



G Data

# Document de présentation technique

## Blocage du comportement

Marco Lauerwald  
Marketing

Go safe. Go safer. **G Data.**



## Table des matières

<b>1</b>	<b>Blocage du comportement – mission : lutter contre les menaces inconnues.....</b>	<b>2</b>
<b>1.1</b>	<b>Programmes malveillants inconnus : l’industrie des logiciels malveillants en plein boom</b>	<b>2</b>
<b>1.2</b>	<b>Niveaux de sécurité d’un ordinateur équipé d’une solution antivirus.....</b>	<b>3</b>
<b>1.2.1</b>	<b>Niveaux de sécurité (Security Layer) lors de la navigation sur Internet.....</b>	<b>3</b>
<b>1.2.2</b>	<b>Niveaux de sécurité (Security Layer) lors de l’utilisation de la messagerie électronique ..</b>	<b>4</b>
<b>1.3</b>	<b>Mode de fonctionnement de l’outil de blocage du comportement.....</b>	<b>4</b>
<b>1.4</b>	<b>Processus de vérification des comportements douteux.....</b>	<b>5</b>
<b>1.5</b>	<b>Exemple : outil de blocage du comportement G Data .....</b>	<b>5</b>

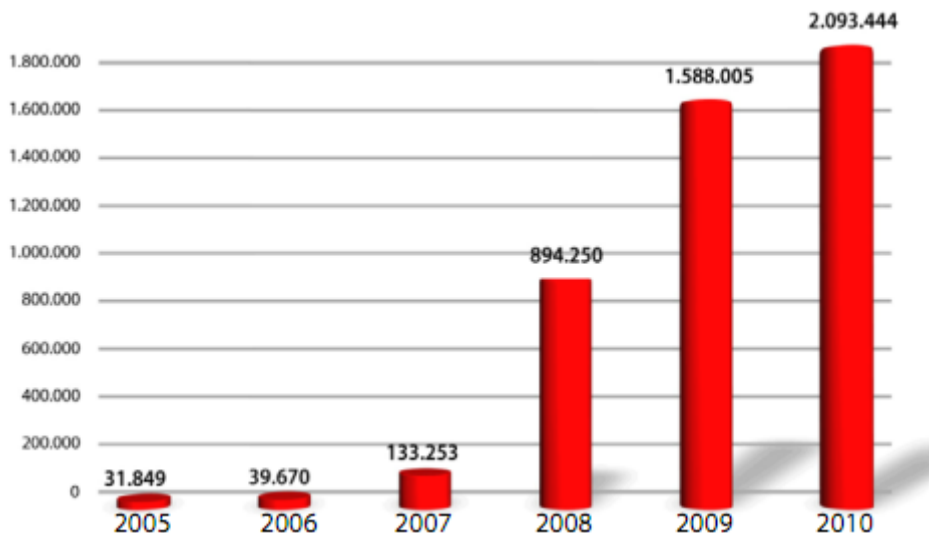
# 1 Blocage du comportement – mission : lutter contre les menaces inconnues

Attention, menace inconnue ! Lorsqu'un ordinateur PC affiche ce message, l'utilisateur peut être sûr que la solution de sécurité a évité le pire : le vol de données privées et de mots de passe ou l'envoi de pollupostage par le biais du compte électronique de l'utilisateur. Nombreux sont les utilisateurs qui pensent que leur logiciel antivirus les protège des logiciels malveillants. Une protection n'est toutefois complète que si elle permet également d'éviter les attaques de type jour J (ou les attaques de logiciels malveillants inconnus). L'outil de blocage du comportement s'attaque précisément au problème : il reconnaît les menaces inconnues pour lesquelles il n'existe pas encore de signatures antivirus en fonction de leur comportement douteux et les supprime.

Ce document de présentation technique décrit le mode de fonctionnement de cette technologie et les avantages qu'elle présente pour l'utilisateur.

