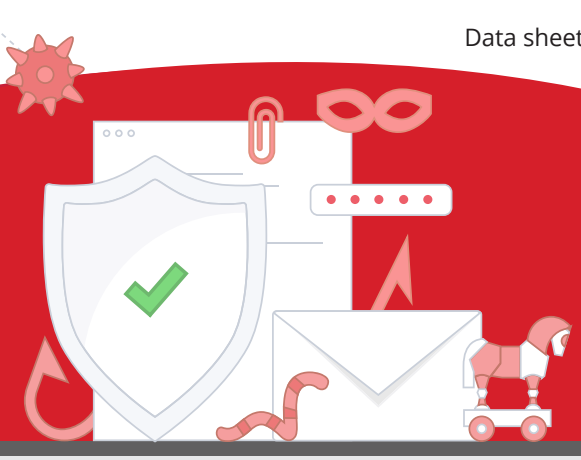
Vade Secure
Predictive Email Defense

Anti-Malware & Ransomware-Lösung

Verhaltensbasierte Analyse und Erkennung unbekannter Malware



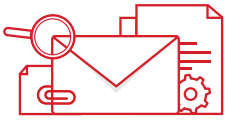
Raffinierte Malware kann ihr Verhalten an die erkannte Umgebung anpassen, sodass sie einfach ruht, ihren Code verändern und sich sogar in neue Strukturen verwandeln kann. E-Mail – die wichtigste Methode zur Zustellung von Malware – ist unter Beschuss.

Die Anti-Malware-/Ransomware-Lösung von Vade Secure geht über die herkömmliche Malware-Erkennung hinaus und bietet einen heuristischen Ansatz, der neben dem Code auch das Verhalten analysiert und Anomalien und verdächtige Verhaltensweisen identifiziert, die von herkömmlichen Filtern übersehen werden.

Der verhaltensbasierte Ansatz zur Erkennung von Malware/Ransomware nutzt Daten und Benutzer-Feedback aus unseren weltweit mehr als 1 Milliarde geschützten Posteingängen. Die Verhaltens-Engine von Vade Secure erkennt böswilliges Verhalten und Verschleierungstechniken in E-Mails, Dokumenten, gemeinsam genutzten Dateien und Webseiten und blockiert Malware und Ransomware ohne Sandboxing und die sich daraus ergebende Latenzzeit für Endbenutzer.

VERHALTENSBASIERTE ANTI-MALWARE-TECHNOLOGIEN

Heuristik-basierte Verhaltensanalyse: Untersucht E-Mails, Webseiten und Anhänge auf der Grundlage heuristischer Regeln, die von Vade Secures F&E entwickelt wurden. Um den Filter basierend auf den aktuellsten Bedrohungen zu optimieren, werden ständig neue heuristische Regeln erstellt und angewandt.



Echtzeit-Analyse von Anhängen: Analysiert Office-Dokumente (Word, Excel, PowerPoint), PDFs und ZIP-Dateien, um böswilliges Verhalten zu erkennen, einschließlich ausführbarer Dateien, verdächtiger Codes, schädlicher Makros und URLs.

Host-Datei-Analyse: Analysiert Dateien von Drittanbietern wie OneDrive, SharePoint, Google und WeTransfer, um in freigegebenen Anhängen versteckte Malware- und Ransomware-Viren zu finden.

Maschinelles Lernen: Analysiert E-Mails und Anhänge, um verdächtige Verhaltensweisen zu identifizieren, die häufig bei Malware- und Ransomware-Angriffen vorkommen. Dabei handelt es sich um einen Filteransatz, der Malware oft identifiziert, ohne die Datei selbst zu untersuchen.

