

Windows Defender est-il efficace?

 malekal.com /efficacite-windows-defender/

malekalmorte

07/07/2016

Windows Defender est un [antivirus gratuit](#) fournit par défaut depuis Windows Vista.

Les avis sur Windows Defender divergent souvent mais la question principale est de savoir si Windows Defender est actuellement suffisant pour se protéger des [virus](#).

Cette page tente de répondre à cette question et donner un avis sur l'efficacité de Windows Defender.

Table des matières [[masquer](#)]

- [1 Historique Windows Defender](#)
- [2 Amélioration de la protection de Windows Defender](#)
- [3 Efficacité de Windows Defender ?](#)
 - [3.1 En 2013 : Microsoft Security Essentials](#)
 - [3.2 Après 2013 : et Windows Defender en version antivirus](#)
 - [3.3 Fin 2014 : Windows Defender et Windows 10](#)
 - [3.4 et la protection sur le terrain](#)
- [4 Conclusion et avis sur Windows Defender](#)



Historique Windows Defender

Plusieurs antivirus Microsoft se sont succédés.

Initialement Microsoft Security Essentials apparu en Septembre 2009 et qui succède Windows Live Oncare. Microsoft Security Essential est devenu alors [antivirus](#) à part entière.

Parallèlement depuis Windows Vista, Windows Defender était fourni par défaut, il s'agit normalement d'un antispypware et est devenu un [antivirus](#) à part entière depuis Windows 8.

Windows Defender étant devenu un antivirus à part entière... Microsoft Security Essentials a été abandonné pour ces versions de Windows (Fusion).

Si Microsoft propose des antivirus gratuits, c'est pour protéger son système d'exploitation qui n'a pas toujours bonne réputation du point de vue sécurité.

En outre, cela permet à Microsoft de suivre [les menaces informatiques](#) et de participer notamment à des opérations conjointes avec les autorités pour faire tomber des [botnets](#).

Cela permet donc à Microsoft de suivre les menaces informatiques et logiciels malveillants en offrant gratuitement un antivirus.

Le but est aussi de proposer un antivirus peu lourd et qui ne pose pas de problèmes de fonctionnement.

En effet, certains antivirus peuvent souvent poser des problèmes (plantages, ralentissement de Windows) de part le fait qu'ils se chargent très bas dans Windows.

Amélioration de la protection de Windows Defender

Microsoft continue de développer Windows Defender qui s'améliore de jours en jours pour mieux protéger les utilisateurs face aux logiciels malveillants.

Notamment sur Windows 10, la protection Windows Defender est bien meilleur.

Dans [la mise à jour Creators Update](#), Windows Defender possède une vérification de fichiers inconnus dans le Cloud.

Lorsque vous tentez d'exécuter un fichier inconnu, ce dernier est soumis aux serveurs de Microsoft et est bloqué

tant que le verdict n'a pas été donnée.

Si le verdict indique que le fichier est malveillant, une alerte est émise et le fichier est alors placé en quarantaine.

La configuration des envois des échantillons dans le Cloud Windows Defender :

Plus de détails sur les améliorations de Windows Defender, dans le cadre global de Windows 10 sur l'article suivant : [Windows 10 et la protection contre les virus et attaques informatiques](#)

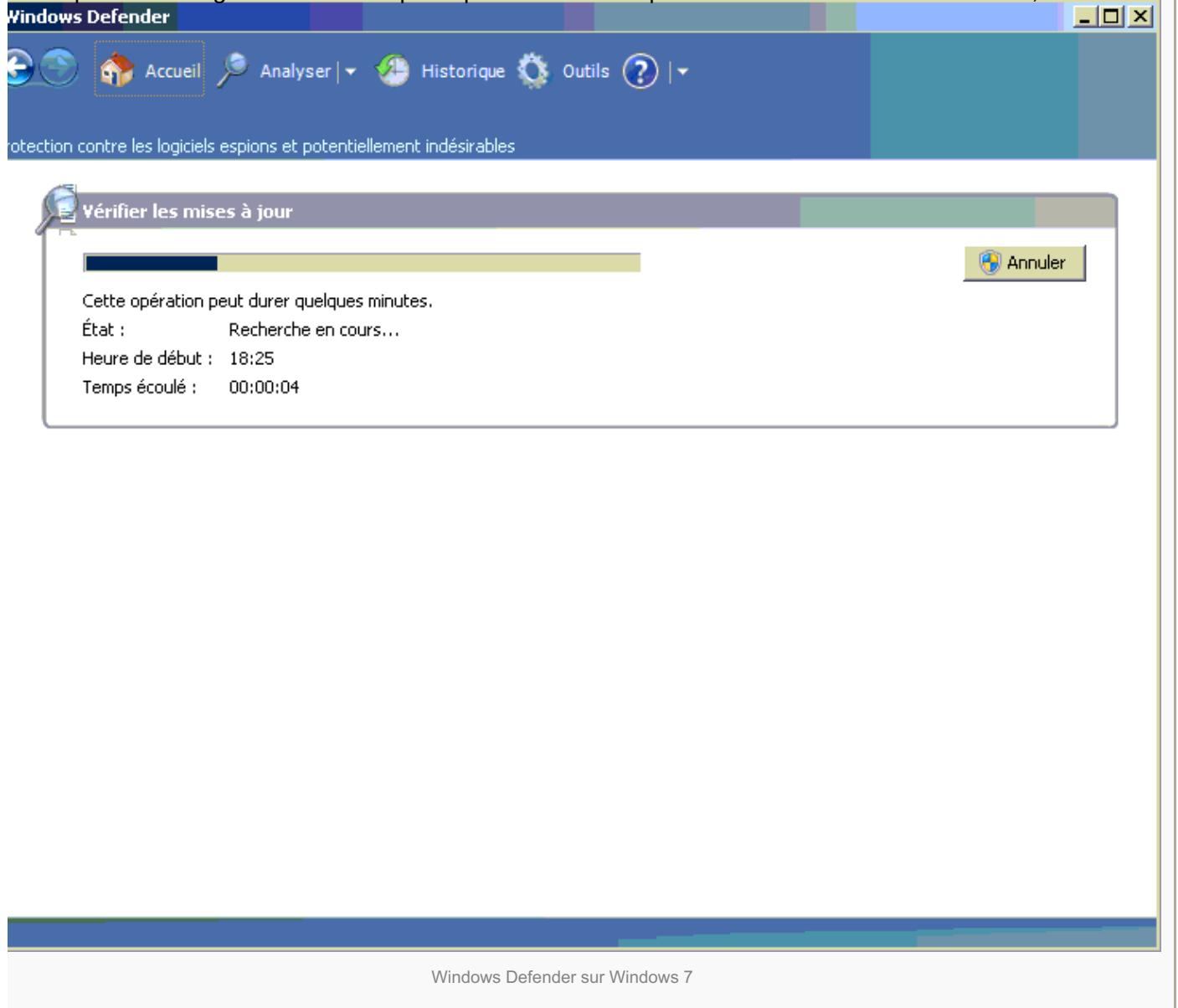
Effacité de Windows Defender ?

Quelques mots concernant l'efficacité de Windows Defender.

Un mot concernant les liens des tests antivirus.

- [av-test.org](#) effectue un test sur des samples directement sur l'antivirus et vérifie si ce dernier est détecté et le système protégé.
- [av-comparatives.org](#) effectue un test en live en tentant de charger des [Web Exploits](#) ou des liens pointant vers des binaires malicieux.

