Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:29:04 UTC

Tool: DoubleFeature

Names	DoubleFeature
Category	Malware
Type	Reconnaissance
Description	(Check Point) To better understand the above structure and flow, we focused our research on a component of DanderSpritz named Doublefeature (or Df for short). According to its own internal documentation, this plugin “Generates a log & report about the types of tools that could be deployed on the target”; a lot of the framework tools, in their own internal documentation, make the chilling claim that DoubleFeature is the only way to confirm their existence on a compromised system. After some pause, we figured that at least this means DoubleFeature could be used as a sort of Rosetta Stone for better understanding DanderSpritz modules, and systems compromised by them. DoubleFeature effectively, well, doubles as a diagnostic tool for victim machines carrying DanderSpritz — It’s an incident response team’s pipe dream.
Information	<https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/>

Last change to this tool card: 25 January 2022

Download this tool card in JSON format

All groups using tool DoubleFeature

Changed	Name	Country	Observed	
APT groups				
	Equation Group		2001-Aug 2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a3223c7e-a8ba-4776-922a-ffdf1f1ec4fe