle les codes malveillant de type Netsky éventuellement présents sur le PC.

(02/11/2004)

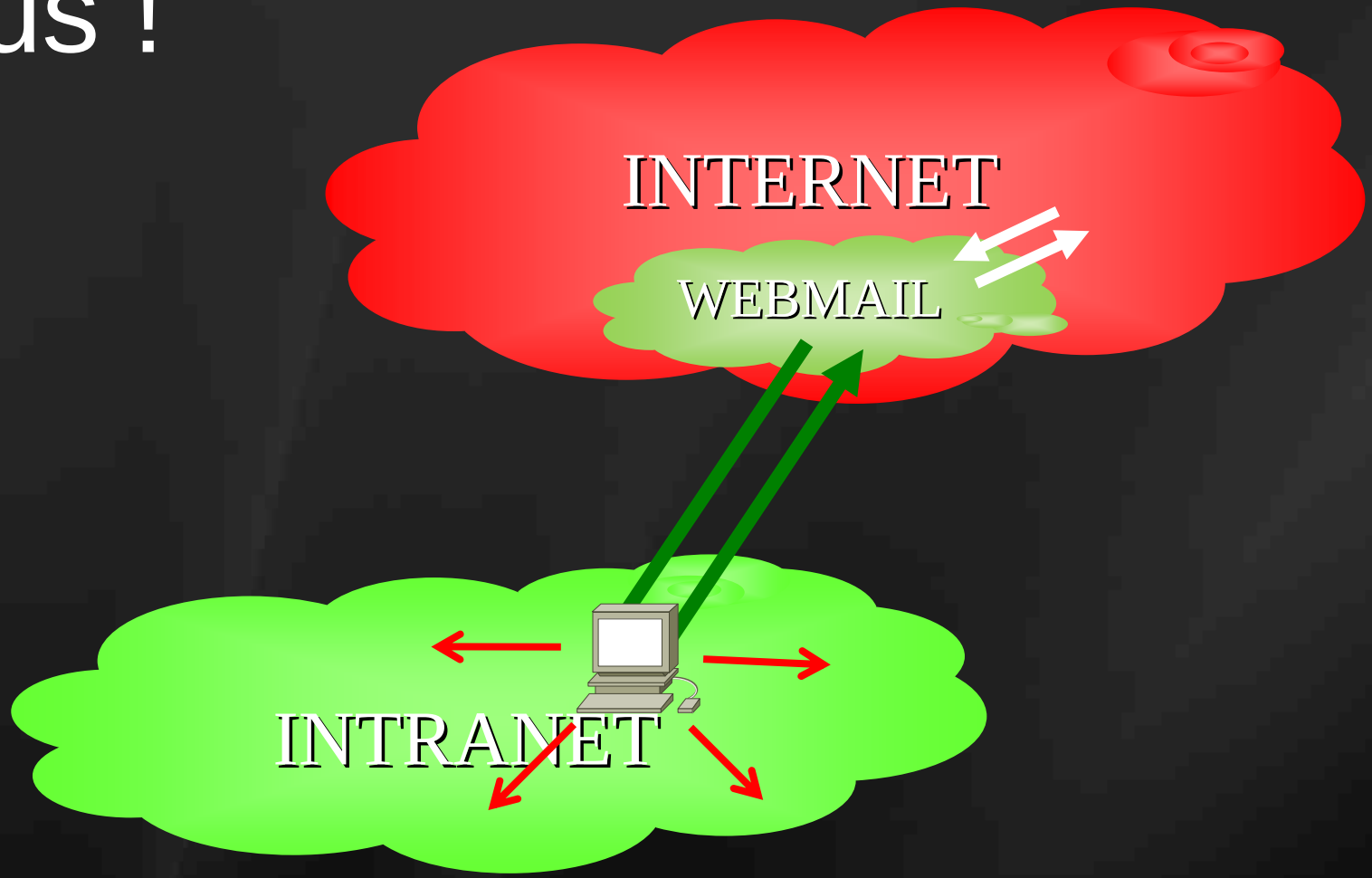
Une nouvelle variant de Bagle (la AT) se répand depuis quelques jours sur Internet. Ce ver de messagerie ciblant Windows s'attaque notamment aux dispositifs de sécurité des ordinateurs infectés, et ouvre une porte de derrière permettant à une personne malintentionnée de prendre le contrôle du système.

L'alerte a notamment été donnée par l'éditeur d'antivirus Trend Micro vendredi matin, alors que des alarmes étaient enregistrées en Asie (Japon, Chine, etc.), en Europe, ainsi qu'aux Etats-Unis.

Le cloisonnement n’existe plus !



Le cloisonnement n’existe plus !



Nato creates computer virus that reveals its secrets

June 18th 2000

BUNGLING Nato scientists have created a computer virus "by mistake", causing military secrets to find their way onto the internet.

The virus, called Anti-Smyser 1, was created by scientists at Nato's Kfor peacekeeping force headquarters in Pristina, Kosovo.

They were seeking protection from virus attacks similar to those launched at Nato by the Serbs during the Kosovo conflict. But the experiment went wrong, and scientists accidentally unleashed the virus on themselves.

Last week it emerged that the virus, which plucks documents from the hard drives of computers and sends invisible attachments to e-mails, recently resurfaced at the Czech ministry of defence.

"Following an investigation into the leaks, I can now tell you that this was started at Kfor by our own people and subsequently spread to Nato headquarters and to other Nato members." said Jamie Shea, a Nato spokesman.

According to Shea, Nato first became aware of the virus in December. It is now believed to be responsible for the leak in April of a restricted nine-page document detailing the rules of

Pla
n

- **Introduction**
- **Historique**
- **Définitions – Généralités**
- **Les différents types d’infection**
- Les modes de propagation
- Conclusion

Microsoft TechDays 09
L’innovation avance avec vous

Les différents types d'infection

- **Les programmes simples :**
  - **Bombes logiques**
  - **Chevaux de Troie**
- **Les programmes autoreproducteurs**
  - **Virus**
  - **Vers**
- **Les "Virus psychologiques"**

Microsoft TechDays 09
L'innovation avance avec vous

Les caractéristiques communes

- Programmes en apparence inoffensifs
- Présence de fonctions illicites et cachées
- Pénétration par effraction dans un système
- Attaque du système :
  - Consultation de l’information
  - Modification de l’information
  - Destruction de l’information

Microsoft TechDays 09
L’innovation avance avec vous

Programmes simples

- **Bombe logique :**
  - *programme résident dont la charge finale est activée en fonction d'un ou plusieurs paramètres fournis par le système ou ses entrées/sorties.*
  - Installation dans le système.
  - Déclenché par une « gâchette ».
  - Charge finale offensive avec un effet de retardement plus ou moins grand.

Microsoft TechDays 09
L'innovation avance avec vous

NETWORKWORLD

REUTERS UK

"Logic bomb" backfires on hacker

Wed Dec 13, 2006 11:02 PM GMT

NEW YORK (Reuters) - A former UBS PaineWebber (UBSN.VX: Quote, Profile , Research) employee was sentenced to eight years in prison on Wednesday for planting a computer "logic bomb" on company networks and betting its stock would go down.

The investment scheme backfired when UBS stock remained stable after the computer attack and Roger Duronio lost more than $23,000.

A federal judge in New Jersey sentenced Duronio, 64, to 97 months in prison and ordered him to make $3.1 million in restitution to his former employer, the U.S. attorney's office said in a statement.

Duronio was convicted on July 19 of one count of securities fraud and one count of computer fraud in the 2002 case.

testimony.

Programmes simples

- **Cheval de Troie :**
  - *programme composé de deux parties, le module serveur et le module client. Le module serveur, installé dans l'ordinateur de la victime, donne discrètement accès à tout ou partie de ses ressources à l'attaquant, qui en dispose via le réseau, grâce un module client.*
  - Deux parties : serveur (victime) – client (pirate) ;
  - Prise de contrôle de la cible.

Microsoft TechDays 09 L'innovation avance avec vous

Programmes simples

- **Cheval de Troie :**

  Le principal risque aujourd'hui est constitué par la création de réseaux (*Botnets*) d'ordinateurs infectés par des chevaux de Troie (*PC Zombies*).

  Ces réseaux sont activement utilisés :

  - Envoi de Spam ;
  - Attaques en déni de service ;
  - Vol de données ;
  - Fraude bancaire…

Microsoft TechDays 09
L'innovation avance avec vous

[SÉCURITÉ]

Un virus infecte plusieurs grandes entreprises françaises

Le site lillois de l'assureur La Mondiale est perturbé depuis une semaine. D'autres sociétés situées dans le même immeuble seraient aussi touchées. Le point sur les mesures à prendre.

Philippe Richard , 01net., le 11/06/2007 à 17h40

Les cas connus de grandes entreprises victimes d'un code malveillant (virus, vers, chevaux de Troie...) sont assez rares. Révélée par le site Zataz, l'infection qui touche l'assureur La Mondiale est suffisamment importante pour que l'activité de son site lillois soit très perturbée depuis une semaine. Selon nos informations, cette infection concernerait aussi, avec plus ou moins d'impact, les réseaux locaux de Decathlon et de Cofidis, deux sociétés installées dans le même immeuble que l'assureur.

