True Type Detection

Ensuring Accurate File Sanitization Through Structural Validation

SOLUTION BRIEF

Overview

Menlo's True Type Detection is a foundational component of our next-gen Content Disarm and Reconstruction (CDR) technology. Unlike conventional approaches that rely on file extensions or MIME types — both of which can be easily spoofed — True Type Detection uses deep file inspection to accurately identify the actual type of each file. This ensures that every file is processed, sanitized, and reconstructed using the correct logic and security policies.

Benefits

- **Enhanced Security:** Prevents attackers from bypassing defenses by mislabeling file types — a common tactic in phishing and malware delivery campaigns.
- **Guaranteed CDR Accuracy:** Files are always sanitized based on their actual content type, not what they pretend to be. No misrouted sanitization paths.
- **Zero Trust Reinforcement:** Treats all incoming files as untrusted by default, and verifies identity before any further action.
- **Broad Format Support:** Supports a wide array of file types and subtypes with dedicated validators, ensuring robust protection across enterprise content flows.
- **Operational Transparency:** Detected types and inconsistencies are logged and available via the Menlo management console and APIs, aiding incident response and compliance.

How It Works

Menlo's detection engine goes beyond surface-level metadata and dives into the internal structure of each file. For instance:

Magic Byte Validation: At the binary level, every file type has a unique header signature known as magic bytes. Menlo reads these bytes to identify the format reliably.

- **Example – PDF Magic Bytes**
  - A valid PDF begins with the following bytes: %PDF-1.4
  - This string must appear within the first few bytes of the file. Any deviation or absence is a red flag.

File Structure Analysis: PDFs must include specific structural components such as a cross-reference table (xref), a trailer dictionary, and an %%EOF end-of-file marker.

- Menlo checks for these to validate integrity and ensure the file isn't malformed or hiding embedded executables.

Validator-Based Confirmation: Instead of using static rules, Menlo employs type-specific validators — purpose-built parsers that can definitively determine whether a file conforms to a recognized type specification (e.g., PDF, Office, image formats, etc.).

Extension Deception Mitigation: Attackers often rename file extensions (e.g., renaming an executable to ".pdf") to bypass filters.

- Menlo neutralizes this tactic by disregarding extensions altogether when determining processing paths.

Once a file's True Type is determined, the appropriate CDR policy is applied, ensuring only valid and expected content survives.

Effectiveness in Real-World Threats

In Real-world Deployments, True Type Detection Has:

- Blocked disguised executables hidden inside renamed Office files.
- Exposed embedded malicious scripts in falsely labeled image files.
- Identified malformed PDFs crafted to evade basic sandboxing tools.

By correctly classifying every file upfront, Menlo guarantees that even evasive and polymorphic threats are neutralized before they reach users or endpoints.

MENLO SECURITY

Learn more: https://www.menlosecurity.com
Contact us: ask@menlosecurity.com