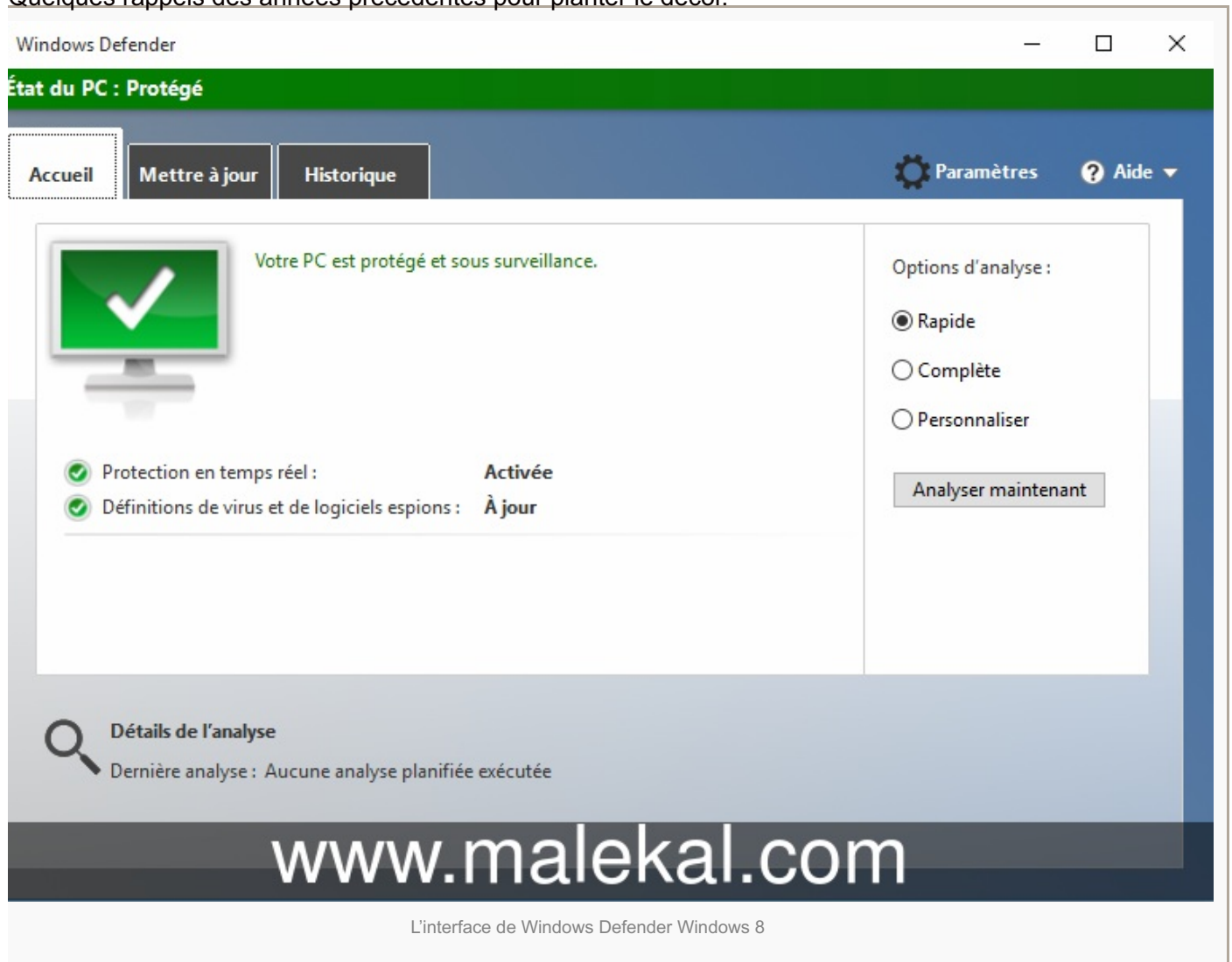
Les tests av-comparatives.org sont probablement plus parlant car tous les modules de l'antivirus sont testés, alors que av-test.org ne va détecter que la protection en temps réel : un binaire non détecté sera, on considérera



que l'antivirus ne protège pas, or si l'antivirus protège 99% des [Web Exploits](#) au final, il protégera mieux les utilisateurs.

En 2013 : Microsoft Security Essentials

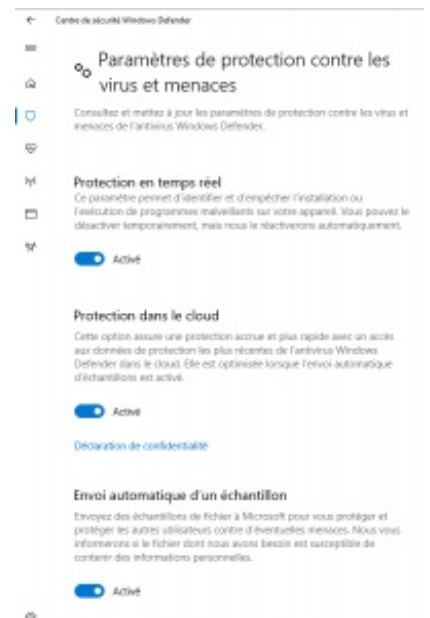
Quelques rappels des années précédentes pour planter le décor.



- 2011 : [Survol de Microsoft Security Essentials](#)
- Janvier 2013 : [Microsoft Security Essentials recalé 2 fois par AV Test](#)

À l'époque la protection de l'antivirus finissait dernier sur le test d'AV-Test : <https://www.av-test.org/fr/antivirus/particuliers-windows/windows-7/d%C3%A9cembre-2012/>





December 2012					
	Name		Protection	Repair	Usability
	Microsoft Security Essentials 4.1				
	AhnLab V3 Internet Security 8.0				
	Lavasoft Ad-Aware Pro Security 10.3 & 10.4				
	Check Point ZoneAlarm Free Antivirus + Firewall...				
	ESET Smart Security 5.2				
	Fortinet FortiClient Lite 4.3				
	GFI VIPRE Internet Security 2013				
	Norman Security Suite Pro 9.0				
	Panda Security Cloud Antivirus FREE 2.0				
	Avast Free AntiVirus 7.0				
	Avira Internet Security 2013				
	McAfee Internet Security 2013				
	PC Tools Internet Security 2012				
	AVG Anti-Virus Free Edition 2013				
	AVG Internet Security 2013				

Sur le terrain, cela se vérifiait notamment avec les Trojans RAT :

- <http://forum.malekal.com/suppression-cheval-troie-zbot-t41884.html#p328394>
- <http://www.commentcamarche.net/forum/affich-27994679-virus-indetectable-au-demarrage-windows-7#8>
- <http://www.commentcamarche.net/forum/affich-28071883-double-accent-circonflexe-et-trema#30>
- <http://www.commentcamarche.net/forum/affich-27009777-survey-enervant#6>
- <http://www.commentcamarche.net/forum/affich-29606184-uc-utilisee-a-100-virus-minerd-exe#15> (janv. 2014)

Et la version antispysware sur Windows 7 avec Av-Comparatives : [Av-Comparatives Mars 2013](#)

La ligne en pointillée correspond aux détections Microsoft, elle est au niveau du plus mauvais antivirus (Ahnlab)



Après 2013 : et Windows Defender en version antivirus

Sur Windows 8, on est à 80% de détection :

Le taux de détection de Windows Defender en Juin 2015 :

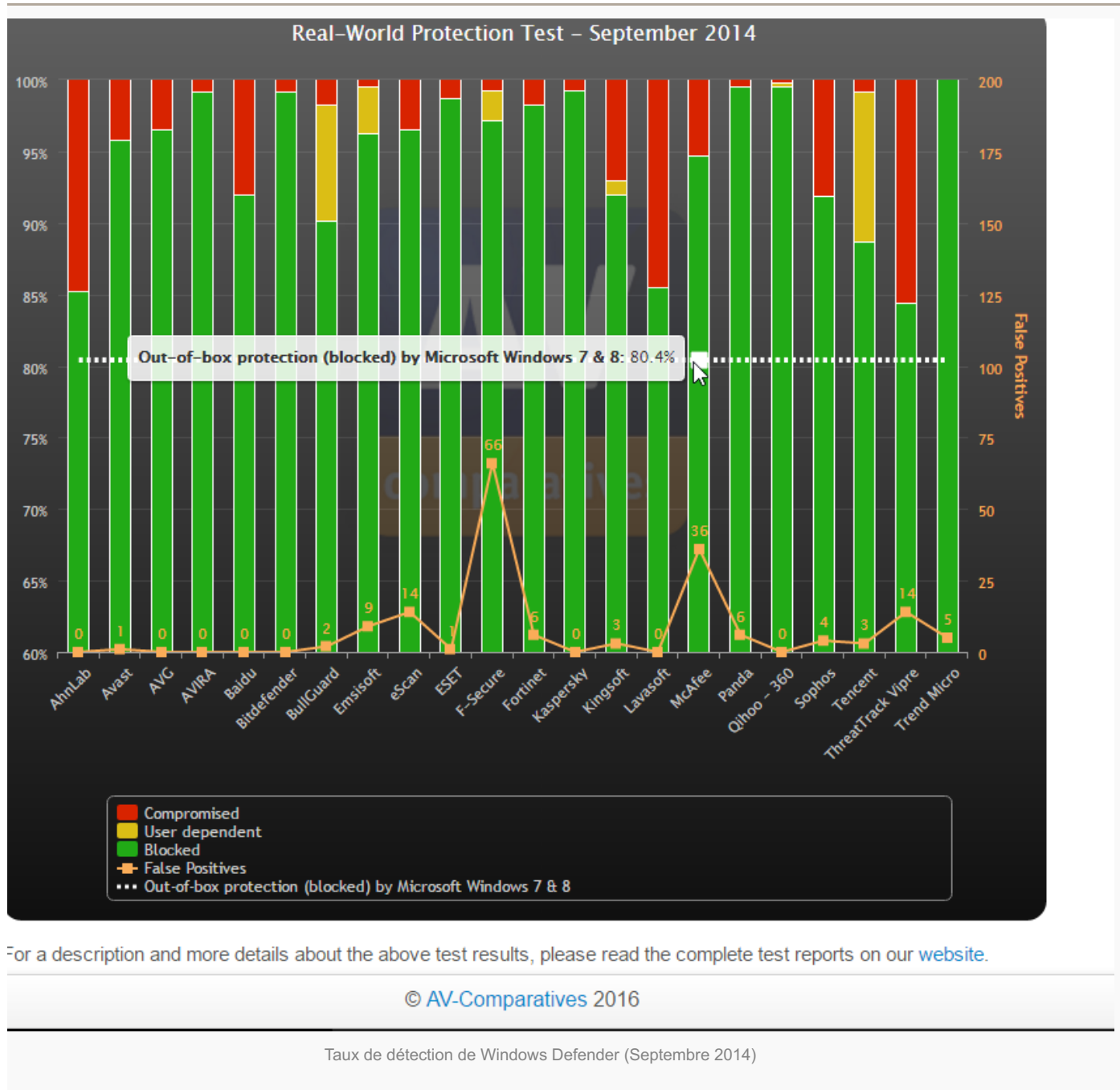
Fin 2014 : Windows Defender et Windows 10