Il est difficile de connaître exactement la cause de cette infection. *« Soit l'entreprise a eu une protection défaillante à un moment donné, soit elle est victime d'une attaque avec un virus modifié dont la signature n'est reconnue par aucun antivirus : nous avons eu des cas comme cela chez nos clients »*, indique l'expert en sécurité Hervé Schauer.

Après avoir constaté l'infection de son réseau, l'entreprise doit agir rapidement pour limiter les dégâts et repartir sur de bonnes bases. Selon le Certa (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques), la première chose à faire est de mettre en quarantaine les postes de travail contaminés. *« Il faut les déconnecter du réseau mais ne pas les éteindre. Il est en effet primordial de repérer les processus actifs au moment de l'intrusion »*, avertit Romain Levy, un

Microsoft TechDays 09
L'innovation avance avec vous

Programmes autoreproducteurs

- **Virus :**
  - *programme se propageant par recopie de son propre code dans des cibles préalablement choisies.*
  - Un virus reste dans l'ordinateur infecté.
  - Sa propagation est liée à l'attachement à un fichier.
  - Son pouvoir infectieux est limité au système infecté.

Microsoft TechDays 09 L'innovation avance avec vous

Programmes autoreproducteurs

- **Ver :**
  - *programme autoreproducteur capable de propager une infection à travers un réseau sans être nécessairement attaché à un fichier pour se propager.*
  - Un ver est un virus « orienté réseau ».
  - Sa propagation n'est pas toujours liée à un fichier.
  - Son pouvoir infectieux plus grand que les virus classiques

Microsoft TechDays 09
L'innovation avance avec vous

SOPHOS

21 mai 2007

Ver SB/BadBunny-A

SB/BadBunny-A est un ver multi-plates-formes écrit en de nombreux langages scripts et distribué comme un **document OpenOffice.org** contenant une macro StarBasic.

SB/BadBunny-A se propage en injectant des fichiers script malveillants qui affectent le comportement de programmes IRC, mIRC et X-Chat populaires et provoquant l'envoi de SB/BadBunny-A à d'autres utilisateurs.

Ces fichiers scripts malveillants sont nommés badbunny.py (pour XChat) et script.ini (pour mIRC, écrasant le fichier mIRC existant) et sont aussi détectés sous le nom de SB/BadBunny-A.

SB/BadBunny-A injecte différents composants supplémentaires sur la plate-forme sur laquelle il s'exécute :

- Sur **Windows**, il injecte un fichier nommé badbunny.js qui est un infecteur de fichier JavaScript aussi détecté sous le nom de SB/BadBunny-A.
- Sur **Linux**, il injecte un fichier nommé badbunny.pl qui est un infecteur de fichier Perl aussi détecté sous le nom de SB/BadBunny-A.
- Sur **MacOS**, il injecte un ou deux fichiers nommés badbunny.rb et badbunnya.rb qui sont des infecteurs de fichiers Ruby aussi détectés sous le nom de SB/BadBunny-A.

Programmes autoreproducteurs

- Vers : essai de classification
  - **Vers simples**
    - Failles logicielles
    - Faiblesses des protocoles réseau
  - **Macro-vers**
    - Liés à une pièce bureautique
    - Activation liée à une action humaine
  - **Vers de messagerie**
    - Pièce jointe exécutable
    - Action humaine ou faille logicielle

Microsoft TechDays 09 L'innovation avance avec vous

Les pirat

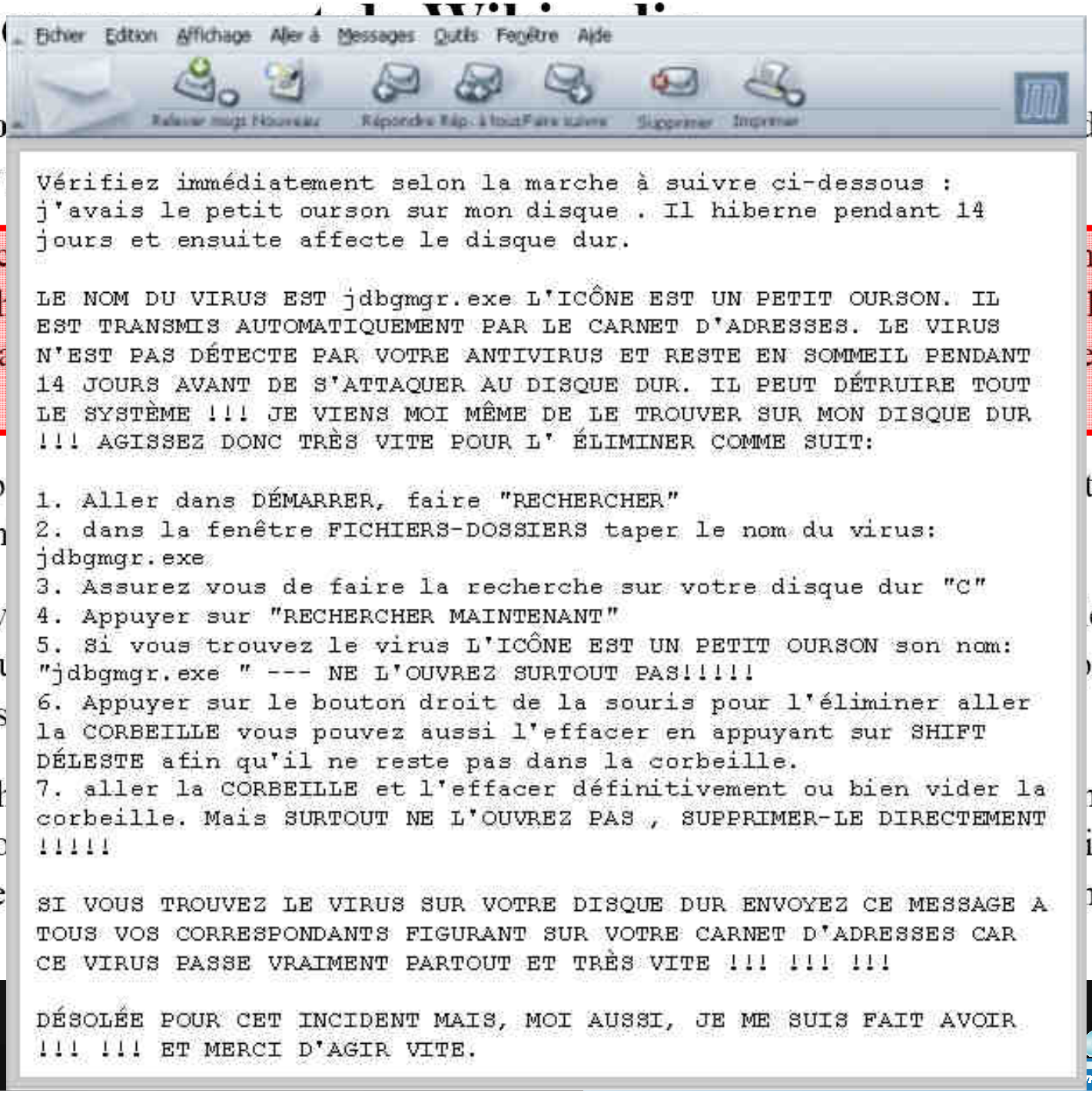
Les pirates info die en
gne *Wikipedia*

l'article de l'enc hyper-
exte pour téléch le va-
iante du virus, a endre-
i.

Heureusement p tiré le
en dès qu'ils on

La bonne nouv e lien
nenant à un viru rinci-
aux consultants

l'expert de Soph nt pris
lus de temps po iser la
ersion archivée nautes
llemands.



Microsoft chDays 09 n avance avec vous

Pla
n

- **Introduction**
- **Historique**
- **Définitions – Généralités**
- **Les différents types d’infection**
- **Les modes de propagation**
- Conclusion

Microsoft TechDays 09
L’innovation avance avec vous

Les modes de propagation

La clé USB faussement oubliée, nouveau vecteur d'attaque

Par Marc Rees - Le 27-04-2007 à 14:11:02
Source : The Reg (http://www.theregister.co.uk/2007/04/25/usb_malware/)

Alors que les attaques par mail sont de plus en plus difficiles à mettre en œuvre à terme, compte tenu de la méfiance aigüe des usagers, les pirates développent de nouvelles techniques d'approche.

Une forme d'attaque informatique a été imaginée par des petits malins outre-Manche. Elle consiste à abandonner dans un parking des clés USB garnies chacune d'un cheval de Troie. Cela fait, ne reste plus qu'à attendre qu'un heureux passant trouve ladite clé piégée pour espérer attendrir la curiosité de l'heureux découvreur.

Le trojan présent sur la clef est alors apte à récupérer des données secrètes telles que mot de passe, données bancaires, etc. La méthode est évidemment freinée par le coût du support, malgré sa démocratisation.

