Small Sieve, Software S1035 | MITRE ATT&CK®

Archived: 2026-04-05 16:51:19 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Small Sieve can contact actor-controlled C2 servers by using the Telegram API over HTTPS.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Small Sieve has the ability to add itself to `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift` for persistence.[2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Small Sieve can use `cmd.exe` to execute commands on a victim's system.[2]
		.006	Command and Scripting Interpreter: Python	Small Sieve can use Python scripts to execute commands.[2]
Enterprise	T1132	.002	Data Encoding: Non-Standard Encoding	Small Sieve can use a custom hex byte swapping encoding scheme to obfuscate tasking traffic.[1][2]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	Small Sieve can use SSL/TLS for its HTTPS Telegram Bot API-based C2 channel.[1]
Enterprise	T1480		Execution Guardrails	Small Sieve can only execute correctly if the word `Platypus` is passed to it on the command line.[2]
Enterprise	T1105		Ingress Tool Transfer	Small Sieve has the ability to download files.[2]

Domain	ID		Name	Use
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Small Sieve can use variations of Microsoft and Outlook spellings, such as "Microsift", in its file names to avoid detection.[2]
Enterprise	T1027		Obfuscated Files or Information	Small Sieve has the ability to use a custom hex byte swapping encoding scheme combined with an obfuscated Base64 function to protect program strings and Telegram credentials.[2]
Enterprise	T1016		System Network Configuration Discovery	Small Sieve can obtain the IP address of a victim host.[2]
Enterprise	T1033		System Owner/User Discovery	Small Sieve can obtain the id of a logged in user.[2]
Enterprise	T1102	.002	Web Service: Bidirectional Communication	Small Sieve has the ability to use the Telegram Bot API from Telegram Messenger to send and receive messages.[2]
