Threat Group Cards: A Threat Actor Encyclopedia

Tool: Cryptcat

Names	Cryptcat
Category	Tools
Type	Tunneling
Description	(FireEye) Four files tested in 2014 are based on the open-source project, cryptcat. Analysis of these cryptcat binaries indicates that the actor continually modified them to decrease AV detection rates. One of these files was deployed in a TEMP.Veles target's network. The compiled version with the least detections was later re-tested in 2017 and deployed less than a week later during TEMP.Veles activities in the target environment.
Information	<https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html> <http://cryptcat.sourceforge.net/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Cryptcat

Changed	Name	Country	Observed	
APT groups				
	TEMP.Veles		2014-Mar 2022	

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