Bonnes pratiques pour les Utilisateurs

CERT OSIRIS

UNIVERSITÉ DE STRASBOURG

Sensibilisation aux menaces Internet
&
Formation aux bonnes pratiques pour les utilisateurs (BPU) de systèmes informatiques

Goodies
Les ANTIVIRUS

Septembre 2013

Que valent les antivirus ?

- Attention : tous les antivirus ne se valent pas !
- Il est toujours possible de contourner un antivirus (chiffrement, polymorphisme...)
- Ce n'est pas parce que l'ordinateur est équipé d'un antivirus que l'on peut faire n'importe quoi sur Internet.
- La sécurité est avant tout affaire d'état d'esprit et de comportement, non pas de produits.

Réf. : http://www.zdnet.fr/actualites/eric-filiol-esiea-les-editeurs-d-antivirus-confondent-le-business-et-le-besoin-des-utilisateurs-39710371.htm

Que valent les antivirus ?

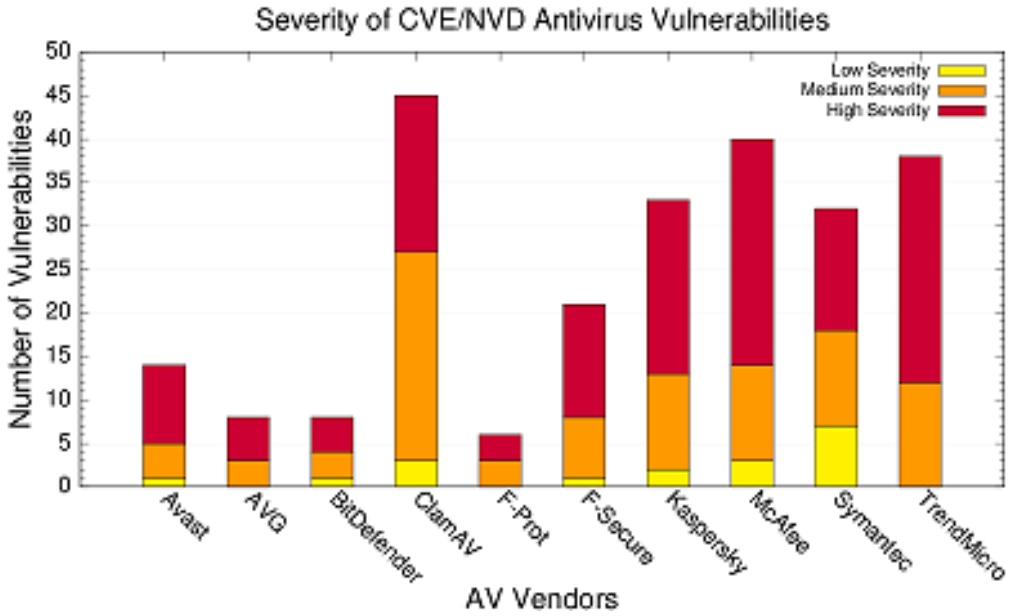
P. 3

	KASPERSKY Internet Security 2011	NORTON Internet Security 2011	G DATA Internet Security 2011	BITDEFENDER Internet Security 2011	AVIRA Premium Security Suite	TREND MICRO Titanium Max. Security 2011	F-SECURE Internet Security 2011	ESET Smart Security 4	TRUSTPORT Internet Security 2011	AVG Internet Security 2011
	Version 11.0.2.556	Version 18.5.0.125	Version 21.1.0.6	Version 14.0.24.337	Version 10.0.0.98	Version 3.0	Version 2011	Version 4.2.40.10	Version 11.0.0.4594	Version 10.0.1191
Note globale	7,9	7,5	7,45	7,42	7,0	6,71	6,67	6,4	6,22	6,16
Mention	BIEN	BIEN	BIEN	BIEN	BIEN	BIEN	BIEN	BIEN	BIEN	BIEN
	1er 50 €	2e 70 €	3e 40 €	4e 40 €	5e 40 €	6e 60 €	7e 45 €	8e 50 €	9e 40 €	10e 50 €
	7,5	5	7	6,8	6,8	7,6	5,5	5,2	4,9	4,9
	Bien 6,2	Passable 6	Passable 5,6	Bien 6,5	Bien 6,3	Excellent 9,1	Bien 6,3	Passable 4,5	Médiocre 3,7	Médiocre 3,8
	Excellent 8,9	Médiocre 3,9	Excellent 8,9	Bien 7,5	Bien 7,9	Bien 6,4	Passable 5	Bien 6,4	Bien 6,4	Bien 6,1
	Excellent 9	Médiocre 4	Médiocre 2,5	Médiocre 4	Recalé 2	Médiocre 4	Médiocre 3	Recalé 2	Recalé 2	Médiocre 4
	8,7	8,3	6,1	6,3	4,8	3,3	3,8	1,8	3,3	2,3
	Excellent 9	Excellent 9	Bien 7	Passable 6	Passable 6	Recalé 1	Médiocre 4	Recalé 1	Recalé 2	Recalé 2
	Excellent 10	Excellent 9	Bien 7	Bien 8	Passable 5	Bien 7	Passable 5	Médiocre 3	Bien 7	Médiocre 3
	Médiocre 3	Passable 6	Recalé 2	Passable 5	Recalé 1	Médiocre 4	Recalé 0	Recalé 1	Recalé 1	Recalé 2
