Metador, Group G1013 | MITRE ATT&CK®

Archived: 2026-04-05 17:22:13 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Metador has used HTTP for C2.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Metador has used the Windows command line to execute commands.[1]
Enterprise	T1546	.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	Metador has established persistence through the use of a WMI event subscription combined with unusual living-off-the-land binaries such as `cdb.exe`.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Metador has quickly deleted `cbd.exe` from a compromised host following the successful deployment of their malware.[1]
Enterprise	T1105		Ingress Tool Transfer	Metador has downloaded tools and malware onto a compromised system.[1]
Enterprise	T1095		Non-Application Layer Protocol	Metador has used TCP for C2.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Metador has encrypted their payloads.[1]
Enterprise	T1588	.001	Obtain Capabilities: Malware	Metador has used unique malware in their operations, including metaMain and Mafalda.[1]

Domain	ID		Name	Use
		.002	Obtain Capabilities: Tool	Metador has used Microsoft's Console Debugger in some of their operations.[1]

Source: https://attack.mitre.org/groups/G1013