Detection Strategy for VBA Stomping, Detection Strategy DET0012

Archived: 2026-04-05 13:04:18 UTC

AN0034

Discrepancies between VBA source code and p-code inside Office documents. Defender perspective: anomalies in file metadata streams, execution of Office processes loading macros without source code consistency, and script execution with no corresponding source metadata.

Log Sources

Mutable Elements

Field	Description
MonitoredExtensions	Expand or restrict which Office file types (.docm, .xlsm, .pptm) are flagged for VBA project analysis.
TimeWindow	Correlate Office process execution with subsequent script execution within a narrow window.

AN0035

Execution of Wine or LibreOffice macros with inconsistent VBA metadata. Defender perspective: file analysis showing p-code embedded without matching source streams.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve calls to soffice.bin with suspicious macro execution flags
File Metadata (DC0059)	linux:syslog	Discrepancies in _VBA_PROJECT p-code vs source code extracted with oletools/pcodedmp

Mutable Elements

Field	Description
ScannerTooling	Choice of OLE/P-code analysis utilities (oletools, pcodedmp, custom disassembler).

AN0036

Opening of Office files where VBA source code appears benign or missing, but p-code remains active. Defender perspective: process execution of Office apps with macro execution lacking visible source components.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Process execution of Microsoft Word, Excel, PowerPoint with macro execution attempts
File Metadata (DC0059)	macos:unifiedlog	Detection of altered _VBA_PROJECT or PerformanceCache streams

Mutable Elements

Field	Description
OfficeVersionScope	Adjust for specific Office versions in use across macOS endpoints.

Source: https://attack.mitre.org/detectionstrategies/DET0012#AN0034