	Excellent 9	Passable 5	Médiocre 3	Médiocre 4	Recalé 2	Médiocre 3	Médiocre 3	Médiocre 3	Recalé 1	Recalé 2
	8,78	8,44	9,2	8,53	8,32	8,81	8,44	8,63	6,43	9,2
	Excellent 9,4	Excellent 9,2	Excellent 9,4	Excellent 8,3	Bien 7,8	Excellent 9,5	Bien 8	Excellent 8,3	Bien 6,1	Excellent 8,8
	Excellent 8,9	Excellent 8,75	Excellent 9,55	Excellent 8,7	Excellent 9,1	Excellent 9,35	Excellent 9,4	Excellent 9,2	Bien 6,85	Excellent 9,25
	Excellent 9,2	Excellent 8,8	Excellent 9,6	Excellent 8,3	Excellent 9	Excellent 9,3	Excellent 9,2	Excellent 8,8	Bien 6,7	Excellent 9,8
	Passable 6	Passable 5	Passable 6	Excellent 9	Médiocre 3	Médiocre 4	Recalé 2	Passable 6	Médiocre 4	Bien 7
	7,7	7,3	8,2	8,1	8,8	6,3	7,9	7,7	8,3	7,9
	Excellent 9,6	Excellent 9,8	Excellent 9,9	Excellent 9,7	Excellent 9,8	Excellent 9,6	Excellent 9,7	Excellent 9,6	Excellent 9,6	Excellent 9,7
	Bien 7	Bien 7,5	Excellent 8,3	Excellent 8,1	Excellent 8,9	Bien 6,6	Bien 7,8	Bien 7,3	Bien 8	Bien 7,8
	Bien 6,5	Passable 4,2	Bien 6,9	Bien 6,5	Excellent 8,2	Médiocre 2,8	Bien 6,4	Bien 6,5	Bien 7,9	Bien 6,4
	Bien 8	Excellent 9	Passable 6	Bien 8	Passable 6	Passable 6	Passable 6	Passable 6	Passable 5	Passable 6
	7	8	7	8	7	7	8	9	8	8
	Bien 8	Bien 8	Bien 7	Bien 7	Bien 7	Bien 7	Bien 7	Excellent 10	Bien 8	Bien 8
	Excellent 9	Excellent 10	Bien 7	Bien 8	Bien 8	Bien 8	Bien 8	Excellent 10	Bien 7	Bien 8
	Passable 5	Bien 7	Passable 6	Passable 6	Passable 5	Passable 5	Bien 7	Bien 7	Bien 8	Passable 6
	Excellent 9	Excellent 9	Excellent 9	Excellent 9	Excellent 9	Excellent 9	Excellent 10	Excellent 9	Excellent 9	Excellent 9
	Passable 6	Bien 7	Bien 7	Bien 8	Passable 5	Bien 8	Passable 6	Excellent 9	Bien 8	Bien 7
	8,2	8,5	6,8	7,5	4,6	6,1	4,7		4,2	NON APPLICABLE
	Bien 7	Bien 7	Bien	Bien 7	Bien 7	Bien 7	Bien 7		Médiocre 4	
	Excellent 9	Excellent 10	Excellent	Bien 8	Bien 8	Bien 8	Bien 8		Bien 8	
	Bien 8	Bien 7	Passable	Passable 6	Passable 5	Passable 5	Bien 7		Médiocre 3	
	Excellent 9	Excellent 10	Passable	Excellent 9	Excellent 9	Excellent 9	Excellent 10		Recalé 0	
				Bien 8	Passable 5	Bien 8	Passable 6			

Remarque : aucun antivirus n'obtient la note maximale (10) dans aucun test !

Que valent les antivirus ?

"Approximately 800 vulnerabilities discovered in antivirus products"
ZDNet, 7 juillet 2008



Les antivirus possèdent eux-mêmes un certain de nombre de vulnérabilités.

