PyDCrypt, Software S1032 | MITRE ATT&CK®

Archived: 2026-04-05 13:40:17 UTC

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	PyDCrypt has attempted to execute with PowerShell.[1]
		.003	Command and Scripting Interpreter: Windows Command Shell	PyDCrypt has used `cmd.exe` for execution.[1]
		.006	Command and Scripting Interpreter: Python	PyDCrypt, along with its functions, is written in Python.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	PyDCrypt has decrypted and dropped the DCSrv payload to disk.[1]
Enterprise	T1562	.004	Impair Defenses: Disable or Modify System Firewall	PyDCrypt has modified firewall rules to allow incoming SMB, NetBIOS, and RPC connections using `netsh.exe` on remote machines.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	PyDCrypt will remove all created artifacts such as dropped executables.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	PyDCrypt has dropped DCSrv under the `svchost.exe` name to disk.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	PyDCrypt has been compiled and encrypted with PyInstaller, specifically using the --key flag during the build phase. [1]

Domain	ID	Name	Use
Enterprise	T1049	System Network Connections Discovery	PyDCrypt has used netsh to find RPC connections on remote machines.[1]
Enterprise	T1033	System Owner/User Discovery	PyDCrypt has probed victim machines with `whoami` and has collected the username from the machine.[1]
Enterprise	T1047	Windows Management Instrumentation	PyDCrypt has attempted to execute with WMIC.[1]

Source: https://attack.mitre.org/software/S1032