Threat Group Cards: A Threat Actor Encyclopedia

Tool: BlueCore

Names	BlueCore
Category	Malware
Type	Backdoor, Downloader
Description	(Kaspersky) When inspecting the NewCore RAT malware delivered during the various attacks we investigated, we were able to distinguish between two variants. Both were deployed as side-loaded DLLs and shared multiple similarities, both in code and behavior. At the same time, we noticed differences that indicate the variants could have been used by different operators. Our analysis shows that the underlying pieces of malware and the way they were used form two clusters of activity. As a result, we named the variants BlueCore and RedCore and examined the artifacts we found around each one in order to profile their related clusters.
Information	<https://securelist.com/cycldek-bridging-the-air-gap/97157/>

Last change to this tool card: 15 May 2021

Download this tool card in JSON format

All groups using tool BlueCore

Changed	Name	Country	Observed	
APT groups				
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	

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