## 1.1 Programmes malveillants inconnus : l'industrie des logiciels malveillants en plein boom

Au cours du deuxième semestre 2010, le nombre de nouveaux programmes malveillants informatiques<sup>1</sup> est passé à 1 076 236. Ce qui correspond à une moyenne quotidienne de 5 840 programmes. Au total, en 2010, plus de deux millions de nouvelles variantes de programmes nuisibles ont fait leur apparition (conformément au schéma 1), soit 32 % de plus qu'en 2009 et quasiment 52 fois plus qu'en 2006. Rien qu'au premier semestre 2008, le nombre de nouveaux programmes malveillants est supérieur à celui de l'année 2008.



**Schéma 1** : nombre de nouveaux programmes malveillants par an depuis 2005

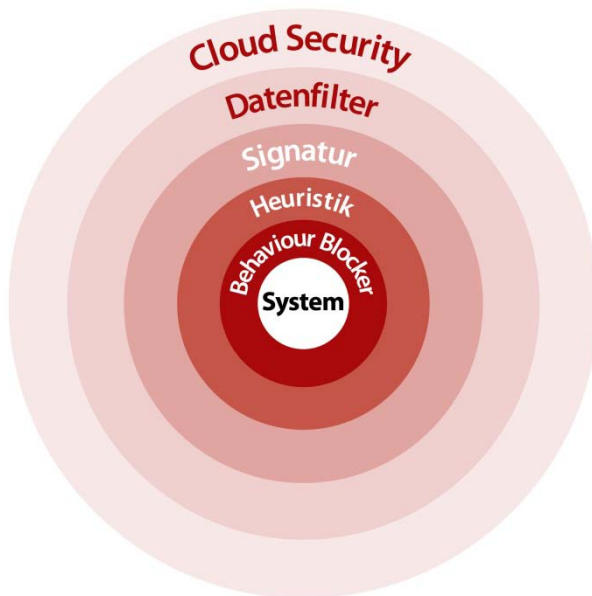
L'industrie des logiciels malveillants est en plein boom et il faut encore et toujours lutter contre des menaces inconnues. L'outil de blocage du comportement fait office de dernier mécanisme de

<sup>1</sup> Selon le compte-rendu des logiciels malveillants G Data 02/2010

protection de la solution de sécurité lors de la navigation sur Internet et de l'utilisation de la messagerie électronique.

## 1.2 Niveaux de sécurité d'un ordinateur équipé d'une solution antivirus

L'ordinateur équipé d'une solution antivirus est protégé de manière optimale par différents niveaux de sécurité (Security Layer). Ces mécanismes sont décrits et expliqués plus en détail dans les sections qui suivent, concernant la navigation sur Internet et l'utilisation de la messagerie électronique :



**Illustration 1 :** vue d'ensemble des niveaux de sécurité d'un ordinateur équipé d'un logiciel antivirus

### 1.2.1 Niveaux de sécurité (Security Layer) lors de la navigation sur Internet

Des logiciels nuisibles infectent de nombreux utilisateurs lors de la simple navigation sur Internet. Un logiciel de sécurité permet, à l'aide des différents niveaux de sécurité, d'éviter les infections. L'outil de blocage du comportement permet, quant à lui, de protéger des programmes malveillants inconnus :

Niveau	Méthode	Effet
Nuage Web	compare les adresses URL à la liste noire des adresses URL de programmes	bloque les sites Web infectés/frauduleux connus

	malveillants connus	
Filtre HTTP	analyse le trafic HTTP lors des téléchargements	bloque les logiciels malveillants connus
Outil de surveillance antivirus (signatures)	détecte les signatures antivirus connues à l'ouverture des fichiers	bloque les logiciels malveillants connus
Outil de surveillance antivirus (heuristique)	détecte les signatures génériques à l'ouverture des fichiers	bloque les variantes inconnues de logiciels malveillants
<b>Outil de blocage du comportement</b>	analyse le modèle de comportement en fonction de propriétés typiques des virus	bloque les logiciels malveillants inconnus

## 1.2.2 Niveaux de sécurité (Security Layer) lors de l'utilisation de la messagerie électronique

Des menaces inconnues peuvent apparaître lors de l'envoi et de la réception de courriers électroniques.

