QuietSieve, Software S0686 | MITRE ATT&CK®

Archived: 2026-04-05 13:47:57 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	QuietSieve can use HTTPS in C2 communications. [1]
Enterprise	T1005		Data from Local System	QuietSieve can collect files from a compromised host.[1]
Enterprise	T1083		File and Directory Discovery	QuietSieve can search files on the target host by extension, including doc, docx, xls, rtf, odt, txt, jpg, pdf, rar, zip, and 7z.[1]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	QuietSieve has the ability to execute payloads in a hidden window.[1]
Enterprise	T1105		Ingress Tool Transfer	QuietSieve can download and execute payloads on a target host.[1]
Enterprise	T1135		Network Share Discovery	QuietSieve can identify and search networked drives for specific file name extensions.[1]
Enterprise	T1120		Peripheral Device Discovery	QuietSieve can identify and search removable drives for specific file name extensions.[1]
Enterprise	T1113		Screen Capture	QuietSieve has taken screenshots every five minutes and saved them to the user's local Application Data folder under `Temp\SymbolSourceSymbols\icons` or `Temp\ModeAuto\icons`.[1]

Domain	ID		Name	Use
Enterprise	T1016	.001	System Network Configuration Discovery: Internet Connection Discovery	QuietSieve can check C2 connectivity with a `ping` to 8.8.8.8 (Google public DNS).[1]

Source: https://attack.mitre.org/software/S0686