Detect Office Startup-Based Persistence via Macros, Forms, and Registry Hooks, Detection Strategy DET0398

Archived: 2026-04-05 17:47:24 UTC

Analytics

- Windows
- Office Suite

AN1116

Office-based persistence via Office template macros, Outlook forms/rules/homepage, or registry-persistent scripts. Adversary modifies registry keys or Office application directories to load malicious scripts at startup.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Tune based on expected Office process tree (e.g., WINWORD.EXE spawning cmd.exe)
RegistryPath	Specific keys related to Office startup such as Outlook Today, AddIns, or Template Macros
TimeWindow	Window of process execution after user login or Outlook launch
UserContext	Detect persistence within high-value user mailboxes (e.g., admin, finance, C-suite)

AN1117

Startup-based persistence mechanisms within Microsoft Office Suite like template macros and home page redirects being configured through internal automation or client-side settings.

Log Sources

Mutable Elements

Field	Description
RuleAction	Identify rule actions that execute scripts, forward emails externally, or start external content

Field	Description
MailboxTarget	Focus on users with sensitive roles or shared mailboxes
TimeWindow	Detect persistence artifacts created shortly after credential access or login from an unusual location

---