Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:42:44 UTC

Tool: PyDCrypt

Names	PyDCrypt
Category	Malware
Type	Remote command, Loader
Description	(Check Point) The main goals of PyDCrypt are to infect other computers and to make sure the main payload, DCSrv, is executed properly. The executable is written in Python and compiled with PyInstaller with encryption, using the --key flag during the build phase. As we mentioned previously, the attackers build a new sample for each infected organization, and hardcode the parameters collected from the victim's environment.
Information	<https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1032/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool PyDCrypt

Changed	Name	Country	Observed	
Other groups				
	Moses Staff		2021-Nov 2022	

1 group listed (0 APT, 1 other, 0 unknown)