TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

DeepRay®

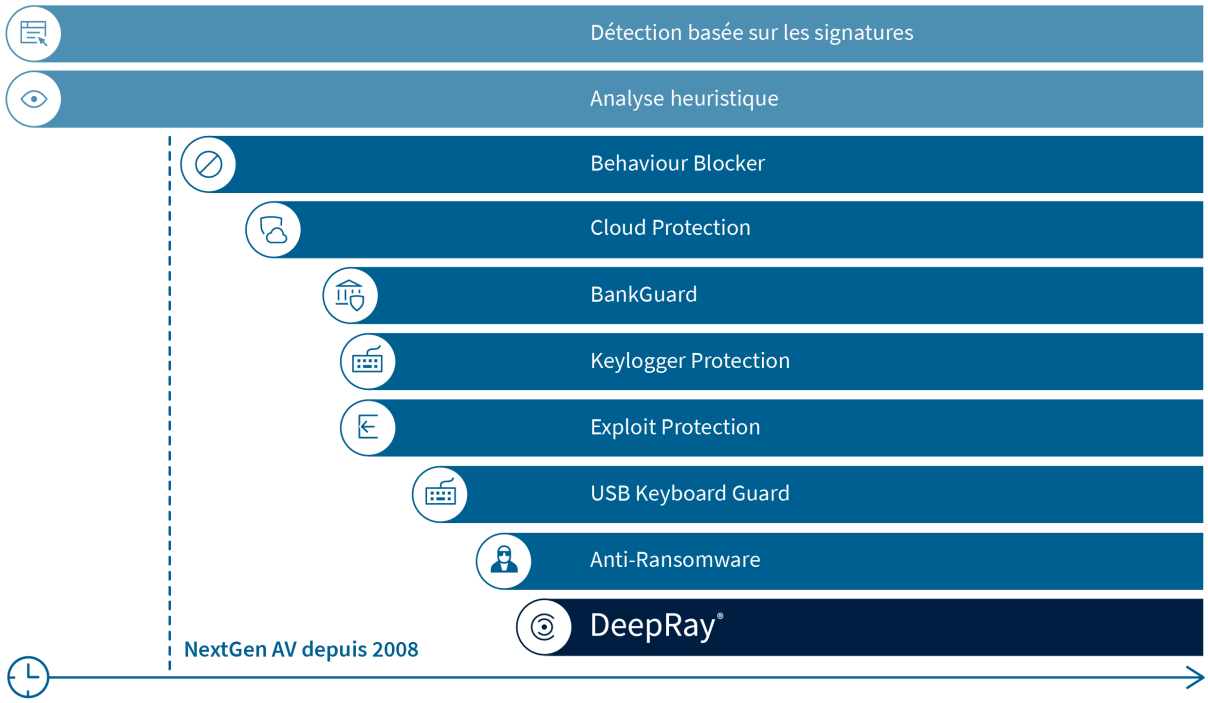
G DATA Software AG

Contents

Intelligence artificielle et apprentissage machine dans les solutions de sécurité informatique

Les cybercriminels et les fournisseurs de solutions de sécurité informatique font la course depuis des années. Les attaques menées à l'aide de méthodes connues se combattent plus facilement et plus rapidement que celles déployant de nouveaux logiciels malveillants. C'est pourquoi les pirates ne cessent de chercher de nouvelles tactiques afin de passer outre les barrages érigés par les solutions de sécurité. Les techniques classiques, telles que la détection par signature, ne peuvent agir que de manière réactive.

Depuis 2008, nos solutions proposent des techniques innovantes, capables de bloquer les menaces inconnues. Avec DeepRay®, l'intelligence artificielle combinée au réseau neuronal d'apprentissage machine permet d'être encore plus performant face au niveau élevé de menace. Les utilisateurs sont protégés contre les méthodes sophistiquées mises au point par les pirates.



Comment un logiciel malveillant se répand-il sur les terminaux ?

Les auteurs de logiciels malveillants agissent selon une logique économique classique. Créer des malwares prend du temps et consomme des ressources, et cet investissement doit générer un bénéfice. Pour être rentable, il est important que le logiciel malveillant infecte le plus grand nombre de terminaux possible. Une fois qu'un malware est identifié, il est détecté par les logiciels antivirus et ne peut plus provoquer de dégât. Il n'est donc plus rentable.

