Pisloader, Software S0124 | MITRE ATT&CK®

Archived: 2026-04-05 15:03:57 UTC

Domain	ID		Name	Use
Enterprise	T1071	.004	Application Layer Protocol: DNS	Pisloader uses DNS as its C2 protocol.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Pisloader establishes persistence via a Registry Run key.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Pisloader uses cmd.exe to set the Registry Run key value. It also has a command to spawn a command shell.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Responses from the Pisloader C2 server are base32-encoded.[1]
Enterprise	T1083		File and Directory Discovery	Pisloader has commands to list drives on the victim machine and to list file information for a given directory.[1]
Enterprise	T1105		Ingress Tool Transfer	Pisloader has a command to upload a file to the victim machine.[1]
Enterprise	T1027		Obfuscated Files or Information	Pisloader obfuscates files by splitting strings into smaller sub-strings and including "garbage" strings that are never used. The malware also uses return-oriented programming (ROP) technique and single-byte XOR to obfuscate data.[1]
Enterprise	T1082		System Information Discovery	Pisloader has a command to collect victim system information, including the system name and OS

Domain	ID	Name	Use
			version.[1]
Enterprise	T1016	System Network Configuration Discovery	Pisloader has a command to collect the victim's IP address.[1]
