Linfo, Software S0211 | MITRE ATT&CK®

Archived: 2026-04-05 12:46:07 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Linfo creates a backdoor through which remote attackers can start a remote shell.[2]
Enterprise	T1005		Data from Local System	Linfo creates a backdoor through which remote attackers can obtain data from local systems.[2]
Enterprise	T1008		Fallback Channels	Linfo creates a backdoor through which remote attackers can change C2 servers.[2]
Enterprise	T1083		File and Directory Discovery	Linfo creates a backdoor through which remote attackers can list contents of drives and search for files.[2]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Linfo creates a backdoor through which remote attackers can delete files.[2]
Enterprise	T1105		Ingress Tool Transfer	Linfo creates a backdoor through which remote attackers can download files onto compromised hosts.[2]
Enterprise	T1057		Process Discovery	Linfo creates a backdoor through which remote attackers can retrieve a list of running processes.[2]

Domain	ID	Name	Use
Enterprise	T1029	Scheduled Transfer	Linfo creates a backdoor through which remote attackers can change the frequency at which compromised hosts contact remote C2 infrastructure.[2]
Enterprise	T1082	System Information Discovery	Linfo creates a backdoor through which remote attackers can retrieve system information.[2]

Source: https://attack.mitre.org/software/S0211/