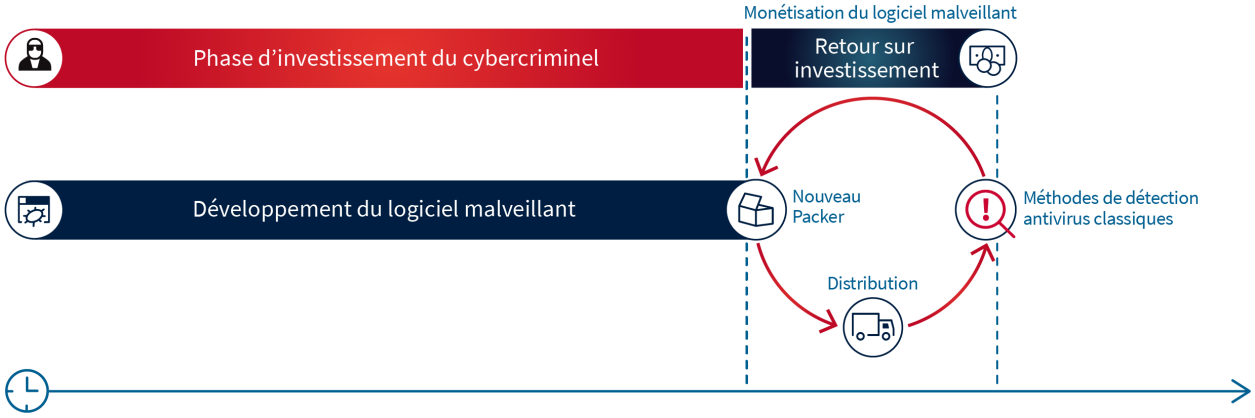
Pour ne pas devoir sans cesse s'atteler à la tâche chronophage du développement de nouveaux codes malveillants, les programmeurs essaient de les camoufler. Cette méthode est simple, moins

onéreuse, et donc plus rentable que de créer de nouveaux logiciels malveillants. Bien souvent, les développeurs ne sont pas les diffuseurs du malware. Ces codes sont revendus à différents cybercriminels qui camouflent eux-mêmes le logiciel malveillant et se chargent de sa diffusion. Dans le cas d'un ransomware par exemple, le programmeur récolte un pourcentage de l'argent extorqué par l'attaquant. Ce modèle économique, appelé « Ransomware as a service », est utilisé par le malware très répandu « Gandcrab ». D'après certains forums spécialisés, les développeurs et leurs clients se partagent l'argent extorqué selon une proportion de 60/40.

Les logiciels malveillants utilisent le camouflage comme tactique

Il est impossible d'estimer le nombre d'outils de camouflage pour logiciels malveillants, mais celui-ci ne cesse de croître. Ces compresseurs, communément appelés Packers, peuvent être modifiés rapidement et facilement afin de tromper et d'esquiver les antivirus. Les méthodes classiques de détection de malwares se heurtent alors à des obstacles.

Les Packers peuvent parfois être utilisés dans plusieurs couches, le logiciel malveillant au cœur du fichier exécutable demeurant inchangé. Il s'agit du moyen le plus rentable de prolonger la durée de vie du malware et d'en maximiser la rentabilité.

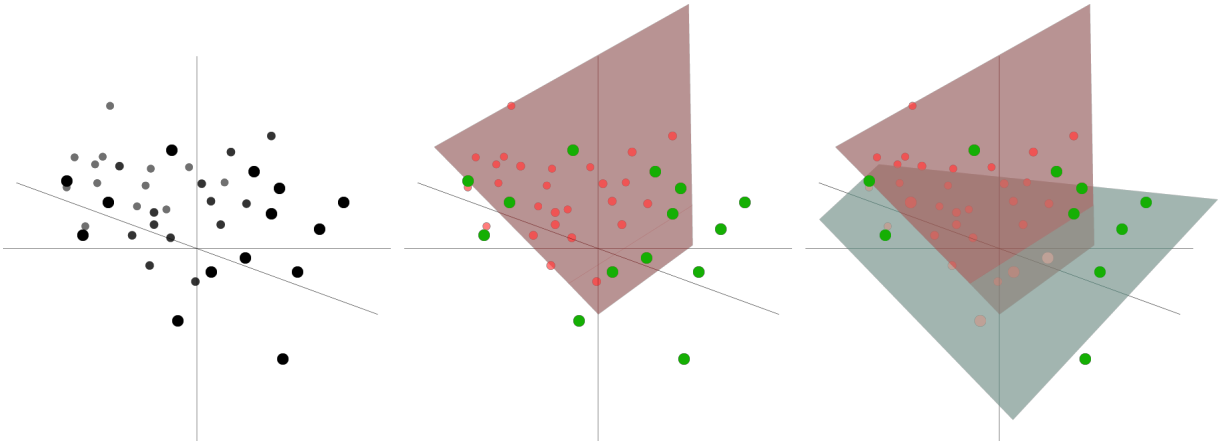


DeepRay® change les règles du jeu

Avec DeepRay®, G DATA a développé une technologie d'apprentissage automatique dont les possibilités constituent un avantage concurrentiel face aux cybercriminels. Généralement, lorsqu'un malware est camouflé, son analyse nécessite l'exécution et la décompression de son contenu sur le disque dur. L'analyse de chaque processus étant consommatrice de ressource, une autre approche a été mise en place. La technologie d'autoapprentissage de G DATA est capable de détecter la dangeroristé d'un fichier sans devoir en analyser le contenu. Pour contourner DeepRay®, les pirates doivent donc modifier le cœur même du logiciel malveillant. Une démarche consommatrice en temps qui réduit à néant la rentabilité du code nuisible.