Niveau	Méthode	Effet
Nuage de messagerie	compare les empreintes des courriers au trafic de messagerie mondial	bloque les courriers infectés et le pollupostage
Filtre de messagerie	analyse les courriers électroniques à la réception	bloque les logiciels malveillants connus
Outil de surveillance antivirus (signatures)	détecte les signatures antivirus connues à l'ouverture des fichiers	bloque les logiciels malveillants connus
Outil de surveillance antivirus (heuristique)	détecte les signatures génériques à l'ouverture des fichiers	bloque les variantes inconnues de logiciels malveillants
<b>Outil de blocage du comportement</b>	analyse le modèle de comportement en fonction de propriétés typiques des virus	bloque les logiciels malveillants inconnus

## 1.3 Mode de fonctionnement de l'outil de blocage du comportement

L'outil de blocage du comportement est un mécanisme de protection qui observe et, le cas échéant, bloque le comportement des programmes exécutés. Les programmes, les téléchargements et autres fichiers tentent d'exécuter différentes actions sur l'ordinateur au démarrage. Pour les programmes classés dans la catégorie des menaces, ce sont surtout les interactions et le type d'actions exécutées qui jouent un rôle.

Un logiciel peut notamment être considéré comme une menace potentielle par la solution de sécurité de l'ordinateur en raison des comportements suivants<sup>2</sup> :

- Entrées de démarrage automatique de quelque type que ce soit, par ajout des fichiers au dossier correct ou manipulation des valeurs du registre
- Fichiers .exe ou .dll qui se copient automatiquement dans le répertoire system32
- Entrées qui manipulent les valeurs du registre en rapport avec la sécurité du système
- Comportements qui modifient les paramètres de l'application Internet Explorer
- Modifications des fichiers hôtes
- Code Injection – exécution d'un code de programme dans le contexte d'un autre programme (pour contourner le pare-feu, le code est par exemple exécuté dans le contexte de l'application Internet Explorer)
- Programme compressé par ExePacker (pour contourner les filtres de signatures)
- Fichiers de programmes endommagés (mais pouvant quand même être exécutés)

## 1.4 Processus de vérification des comportements douteux

L'outil de blocage du comportement G Data repose sur un système d'experts, basé sur des règles. Des règles de comportement sont ainsi créées et modifiées manuellement, ce qui permet d'optimiser les taux de détection et de faux positifs. Lors de l'exécution d'un programme, une action générale est extraite du comportement. Les règles sont ensuite appliquées à la totalité des actions, afin d'obtenir d'autres propriétés et une valeur en matière de risques. Dans le cadre du processus, nous étudions soigneusement certaines associations récurrentes.

## 1.5 Exemple : outil de blocage du comportement G Data

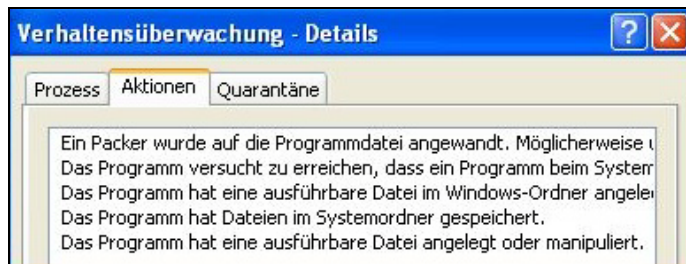
Si un programme inclut un logiciel malveillant et présente plusieurs des comportements susmentionnés, il est considéré par l'outil de blocage du comportement G Data comme une menace inconnue et il est bloqué :



**Capture d'écran 1** : en cas d'exécution d'une action douteuse, la surveillance du comportement G Data est activée.

<sup>2</sup> Exemples d'illustration

L'utilisateur doit alors décider de la manière de répondre à la menace. Il est généralement conseillé de placer le programme nuisible en quarantaine. Il arrive cependant parfois que des programmes inoffensifs soient considérés comme dangereux. Nous vous recommandons donc de consulter les détails et de déterminer les raisons pour lesquelles le programme a été bloqué :



**Capture d'écran 2 :** vue détaillée de la surveillance du comportement

Il est généralement utile de ne pas installer les programmes à l'aveugle. Les utilisateurs doivent s'interroger sur l'utilité, ainsi que sur l'origine du programme.

L'outil de blocage du comportement fait office de protection contre les menaces inconnues, il ne peut cependant pas remplacer les autres composants de la solution antivirus. Il est très important d'identifier les logiciels malveillants avant de devoir activer l'outil de blocage du comportement.