

QUIETCANARY, Software S1076 | MITRE ATT&CK®

Archived: 2026-04-05 14:42:22 UTC

Domain	ID	Name	Use
Enterprise	T1071 .001	Application Layer Protocol: Web Protocols	QUIETCANARY can use HTTPS for C2 communications. ^[1]
Enterprise	T1132 .001	Data Encoding: Standard Encoding	QUIETCANARY can base64 encode C2 communications. ^[1]
Enterprise	T1074	Data Staged	QUIETCANARY has the ability to stage data prior to exfiltration. ^[1]
Enterprise	T1140	Deobfuscate/Decode Files or Information	QUIETCANARY can use a custom parsing routine to decode the command codes and additional parameters from the C2 before executing them. ^[1]
Enterprise	T1573 .001	Encrypted Channel: Symmetric Cryptography	QUIETCANARY can RC4 encrypt C2 communications. ^[1]
Enterprise	T1564 .003	Hide Artifacts: Hidden Window	QUIETCANARY can execute processes in a hidden window. ^[1]
Enterprise	T1106	Native API	QUIETCANARY can call <code>System.Net.HttpWebRequest</code> to identify the default proxy configured on the victim computer. ^[1]
Enterprise	T1012	Query Registry	QUIETCANARY has the ability to retrieve information from the Registry. ^[1]

Domain	ID	Name	Use
Enterprise	T1016	System Network Configuration Discovery	QUIETCANARY can identify the default proxy setting on a compromised host. [1]

Source: <https://attack.mitre.org/software/S1076>