Carbon, Software S0335 | MITRE ATT&CK®

Archived: 2026-04-05 18:03:08 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Carbon can use HTTP in C2 communications.[3]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Carbon establishes persistence by creating a service and naming it based off the operating system version running on the current machine.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Carbon creates a base directory that contains the files and folders that are collected.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Carbon decrypts task and configuration files for execution.[1][3]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	Carbon has used RSA encryption for C2 communications.[3]
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Carbon uses HTTP to send data to the C2 server.[1]
Enterprise	T1095		Non-Application Layer Protocol	Carbon uses TCP and UDP for C2.[1]
Enterprise	T1027		Obfuscated Files or Information	Carbon encrypts configuration files and tasks for the malware to complete using CAST-128 algorithm.[1][3]

Domain	ID		Name	Use
Enterprise	T1069		Permission Groups Discovery	Carbon uses the `net group` command. [4]
Enterprise	T1057		Process Discovery	Carbon can list the processes on the victim's machine.[1]
Enterprise	T1055	.001	Process Injection: Dynamic-link Library Injection	Carbon has a command to inject code into a process.[1]
Enterprise	T1012		Query Registry	Carbon enumerates values in the Registry. [1]
Enterprise	T1018		Remote System Discovery	Carbon uses the `net view` command.[4]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Carbon creates several tasks for later execution to continue persistence on the victim's machine.[1]
Enterprise	T1016		System Network Configuration Discovery	Carbon can collect the IP address of the victims and other computers on the network using the commands: `ipconfig -all` `nbtstat -n` , and `nbtstat -s` .[1] [4]
Enterprise	T1049		System Network Connections Discovery	Carbon uses the `netstat -r` and `netstat -an` commands.[4]
Enterprise	T1124		System Time Discovery	Carbon uses the command `net time \127.0.0.1` to get information the system's time.[4]

Domain	ID	Name	Use
Enterprise	T1102	Web Service	Carbon can use Pastebin to receive C2 commands.[3]

Source: https://attack.mitre.org/software/S0335