Avant tout, un business…

MessageLabs®

Email Anti-Virus Service v5.1

La différence MessageLabs

- 100% de protection contre des virus connus et inconnus
- Utilise la technologie Skeptic™,

Le New York Times piraté et Symantec n'a rien vu, mais se défend

Sécurité : Attaqué durant plusieurs mois, son réseau et des postes compromis par des virus, le New York Times accuse des hackers chinois d'être les auteurs de ces attaques. Le journal reproche aussi à son antivirus, Symantec, d'avoir été totalement aveugle. Mais pour l'éditeur, il ne peut y avoir un seul responsable.

Par La rédaction de ZDNet.fr | Vendredi 01 Février 2013

« Le célèbre journal américain, le New York Times a eu quelques démêlés avec des hackers, chinois d'après son enquête. Pendant quatre mois, le NYT a été attaqués et des pirates ont pu s'introduire dans son réseau, compromettant notamment des postes et dérobant des mots de passe.

Le NYT a dû faire appel à des experts en sécurité, entre autres afin de venir à bout des différents programmes malveillants disséminés sur son réseau et ses ordinateurs. Des malware qui avaient échappé à la vigilance (ou sa non-vigilance) de l'antivirus du journal, à savoir celui de Symantec.

Sur les 45 virus installés, Symantec n'en a détecté qu'un seul. Un bilan peu flatteur pour l'éditeur de sécurité. Symantec est donc sorti de sa réserve par le biais d'un communiqué, expliquant que les solutions de sécurité ne pouvaient à elles seules combattre les attaques.

« Le bon sens doit prévaloir, et d'autres actions préventives doivent être employées » explique encore l'éditeur. Un bon sens dont les salariés et informaticiens réseaux du NYT auraient fait défaut ? Symantec pourrait le sous-entendre. Mais l'éditeur explique aussi qu'une approche antivirale par signatures n'est plus suffisante pour combattre les menaces actuelles. »

Les virus du futurs : vers une menace imparable ?

Utilisation des mathématiques : théorie de l'information, théorie de la calculabilité

Complexification des codes viraux : Polymorphisme, métamorphisme, Codes de Bradley, virus cryptographiques, vers combinatoires, vers furtifs, virus stéganographiques…

Un antivirus peut toujours être contourné : en amont par l'absence de détection face à un code innovant et en aval avec un blindage viral efficace

BELGIQUE - Un logiciel malveillant paralyse le ministère des finances belge : depuis jeudi dernier, un service public fédéral du ministère belge des finances est paralysé par un logiciel malveillant. Non détecté par les antivirus, ce programme (*sality.gen*, connu depuis 2009) n'aurait pas eu accès aux données des contribuables. (*RTBF* du 11/02/12)

[L'indisponibilité de services financiers touchant tout le pays témoigne de l'ampleur que peut prendre une attaque informatique, ici un simple ver non identifié.]

GÉORGIE - Un *botnet* mis en place à des fins d'espionnage : cet ensemble de plus de 200 machines zombies se concentre essentiellement sur le pays mais se développe encore actuellement. Il recherche avec des mots-clés des documents sensibles sur les ordinateurs infectés, probablement en vue de les revendre. Le code malveillant se met régulièrement à jour **afin de ne pas être détecté par les logiciels antivirus**. (*Eset* du 21/03/12, *ITworld* du 24/03/12)

MONDE - Une mise à jour des versions payantes du logiciel antivirus *Avira* bloque des millions d'ordinateurs : elle considérait des composants critiques du système d'exploitation *Windows* comme étant des logiciels malveillants. (*ZDNet* et *Avira* du 15/05/12)

JAPON - Une centaine d'ordinateurs du ministère des finances victimes d'une attaque d'espionnage informatique : le logiciel malveillant, **non détecté par les antivirus**, aurait été actif de janvier 2010 à novembre 2011. L'analyse du système d'information fait apparaître que des documents sensibles relatifs à des réunions internes au ministère auraient pu être exfiltrés. Selon le gouvernement, aucun dossier fiscal de contribuable n'a été compromis.
(*The Japan Times* du 21/07/12)

[L'envoi de courriels malveillants constitue souvent la première étape à une attaque de grande ampleur. Des mesures de défense en profondeur, de sensibilisation des utilisateurs, de journalisation et de surveillance des activités sur les réseaux sont nécessaires.]

MAROC - Attaque informatique sophistiquée contre des journalistes indépendants : ces derniers ont réceptionné un courriel accompagné d'un fichier contenant un programme malveillant non reconnu par les logiciels antivirus, d'après la société *Defensive Lab*.
(*Yabiladi* du 31/07/12)