BLACKCOFFEE, Software S0069 | MITRE ATT&CK®

Archived: 2026-04-05 15:36:39 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	BLACKCOFFEE has the capability to create a reverse shell.[1]
Enterprise	T1083		File and Directory Discovery	BLACKCOFFEE has the capability to enumerate files.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	BLACKCOFFEE has the capability to delete files.[1]
Enterprise	T1104		Multi-Stage Channels	BLACKCOFFEE uses Microsoft's TechNet Web portal to obtain an encoded tag containing the IP address of a command and control server and then communicates separately with that IP address for C2. If the C2 server is discovered or shut down, the threat actors can update the encoded IP address on TechNet to maintain control of the victims' machines.[1]
Enterprise	T1057		Process Discovery	BLACKCOFFEE has the capability to discover processes.[1]
Enterprise	T1102	.001	Web Service: Dead Drop Resolver	BLACKCOFFEE uses Microsoft's TechNet Web portal to obtain a dead drop resolver containing an encoded tag with the IP address of a command and control server.[1][2]
		.002	Web Service: Bidirectional Communication	BLACKCOFFEE has also obfuscated its C2 traffic as normal traffic to sites such as Github.[1][2]

Source: https://attack.mitre.org/software/S0069