Threat Group Cards: A Threat Actor Encyclopedia

Tool: FuxosDoor

Names	FuxosDoor
Category	Malware
Type	Backdoor
Description	(Trend Micro) FuxosDoor is an IIS backdoor which was deployed and ran on the compromised exchange server. Once it receives a request with a specific URL path, /web.config from the attacker, it will try to extract the encrypted command from the field (ASP.NET_SessionId) in the HTTP header and then execute the received command by using the command prompt (cmd.exe). After, the results will be encrypted and sent back to the attacker's server.
Information	<https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html>

Last change to this tool card: 26 December 2024

Download this tool card in JSON format

All groups using tool FuxosDoor

Changed	Name	Country	Observed	
APT groups				
	Salt Typhoon, GhostEmperor		2020-Feb 2025	

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