NanHaiShu, Software S0228 | MITRE ATT&CK®

Archived: 2026-04-05 17:50:13 UTC

Domain	ID		Name	Use
Enterprise	T1071	.004	Application Layer Protocol: DNS	NanHaiShu uses DNS for the C2 communications.[2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	NanHaiShu modifies the %regrun% Registry to point itself to an autostart mechanism.[2]
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	NanHaiShu executes additional VBScript code on the victim's machine. [2]
		.007	Command and Scripting Interpreter: JavaScript	NanHaiShu executes additional Jscript code on the victim's machine.[2]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	NanHaiShu can change Internet Explorer settings to reduce warnings about malware activity.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	NanHaiShu launches a script to delete their original decoy file to cover tracks. [2]
Enterprise	T1105		Ingress Tool Transfer	NanHaiShu can download additional files from URLs.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	NanHaiShu encodes files in Base64.[2]

Domain	ID		Name	Use
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	NanHaiShu uses mshta.exe to load its program and files.[2]
Enterprise	T1082		System Information Discovery	NanHaiShu can gather the victim computer name and serial number.[1]
Enterprise	T1016		System Network Configuration Discovery	NanHaiShu can gather information about the victim proxy server.[1]
Enterprise	T1033		System Owner/User Discovery	NanHaiShu collects the username from the victim.[2]
