

Covenant, Software S1155 | MITRE ATT&CK®

Archived: 2026-04-05 16:12:41 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Covenant can establish command and control via HTTP. ^[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Covenant can create PowerShell-based launchers for Grunt installation. ^[1]
		.003	Command and Scripting Interpreter: Windows Command Shell	Covenant provides access to a Command Shell in Windows environments for follow-on command execution and tasking. ^[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	Covenant can utilize SSL to encrypt command and control traffic. ^[1]
Enterprise	T1571		Non-Standard Port	Covenant listeners and controllers can be configured to use non-standard ports. ^[1]
Enterprise	T1218	.004	System Binary Proxy Execution: InstallUtil	Covenant can create launchers via an InstallUtil XML file to install new Grunt listeners. ^[1]
		.005	System Binary Proxy Execution: Mshta	Covenant can create HTA files to install Grunt listeners. ^[1]
		.010	System Binary Proxy Execution: Regsvr32	Covenant can create SCT files for installation via <code>Regsvr32</code> to deploy new Grunt listeners. ^[1]

Domain	ID	Name	Use
Enterprise	T1082	System Information Discovery	Covenant implants can gather basic information on infected systems. ^[1]
Enterprise	T1047	Windows Management Instrumentation	Covenant can utilize WMI to install new Grunt listeners through XSL files or command one-liners. ^[1]

Source: <https://attack.mitre.org/software/S1155>