Mosquito, Software S0256 | MITRE ATT&CK®

Archived: 2026-04-05 15:46:23 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Mosquito establishes persistence under the Registry key `HKCU\Software\Run auto_update`.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Mosquito can launch PowerShell Scripts.[1]
		.003	Command and Scripting Interpreter: Windows Command Shell	Mosquito executes cmd.exe and uses a pipe to read the results and send back the output to the C2 server.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Mosquito uses a custom encryption algorithm, which consists of XOR and a stream that is similar to the Blum Blum Shub algorithm.[1]
Enterprise	T1546	.015	Event Triggered Execution: Component Object Model Hijacking	Mosquito uses COM hijacking as a method of persistence.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Mosquito deletes files using DeleteFileW API call. [1]
Enterprise	T1105		Ingress Tool Transfer	Mosquito can upload and download files to the victim.[1]
Enterprise	T1112		Modify Registry	Mosquito can modify Registry keys under `HKCU\Software\Microsoft[dllname]` to store configuration values. Mosquito also modifies Registry keys under

Domain	ID		Name	Use
				`HKCR\CLSID...\InprocServer32` with a path to the launcher.[1]
Enterprise	T1106		Native API	Mosquito leverages the CreateProcess() and LoadLibrary() calls to execute files with the .dll and .exe extensions.[1]
Enterprise	T1027	.011	Obfuscated Files or Information: Fileless Storage	Mosquito stores configuration values under the Registry key `HKCU\Software\Microsoft[dllname]`.[1]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	Mosquito's installer is obfuscated with a custom crypter to obfuscate the installer.[1]
Enterprise	T1057		Process Discovery	Mosquito runs `tasklist` to obtain running processes.[1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Mosquito's installer searches the Registry and system to see if specific antivirus tools are installed on the system.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	Mosquito's launcher uses rundll32.exe in a Registry Key value to start the main backdoor capability.[1]
Enterprise	T1016		System Network Configuration Discovery	Mosquito uses the `ipconfig` command.[1]
Enterprise	T1033		System Owner/User Discovery	Mosquito runs `whoami` on the victim's machine.[1]

Domain	ID	Name	Use
Enterprise	T1047	Windows Management Instrumentation	Mosquito's installer uses WMI to search for antivirus display names.[1]

Source: https://attack.mitre.org/software/S0256/