Microsoft TechDays 09
L'innovation avance avec vous

Les modes de propagation

- **Les échanges de fichiers**
- **L’informatique mobile :**
  - mise en connexion directe LAN-WAN ;
  - connexion de Palm, Pocket PC…
  - Informatique embarquée.

Microsoft TechDays 09
L'innovation avance avec vous

Les modes de propagation

- **Les échanges de fichiers**
- **L’informatique mobile :**
- **L’ingénierie sociale :**
  - goûts des utilisateurs ;
  - comportement à risque des utilisateurs ;
  - laxisme, manque de conscience professionnelle.

Microsoft TechDays 09
L’innovation avance avec vous

Les modes de propagation

- **Les échanges de fichiers**
- **L’informatique mobile**
- **L’ingénierie sociale**
- **Carences et vulnérabilités**
  - défauts d’administration et de paramétrage ;
  - vulnérabilités.

Microsoft TechDays 09
L'innovation avance avec vous

La Lutte anti virale

Microsoft TechDays 09
L'innovation avance avec vous

Plan

- Introduction
- Quelques attaques virales
- Les antivirus
- « Hygiène informatique »
- Conclusion

Microsoft TechDays 09
L'innovation avance avec vous

La lutte antivirale

Il n'existe pas de solution infaillible…

Affirmer « *pouvoir détecter tous les virus, y compris les virus inconnus* » est une affirmation fausse et mensongère

… mais il faut :

- utiliser un logiciel antivirus ;
- appliquer des règles de comportement strictes.

La combinaison des deux constitue la meilleure protection.

Microsoft TechDays 09 L'innovation avance avec vous

Plan

- **Introduction**
- **Quelques attaques virales**
- Les antivirus
- « Hygiène informatique »
- Politique antivirale de l’armée de terre
- Conclusion

Microsoft TechDays 09
L'innovation avance avec vous

Quelques attaques virales

Deux cas concrets d'attaques virales permettent de faire un panorama complet de la lutte antivirale avec ses forces et (surtout) ses faiblesses :

- CIH (Chernobyl)
- Cheval de Troie israélien

Microsoft TechDays 09
L'innovation avance avec vous

CIH (Chernobyl)

- Virus découvert en juin 1998
- Infection par fichiers infectés
  - Téléchargement (sites « warez », sites de Shareware…)
  - CD-ROM de certaines revues
  - Des professionnels ont propagé l'infection
- Attaque CIH v1 le 26 avril 1999

Microsoft TechDays 09
L'innovation avance avec vous

Chernobyl virus causes Asian meltdown

By Internet Correspondent Chris Nuttall

Like its namesake, the Chernobyl virus has caused global alarm

Hundreds of thousands of computers in Asia and the Middle East have had their data wiped by a malicious program known as the Chernobyl virus.

It was timed to strike on Monday, the 13th anniversary of the nuclear reactor disaster, and computer network managers in the regions have since been counting the cost.

While Chernobyl, a variant of the CIH virus, had a damaging impact in some parts of the world, the US and Europe seem to have largely escaped its effects.

Chernobyl around since June

CIH was discovered as long ago as last June in Taiwan. But despite warnings about its deadly effects on Windows 95 or 98 machines from anti-virus software companies since then, it still appears to have wreaked havoc in certain countries.

Microsoft Days 09
L'innovation avance avec vous

JDN solutions

Un cheval de Troie déterre la plus vaste affaire d'espionnage industriel en Israël

Conçu à la main pour un usage tactique, le cheval de Troie était utilisé par des multinationales israéliennes qui écoutaient ainsi le réseau informatique de leurs concurrents. Le scandale affecte durement la crédibilité des grands acteurs nationaux.

03 Juin 2005

L'information fait parler d'elle dans la presse israélienne : la police annonçait ce dimanche 29 mai avoir découvert une des plus grandes affaires d'espionnage industriel du pays, l'ensemble orchestré par l'outil informatique. A ce jour, la sécurité israélienne a procédé à vingt-deux interpellations de grands dirigeants d'entreprises dans le pays. L'affaire qui possède des ramifications internationales, a bénéficié de l'aide d'Interpol.

L'affaire remonte en novembre 2004, date à laquelle un écrivain israélien, Amnon Jacont, découvre sur Internet des extraits de son dernier roman encore en cours d'écriture. L'auteur porte alors plainte à la police de Tel Aviv qui découvre un cheval de Troie inconnu sur le poste de la victime. La police remonte peu à peu la piste jusqu'au suspect numéro un, Michael Haephrati, gendre de l'écrivain résidant en Grande-Bretagne et en Allemagne.

A distance, M. Haephrati pouvait ainsi prendre le contrôle de la machine infectée pour en altérer le fonctionnement ou y dérober des informations confidentielles. Mais le pirate n'en était pas à son premier coup d'essai. L'homme avait déjà vendu ses propres créations à des sociétés de détectives privés installées en Israël. Elles-mêmes proposaient par la suite le logiciel à des entreprises afin d'espionner leur concurrent.

Résultats financiers, clients démarchés, montant des enchères, argumentaire commercial : potentiellement toutes communications archivées ou tout fichier stocké pouvaient être récupéré par la concurrence. Les informations volées étaient ensuite renvoyées vers des serveurs distants basés aux Etats-Unis, en

L’affaire du cheval de Troie israélien

- Cheval de Troie connu, modifié pour éviter la détection ;
- mise en place par ingénierie sociale :
  - e-mail ;
  - CD contenant des propositions commerciales ;
- vol de données et envoi vers un serveur FTP.

- Pas de détection avant l’enquête de police.

Microsoft TechDays 09
L’innovation avance avec vous

Plan

- **Introduction**
- **Quelques attaques virales**
- **Les antivirus**
- « Hygiène informatique »
- Politique antivirale de l’armée de terre
- Conclusion

Microsoft TechDays 09
L'innovation avance avec vous

mythes

Quelques ~~faits~~ sur les antivirus

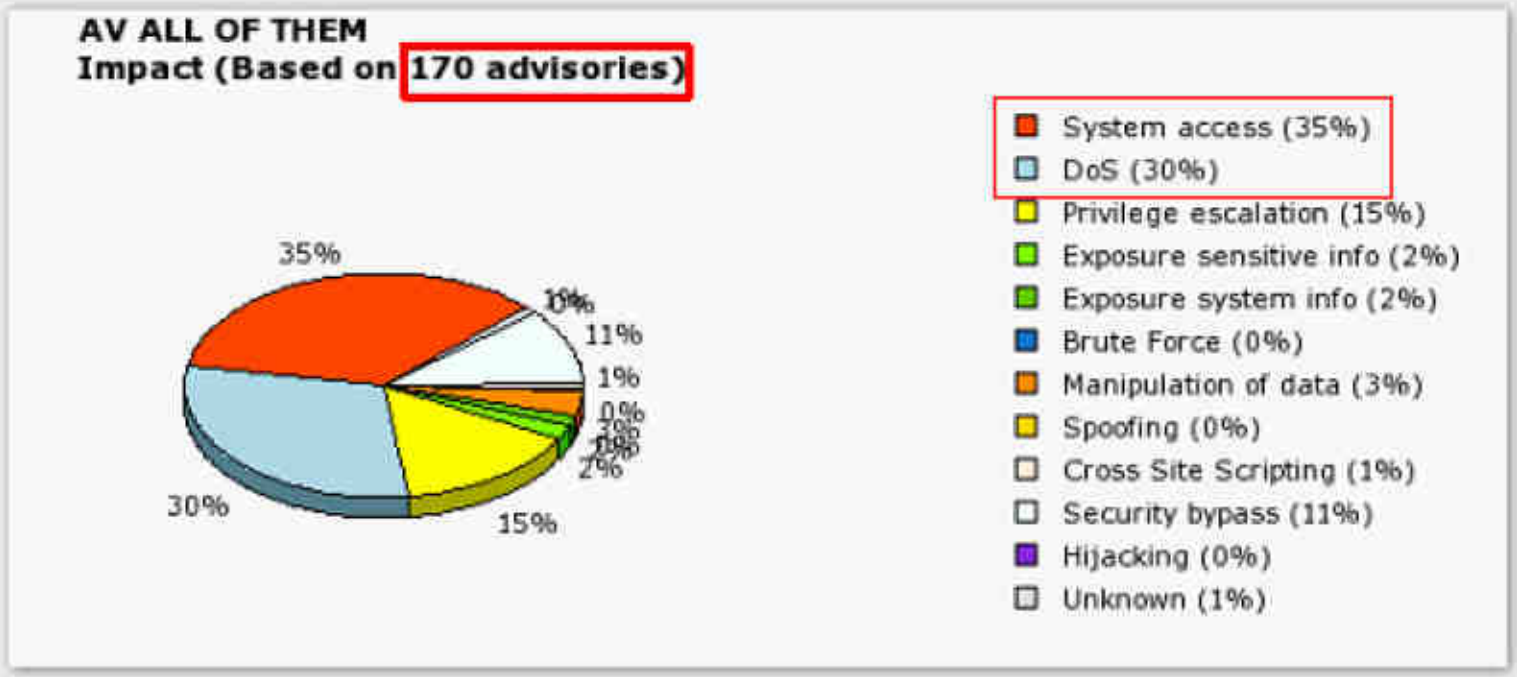
- **la sûreté :**
  - Un logiciel antivirus est sûr et rend vos systèmes plus sûrs ;
- **le développement :**
  - Les logiciels AV sont développés par des experts en sécurité ;
- **la détection :**
  - Si on utilise un antivirus, on ne sera pas infecté ;
  - Un antivirus détecte même les virus inconnus.

