IronNetInjector, Software S0581 | MITRE ATT&CK®

Archived: 2026-04-05 18:00:38 UTC

Domain	ID		Name	Use
Enterprise	T1059	.006	Command and Scripting Interpreter: Python	IronNetInjector can use IronPython scripts to load payloads with the help of a .NET injector. [1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	IronNetInjector has the ability to decrypt embedded .NET and PE payloads.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	IronNetInjector has been disguised as a legitimate service using the name PythonUpdateSrvc.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	IronNetInjector can obfuscate variable names, encrypt strings, as well as base64 encode and Rijndael encrypt payloads.[1]
Enterprise	T1057		Process Discovery	IronNetInjector can identify processes via C# methods such as `GetProcessesByName` and running Tasklist with the Python `os.popen` function.[1]
Enterprise	T1055		Process Injection	IronNetInjector can use an IronPython scripts to load a .NET injector to inject a payload into its own or a remote process.[1]
		.001	Dynamic-link Library Injection	IronNetInjector has the ability to inject a DLL into running processes, including the IronNetInjector DLL into explorer.exe.[1]

Domain	ID		Name	Use
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	IronNetInjector has used a task XML file named `mssch.xml` to run an IronPython script when a user logs in or when specific system events are created.[1]

Source: https://attack.mitre.org/software/S0581/