Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:44:31 UTC

Tool: BloodHound

Names	BloodHound
Category	Tools
Type	Reconnaissance
Description	(PenTestPartners) BloodHound is an application used to visualize active directory environments. The front-end is built on electron and the back-end is a Neo4j database, the data leveraged is pulled from a series of data collectors also referred to as ingestors which come in PowerShell and C# flavours. It can be used on engagements to identify different attack paths in Active Directory (AD), this encompasses access control lists (ACLs), users, groups, trust relationships and unique AD objects. The tool can be leveraged by both blue and red teams to find different paths to targets. The subsections below explain the different and how to properly utilize the different ingestors.
Information	<https://www.pentestpartners.com/security-blog/bloodhound-walkthrough-a-tool-for-many-tradecrafts/> <https://github.com/BloodHoundAD/BloodHound>
MITRE ATT&CK	<https://attack.mitre.org/software/S0521/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool BloodHound

Changed	Name	Country	Observed	
APT groups				
	APT 20, Violin Panda		2014-2017	

	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	●
	Stone Panda, APT 10, menuPass		2006-Mar 2025	●
	TA2101, Maze Team	[Unknown]	2019-Feb 2024	●
	Traveling Spider	[Unknown]	2019-Mar 2021	
	UNC2447	[Unknown]	2020	
	Wizard Spider, Gold Blackburn		2014-May 2025	●

7 groups listed (7 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2bfed9a7-09bb-469b-a297-c7d6f39a0df7