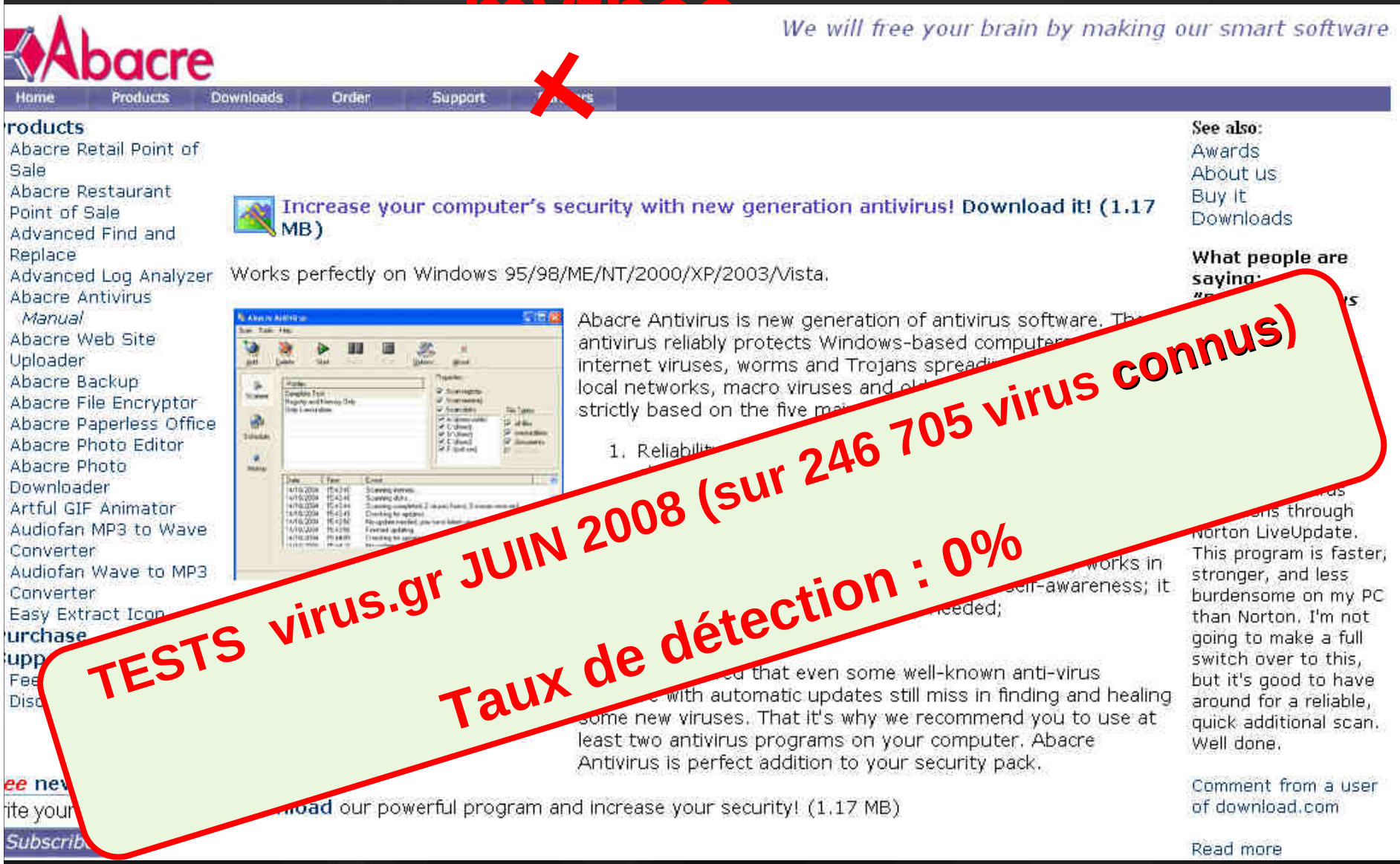
Microsoft TechDays 09
L'innovation avance avec vous

Approximately 800 vulnerabilities discovered in antivirus products

Posted by Dancho Danchev
July 7th, 2008

UPDATE: McAfee debunks recent vulnerabilities in AV software research, n.runs restates its position. In what appears to be either a common scenario of "when the security solution ends up the security problem itself", or a product launch basing its strategy on outlining the increasing number of critical vulnerabilities found in competing antivirus products, the IT/Security consulting firm n.runs AG claims to have discovered approximately 800 vulnerabilities within antivirus products based on exploiting a standard malware scanning process known as "parsing" :





Microsoft TechDays 09
L'innovation avance avec vous

NOTE DE COMMUNICATION DU CERTA

26 janvier 2006

Un message électronique semblant provenir de la direction de la communication et de l'information du ministère des affaires étrangères (webmestre.paris-dci@diplomatie.gouv.fr) est diffusé depuis hier soir, notamment vers les ambassades et consulats Étrangers en France.

Ce message qui a pour titre "changement de visa régime", mentionne dans le corps du texte l'adresse du service central d'Etat civil du ministère des affaires étrangères à NANTES. Il comporte en pièce jointe le fichier "visa regime.zip", qui contient une charge virale du même nom et dont l'extension est .scr. En cas d'exécution, un document rédigé en langue française s'ouvre automatiquement. Par ailleurs, des tentatives de connexion sont effectuées vers des serveurs situés à l'étranger. Ce virus polymorphe ne semble pas, à ce jour, être détecté par tous les éditeurs d'anti-virus.

En cas de réception de ce message, il est impératif de ne pas ouvrir la pièce jointe et d'en aviser le COSSI dans les meilleurs délais.

Nous vous remercions par avance de nous faire un état des lieux des réceptions de ce message électronique et des éventuelles infections avant 15h00, vendredi 27 janvier 2006.

Les malwares évoluent trop rapidement face aux antivirus

02-01-2008
Par la rédaction

Les cybercriminels utilisent les mêmes techniques que les éditeurs de sécurité pour tester leurs codes malveillants avant diffusion sur le 3W...

En matière de sécurité informatique, il n'existe pas encore de solution universelle capable de surveiller l'ensemble des menaces et de déjouer les techniques de piratage. Et face à une attaque ciblée, menée par des 'hackers' déterminés, il est quasiment impossible de se protéger.

(…) Aussi, la question mérite-t-elle d'être posée : les antivirus sont-ils encore efficaces ?

(…)

Une de ces études, commandées par 'PC World', montre que les solutions disponibles sur le marché ne bloquent qu'une fois sur quatre les nouveaux codes malveillants et que d'une manière générale quand la menace est nouvelle, elle traverse sans difficulté les barrières de sécurité des logiciels en place sur un système. Selon le magazine spécialisé, les solutions actuelles ne bloquent que la moitié des codes malveillants.

Et ce combat semble perdu d'avance pour les éditeurs de sécurité, car de nos jours, ce sont les cybercriminels qui ont les cartes en mains, ils ont l'avantage de l'effet de surprise et ils connaissent suffisamment les solutions de protection disponibles sur le marché pour les contourner. Hacker et éditeurs sont donc en guerre. Et pour l'instant l'avantage est aux malfaiteurs du Net.

Quelques ~~faits~~ mythes sur les antivirus

- **la sûreté :**
  - Un logiciel antivirus **est sûr** et **rend vos systèmes plus sûrs** ;
- **le développement :**
  - Les logiciels AV sont **développés par des experts en sécurité** ;
- **la détection :**
  - Si **on utilise un antivirus, on ne sera pas infecté** ;
  - Un antivirus **détecte même les virus inconnus**.

