Threat Group Cards: A Threat Actor Encyclopedia

Tool: TABLEFLIP

Names	TABLEFLIP
Category	Malware
Type	Tunneling
Description	(Mandiant) To enable continued access directly from the Internet, the threat actor implemented TABLEFLIP (MD5: b6e92149efaf78e9ce7552297505b9d5), a passive traffic redirection utility that listens on all active interfaces for specialized command packets. With this utility in place, and regardless of the ACL's in place, the threat actor would be able to connect directly to the FortiManager as seen in Figure 15.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/fortinet-malware-ecosystem/>

Last change to this tool card: 26 August 2024

Download this tool card in JSON format

All groups using tool TABLEFLIP

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

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