MEHR ALS FINGERPRINTING

Bekannter Malware-Code kann von E-Mailfiltern, die Fingerprinting verwenden, um bösartige E-Mails zu erkennen, ganz einfach erkannt werden. Deshalb haben Hacker raffinierte Techniken entwickelt, die den Filter umgehen und damit die Erkennung vermeiden, unter anderem:

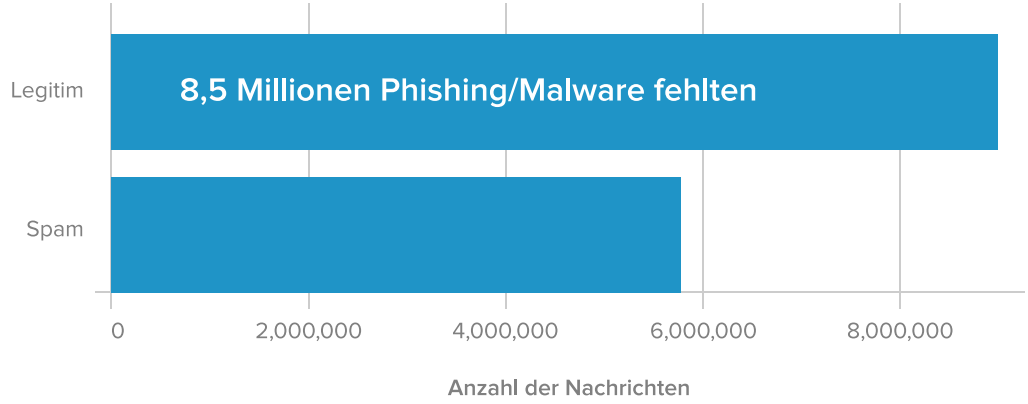
Code-Verschleierung Das Manipulieren von Code in Dateien und Makros, um den Code entweder unverständlich zu machen oder den wahren Zweck des Codes zu verdecken.

Zu viel „Lärm“: Durch das Hinzufügen von unwichtigem, nutzlosen Code zu Dateien und Makros wird der „Fingerprint“ einer bekannten Bedrohung verändert und damit der Filter verwirrt. Hierzu können auch Millionen von Bytes nutzloser Daten gehören, die eine Sandbox überlasten sollen.

Umgebungsbewusstsein: Entwicklung von Anti-Analyse-Fähigkeiten, mit denen ein Umgebungsscan angestoßen wird. Umgebungsbewusste Malware ist so konzipiert, dass sie nur in bestimmten Umgebungen ausgeführt wird, sie erkennt Sandboxes und ruht während der Analyse.

Anti-Malware-Lösungen, die sich auf Fingerprinting und traditionelle Methoden zur Bedrohungserkennung stützen, scheitern immer wieder daran, neue und aufkommende Malware-Techniken zu erkennen. Die verhaltensbasierte Erkennung von Vade Secure schneidet zuverlässig besser ab als konkurrierende Lösungen, die auf Fingerprint-Technologie basieren.

“Vade Secure blockierte 8,5 Millionen böswillige E-Mails, die von der Anbieterlösung als legitim eingestuft wurden”



Vade Secure vs. Fingerprint-basierte Lösung

Sofortige Analyse: Kein Sandboxing und keine Quarantäne: Die Anti-Malware- und Ransomware-Lösung von Vade Secure untersucht E-Mails und Anhänge in Echtzeit und liefert ein sofortiges Urteil ohne Verzögerung bei der Zustellung der E-Mail. Die heuristische Analyse erlaubt es der Filter-Engine, das Verhalten zu untersuchen, das andernfalls von einem Virus in einer Sandbox verdeckt sein könnte.

Kontinuierliche Feedback-Schleife: Die 1 Milliarde geschützten Posteingänge von Vade Secure liefern unserem SOC kontinuierlich Informationen über Bedrohungen, was zu einer branchenweit hohen Erkennungsrate von Malware und einer niedrigen False-Positive-Rate führt. Mehr als 10.000 Heuristikregeln werden ständig aktualisiert, um die neusten Bedrohungsdaten zu berücksichtigen, die von Vade Secure erfasst werden und aus Benutzermeldungen stammen.

Über Vade Secure

- 1 Milliarde Postfächer geschützt
- 1.400 Partner weltweit
- 95 % Erneuerungsquote
- 11 aktive internationale Patente
- 2 Milliarden Nachrichten wurden letztes Jahr gefiltert

Kontakt

Vade Secure Sales
EMEA
sales@vadesecure.com