Donut, Software S0695 | MITRE ATT&CK®

Archived: 2026-04-05 17:01:33 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Donut can use HTTP to download previously staged shellcode payloads.[1]
Enterprise	T1059		Command and Scripting Interpreter	Donut can generate shellcode outputs that execute via Ruby.[1]
		.001	PowerShell	Donut can generate shellcode outputs that execute via PowerShell.[1]
		.005	Visual Basic	Donut can generate shellcode outputs that execute via VBScript.[1]
		.006	Python	Donut can generate shellcode outputs that execute via Python.[1]
		.007	JavaScript	Donut can generate shellcode outputs that execute via JavaScript or JScript.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Donut can patch Antimalware Scan Interface (AMSI), Windows Lockdown Policy (WLDP), as well as exit-related Native API functions to avoid process termination.[1]
Enterprise	T1070		Indicator Removal	Donut can erase file references to payloads in-memory after being reflectively loaded and executed.[1]

Domain	ID		Name	Use
Enterprise	T1105		Ingress Tool Transfer	Donut can download and execute previously staged shellcode payloads.[1]
Enterprise	T1106		Native API	Donut code modules use various API functions to load and inject code.[1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Donut can generate packed code modules.[1]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	Donut can generate encrypted, compressed/encoded, or otherwise obfuscated code modules.[1]
		.015	Obfuscated Files or Information: Compression	Donut can generate encrypted, compressed/encoded, or otherwise obfuscated code modules.[1]
Enterprise	T1057		Process Discovery	Donut includes subprojects that enumerate and identify information about Process Injection candidates.[1]
Enterprise	T1055		Process Injection	Donut includes a subproject `DonutTest` to inject shellcode into a target process.[1]
Enterprise	T1620		Reflective Code Loading	Donut can generate code modules that enable in-memory execution of VBScript, JScript, EXE, DLL, and dotNET payloads.[1]

Source: https://attack.mitre.org/software/S0695