IMAPLoader, Software S1152 | MITRE ATT&CK®

Archived: 2026-04-05 17:14:25 UTC

Domain	ID		Name	Use
Enterprise	T1071	.003	Application Layer Protocol: Mail Protocols	IMAPLoader uses the IMAP email protocol for command and control purposes.[1]
Enterprise	T1543		Create or Modify System Process	IMAPLoader modifies Windows tasks on the victim machine to reference a retrieved PE file through a path modification.[1]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	IMAPLoader hides the Windows Console window created by its execution by directly importing the `kernel32.dll` and `user32.dll` libraries `GetConsoleWindow` and `ShowWindow` APIs.[1]
Enterprise	T1574	.014	Hijack Execution Flow: AppDomainManager	IMAPLoader is executed via the AppDomainManager injection technique.[1]
Enterprise	T1105		Ingress Tool Transfer	IMAPLoader is a loader used to retrieve follow-on payload encoded in email messages for execution on victim systems.[1]
Enterprise	T1106		Native API	IMAPLoader imports native Windows APIs such as `GetConsoleWindow` and `ShowWindow`.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	IMAPLoader creates scheduled tasks for persistence based on the operating system version of the victim machine.[1]

Domain	ID	Name	Use
Enterprise	T1082	System Information Discovery	IMAPLoader uses WMI queries to gather information about the victim machine.[1]
Enterprise	T1047	Windows Management Instrumentation	IMAPLoader uses WMI queries to query system information on victim hosts.[1]

Source: https://attack.mitre.org/software/S1152