Les tests sur Windows 10, les performances de Windows Defender montent :

Taux de détection Windows Defender sur Windows 10 (Avril 2016) :

En Décembre 2015, Windows Defender monte même à 4,5 :

Même constatation chez av-comparatives, les détections montent, en novembre 2015, Windows Defender atteint 95%



	Bitdefender Internet Security 2015					
	BullGuard Internet Security 15.0 & 15.1					
	Check Point ZoneAlarm Extreme Security 13.4					
	Comodo Internet Security Premium 8.2					
	ESET Smart Security 8.0					
	F-Secure Internet Security 2015					
	G Data InternetSecurity 2015					
	K7 Computing Total Security 14.2					
	Kaspersky Lab Internet Security 2015					
	McAfee Internet Security 2015					
	MicroWorld eScan Internet Security Suite 14.0					
	Norman Security Suite Pro 11.0					
	Norton Norton Security 2015					
	Panda Security Free Antivirus 15.1					
	Quick Heal Total Security 16.0					
	ThreatTrack VIPRE Internet Security 2015					
	Trend Micro Internet Security 2015					
	Microsoft Windows Defender 4.7					

Taux de détection de Windows Defender (Juin 2015)

AVIRAS	AVIRAS Free Internet Security 2015	AVIRAS	AVIRAS	AVIRAS	AVIRAS
	Avast Free AntiVirus 2015				
	AVG Internet Security 2015 & 2016				
	Avira Antivirus Pro 2015				
	Bitdefender Internet Security 2015 & 2016				
	BullGuard Internet Security 15.1				
	Comodo Internet Security Premium 8.2				
	ESET Smart Security 8.0 & 9.0				
	F-Secure Internet Security 2015				
	G Data InternetSecurity 2015				
	K7 Computing Total Security 15.1				
	Kaspersky Lab Internet Security 2016				
	McAfee Internet Security 2015				
	MicroWorld eScan Internet Security Suite 14.0				
	Norton Norton Security 2015				
	Panda Security Free Antivirus 16.0				
	Quick Heal Total Security 16.0				
	ThreatTrack VIPRE Internet Security 2015 & 2016				
	Trend Micro Internet Security 2016				
	Microsoft Windows Defender 4.8				

Taux de détection Windows Defender sur Windows 10 (Octobre 2015)

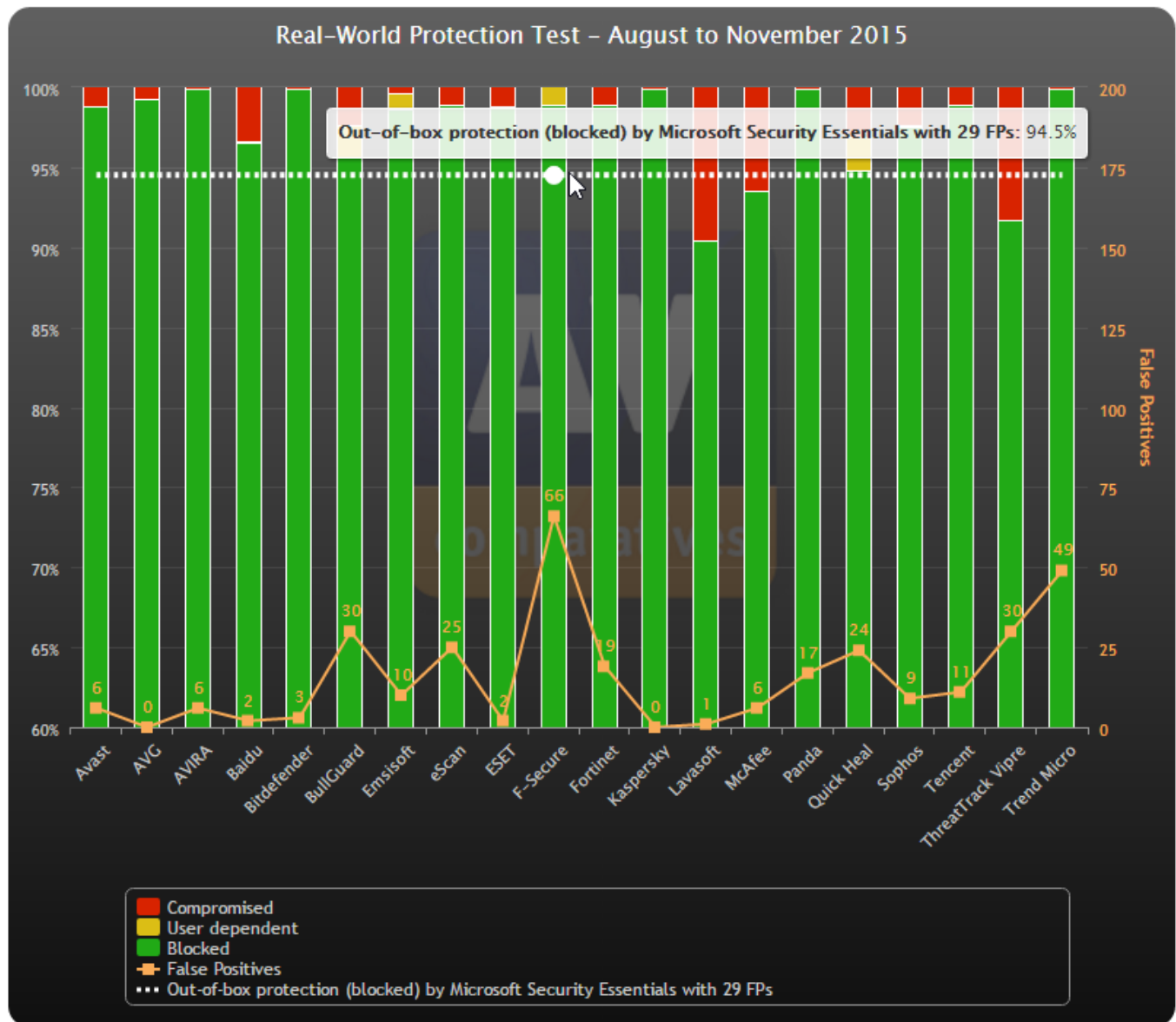
in 2015
 vrier 2015
 ctobre 2014
 vril 2014
 écembre 2013
 vrier 2013



	AhnLab V3 Internet Security 9.0		●●●●●●	●●●●●●	●●●●●● ▶
	Avast Free AntiVirus 2016		●●●●●●	●●●●●●	●●●●●● ▶
	AVG Internet Security 2016		●●●●●●	●●●●●●	●●●●●● ▶
	Avira Antivirus Pro 2015		●●●●●●	●●●●●●	●●●●●● ▶
	Bitdefender Internet Security 2016		●●●●●●	●●●●●●	●●●●●● ▶
	BullGuard Internet Security 16.0		●●●●●●	●●●●●●	●●●●●● ▶
	Comodo Internet Security Premium 8.2		●●●●●●	●●●●●●	●●●●●● ▶
	ESET Smart Security 9.0		●●●●●●	●●●●●●	●●●●●● ▶
	F-Secure Internet Security 2015		●●●●●●	●●●●●●	●●●●●● ▶
	G Data InternetSecurity 2016		●●●●●●	●●●●●●	●●●●●● ▶
	K7 Computing Total Security 15.1		●●●●●●	●●●●●●	●●●●●● ▶
	Kaspersky Lab Internet Security 2016		●●●●●●	●●●●●●	●●●●●● ▶
	McAfee Internet Security 2016		●●●●●●	●●●●●●	●●●●●● ▶
	MicroWorld eScan Internet Security Suite 14.0		●●●●●●	●●●●●●	●●●●●● ▶
	Norton Norton Security 2015		●●●●●●	●●●●●●	●●●●●● ▶
	Panda Security Free Antivirus 16.0		●●●●●●	●●●●●●	●●●●●● ▶
	Quick Heal Total Security 16.0		●●●●●●	●●●●●●	●●●●●● ▶
	ThreatTrack VIPRE Internet Security 2016		●●●●●●	●●●●●●	●●●●●● ▶
	Trend Micro Internet Security 2016		●●●●●●	●●●●●●	●●●●●● ▶
	Microsoft Windows Defender 4.8		●●●●●●	●●●●●●	●●●●●● ▶