Comment fonctionne DeepRay®?

Pour la première étape de détection, G DATA utilise un réseau neuronal composé de plusieurs perceptrons. Sur la base de plusieurs centaines de critères, ce réseau détermine si le fichier a été camouflé de manière suspecte avant que celui-ci ne soit décompressé et qu'il révèle son noyau central.Parmi ces critères, on retrouve la taille du fichier général et du code de programmation qu'il contient, la version de l'environnement de programmation utilisée pour créer le fichier ou le nombre de fonctions système importées.



Comme le montre le graphique, les perceptrons partagent un espace d'attributs. Dans le cas de DeepRay®, il s'agit des catégories « Packer » ou « non Packer », c'est-à-dire dangereux ou inoffensif. Toutefois, cela comprend bien plus que les deux plans représentés ici en trois dimensions. Chacun des critères correspond à un plan, de façon à ce que la ligne séparatrice de chaque perceptron passe par des centaines de plans. Ce nombre élevé est nécessaire pour tracer une ligne séparatrice fiable. Le perceptron apprend le tracé optimal à l'aide d'un ensemble d'apprentissages classés au préalable. Ces ensembles sont continuellement mis à jour par garantir les meilleurs résultats d'apprentissage. Afin d'optimiser la précision du processus dans DeepRay®, plusieurs perceptrons sont reliés à un réseau neuronal.

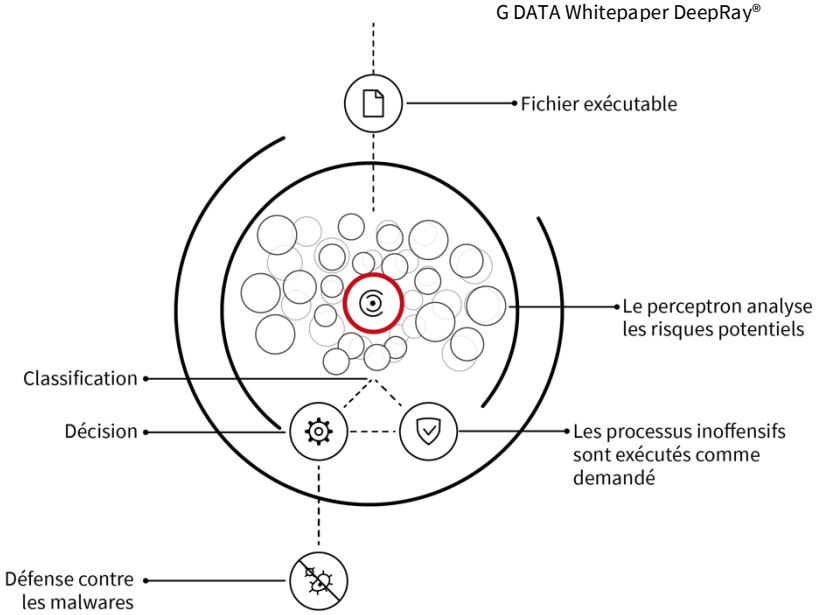
Une défense rapide contre tout type de menace

Si le réseau neuronal de DeepRay® décide qu'un fichier est suspect, une analyse approfondie des processus est alors exécutée en mémoire . Il est important d'identifier ces processus, car les logiciels malveillants tentent généralement de relocaliser les comportements malveillants dans des processus inoffensifs en apparence.

La méthode de détection s'appelle le « Taint Tracking ». Afin de détecter les éventuels dangers, les fonctions système permettant d'accéder à un processus depuis un autre sont surveillées. Si un accès de ce genre est détecté, le processus correspondant est immédiatement considéré comme dangereux (« taint » signifiant « infecter »). Cette « infection » peut être transmise à d'autres processus à n'importe quel niveau. Ces processus sont ensuite également soumis à une analyse.

Ainsi, les malwares sans fichier (« Fileless Malware ») qui ne sont pas stockés dans le système peuvent aussi être détectés.

Cette analyse approfondie permet d'identifier des modèles qui peuvent être attribués à des familles de malwares connues ou généralement à un comportement néfaste.



Niveau de protection optimal dès le départ

Afin d'atteindre un niveau de protection optimal, le réseau neuronal a été entraîné avec les informations que nous récoltons depuis plus de 30 ans dans le cadre de la détection de malwares. Analyser les menaces et informations tirées des G DATA SecurityLabs permet de renforcer continuellement la puissance de la technologie DeepRay®.

Chaque détection est également utilisée pour entraîner le réseau neuronal. Le système d'intelligence artificielle apprend alors de manière adaptative.

Les fichiers inoffensifs sont exécutés comme prévu pour garantir les performances optimales de l'appareil de l'utilisateur.

DeepRay® est la dernière fonction nouvelle génération des solutions de sécurité de G DATA détectant les menaces de manière proactive et protégeant les utilisateurs contre tout dommage.