Microsoft TechDays 09 L'innovation avance avec vous

Les logiciels antivirus

- But :
  - détecter les programmes ayant un comportement supposé dangereux ;
  - en bloquer l'exécution.
- Deux modes de fonctionnement :
  - statique ;
  - dynamique.
- Deux techniques de détection :
  - Analyse de forme
  - Surveillance comportementale

Microsoft TechDays 09
L'innovation avance avec vous

Modes de fonctionnement

- Mode statique
  - Surveillance hors contexte d’exécution
  - Ex. : scan manuel, programmé
- Mode dynamique
  - Surveillance dans un contexte d’exécution
  - Ex. : surveillance en tâche de fond

Microsoft TechDays 09
L’innovation avance avec vous

Techniques de détection

- Analyse de forme :
  - Recherche de schémas caractéristiques dans un fichier.
  - Exemples :
    - Recherche de signature
      - Suite de bits caractéristique d'un virus
    - Analyse heuristique
      - Cherche des types de comportement suspects
    - Analyse spectrale
      - Fréquence d'utilisation des instructions
    - Contrôle d'intégrité
      - Surveille la modification des fichiers sensibles

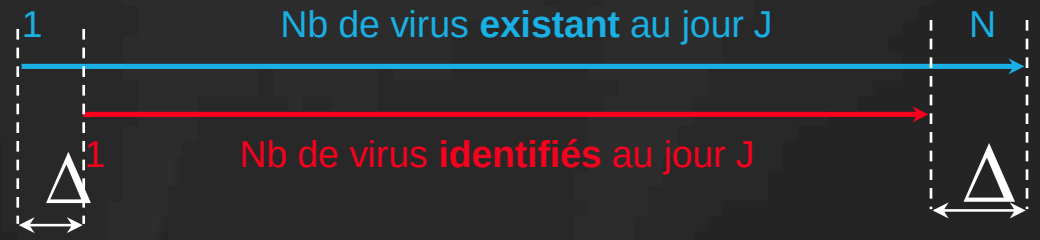
Microsoft TechDays 09 L'innovation avance avec vous

Techniques de détection

- Analyse comportementale :
  - Surveillance du comportement d ’un ficher à l’ouverture (base de comportement).
  - Exemples :
    - Analyse heuristique
      - Cherche des types de comportement suspects
    - Émulation de code
      - Chargement du code en zone mémoire confinée pour déterminer son comportement

Microsoft TechDays 09
L'innovation avance avec vous

Garder son antivirus à jour



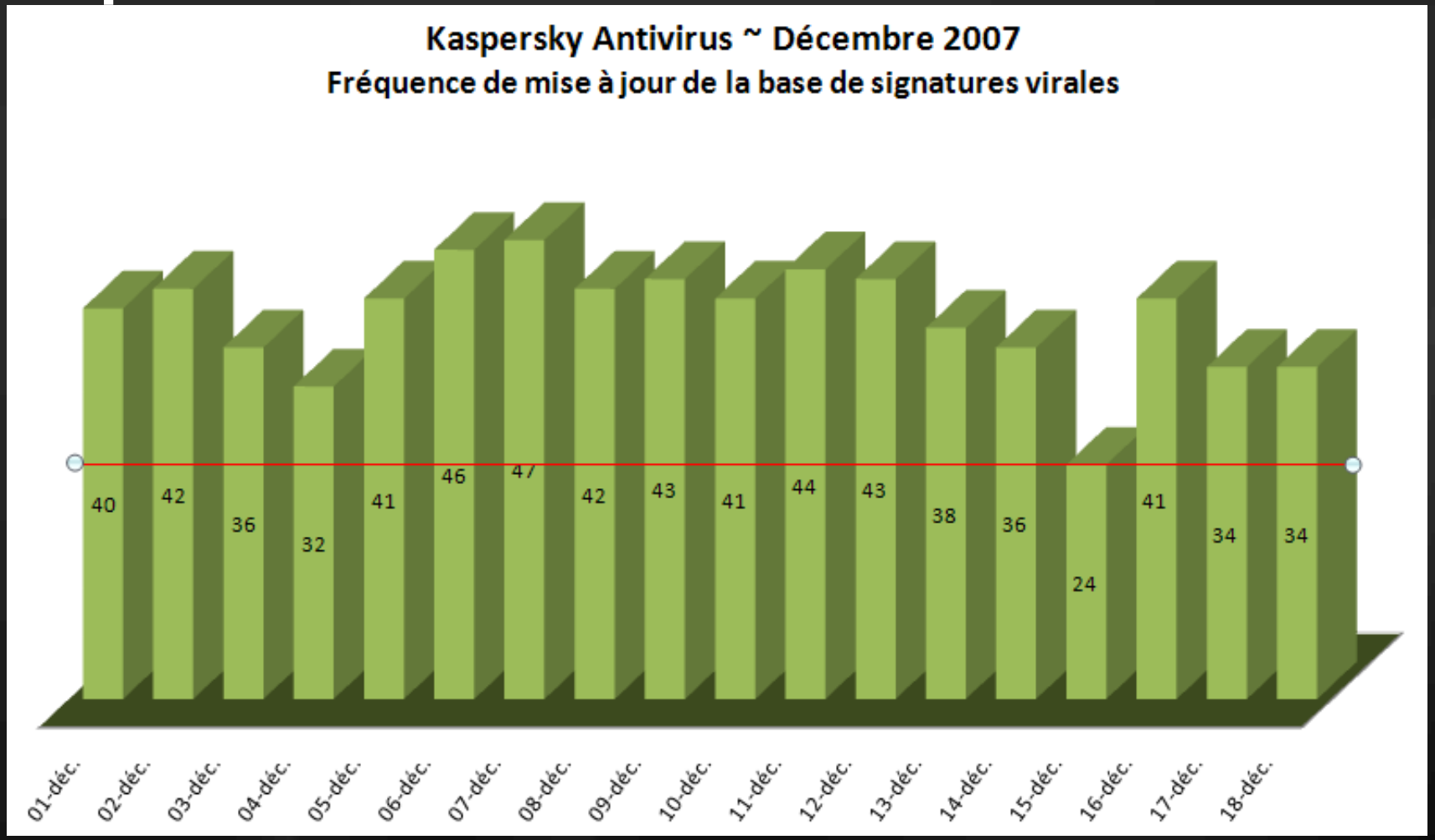
Nb de virus **existant** au jour J Nb de virus **identifiés** au jour J

Δ doit être le plus petit possible !

L'éditeur de l'antivirus doit mettre à la disposition du client des mises à jour régulières des fichiers de signatures

Microsoft TechDays 09 L'innovation avance avec vous

Garder son antivirus à



TechDays 09
L'innovation avance avec vous

Les qualités relatives des différents logiciels anti-virus

- Tous les anti-virus fondent presque exclusivement sur une analyse de forme.
- Sur 14 antivirus analysés :
  - Les fonctions et motifs de détection utilisés sont tous très faibles.
  - Très grande similitude d'un produit `a un autre.

➔Les produits actuels sont faciles à leurrer et à contourner.

Microsoft TechDays 09 L'innovation avance avec vous

Products	Version	Viral Definition
Avast	4.6.691	0527-2
AVG	7.0.338	267.9.2/52
Bit Defender	7.2	09/16/05
DrWeb	4.33.2.12231	02/25/06 (104186)
eTrust	7.1.194	11.5.8400 (Vet)
eTrust	7.1.194	23.65.44 (InoculateIT)
F-Secure 2005	5.10-480	09/15/05
G-Data	AVK 16.0.3	KAV-6.818/BD-16.864
KAV Pro	5.0.383	09/19/05
McAfee 2006	-	DAT 4535
NOD 32	2.5	1.1189 (08/08/05)
Norton 2005	11.0.2.4	09/15/05
Panda Titanium 2006	5.01.02	01/17/06
Sophos	5.0.5 R2	3.98
Trend Office Scan	6.5 - 7.100	2.837.00

Table 3: Tested antivirus software (versions & viral definitions)

Microsoft TechDays 09 L'innovation avance avec vous

Product name	Signature size (in bytes)	Signature (indices)
Avast	29	14,128 → 14,144, 14,146 → 14,157, 14,159
AVG	7,297	0 - 1 - 60 - 200 - 201 - 220 - 469...
Bit Defender	6	0 - 1 - 60 - 200 - 201 - 206
DrWeb	12	0 - 1 - 60 - 200 - 201 - 206 - 220... 222 - 461 - 465 - 469
eTrust/Vet	3,700	0 - 1 - 60 - 200 - 201 - 206 - ...
eTrust/InoculateIT	3,700	0 - 1 - 60 - 200 - 201 - 206 - ...
F-Secure 2005	11	0 - 1 - 60 - 200 - 201 - 206 220 - 240 - 241 - 461 - 469
G-Data	6	0 - 1 - 60 - 200 - 201 - 206
KAV Pro	11	The same as *F-Secure 2005*
McAfee 2006	7	0 - 1 - 60 - 200 - 201 - 206 - 220
NOD 32	7,449	0 - 1 - 60 - 200 - 201 - 204 - 205...
Norton 2005	0	(not an AND function)
Panda Tit. 2006	9	0 - 1 - 60 - 200 - 201 - 206 220 - 461 - 541
Sophos	28	0 - 1 - 60 - 200 - 201 - 206 - 220...
Trend Office Scan	7	0 - 1 - 60 - 200 - 201 - 206 - 220

Table 4: Viral patterns for *W32/Bagle.A*

Product name	Signature size (in bytes)	Signature (indices)
Avast	9	8,162 - 8,166 - 8,170 - 8,173 - 8,175 8,180 - 8,181 - 8,187 - 8189
AVG	13,288	0 - 1 - 60 - 216 - 217 - 222 - 236...
Bit Defender	87	2,831 - 2,964 - ....
DrWeb	1,773	0 - 1 - 60 - 216 - 217 - 222 - 236...
eTrust/Vet	4,306	0 - 1 - 60 - 216 - 217 - 222 - ...
eTrust/InoculateIT	4,306	0 - 1 - 60 - 216 - 217 - 222 - ...
F-Secure 2005	105	0 - 1 - 60 - 216 - 217 - 222 - ...
G-Data	3	2831 - 2964 - 2965
KAV Pro	105	The same as *F-Secure 2005*
McAfee 2006	12,039	0 - 1 - 60 - 216 - 217 - 222 - ...
NOD 32	4,793	0 - 1 - 60 - 216 - 217 - 220 - 221...
Norton 2005	0	(not an AND function)
Panda Tit. 2006	37	0 - 1 - 59 - 60 - 216 - 217 - 222...
Sophos	15,028	0 - 1 - 2 - 4 - 8 - 12 - 13 - 16 - 24...
Trend Office Scan	146	0 - 1 - 60 - 216 - 217 - 222 - ...

