

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:17:22 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool MagicWeb

Tool: MagicWeb

Names	MagicWeb
Category	Malware
Type	Backdoor
Description	(Microsoft) MagicWeb goes beyond the collection capabilities of FoggyWeb by facilitating covert access directly. MagicWeb is a malicious DLL that allows manipulation of the claims passed in tokens generated by an Active Directory Federated Services (AD FS) server. It manipulates the user authentication certificates used for authentication, not the signing certificates used in attacks like Golden SAML.
Information	< https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/ >

Last change to this tool card: 12 September 2022

Download this tool card in [JSON](#) format

All groups using tool MagicWeb

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

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4785839c-bd5f4eee-a4ad-d18415ac2300>