BabyShark, Software S0414 | MITRE ATT&CK®

Archived: 2026-04-05 12:37:17 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	BabyShark has added a Registry key to ensure all future macros are enabled for Microsoft Word and Excel as well as for additional persistence.[1][3]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	BabyShark has used cmd.exe to execute commands.[1]
		.005	Command and Scripting Interpreter: Visual Basic	BabyShark can execute additional VisualBasic content.[4]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	BabyShark has encoded data using certutil before exfiltration.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	BabyShark has the ability to decode downloaded files prior to execution.[3]
Enterprise	T1083		File and Directory Discovery	BabyShark has used `dir` to search for "programfiles" and "appdata".[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	BabyShark has cleaned up all files associated with the secondary payload execution.[5]
Enterprise	T1105		Ingress Tool Transfer	BabyShark has downloaded additional files from the C2.[5][3]

Domain	ID		Name	Use
Enterprise	T1056	.001	Input Capture: Keylogging	BabyShark has a PowerShell-based remote administration ability that can implement a PowerShell or C# based keylogger.[5]
Enterprise	T1057		Process Discovery	BabyShark has executed the `tasklist` command.[1]
Enterprise	T1012		Query Registry	BabyShark has executed the `reg query` command for `HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default`.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	BabyShark has used scheduled tasks to maintain persistence.[6]
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	BabyShark has used mshta.exe to download and execute applications from a remote server.[3]
Enterprise	T1082		System Information Discovery	BabyShark has executed the `ver` command.[1]
Enterprise	T1016		System Network Configuration Discovery	BabyShark has executed the `ipconfig /all` command.[1]
Enterprise	T1033		System Owner/User Discovery	BabyShark has executed the `whoami` command.[1]

Source: https://attack.mitre.org/software/S0414/