BadPatch, Software S0337 | MITRE ATT&CK®

Archived: 2026-04-05 18:42:28 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	BadPatch uses HTTP for C2.[1]
		.003	Application Layer Protocol: Mail Protocols	BadPatch uses SMTP for C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	BadPatch establishes a foothold by adding a link to the malware executable in the startup folder.[1]
Enterprise	T1005		Data from Local System	BadPatch collects files from the local system that have the following extensions, then prepares them for exfiltration: .xls, .xlsx, .pdf, .mdb, .rar, .zip, .doc, .docx.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	BadPatch stores collected data in log files before exfiltration.[1]
Enterprise	T1083		File and Directory Discovery	BadPatch searches for files with specific file extensions.[1]
Enterprise	T1105		Ingress Tool Transfer	BadPatch can download and execute or update malware.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	BadPatch has a keylogging capability.[1]

Domain	ID		Name	Use
Enterprise	T1113		Screen Capture	BadPatch captures screenshots in .jpg format and then exfiltrates them.[1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	BadPatch uses WMI to enumerate installed security products in the victim's environment.[1]
Enterprise	T1082		System Information Discovery	BadPatch collects the OS system, OS version, MAC address, and the computer name from the victim's machine.[1]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	BadPatch attempts to detect if it is being run in a Virtual Machine (VM) using a WMI query for disk drive name, BIOS, and motherboard information. [1]