Taux de détection Windows Defender (Décembre 2015)

	Avast Free Antivirus 2016					
	AVG Internet Security 2016					
	Avira Antivirus Pro 2016	 				
	Bitdefender Internet Security 2016	 				
	BullGuard Internet Security 16.0					
	Comodo Internet Security Premium 8.2					
	Emsisoft Anti-Malware 11.5 & 11.6					
	ESET Smart Security 9.0					
	F-Secure Safe 2016					
	G Data InternetSecurity 2016					
	K7 Computing Total Security 15.1					
	Kaspersky Lab Internet Security 2016	 				
	McAfee Internet Security 2016					
	Microsoft Windows Defender 4.8					
	MicroWorld eScan Internet Security Suite 14.0					
	Norton Norton Security 2016	 				
	Panda Security Free Antivirus 16.1					
	Qihoo 360 360 AntiVirus 5.0					
	Quick Heal Total Security 17.0					
	ThreatTrack VIPRE Internet Security 2016					



© AV-Comparatives 2016

Néanmoins Windows Defender souvent dans les 6 derniers :

et la protection sur le terrain

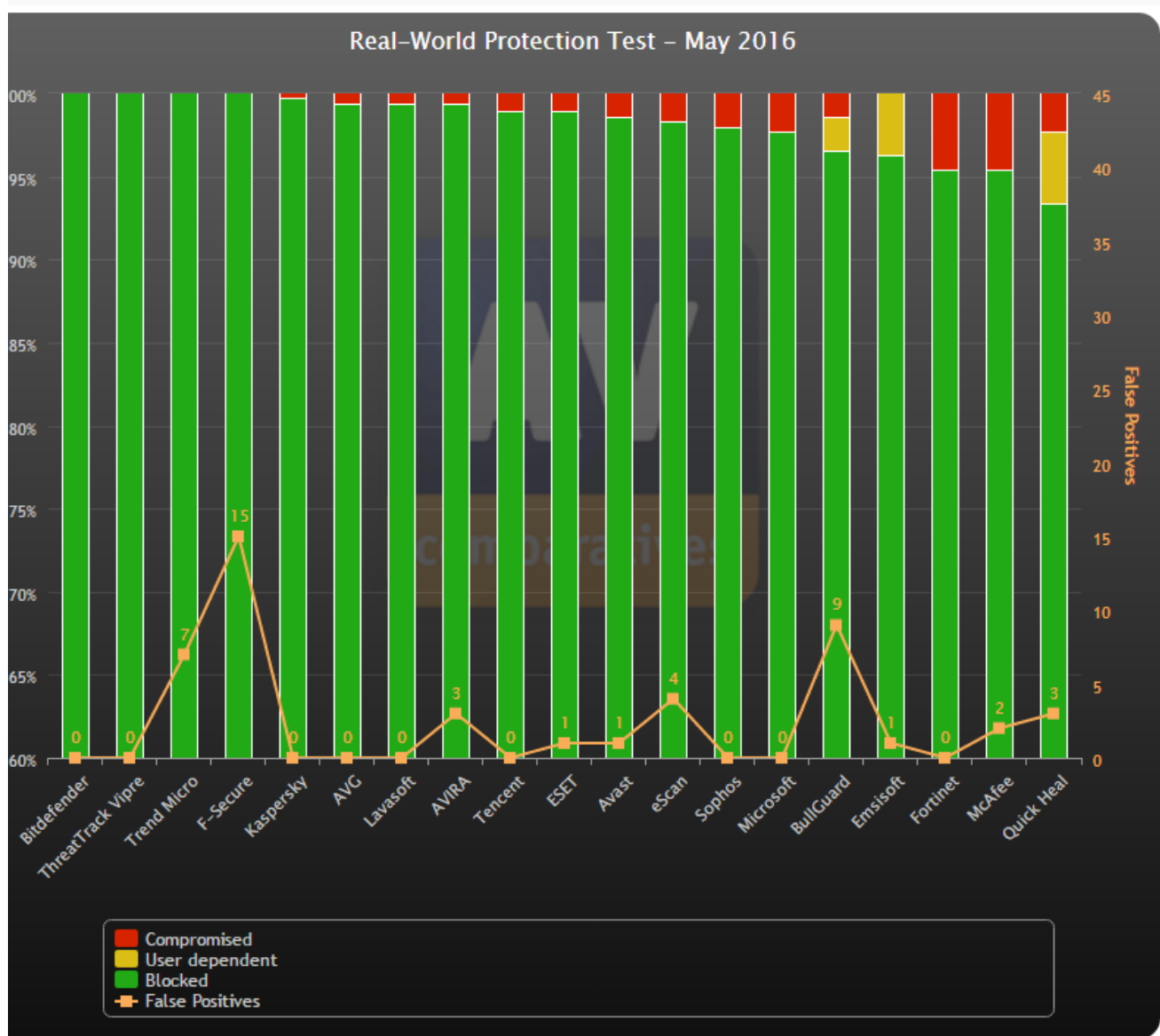
Sur le terrain, j'avais aussi fait quelques essais lors des premières vagues de [ransomwares](#), début Décembre 2015 avec les premières campagnes TeslaCrypt.

- Windows Defender qui laisse passer des droppers Locky : [Email malicieux – Ransomware Locky](#)
- [TeslaCrypt Ransomware](#) (Le test avec un MSE sur Windows 7 et non Windows Defender)

Il est n'est « pas très difficile » de trouver des Trojans non détectés par Windows Defender.



Taux de détection Windows Defender sur Windows 10 (Fev 2016)



Taux de détection Windows Defender sur Windows 10 (Mai 2016)

Windows Defender

État du PC : Potentiellement non protégé

Accueil Mettre à jour Historique Paramètres Aide

Affichez les éléments détectés comme étant potentiellement dangereux, ainsi que les actions que vous avez prises à cet effet :

☐ Éléments en quarantaine
 Éléments qui ne peuvent pas s'exécuter, mais qui ne sont pas supprimés de votre PC.

☐ Éléments autorisés
 Éléments dont l'exécution est autorisée sur votre PC.

☒ **Tous les éléments détectés**
 Éléments détectés sur votre PC.

Élément détecté	Niveau d'alerte	Date	Action entreprise
-----------------	-----------------	------	-------------------

Supprimer tout Autoriser l'élément

Process CPU Privé

Process	CPU	Privé
services.exe	0.11	
svchost.exe	0.01	
WmiPrvSE.exe	1.03	
dllhost.exe		
svchost.exe	0.09	
svchost.exe		
svchost.exe	1.01	
taskhost.exe	0.01	
taskeng.exe		
svchost.exe	0.13	
svchost.exe		
WUDFHost.exe		
TabTip.exe	0.21	
TabTip32.exe		
svchost.exe	0.01	
spoolsv.exe		
svchost.exe	0.25	
Service_KMS.exe		
MsMpEng.exe	0.11	
NisSrv.exe		
svchost.exe		
svchost.exe		
SearchIndexer.exe		
SearchFilterHost.exe		
SearchProtocolHost.exe		
svchost.exe		
msiexec.exe		
lsass.exe	0.13	
csrss.exe	0.39	
winlogon.exe		
dwm.exe	3.84	
explorer.exe	0.56	
MSASCUi.exe	0.04	
WinSCP.exe	0.05	
bla.exe		
bla64.exe	22.37	
l.exe	0.09	
inst1.exe	62.14	
zap.exe	0.04	
zap.exe	6.09	
zap.exe	0.16	

www.malekal.com

ou encore :

Windows Defender

État du PC : Potentiellement non protégé

Accueil Mettre à jour Historique Paramètres Aide

Affichez les éléments détectés comme étant potentiellement dangereux, ainsi que les actions que vous avez prises à cet effet :

☐ Éléments en quarantaine
 Éléments qui ne peuvent pas s'exécuter, mais qui ne sont pas supprimés de votre PC.

