Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:20:19 UTC

Tool: DoubleT

Names	DoubleT
Category	Malware
Type	Backdoor
Description	(Kaspersky) This quarter, we described another CactusPete attack campaign which started in December 2019 In this campaign, the CactusPete threat actor used a new method to drop an updated version of the DoubleT backdoor onto the computers. The attackers implanted a new dropper module in the Microsoft Word Startup directory, most likely through a malicious document. This malicious dropper is responsible for dropping and executing a new version of the DoubleT backdoor, which utilizes a new method of encrypting the C2 server address.
Information	<https://securelist.com/apt-trends-report-q2-2020/97937/>

Last change to this tool card: 30 July 2020

Download this tool card in JSON format

All groups using tool DoubleT

Changed	Name	Country	Observed	
APT groups				
	Tonto Team, HartBeat, Karma Panda		2009-Apr 2023	

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