

Machine Learning

- Brief technique

Techniques de détection multi-niveaux :

1. Machine Learning

2. HyperDetect

3. Sandbox Analyzer

4. Protection de la mémoire

5. Process Inspector

Présentation

Dans le paysage actuel de la cybersécurité, les cybercriminels réalisent régulièrement des tests et modifient fréquemment leurs techniques d'attaques, rendant les entreprises plus vulnérables aux incidents et épidémies de malwares, aux interruptions d'activité et aux violations de données. La plateforme Bitdefender GravityZone Endpoint Security protège vos endpoints contre l'ensemble des cyberattaques sophistiquées avec une grande efficacité, un faible impact pour l'utilisateur final et en limitant la charge de travail des administrateurs. Elle est composée de multiples couches de protection pour entraver les activités de toute personne mal intentionnée. Chaque couche de sécurité est conçue pour stopper certains types précis de menaces, outils ou techniques, assurant ainsi une protection à plusieurs niveaux contre les cyberattaques.

L'ensemble des solutions Bitdefender intègre des modèles de Machine Learning. Les moteurs d'analyse, HyperDetect, Sandbox Analyzer, le contrôle des contenus et Global Protective Network sont quelques exemples des technologies de Bitdefender utilisant le Machine Learning. Ce document se concentre principalement sur la détection à base de Machine Learning (moteurs d'analyse). La détection des menaces basée sur le Machine Learning de Bitdefender est intégrée à la plateforme GravityZone Endpoint Security. Elle assure notamment une protection contre les menaces Zero-day, dès la phase de pré-exécution.

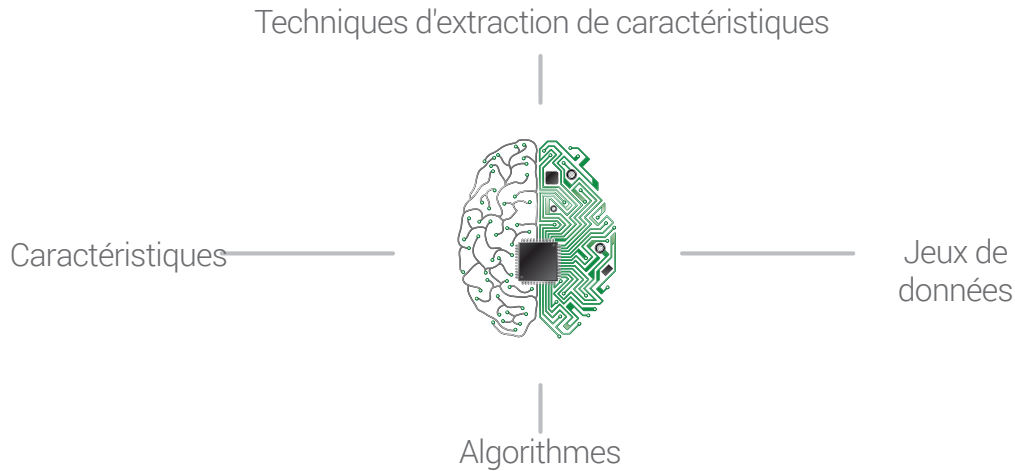
Phase de détection	Type de technologie	Types de menaces détectées
Pré-exécution	Machine Learning	Malwares sous forme de fichier, chevaux de Troie, voleurs de mot de passe, exploits, malwares obfusqués, attaques ciblées, attaques par script, malwares mutants et polymorphes, ransomwares

Intérêt du Machine Learning

Le Machine Learning est la capacité pour des programmes informatiques d'analyser le big data et d'en extraire automatiquement des informations pour en tirer des enseignements. En matière de cybersécurité, il peut jouer un rôle important en permettant de prédire si un objet (tel qu'un fichier ou une URL) a une intention malveillante sans avoir aucune connaissance préalable de celui-ci. La technologie brevetée de Machine Learning de Bitdefender utilise des algorithmes ayant déjà bénéficié d'un très grand nombre d'informations – ces algorithmes sont spécialisés dans des formes précises d'attaques tandis que d'autres, plus génériques, prédisent, détectent et bloquent les menaces Zero-day.