☐ Éléments autorisés
 Éléments dont l'exécution est autorisée sur votre PC.

☒ **Tous les éléments détectés**
 Éléments détectés sur votre PC.

Élément détecté	Niveau d'alerte	Date	Action entreprise
-----------------	-----------------	------	-------------------

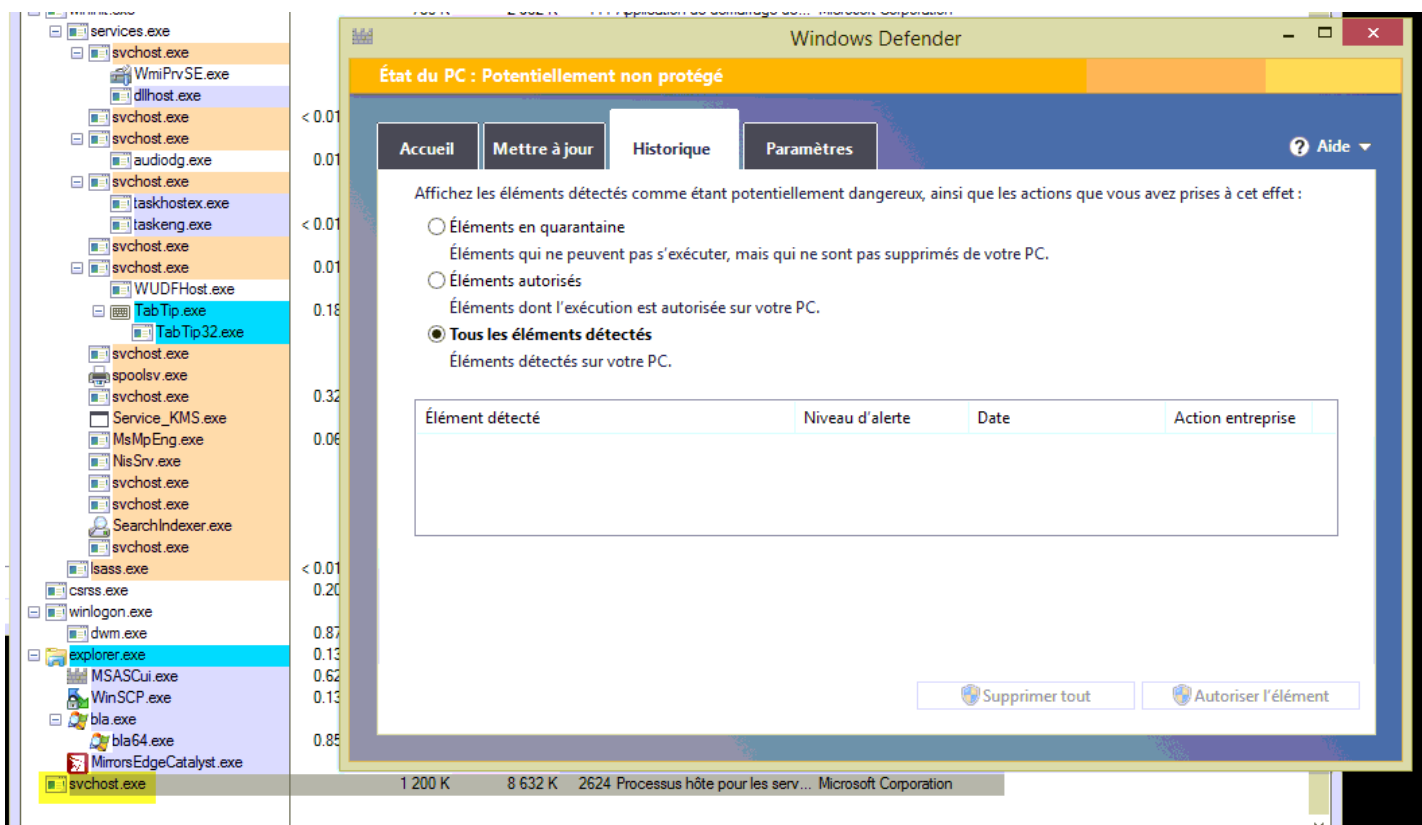
Supprimer tout Autoriser l'élément

Process CPU Privé

Process	CPU	Privé
smss.exe		
csrss.exe		
wininit.exe		
services.exe		
svchost.exe		
WmiPrvSE.exe		
dllhost.exe		
svchost.exe		
svchost.exe		
svchost.exe	0.01	
audiodg.exe		
svchost.exe	< 0.01	
taskhost.exe	0.01	
svchost.exe		
svchost.exe		
WUDFHost.exe		
TabTip.exe	0.14	
TabTip32.exe		
svchost.exe		
spoolsv.exe		
svchost.exe	0.27	
Service_KMS.exe		
MsMpEng.exe	0.07	
NisSrv.exe		
svchost.exe		
svchost.exe		
SearchIndexer.exe		
svchost.exe		
lsass.exe		
csrss.exe	0.17	
winlogon.exe		
dwm.exe	0.86	
explorer.exe	0.23	
MSASCUi.exe	0.08	
WinSCP.exe	0.26	
bla.exe		
bla64.exe	4.60	
MirrorsEdgeCatalyst.exe		
cmd.exe		
conhost.exe		
rad05451.tmp		

CPU Usage: 7.47% Commit Charge: 34.75% Processes: 42 Physical Usage: 41.10%

et hop [svchost.exe](#) injecté :



Le lendemain après mise à jour de Windows Defender, ce dernier détecte [Trojan:Win32/Dynamer](#) pour le [Trojan RAT](#) (MirrorsEdgeCatalyst) et Backdoor:Win32/Vawtrak, il s'agit d'un [Trojan Banker](#), cependant, il semble malgré la détection, il semble toujours actif puisque le svchost.exe est encore présent.

Et du côté du [ransomware Locky](#)...

Windows Defender laisse souvent passer des dropers Locky...

Windows Defender

État du PC : Risque

Accueil Mettre à jour Historique Paramètres Aide

Affichez les éléments détectés comme étant potentiellement dangereux, ainsi que les actions que vous avez prises à cet effet :

- ☐ Éléments en quarantaine
Éléments qui ne peuvent pas s'exécuter, mais qui ne sont pas supprimés de votre PC.
- ☐ Éléments autorisés
Éléments dont l'exécution est autorisée sur votre PC.
- ☒ **Tous les éléments détectés**
Éléments détectés sur votre PC.

Élément détecté	Niveau d'alerte	Date	Action entreprise
☐ Backdoor:Win32/Vawtrak.E	Grave	08/07/2016 11:37	En quarantaine
☐ Trojan:Win32/Dynamer!ac	Grave	08/07/2016 11:36	En quarantaine
☐ Trojan:Win32/Dynamer!ac	Grave	08/07/2016 11:19	En quarantaine

file:C:\Users\Vincent\AppData\Roaming\UutePsuq\UicEhda.exe
 regkey:HKCU@S-1-5-21-270738741-1668383648-2888775521-1001\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION
 \RUN\\VoceTgop
 runkey:HKCU@S-1-5-21-270738741-1668383648-2888775521-1001\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION
 \RUN\\VoceTgop

Supprimer tout Autoriser l'élément

Process	Private Bytes	Working Set	Private Bytes	Working Set	Process Name	Company Name
0.74	2 288 K	7 580 K	3356	3356	Sysinternals Process Explorer	Sysinternals - www.sysinter...
0.74	13 132 K	29 336 K	3896	3896	Sysinternals Process Explorer	Sysinternals - www.sysinter...
0.40	5 592 K	19 904 K	2456	2456	Windows Defender User Inte...	Microsoft Corporation
	1 244 K	3 748 K	2820	2820	Processus hôte pour les serv...	Microsoft Corporation

Backdoor Vawtrak et Trojan_Dynamer détecté par Windows Defender

Windows Defender

État du PC : Potentiellement non protégé

Accueil Mettre à jour Historique Paramètres Aide

Affichez les éléments détectés comme étant potentiellement dangereux, ainsi que les actions que vous avez prises à cet effet :

- ☐ Éléments en quarantaine
Éléments qui ne peuvent pas s'exécuter, mais qui ne sont pas supprimés de votre PC.
- ☐ Éléments autorisés
Éléments dont l'exécution est autorisée sur votre PC.
- ☒ **Tous les éléments détectés**
Éléments détectés sur votre PC.