Table 5: Viral patterns for *W32/Bagle.E*

Microsoft TechDays 09 L'innovation avance avec vous

Product name	Signature size (in bytes)	Signature (indices)
Avast	8	7,256 → 7,259 7,278 → 7,281
AVG	7,276	5739 - 5864 - 5866 - ...
Bit Defender	3,342	7,385 - 7,386 - ....
DrWeb	2,896	0 - 1 - 60 - 144 - 145 - 150 - 164...
eTrust/Vet	4,320	0 - 1 - 60 - 144 - 145 - 150 - 164...
eTrust/InoculateIT	1,311	0 - 1 - 60 - 144 - 145 - 150 - 164...
F-Secure 2005	3,128	0 - 1 - 60 - 144 - 145 - 150 - 164...
G-Data	2,954	0 - 1 - 60 - 144 - 145 - 150 - 445...
KAV Pro	3,128	The same as *F-Secure 2005*
McAfee 2006	8,084	0 - 1 - 60 - 144 - 145 - 150 - 164...
NOD 32	9,629	0 - 60 - 144 - 145 - 148 - 149 - ...
Norton 2005	8	0 - 1 - 60 - 144 - 145 150 - 164 - 445
Panda Tit. 2006	437	0 - 1 - 32 → 35 - 60 - 64...
Sophos	3,429	0 - 1 - 60 - 144 - 145 - 150 - 164...
Trend Office Scan	63	7,750 - ...

Table 6: Viral patterns for *W32/Bagle.J*

Microsoft TechDays 09
L'innovation avance avec vous

Product name	Signature size (in bytes)	Signature (indices)
Avast	10	14,567 - 14,574 → 14,577 14,581 - 14,585 → 14,588
AVG	13,112	533 → 663 - 665 - ...
Bit Defender	6,093	0 - 1 - 60 - 128 - 129 - 134 - ...
DrWeb	6,707	0 - 1 - 60 - 128 - 129 - 132 - 133...
eTrust/Vet	4,343	0 - 1 - 60 - 128 - 129 - 134 - ...
eTrust/InoculateIT	1,276	0 - 1 - 60 - 128 - 129 - 134 - ...
F-Secure 2005	54	0 - 1 - 60 - 128 - 129 - 548 - ...
G-Data	53	0 - 1 - 60 - 128 - 129 - 548 - ...
KAV Pro	54	The same as *F-Secure 2005*
McAfee 2006	4,076	0 - 1 - 60 - 128 - 129 - 134 - ...
NOD 32	17,777	0 - 1 - 60 - 128 - 129 - 132 - 133...
Norton 2005	51	0 - 1 - 60 - 128 - 129 - 134 - 429 - ...
Panda Tit. 2006	1659	0 - 1 - 4 - 8 - 12 - 13 - 16 - 24...
Sophos	7,538	0 - 1 - 60 - 128 - 129 - 134 - 148...
Trend Office Scan	44	0 - 1 - 60 - 128 - 129 - ...

Table 7: Viral patterns for *W32/Bagle.N*

Microsoft TechDays 09
L'innovation avance avec vous

Product name	Signature size (in bytes)	Signature (indices)
Avast	8	12,916 → 12,919 12,937 → 12,940
AVG	14,575	533 → 536 - 538 - ...
Bit Defender	8,330	0 - 1 - 60 - 128 - 129 - 134 - ...
DrWeb	6,169	0 - 1 - 60 - 128 - 129 - 134 - ...
eTrust/Vet	1,284	0 - 1 - 60 - 128 - 129 - 134 - ...
eTrust/InoculateIT	1,284	0 - 1 - 60 - 128 - 129 - 134 - ...
F-Secure 2005	59	0 - 1 - 60 - 128 - 129 - 546 - ...
G-Data	54	0 - 1 - 60 - 128 - 129 - 546 - ...
KAV Pro	59	The same as *F-Secure 2005*
McAfee 2006	12,1278	0 - 1 - 60 - 128 - 129 - 134 - ...
NOD 32	21,849	0 - 1 - 60 - 128 - 129 - 132 - 133 - ...
Norton 2005	6	0 - 1 - 60 - 128 - 129 - 134
Panda Tit. 2006	7,579	0 - 1 - 60 - 134 - 148 - 182 - 209...
Sophos	8,436	0 - 1 - 60 - 128 - 129 - 134 - 148...
Trend Office Scan	88	0 - 1 - 60 - 128 - 129 - ...

Table 8: Viral patterns for *W32/Bagle.P*

Microsoft TechDays 09
L'innovation avance avec vous

Les différ logic

$$
\begin{aligned}
\overline{f_{\mathrm{W32/Bagle.E}}} = \\
& \overline{x_0}.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & \overline{x_0}.\overline{x_1}.\overline{x_{60}}.\overline{x_{61}}.\overline{x_{62}}.\overline{x_{63}}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{646}.x_{646}.x_{647}.x_{648} \\
\vee\ & \overline{x_0}.\overline{x_1}.\overline{x_{60}}.\overline{x_{61}}.\overline{x_{62}}.\overline{x_{63}}.\overline{x_{216}}.\overline{x_{217}}.\overline{x_{222}}.\overline{x_{223}}.\overline{x_{236}}.\overline{x_{237}}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & \overline{x_0}.\overline{x_1}.\overline{x_{60}}.\overline{x_{61}}.\overline{x_{62}}.\overline{x_{63}}.\overline{x_{216}}.\overline{x_{217}}.\overline{x_{222}}.\overline{x_{223}}.\overline{x_{236}}.\overline{x_{237}}.\overline{x_{645}}.\overline{x_{646}}.\overline{x_{647}}.\overline{x_{648}} \\
\vee\ & x_0.\overline{x_1}.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.\overline{x_{60}}.\overline{x_{61}}.\overline{x_{62}}.\overline{x_{63}}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.\overline{x_{60}}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.\overline{x_{60}}.\overline{x_{61}}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.\overline{x_{60}}.\overline{x_{61}}.\overline{x_{62}}.\overline{x_{63}}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.\overline{x_{61}}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.\overline{x_{62}}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.\overline{x_{63}}.x_{216}.x_{217}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.\overline{x_{648}} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.\overline{x_{216}}.\overline{x_{217}}.\overline{x_{222}}.\overline{x_{223}}.\overline{x_{236}}.\overline{x_{237}}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.\overline{x_{216}}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.\overline{x_{216}}.\overline{x_{217}}.\overline{x_{222}}.\overline{x_{223}}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.\overline{x_{217}}.x_{222}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.\overline{x_{222}}.x_{223}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.\overline{x_{223}}.x_{236}.x_{237}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.\overline{x_{236}}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.\overline{x_{237}}.x_{645}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{237}.\overline{x_{645}}.\overline{x_{646}}.\overline{x_{647}} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{237}.\overline{x_{645}}.\overline{x_{646}}.\overline{x_{647}}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{237}.\overline{x_{645}}.x_{646}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{237}.x_{645}.\overline{x_{646}}.x_{647}.x_{648} \\
\vee\ & x_0.x_1.x_{60}.x_{61}.x_{62}.x_{63}.x_{216}.x_{217}.x_{222}.x_{223}.x_{237}.x_{645}.\overline{x_{647}}.x_{648}
\end{aligned}
$$

Microsoft TechDays 09
L'innovation avance avec vous

Les qualités relatives des différents logiciels anti-virus

- Tests du site www.virus.gr (Juin 2008)

Produits	%
G-Data	99,05
F-Secure	98,75
TrustPort	98,06
Kaspersky	97,75
Mc Afee	86,39
Norton	83,34
Panda	61,41

246 705 virus connus

Antivirus paramétrés pour une configuration de détection optimale

Microsoft TechDays 09 L'innovation avance avec vous

Pourquoi des « non détections » ?

