Felismus, Software S0171 | MITRE ATT&CK®

Archived: 2026-04-05 13:10:58 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Felismus uses HTTP for C2.[2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Felismus uses command line for execution.[2]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Some Felismus samples use a custom method for C2 traffic that utilizes Base64.[2]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Some Felismus samples use a custom encryption method for C2 traffic that utilizes AES and multiple keys.[2]
Enterprise	T1105		Ingress Tool Transfer	Felismus can download files from remote servers.[2]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Felismus has masqueraded as legitimate Adobe Content Management System files.[3]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Felismus checks for processes associated with anti-virus vendors.[2]
Enterprise	T1082		System Information Discovery	Felismus collects the system information, including hostname and OS version, and sends it to the C2 server.[2]

Domain	ID	Name	Use
Enterprise	T1016	System Network Configuration Discovery	Felismus collects the victim LAN IP address and sends it to the C2 server.[2]
Enterprise	T1033	System Owner/User Discovery	Felismus collects the current username and sends it to the C2 server.[2]

Source: https://attack.mitre.org/software/S0171/