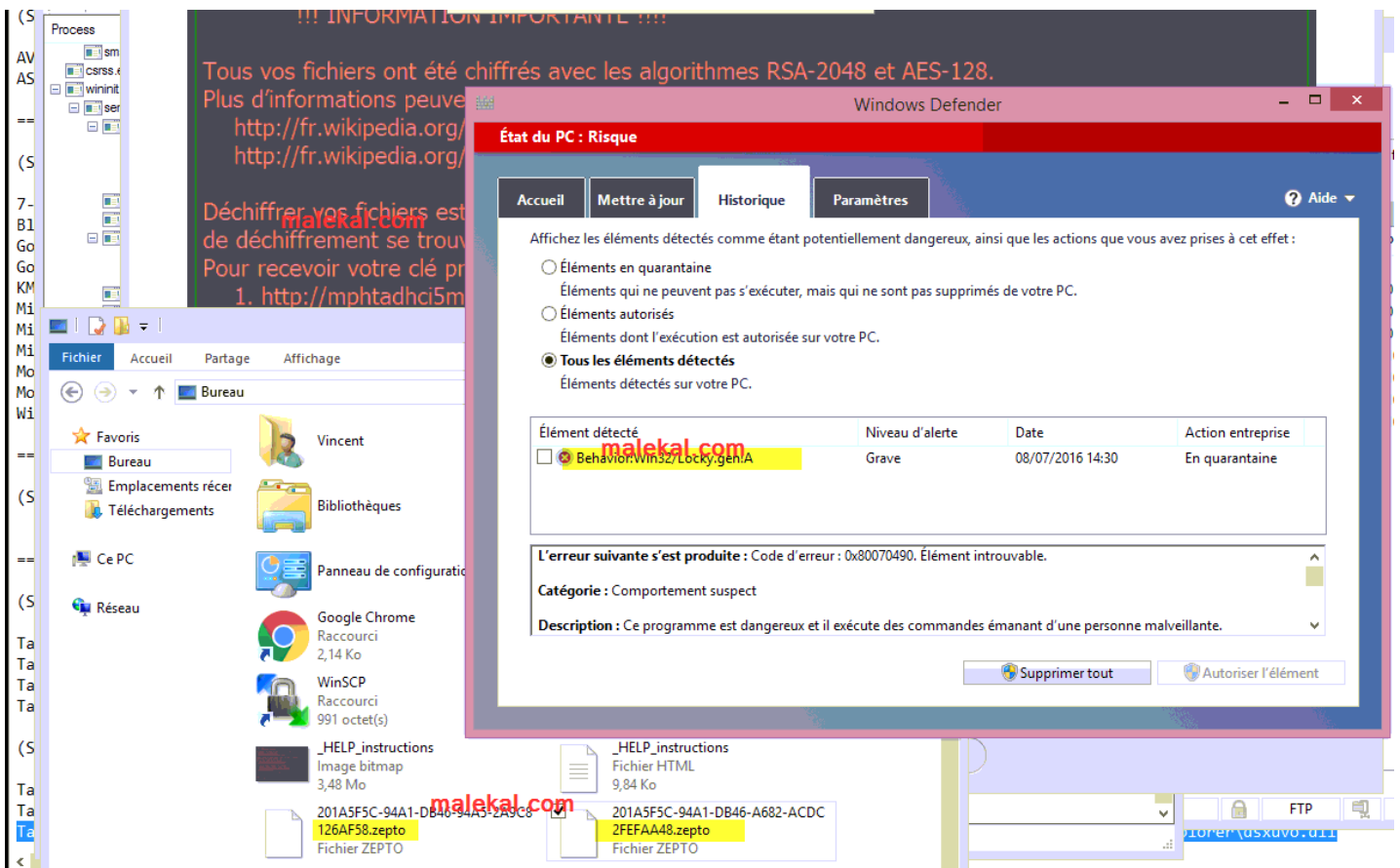
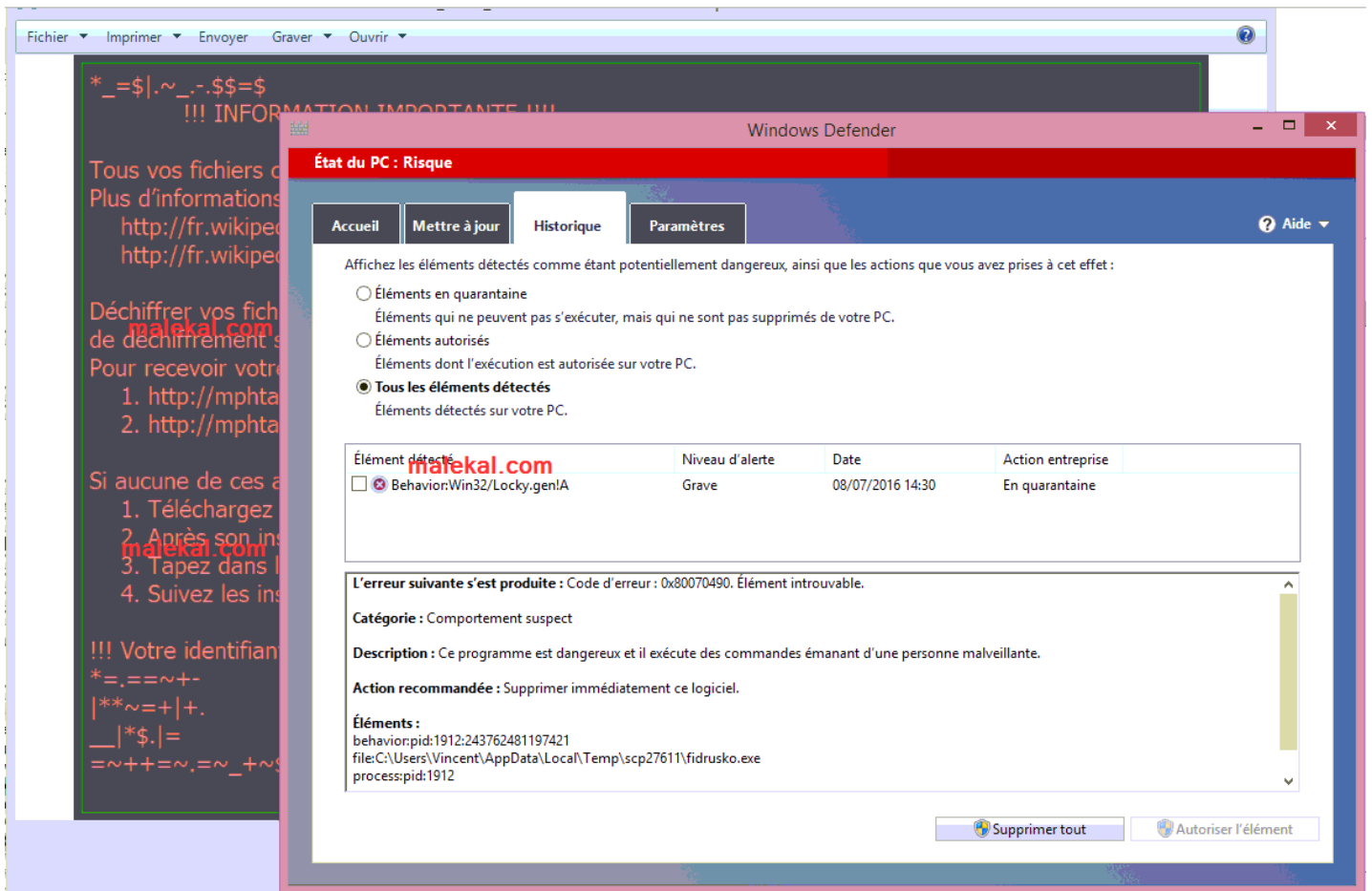
Élément détecté	Niveau d'alerte	Date	Action entreprise
-----------------	-----------------	------	-------------------