- Détection par analyse de forme :

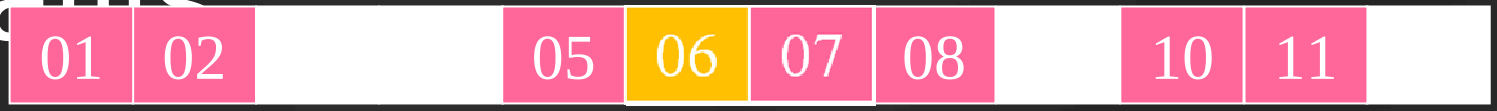
Signature : 01-02-05-06-08-10

Faux positifs…

- Signature : 01-02-05-06-08-10

- Signature : 01-02-05-06-08-10-11

Faux positifs… … et faux négatifs



- Signature : 01-02-05-06-08-10

- Signature : 01-02-05-08-10 11

Plan

- **Introduction**
- **Quelques attaques virales**
- **Les antivirus**
- **« Hygiène informatique »**
- Conclusion

Microsoft TechDays 09
L'innovation avance avec vous

« Hygiène informatique »

Le comportement des utilisateurs :

- L’utilisateur, maillon faible ?
- Eviter les conduites à risque
- Ne pas mélanger informatique familiale et professionnelle
- Former / Sensibiliser

Microsoft TechDays 09
L'innovation avance avec vous

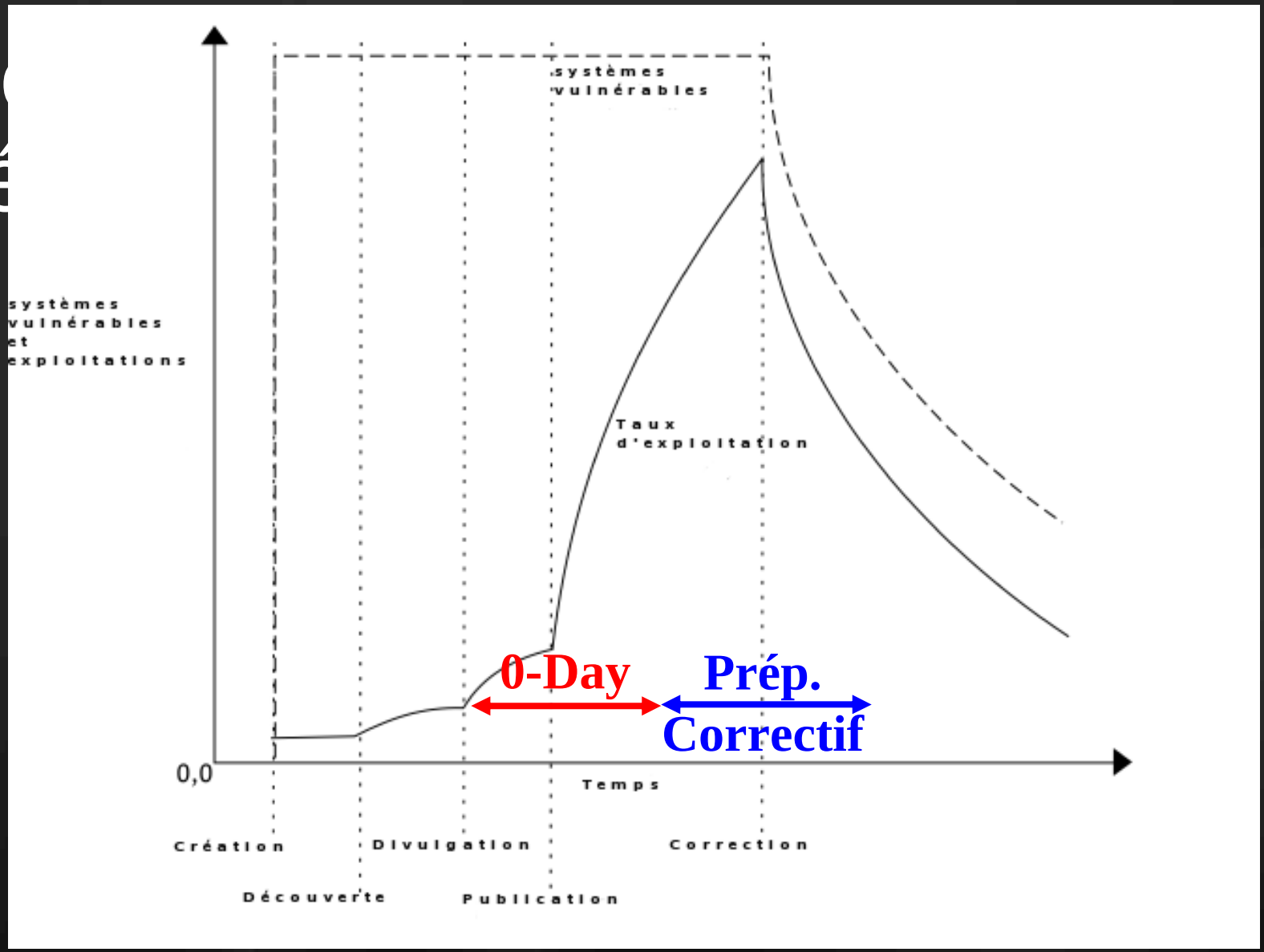
« Hygiène informatique »

Contrôle des contenus :

- Création d’un sas entre le système à protéger et le monde extérieur
  - Interdire à l’utilisateur la possibilité d’installer des logiciels
- Contrôle des licences
- Sauvegarde du système

Microsoft TechDays 09
L'innovation avance avec vous

D
sé



Microsoft TechDays 09
L'innovation avance avec vous

Réaction élémentaire à une infection

- **Déconnecter la machine du réseau**
  - Eviter la propagation de l'infection
- **NE PAS L'ARRETER**
  - Eviter d'éventuels effets secondaires
- **Rendre-compte**

CE DOIT ETRE UN ACTE REFLEXE !!!

Microsoft TechDays 09 L'innovation avance avec vous

Plan

- Introduction
- Quelques attaques virales
- Les antivirus
- « Hygiène informatique »
- Conclusion

Microsoft TechDays 09
L'innovation avance avec vous

Conclusion

- Les solutions ne sont que partiellement techniques
- Si les règles organisationnelles ne sont pas respectées, toute protection est illusoire

Microsoft TechDays 09
L'innovation avance avec vous

Conclusion

- Appliquer les règles de bases en matière d’hygiène informatique :
  - Contrôle du contenu.
  - Contrôle de l’origine.
  - Contrôle du paramétrage.

Microsoft TechDays 09
L’innovation avance avec vous

RAPPEL

LUTTE ANTIVIRALE EFFICACE

=

Antivirus à jour

+

Système à jour

+

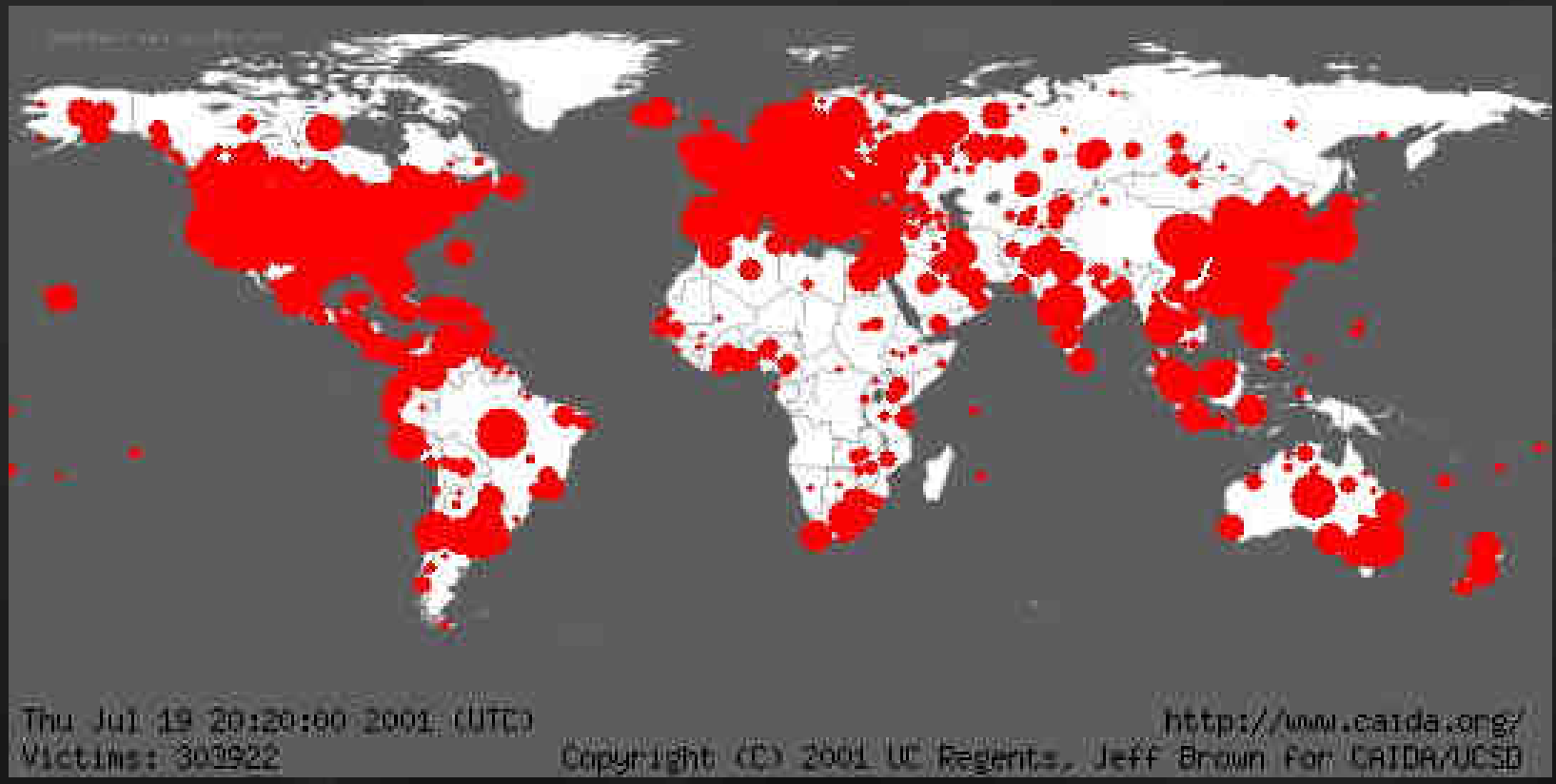
Règles de comportement strictes à respecter

Microsoft TechDays 09
L'innovation avance avec vous

?

