DATA SHEET

Anti-Malware/Ransomware Solution

AI-POWERED ANALYSIS AND DETECTION OF EMERGING MALWARE ATTACKS

AI-powered analysis and detection of emerging malware attacks

Businesses of all sizes are increasingly under attack. SMBs are facing the same attacks that target enterprise companies – but have fewer resources to combat them. Hackers are leveraging the method that works best to insert increasingly adaptable and sophisticated malware into company networks: email.

Vade for M365's Anti-Malware/Ransomware Solution goes beyond traditional malware detection with an AI-powered approach that utilizes Natural Language Processing and Machine Learning in addition to code analysis, identifying anomalies and suspicious behaviors that traditional filters miss.

Vade's approach to malware/ransomware detection draws on threat intelligence and user feedback from more than 1.4 billion protected mailboxes globally. The Vade AI-powered engine detects malicious behaviors and obfuscation techniques in emails, documents, shared files, and webpages—blocking malware and ransomware without the need for sandboxing and the resulting latency to end users.

BEHAVIORAL-BASED ANTI-MALWARE TECHNOLOGIES

Real-time attachment parsing: Parses Office documents (Word, Excel, PowerPoint), PDFs, and ZIP files to detect malicious behaviors, including executable files, suspicious code, malicious macros, and URLs.

Hosted-file analysis: Analyzes URLs in files from third-party hosts, such as OneDrive, SharePoint, Google, and WeTransfer, to detect URLs hidden in shared attachments.

Machine Learning: Analyzes emails and attachments to identify suspicious behaviors common to malware and ransomware attacks, a behavioral approach to filtering that often identifies malware without examining the file itself.

Natural Language Processing: Examines email text and contents for patterns common to enticing users to open malicious attachments or download malware. Vade also leverages Large Language Models to provide adaptive protection for attacks aided by generative AI, including ChatGPT.

BEYOND FINGERPRINTING

Excess "Noise": Adding non-essential and otherwise useless code to files and macros, altering the "fingerprint" of a known threat and confusing a filter. Excess noise can include millions of bytes of useless data designed to exhaust a sandbox.

Environmental Awareness: Creating anti-analysis capabilities that initiate an environmental scan before execution. Environmentally aware malware is designed to execute only in certain environments, detecting sandboxes and remaining dormant for the duration of the analysis.

Anti-malware solutions that rely on fingerprinting and traditional methods of threat detection consistently fail to detect new and emerging malware techniques. Vade's behavioral-based detection consistently outperforms competitive solutions that use fingerprinting technology.

Instant Analysis/No sandboxing or quarantine: Vade for M365's anti-malware and ransomware solution examines emails and attachments in real-time, delivering an instant verdict with no delay in email delivery. Machine Learning and Natural Language Processing analysis allows the filter engine to examine the behaviors that could otherwise be concealed by a virus in a sandbox.

Continuous feedback loop: Vade's more than 1.4 billion protected mailboxes provide continual threat intelligence to our SOC, resulting in an industry-high malware catch rate and low false-positive rate. More than 10,000 heuristic rules are consistently updated to reflect the latest threat data captured by Vade and from user reports.

3.5 million
malware emails detected globally in 2023

+1.4 billion
mailboxes feeding AI engine

100 billion
emails analyzed per day

Vade is a leading cybersecurity firm specializing in AI-driven threat detection and response solutions for Microsoft collaboration suite, with a focus on serving Small to Medium-sized Businesses (SMBs) and their Managed Service Providers (MSPs). With a global presence across eight locations, including the United States, France, Japan, Canada, and Israel, Vade's flagship product, Vade for Microsoft 365, seamlessly provides supplementary cybersecurity services for Microsoft's collaboration suite. The company's best-in-class security solutions integrate robust AI-driven protection and automated threat remediation, resulting in improved efficiency, reduced administrative overhead, and optimized cybersecurity investments.

Vade provides distinctive protection against phishing, spear phishing, and malware, ensuring error-free configurations and enabling rapid deployment. Vade is a trusted choice for some of the world's leading internet service providers and security solution providers, ensuring the security of 1.4 billion email inboxes.

To learn more, please visit: **vadesecure.com**

Follow us :

@vadesecure