Dyre, Software S0024 | MITRE ATT&CK®

Archived: 2026-04-05 17:51:32 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Dyre uses HTTPS for C2 communications.[1][2]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Dyre registers itself as a service by adding several Registry keys.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Dyre has the ability to create files in a TEMP folder to act as a database to store information.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Dyre decrypts resources needed for targeting the victim.[1][2]
Enterprise	T1041		Exfiltration Over C2 Channel	Dyre has the ability to send information staged on a compromised host externally to C2.[2]
Enterprise	T1105		Ingress Tool Transfer	Dyre has a command to download and executes additional files.[1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Dyre has been delivered with encrypted resources and must be unpacked for execution.[2]
Enterprise	T1055		Process Injection	Dyre has the ability to directly inject its code into the web browser process.[2]

Domain	ID		Name	Use
		.001	Dynamic-link Library Injection	Dyre injects into other processes to load modules.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Dyre has the ability to achieve persistence by adding a new task in the task scheduler to run every minute.[2]
Enterprise	T1518		Software Discovery	Dyre has the ability to identify installed programs on a compromised host.[2]
Enterprise	T1082		System Information Discovery	Dyre has the ability to identify the computer name, OS version, and hardware configuration on a compromised host.[2]
Enterprise	T1016		System Network Configuration Discovery	Dyre has the ability to identify network settings on a compromised host.[2]
Enterprise	T1033		System Owner/User Discovery	Dyre has the ability to identify the users on a compromised host.[2]
Enterprise	T1007		System Service Discovery	Dyre has the ability to identify running services on a compromised host.[2]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	Dyre can detect sandbox analysis environments by inspecting the process list and Registry.[1][2]

Source: https://attack.mitre.org/software/S0024