Microsoft TechDays 09
L'innovation avance avec vous

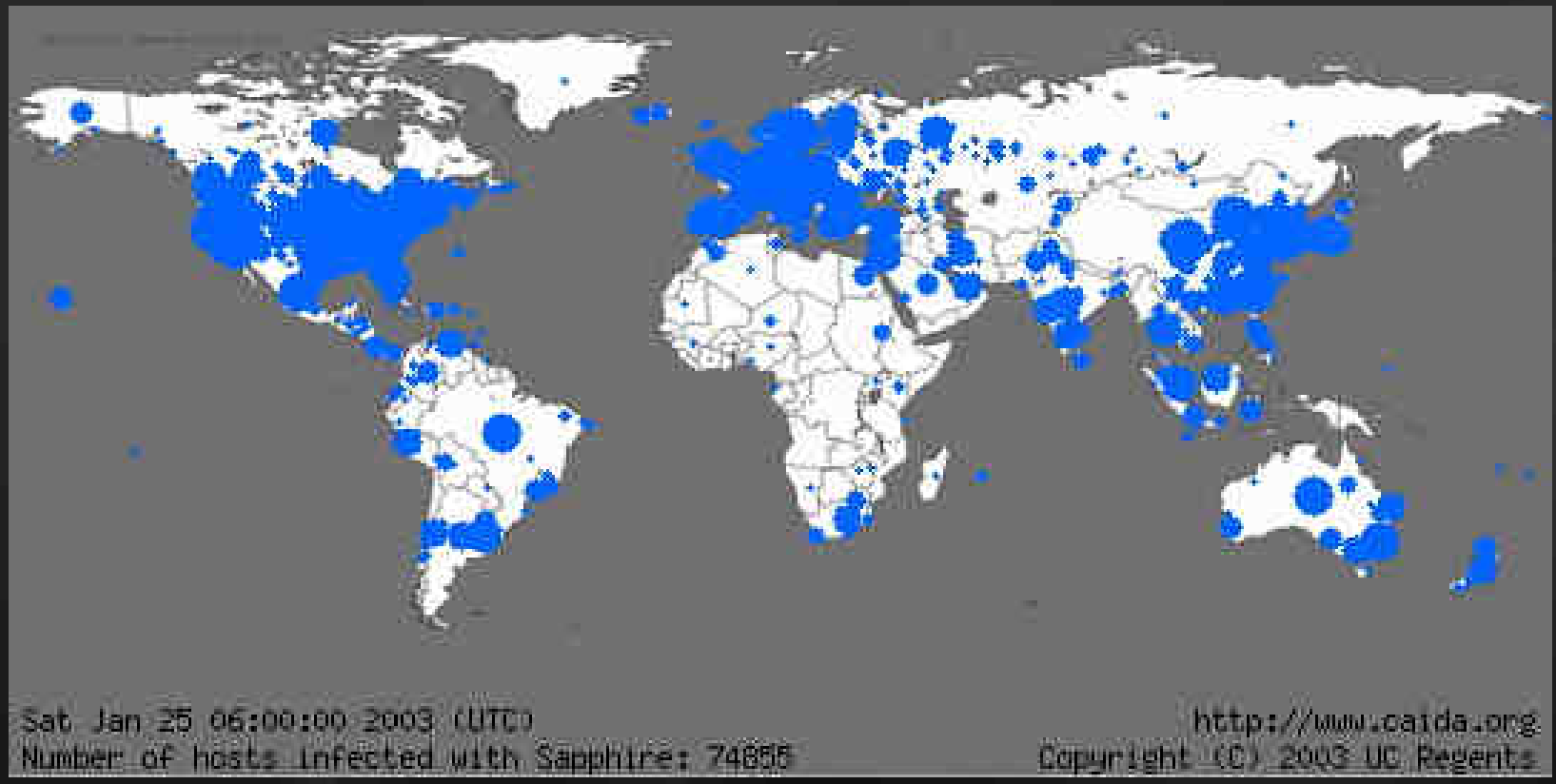
2001 : Code Red



20 heures après le déclenchement de l'épidémie

Microsoft TechDays 09
L'innovation avance avec vous

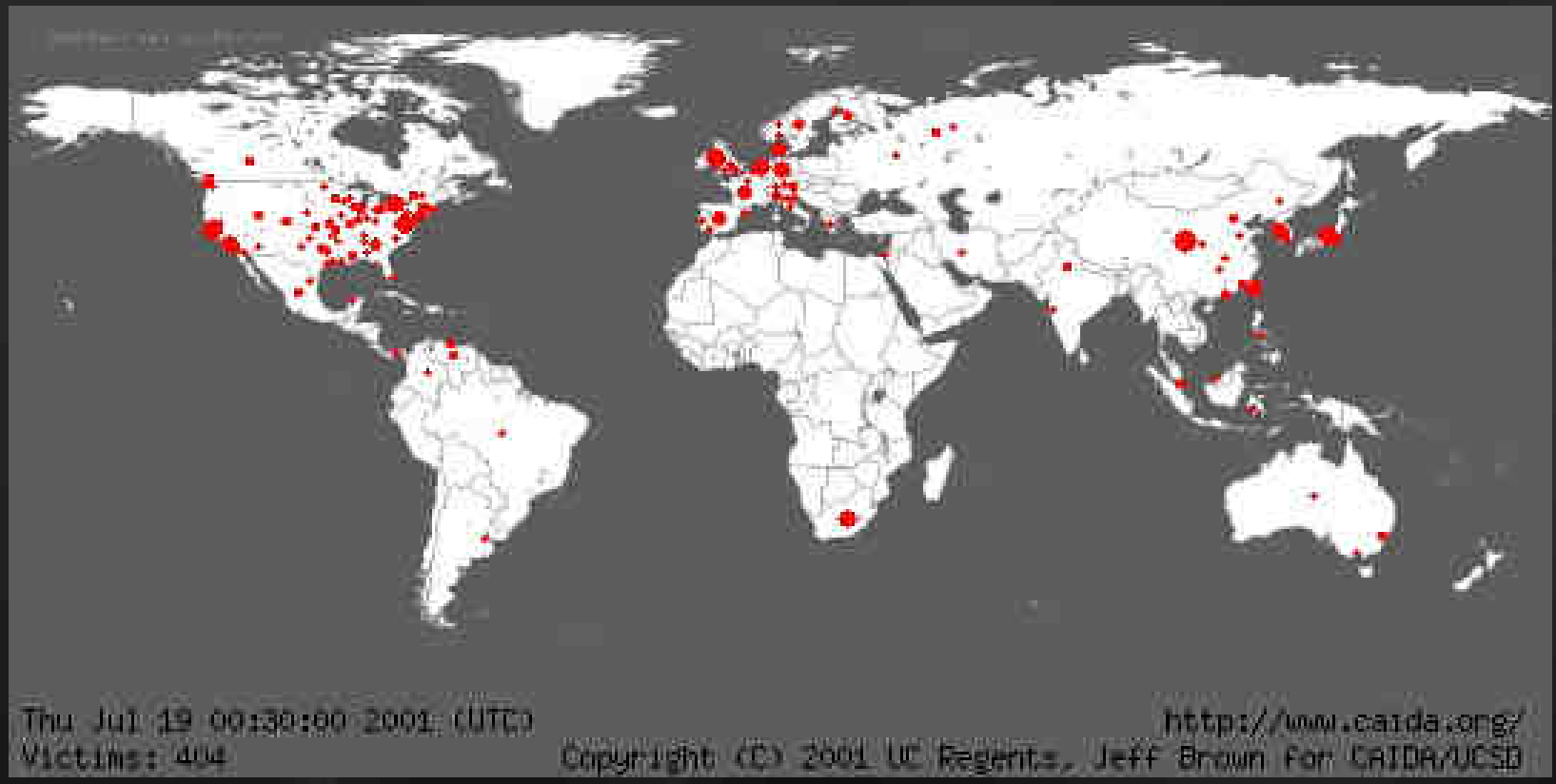
2003 : Saphire / Slammer



30 minutes après le déclenchement de l'épidémie

Microsoft TechDays 09
L'innovation avance avec vous

2001 : Code Red



30 minutes après le déclenchement de l'épidémie

Microsoft TechDays 09
L'innovation avance avec vous