Supprimer tout Autoriser l'élément

CPU Usage: 6.53% Commit Charge: 35.24% Processes: 45 Physical Usage: 19.3%

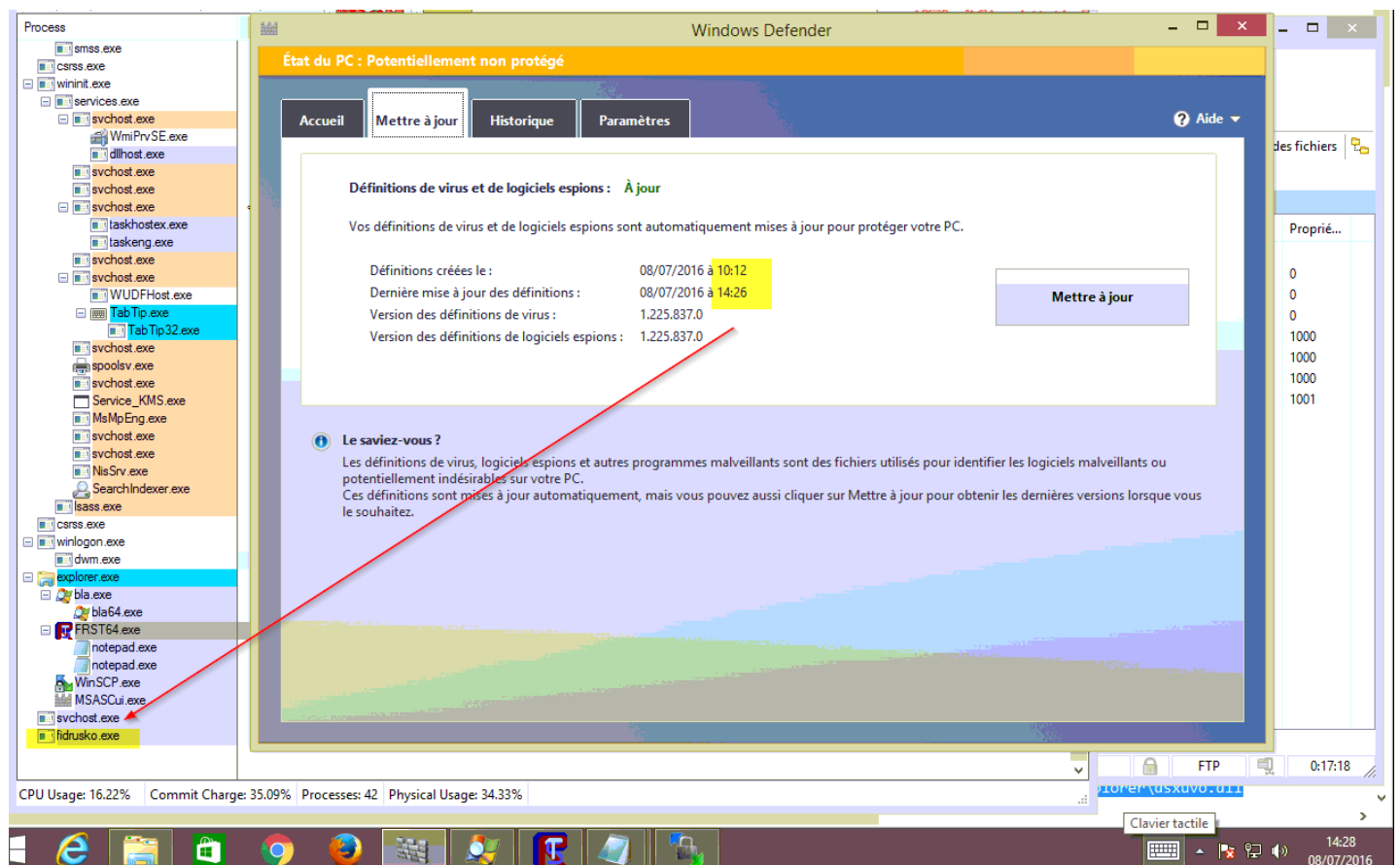
www.malekal.com

Windows Defender émet tout de même une alerte, seulement celle-ci arrive après que les fichiers aient été chiffrés, on peut voir l'extension .zepto

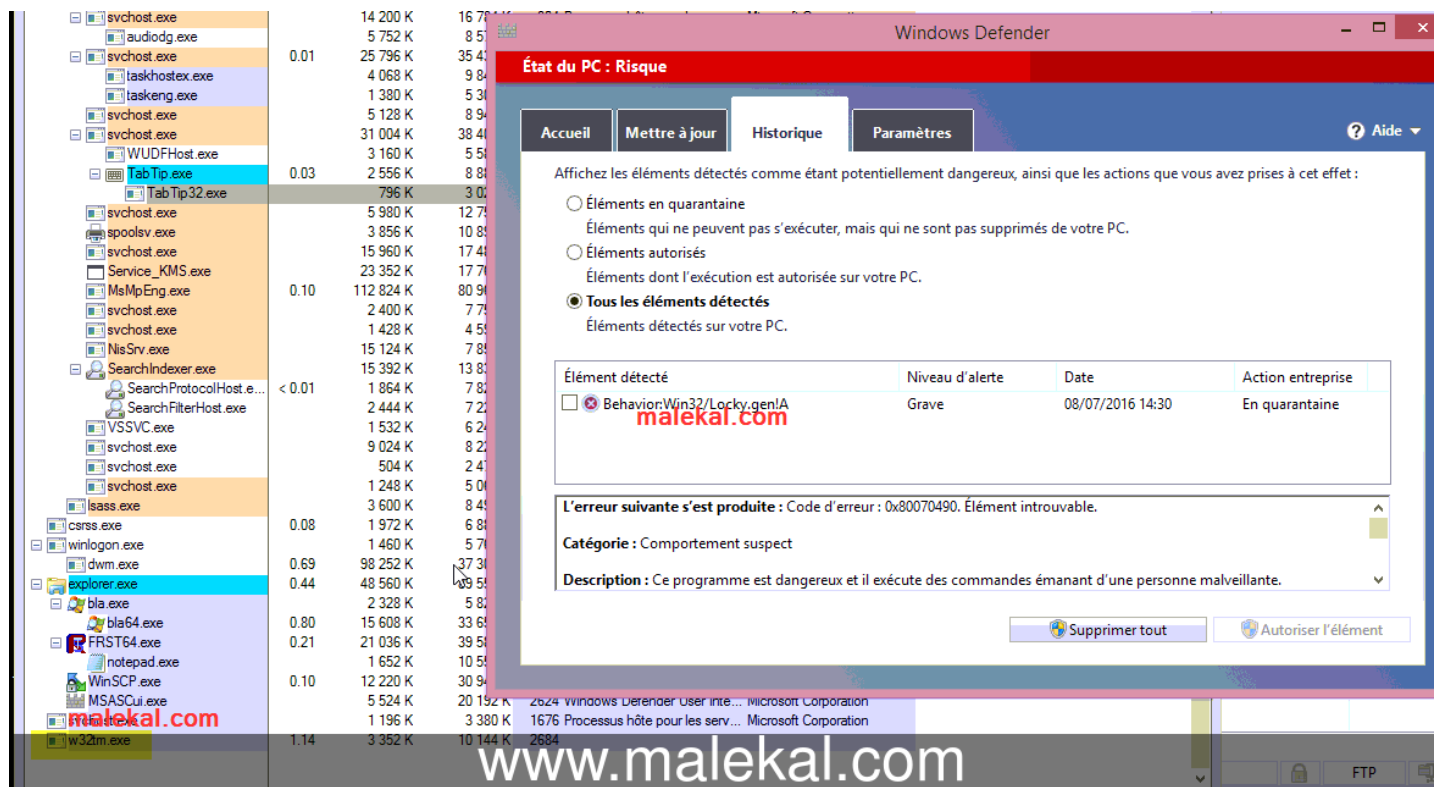


Le gros problème provient du fait que les mises à jour des définitions virales sont trop rares... Plusieurs heures sans et de ce fait, si vous ouvrez le malware entre le laps de temps où la mise à jour n'a pas été faite, vous êtes

