DnsSystem, Software S1021 | MITRE ATT&CK®

Archived: 2026-04-05 15:38:28 UTC

Domain	ID		Name	Use
Enterprise	T1071	.004	Application Layer Protocol: DNS	DnsSystem can direct queries to custom DNS servers and return C2 commands using TXT records.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	DnsSystem can write itself to the Startup folder to gain persistence.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	DnsSystem can use `cmd.exe` for execution.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	DnsSystem can Base64 encode data sent to C2.[1]
Enterprise	T1005		Data from Local System	DnsSystem can upload files from infected machines after receiving a command with `uploaddd` in the string.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	DnsSystem can exfiltrate collected data to its C2 server.[1]
Enterprise	T1105		Ingress Tool Transfer	DnsSystem can download files to compromised systems after receiving a command with the string `downloaddd`.[1]
Enterprise	T1033		System Owner/User Discovery	DnsSystem can use the Windows user name to create a unique identification for infected users and systems.[1]

Domain	ID		Name	Use
Enterprise	T1204	.002	User Execution: Malicious File	DnsSystem has lured victims into opening macro-enabled Word documents for execution.[1]

Source: https://attack.mitre.org/software/S1021