PoisonIvy, Software S0012 | MITRE ATT&CK®

Archived: 2026-04-05 13:22:09 UTC

Domain	ID		Name	Use
Enterprise	T1010		Application Window Discovery	PoisonIvy captures window titles.[3]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	PoisonIvy creates run key Registry entries pointing to a malicious executable dropped to disk.[3]
		.014	Boot or Logon Autostart Execution: Active Setup	PoisonIvy creates a Registry key in the Active Setup pointing to a malicious executable.[6][7][8]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	PoisonIvy creates a backdoor through which remote attackers can open a command-line interface.[3]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	PoisonIvy creates a Registry subkey that registers a new service. PoisonIvy also creates a Registry entry modifying the Logical Disk Manager service to point to a malicious DLL dropped to disk.[3]
Enterprise	T1005		Data from Local System	PoisonIvy creates a backdoor through which remote attackers can steal system information.[3]
Enterprise	T1074	.001	Data Staged: Local Data Staging	PoisonIvy stages collected data in a text file.[3]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	PoisonIvy uses the Camellia cipher to encrypt communications.[1]

Domain	ID		Name	Use
Enterprise	T1480	.002	Execution Guardrails: Mutual Exclusion	PoisonIvy creates a mutex using either a custom or default value.[1]
Enterprise	T1105		Ingress Tool Transfer	PoisonIvy creates a backdoor through which remote attackers can upload files.[3]
Enterprise	T1056	.001	Input Capture: Keylogging	PoisonIvy contains a keylogger.[1][3]
Enterprise	T1112		Modify Registry	PoisonIvy creates a Registry subkey that registers a new system device.[3]
Enterprise	T1027		Obfuscated Files or Information	PoisonIvy hides any strings related to its own indicators of compromise.[3]
Enterprise	T1055	.001	Process Injection: Dynamic-link Library Injection	PoisonIvy can inject a malicious DLL into a process.[1][3]
Enterprise	T1014		Rootkit	PoisonIvy starts a rootkit from a malicious file dropped to disk.[3]

Source: https://attack.mitre.org/software/S0012