BISCUIT, Software S0017 | MITRE ATT&CK®

Archived: 2026-04-05 18:07:24 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	BISCUIT has a command to launch a command shell on the system.[2]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	BISCUIT uses SSL for encrypting C2 communications.[2]
Enterprise	T1008		Fallback Channels	BISCUIT malware contains a secondary fallback command and control server that is contacted after the primary command and control server.[1][2]
Enterprise	T1105		Ingress Tool Transfer	BISCUIT has a command to download a file from the C2 server.[2]
Enterprise	T1056	.001	Input Capture: Keylogging	BISCUIT can capture keystrokes.[2]
Enterprise	T1057		Process Discovery	BISCUIT has a command to enumerate running processes and identify their owners.[2]
Enterprise	T1113		Screen Capture	BISCUIT has a command to periodically take screenshots of the system.[2]
Enterprise	T1082		System Information Discovery	BISCUIT has a command to collect the processor type, operation system, computer name, and whether the system is a laptop or PC.[1]

Domain	ID	Name	Use
Enterprise	T1033	System Owner/User Discovery	BISCUIT has a command to gather the username from the system.[2]
Enterprise	T1124	System Time Discovery	BISCUIT has a command to collect the system `UPTIME`.[1]

Source: https://attack.mitre.org/software/S0017/