BACKSPACE, Software S0031 | MITRE ATT&CK®

Archived: 2026-04-05 13:28:16 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	BACKSPACE uses HTTP as a transport to communicate with its command server.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	BACKSPACE achieves persistence by creating a shortcut to itself in the CSIDL_STARTUP directory.[1]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	BACKSPACE achieves persistence by creating a shortcut to itself in the CSIDL_STARTUP directory.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Adversaries can direct BACKSPACE to execute from the command line on infected hosts, or have BACKSPACE create a reverse shell.[1]
Enterprise	T1132	.002	Data Encoding: Non-Standard Encoding	Newer variants of BACKSPACE will encode C2 communications with a custom system.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Adversaries can direct BACKSPACE to upload files to the C2 Server.[1]
Enterprise	T1083		File and Directory Discovery	BACKSPACE allows adversaries to search for files.[1]
Enterprise	T1562	.004	Impair Defenses: Disable or Modify System Firewall	The "ZR" variant of BACKSPACE will check to see if known host-based firewalls are installed on the infected systems. BACKSPACE will attempt to

Domain	ID		Name	Use
				establish a C2 channel, then will examine open windows to identify a pop-up from the firewall software and will simulate a mouse-click to allow the connection to proceed.[1]
Enterprise	T1112		Modify Registry	BACKSPACE is capable of deleting Registry keys, sub-keys, and values on a victim system.[1]
Enterprise	T1104		Multi-Stage Channels	BACKSPACE attempts to avoid detection by checking a first stage command and control server to determine if it should connect to the second stage server, which performs "louder" interactions with the malware.[1]
Enterprise	T1057		Process Discovery	BACKSPACE may collect information about running processes.[1]
Enterprise	T1090	.001	Proxy: Internal Proxy	The "ZJ" variant of BACKSPACE allows "ZJ link" infections with Internet access to relay traffic from "ZJ listen" to a command server.[1]
Enterprise	T1012		Query Registry	BACKSPACE is capable of enumerating and making modifications to an infected system's Registry.[1]
Enterprise	T1082		System Information Discovery	During its initial execution, BACKSPACE extracts operating system information from the infected host. [1]