Threat Group Cards: A Threat Actor Encyclopedia

Tool: Truvasys

Names	Truvasys
Category	Malware
Type	Loader
Description	(Microsoft) A first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk.
Information	<https://www.microsoft.com/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0178/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool Truvasys

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

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