Avaddon, Software S0640 | MITRE ATT&CK®

Archived: 2026-04-05 14:42:07 UTC

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Avaddon bypasses UAC using the CMSTPLUA COM interface.[2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Avaddon uses registry run keys for persistence.[2]
Enterprise	T1059	.007	Command and Scripting Interpreter: JavaScript	Avaddon has been executed through a malicious JScript downloader.[3][1]
Enterprise	T1486		Data Encrypted for Impact	Avaddon encrypts the victim system using a combination of AES256 and RSA encryption schemes.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Avaddon has decrypted encrypted strings.[2]
Enterprise	T1083		File and Directory Discovery	Avaddon has searched for specific files prior to encryption.[2]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Avaddon looks for and attempts to stop anti-malware solutions.[2]
Enterprise	T1490		Inhibit System Recovery	Avaddon deletes backups and shadow copies using native system tools.[3][2]

Domain	ID		Name	Use
Enterprise	T1112		Modify Registry	Avaddon modifies several registry keys for persistence and UAC bypass.[2]
Enterprise	T1106		Native API	Avaddon has used the Windows Crypto API to generate an AES key.[3]
Enterprise	T1135		Network Share Discovery	Avaddon has enumerated shared folders and mapped volumes.[2]
Enterprise	T1027		Obfuscated Files or Information	Avaddon has used encrypted strings.[2]
Enterprise	T1057		Process Discovery	Avaddon has collected information about running processes.[2]
Enterprise	T1489		Service Stop	Avaddon looks for and attempts to stop database processes.[2]
Enterprise	T1614	.001	System Location Discovery: System Language Discovery	Avaddon checks for specific keyboard layouts and OS languages to avoid targeting Commonwealth of Independent States (CIS) entities.[2]
Enterprise	T1016		System Network Configuration Discovery	Avaddon can collect the external IP address of the victim.[1]
Enterprise	T1047		Windows Management Instrumentation	Avaddon uses wmic.exe to delete shadow copies.[3]