Threat Group Cards: A Threat Actor Encyclopedia

Tool: FoggyWeb

Names	FoggyWeb
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Microsoft) FoggyWeb is a passive and highly targeted backdoor capable of remotely exfiltrating sensitive information from a compromised AD FS server. It can also receive additional malicious components from a command-and-control (C2) server and execute them on the compromised server.
Information	<https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0661/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool FoggyWeb

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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