Gold Dragon, Software S0249 | MITRE ATT&CK®

Archived: 2026-04-05 14:18:43 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Gold Dragon uses HTTP for communication to the control servers.[1]
Enterprise	T1560		Archive Collected Data	Gold Dragon encrypts data using Base64 before being sent to the command and control server.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Gold Dragon establishes persistence in the Startup folder.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Gold Dragon uses cmd.exe to execute commands for discovery.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Gold Dragon stores information gathered from the endpoint in a file named 1.hwp.[1]
Enterprise	T1083		File and Directory Discovery	Gold Dragon lists the directories for Desktop, program files, and the user’s recently accessed files.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or	Gold Dragon terminates anti-malware processes if they’re found running on the system.[1]

Domain	ID		Name	Use
			Modify Tools	
Enterprise	T1070	.004	Indicator Removal: File Deletion	Gold Dragon deletes one of its files, 2.hwp, from the endpoint after establishing persistence.[1]
Enterprise	T1105		Ingress Tool Transfer	Gold Dragon can download additional components from the C2 server.[1]
Enterprise	T1057		Process Discovery	Gold Dragon checks the running processes on the victim’s machine.[1]
Enterprise	T1012		Query Registry	Gold Dragon enumerates registry keys with the command `regkeyenum` and obtains information for the Registry key `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`. [1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Gold Dragon checks for anti-malware products and processes.[1]
Enterprise	T1082		System Information Discovery	Gold Dragon collects endpoint information using the `systeminfo` command.[1]
Enterprise	T1033		System Owner/User Discovery	Gold Dragon collects the endpoint victim's username and uses it as a basis for downloading additional components from the C2 server.[1]

Source: https://attack.mitre.org/software/S0249