Principales composantes du Machine Learning de Bitdefender :

- **Caractéristiques** : une caractéristique est une propriété individuelle mesurable d'un phénomène observé. Bitdefender extrait les caractéristiques statiques et dynamiques des fichiers et des URL. La connaissance approfondie de Bitdefender en matière de comportement d'un malware lui permet d'identifier un jeu pertinent de caractéristiques.
- **Techniques d'extraction de caractéristiques** : Bitdefender utilise un émulateur spécialisé et des techniques de décompression et de désobfuscation pour extraire les caractéristiques statiques et dynamiques des fichiers et des URL.
- **Algorithmes de Machine Learning** : un algorithme est un programme qui déduit des informations depuis un ensemble de données. Bitdefender utilise de nombreux algorithmes différents. Ces algorithmes se recoupent également dans une faible mesure pour les rendre plus résistants aux attaques avancées. Des algorithmes de Machine Learning personnalisés viennent également améliorer la précision de la détection.
- **Jeux de données** : les jeux de données sont primordiaux pour former et tester les modèles. La bases de données d'échantillons de fichiers sains et malveillants de Bitdefender est l'une des plus grandes du secteur, permet de former et de tester ses modèles de Machine Learning, et ainsi d'améliorer significativement l'efficacité et la précision des détections.



Caractéristiques

- Modèles de Machine Learning dans le cloud et en local pour la détection des URL et des fichiers malveillants.
- De multiples algorithmes de Machine Learning avec plus de 75 000 modèles, notamment : perceptrons, arbres binaires de décision, machine de Boltzmann restreinte, algorithmes génétiques, machines à vecteurs de support, réseaux neuronaux artificiels, algorithmes personnalisés pour la migration des faux positifs, plus de 40 000 caractéristiques statiques et dynamiques.

Quelques exemples de caractéristiques extraites des fichiers par Bitdefender :

- Le code de décompression contient des chaînes de caractères qui peuvent indiquer une persistance dans le système.
- Le fichier est compressé avec un outil inconnu.
- Le fichier est obfusqué (outil de compression et compilateur inconnus).
- Utilisation anormale de différentes instructions en assembleur (call, jump, etc.).
- Techniques d'extraction de multiples caractéristiques : **émulateur** qui émule le code (instructions en assembleur), analyse son comportement ainsi que son but et extrait des caractéristiques ; **routine de décompression** spécialisée qui peut extraire les caractéristiques dynamiques telles que les chaînes de caractères, le code, les scripts HTML injectés, les URL, etc. ; **filtres cryptographiques** qui extraient des caractéristiques des données chiffrées.
- Des jeux de données exhaustifs pour former et tester les modèles de Machine Learning : échantillons récents, malwares variés, malwares représentatifs, Machine Learning non supervisé dans le cloud.

Avantages

- Détecte les attaques avancées en amont et empêche les violations de données, réduit les coûts et les efforts en réponse aux incidents.
- Réduit les efforts de recherche des menaces.
- Améliore grandement le taux de détection des menaces Zero-day lors de la phase de pré-exécution, notamment des malwares sous forme de fichier, des chevaux de Troie, des voleurs de mot de passe, des exploits, des malwares obfusqués, des attaques ciblées, des attaques par script, des malwares mutants et polymorphes, des ransomwares.
- Assure la protection des appareils hors ligne grâce à du Machine Learning en local.
- Est intégré à l'agent de sécurité unifié pour endpoint GravityZone et à la plateforme centralisée d'administration, réduisant ainsi la charge de travail des administrateurs. Ces derniers n'ont ainsi pas à déployer plusieurs solutions de sécurité pour endpoints.



Bitdefender est une entreprise mondiale de sécurité qui développe des solutions de cybersécurité de pointe et qui protège plus de 500 millions d'utilisateurs dans plus de 150 pays. Depuis 2001, Bitdefender développe des technologies régulièrement récompensées, pour les marchés des entreprises et des particuliers, et est un fournisseur recommandé pour sécuriser les infrastructures hybrides et protéger les endpoints. Grâce à ses équipes R&D, ses alliances et partenariats, Bitdefender est reconnu pour être un éditeur innovant, proposant des solutions de sécurité fiables et efficaces, sur lesquelles vous pouvez compter. Plus d'informations sur www.bitdefender.fr

Tous droits réservés. © 2018 Bitdefender. Toutes les marques, noms commerciaux et produits cités dans ce document sont la propriété exclusive de leurs détenteurs respectifs. Pour plus d'informations, veuillez consulter www.bitdefender.fr/business