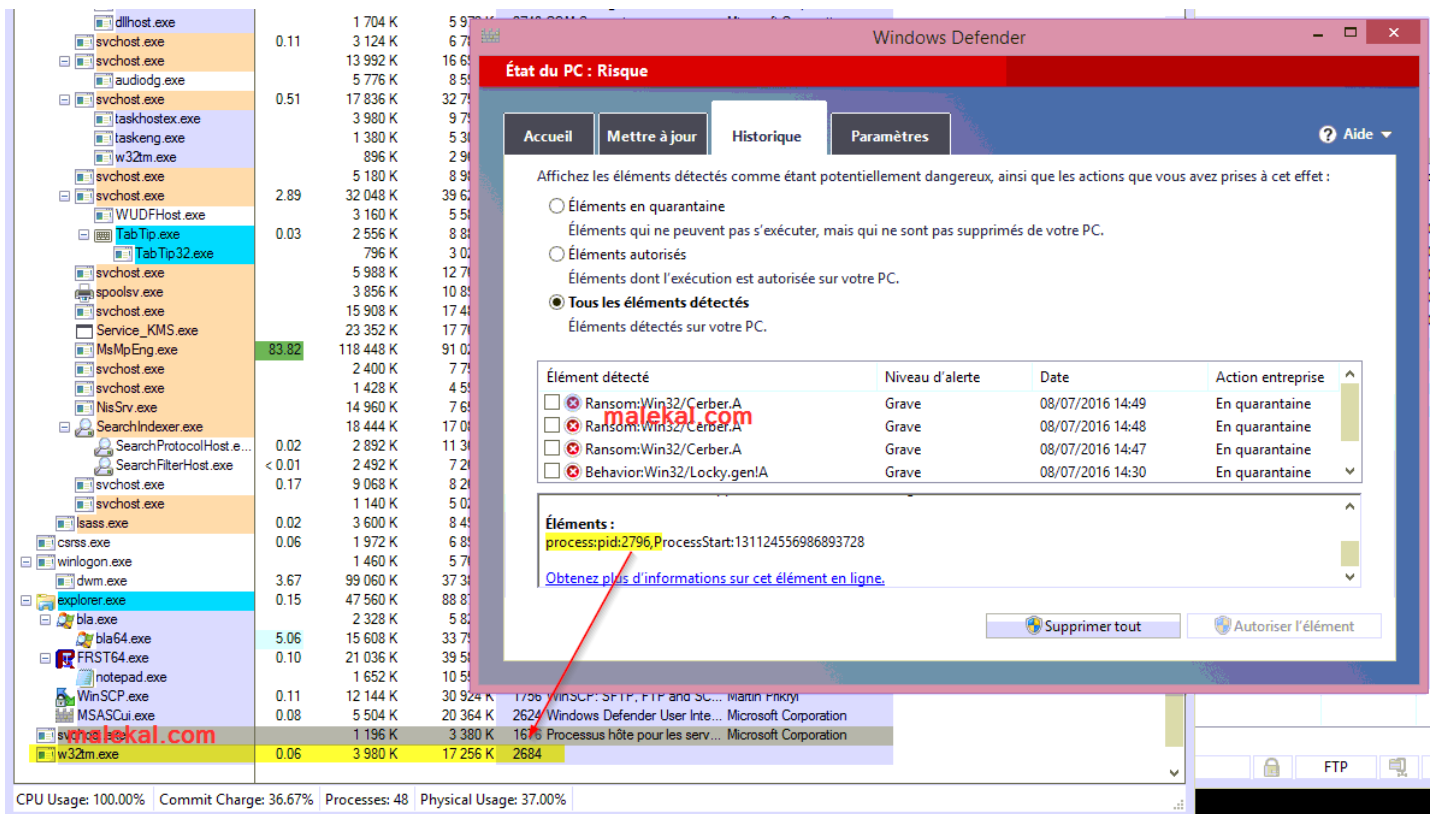
vulnérables.. d'où les intérêts des solutions **Cloud Antivirus** .



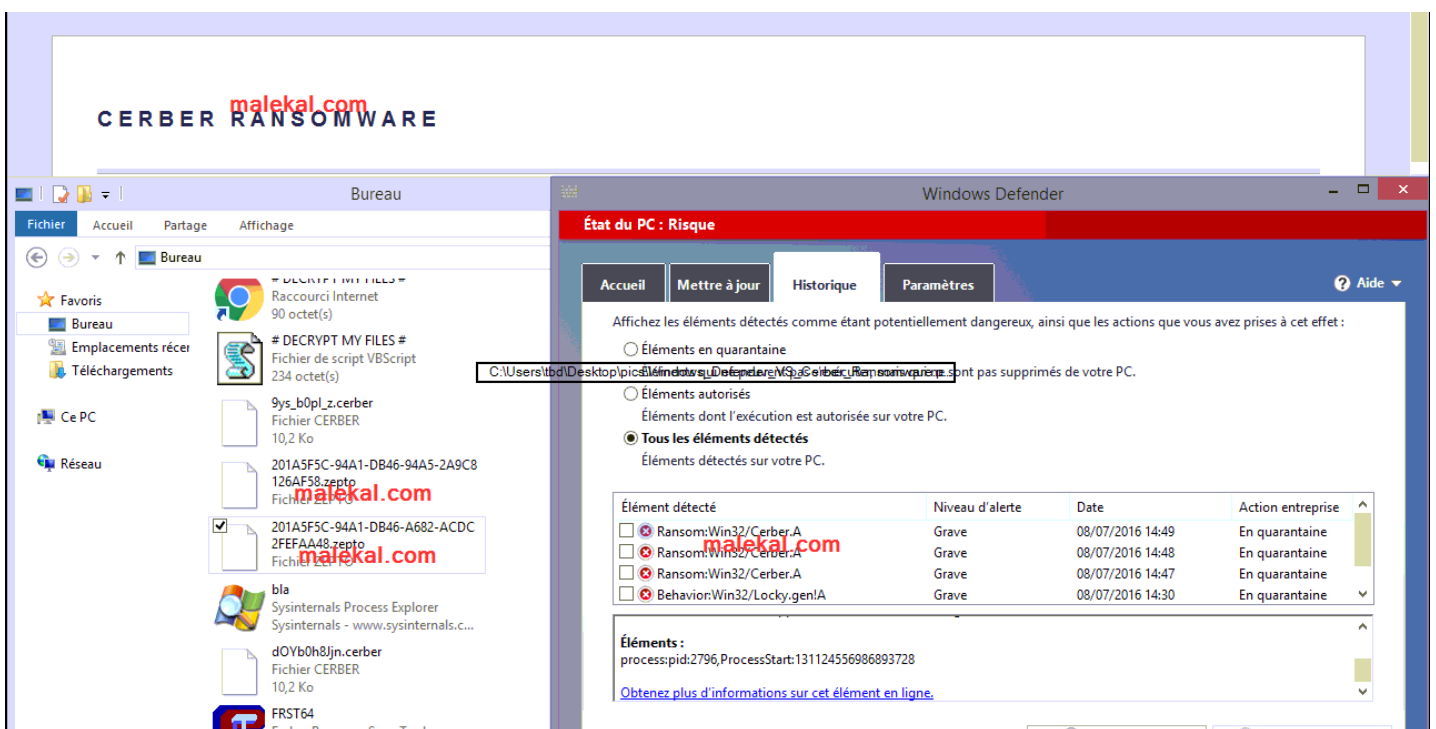
Et **Ransomware Cerber**.. il se passe exactement la même chose que Locky...



et Windows Defender émet une alerte Ransom:Win32/Cerber.A car il détecte le chiffrement des documents...



mais c'est trop tard.... les fichiers sont chiffrés on voit des documents en .cerber et les fichiers instructions sont installés et ouverts...



Bonus – une vidéo du 28/11/2016 où Windows Defender laisse passer Locky :

Je tiens à préciser qu'Avast! détecte tout ce beau monde, je pense que les autres antivirus gratuits aussi. Ci-dessous le dropper Locky détecté en FileRepMalware et derrière les détections des autres dropers (4/4)

Conclusion et avis sur Windows Defender

Microsoft depuis la sortie de Windows 10 a fait d'énormes progrès de détection avec Windows Defender mais il faut dire qu'il partait de loin. Néanmoins il reste beaucoup moins efficaces que ses autres homologues gratuits.

Il faut savoir aussi que pendant ce temps là, les antivirus gratuits continuent de s'améliorer, notamment [Avast!](#) continue de développer son Cloud (voir [Cloud Antivirus](#)) et sa version [Avast! Nitro](#).

D'un autre côté, il faut aussi prendre en compte que [les antivirus gratuits](#) sont de plus en plus pénibles du côté marketing en proposant et parfois même en installant des logiciels additifs. De ce côté là, nous vous invitons à lire la page : [Antivirus gratuits : désinstaller les composants inutiles](#).

Microsoft à travers Windows Defender n'a pas du tout cette politique et vous ne serez pas harcelé de popups et autres.

Faut-il délaissier Windows Defender ?

Tout dépend de votre activité sur internet, comme cela est expliqué sur la page : [La sécurité de son PC, c'est quoi ?](#)

[Vos chances d'infections dépendent de votre activité sur la toile et si vous avez suivi d'autres éléments de sécurité \(hors antivirus\)](#).

En d'autre terme, un utilisateur avertit avec Windows Defender qui lit juste ses emails et les sites actualités, a probablement moins de chance de se faire infecter qu'un utilisateur qui va sur des sites de streaming illégaux, pornographiques ou torrent avec des plugins non à jour et [Avast!](#) installé.

Tous les tutoriels pour sécuriser Windows :

Et pour sécuriser Windows : [Quelles protections pour Windows 10 ?](#)

Nous vous recommandons de sécuriser votre ordinateur en suivant le guide : [Sécuriser son Windows \(version courte\)](#) et [Virus : Surveiller Windows](#)

ou encore comment protéger Windows 10 des virus, lire le tuto [Quelles protections pour Windows 10 contre les virus ?](#) et en vidéo :

