Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:11:00 UTC

Tool: StrongPity3

Names	StrongPity3
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Talos) StrongPity3 is the evolution of StrongPity2, with a few differences. The latter does not use libcurl anymore and now uses winhttp to perform all requests to C2. The usage of the HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key has a persistence mechanism that has been replaced by the creation of a service. This service changes its name from package to package. The service executable's only job is to launch the C2 contact module upon service startup. The remaining malware flow is the same on both versions.
Information	<https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html>

Last change to this tool card: 01 July 2020

Download this tool card in JSON format

All groups using tool StrongPity3

Changed	Name	Country	Observed	
APT groups				
	Promethium, StrongPity		2012-Nov 2021	

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