Carbanak, Anunak, Group G0008 | MITRE ATT&CK®

Archived: 2026-04-05 15:24:12 UTC

Domain	ID		Name	Use
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Carbanak malware installs itself as a service to provide persistence and SYSTEM privileges.[1]
Enterprise	T1562	.004	Impair Defenses: Disable or Modify System Firewall	Carbanak may use netsh to add local firewall rule exceptions.[7]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	Carbanak has copied legitimate service names to use for malicious services.[1]
		.005	Masquerading: Match Legitimate Resource Name or Location	Carbanak has named malware "svchost.exe," which is the name of the Windows shared service host program.[1]
Enterprise	T1588	.002	Obtain Capabilities: Tool	Carbanak has obtained and used open-source tools such as PsExec and Mimikatz.[1]
Enterprise	T1219		Remote Access Tools	Carbanak used legitimate programs such as AmmyyAdmin and Team Viewer for remote interactive C2 to target systems.[7]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	Carbanak installs VNC server software that executes through rundll32.[1]
Enterprise	T1078		Valid Accounts	Carbanak actors used legitimate credentials of banking employees to perform operations that sent them millions of dollars.[1]

Domain	ID		Name	Use
Enterprise	T1102	.002	Web Service: Bidirectional Communication	Carbanak has used a VBScript named "ggldr" that uses Google Apps Script, Sheets, and Forms services for C2.[8]

Source: https://attack.mitre.org/groups/G0008