Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:19:05 UTC

Tool: StrongPity2

Names	StrongPity2
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Kasperksy) In this campaign, StrongPity updated its latest signature backdoor, named StrongPity2, and added more files to exfiltrate to its list of common Office and PDF documents, including Dagesh Pro Word Processor files used for Hebrew dotting, RiverCAD files used for river flow and bridge modelling, plain-text files, archives as well as GPG encrypted files and PGP keys.
Information	<https://securelist.com/apt-trends-report-q1-2020/96826/>

Last change to this tool card: 01 July 2020

Download this tool card in JSON format

All groups using tool StrongPity2

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

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