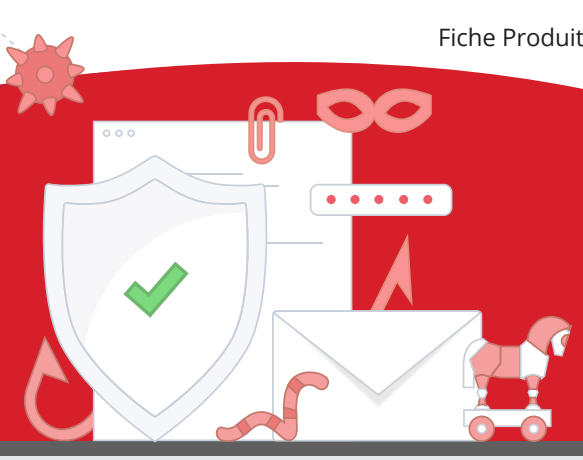
Vade Secure
Predictive Email Defense

Solution de protection contre les malwares et les ransomwares

Analyse comportementale et détection des malwares inconnus



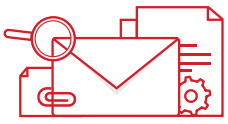
Les malwares les plus sophistiqués sont capables d'adapter leur comportement à l'environnement qu'ils détectent. Ils peuvent ainsi rester dormants, modifier leur code et même se transformer en de nouvelles structures. L'email, principal vecteur des malwares, fait l'objet de toutes les attentions des hackers.

La solution de protection contre les malwares et les ransomwares de Vade Secure ne se limite pas à la détection traditionnelle et adopte une approche heuristique qui analyse les comportements en plus du code pour repérer les anomalies et comportements suspects que les filtres traditionnels ne voient pas.

Cette approche tire parti des informations sur les menaces et retours des utilisateurs issus du 1 milliard de boîtes aux lettres que nous protégeons dans le monde entier. Le moteur de Vade Secure détecte les comportements malveillants et les techniques d'obfuscation dans les emails, documents, fichiers partagés et pages Web pour bloquer les malwares et ransomwares sans recourir au sandboxing. Il évite ainsi la latence inhérente à cette dernière technologie, très perceptible par les utilisateurs.

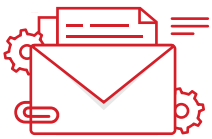
TECHNOLOGIES ANTI-MALWARES BASÉES SUR LE COMPORTEMENT

Analyse comportementale heuristique : examine les emails, pages Web et pièces jointes en s'appuyant sur des règles heuristiques créées par les équipes de R&D de Vade Secure. Nous créons en permanence de nouvelles règles et les utilisons pour adapter notre filtre aux menaces émergentes.



Analyse en temps réel des pièces jointes : analyse les documents Office (Word, Excel, PowerPoint), PDF et ZIP pour détecter les comportements malveillants, y compris les fichiers exécutables, les codes suspects, les macros malveillantes et les URL.

Analyse des fichiers hébergés : Analyse les URL contenus dans les fichiers hébergés sur des services tiers, tels que OneDrive, SharePoint, Google et WeTransfer, pour détecter les URL malveillantes masquées dans les pièces jointes partagées.



Apprentissage automatique : analyse les emails et pièces jointes pour repérer les comportements suspects typiques des malwares et ransomwares. Cette approche comportementale du filtrage permet souvent de détecter un malware sans examiner le fichier à proprement parler.

AU-DELÀ DE LA VÉRIFICATION DE L'EMPREINTE

Les filtres de messagerie basés sur l'analyse de l'empreinte n'ont aucun mal à détecter le code des malwares connus. Pour contourner ce problème, les hackers ont imaginé des techniques sophistiquées, notamment :

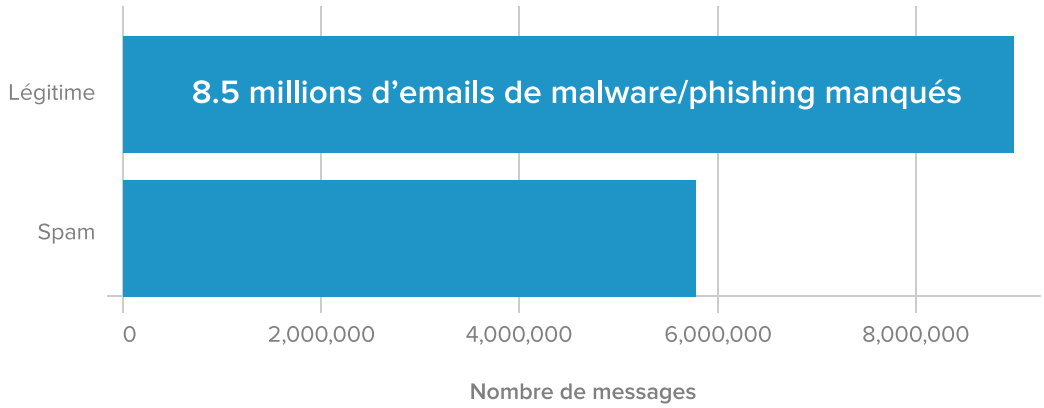
Obfuscation du code : manipulation du code des fichiers et macros pour le rendre incompréhensible ou masquer son véritable objectif.

Génération de bruit : ajout de code superflu ou inutile aux fichiers et macros pour modifier son empreinte et tromper le filtre. Cette technique peut générer des millions d'octets de données inutiles destinées à épuiser les sandboxes.

Sensibilité à l'environnement : fonctions visant à contrer les analyses en étudiant l'environnement avant l'exécution. Les malwares sensibles à leur environnement sont conçus pour ne s'exécuter que dans certains cas. Ils détectent les sandboxes et restent dormants pendant l'analyse.

Les solutions de lutte contre les malwares qui s'appuient sur l'empreinte et des méthodes classiques de détection des menaces échouent régulièrement à détecter les techniques inédites ou émergentes des malwares. La solution de détection comportementale de Vade Secure obtient de bien meilleurs résultats.

"Vade Secure bloque 8,5 millions d'emails malicieux classifiés comme légitimes par les solutions concurrentes"



Comparaison entre Vade Secure et les solutions basées sur l'empreinte

Analyse instantanée, aucun sandboxing, aucune quarantaine : la solution Vade Secure de protection contre les malwares et les ransomwares analyse les emails et les pièces jointes en temps réel, en rendant un verdict sans retarder la remise des emails. L'analyse heuristique permet au moteur du filtre d'examiner les comportements susceptibles d'être cachés par un virus dans une sandbox.

Boucle de rétroaction continue : le 1 milliard de boîtes aux lettres protégées fournissent en continu des informations sur les menaces à notre SOC, ce qui nous permet d'obtenir un taux d'interception des malwares parmi les plus élevés du secteur et un taux de faux positifs très faible. Plus de 10 000 règles heuristiques sont régulièrement mises à jour pour tenir compte des données sur les menaces les plus récentes obtenues par Vade Secure et issues des signalements des utilisateurs.

À propos de Vade Secure

- 1 milliard de boîtes aux lettres protégées
- 1, 400 partenaires dans le monde
- Taux de renouvellement annuel de 95 %
- 11 brevets internationaux actifs
- 2 milliards de messages filtrés l'an dernier

Contact

Siège Social France
sales@vadesecure.com
www.vadesecure.com