SodaMaster, Software S0627 | MITRE ATT&CK®

Archived: 2026-04-05 16:07:18 UTC

Domain	ID		Name	Use
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	SodaMaster can use RC4 to encrypt C2 communications. [1]
		.002	Encrypted Channel: Asymmetric Cryptography	SodaMaster can use a hardcoded RSA key to encrypt some of its C2 traffic.[1]
Enterprise	T1105		Ingress Tool Transfer	SodaMaster has the ability to download additional payloads from C2 to the targeted system.[1]
Enterprise	T1106		Native API	SodaMaster can use `RegOpenKeyW` to access the Registry.[1]
Enterprise	T1027		Obfuscated Files or Information	SodaMaster can use "stackstrings" for obfuscation.[1]
Enterprise	T1057		Process Discovery	SodaMaster can search a list of running processes.[1]
Enterprise	T1012		Query Registry	SodaMaster has the ability to query the Registry to detect a key specific to VMware.[1]
Enterprise	T1082		System Information Discovery	SodaMaster can enumerate the host name and OS version on a target system.[1]
Enterprise	T1033		System Owner/User Discovery	SodaMaster can identify the username on a compromised host.[1]

Domain	ID		Name	Use
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	SodaMaster can check for the presence of the Registry key `HKEY_CLASSES_ROOT\Applications\VMwareHostOpen.exe` before proceeding to its main functionality.[1]
		.003	Virtualization/Sandbox Evasion: Time Based Checks	SodaMaster has the ability to put itself to "sleep" for a specified time.[1]

Source: https://attack.mitre.org/software/S0627