Emissary, Software S0082 | MITRE ATT&CK®

Archived: 2026-04-05 18:39:16 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Emissary uses HTTP or HTTPS for C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Variants of Emissary have added Run Registry keys to establish persistence.[2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Emissary has the capability to create a remote shell and execute specified commands.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Emissary is capable of configuring itself as a service.[2]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	The C2 server response to a beacon sent by a variant of Emissary contains a 36-character GUID value that is used as an encryption key for subsequent network communications. Some variants of Emissary use various XOR operations to encrypt C2 data.[1]
Enterprise	T1615		Group Policy Discovery	Emissary has the capability to execute `gpresult`.[2]
Enterprise	T1105		Ingress Tool Transfer	Emissary has the capability to download files from the C2 server.[1]

Domain	ID		Name	Use
Enterprise	T1027	.001	Obfuscated Files or Information: Binary Padding	A variant of Emissary appends junk data to the end of its DLL file to create a large file that may exceed the maximum size that anti-virus programs can scan.[2]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	Variants of Emissary encrypt payloads using various XOR ciphers, as well as a custom algorithm that uses the "srand" and "rand" functions.[1][2]
Enterprise	T1069	.001	Permission Groups Discovery: Local Groups	Emissary has the capability to execute the command `net localgroup administrators`. [2]
Enterprise	T1055	.001	Process Injection: Dynamic-link Library Injection	Emissary injects its DLL file into a newly spawned Internet Explorer process.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	Variants of Emissary have used rundll32.exe in Registry values added to establish persistence. [2]
Enterprise	T1082		System Information Discovery	Emissary has the capability to execute ver and systeminfo commands.[2]
Enterprise	T1016		System Network Configuration Discovery	Emissary has the capability to execute the command `ipconfig /all`.[2]
Enterprise	T1007		System Service Discovery	Emissary has the capability to execute the command `net start` to interact with services. [2]

Source: https://attack.mitre.org/software/S0082