


Cyber Berkut - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:56:12 UTC

APT group: Cyber Berkut

Names	Cyber Berkut (<i>self given</i>) Kiberberkut (<i>self given</i>)	
Country	 Russia	
Motivation	Information theft and espionage , Sabotage and destruction	
First seen	2014	
Description	<p>(Recorded Future) Recorded Future has collected threat intelligence on the hacking activities of Cyber Berkut for over a year, aligning with the first month of ground fighting in Ukraine, at which time the group began coordinated cyber attacks. This article presents temporal and technical analysis of these activities, based on open source intelligence (OSINT) from the Web. Appropriating the Ukrainian special police force name and logo, the group has aligned itself as pro-Russian, anti-Ukrainian, and most recently attacked Western intervention efforts in the Ukrainian conflict. While the group has taken Ukrainian identities, technical links and contextual analysis connect the group to Russia.</p> <p>The group began with successful distributed denial of service (DDoS) attacks on multiple NATO websites just as separatists in the physical world were beginning to storm military buildings. Since their initial attacks the group has continued to take down websites, and most recently leaked confidential documents between US billionaire George Soros and the Ukrainian prime minister and president which contained plans for Western intervention.</p>	
Observed	Sectors: Defense , Financial , Government . Countries: Estonia , Germany , Ukraine , USA , NATO .	
Tools used		
Operations performed	Mar 2014	Nato websites disabled by cyber attack on eve of Crimea vote < https://www.ft.com/content/b822d5cc-ace6-11e3-8ba3-00144feab7de >
	Jul 2014	'Cyber Berkut' Hackers Target Major Ukrainian Bank < https://www.themoscowtimes.com/2014/07/04/cyber-berkut-

	hackers-target-major-ukrainian-bank-a37033 >
Jan 2015	German government websites, including Chancellor Angela Merkel's page, were hacked on Wednesday in an attack claimed by a group demanding Berlin end support for the Ukrainian government, shortly before their leaders were to meet. < https://www.reuters.com/article/us-germany-cyberattack/pro-russian-group-claims-cyber-attack-on-german-government-websites-idUSKBN0KG15320150107 >
May 2015	Cyber Berkut Graduates From DDoS Stunts to Purveyor of Cyber Attack Tools < https://www.recordedfuture.com/cyber-berkut-analysis/ >
Information	< https://www.recordedfuture.com/cyber-berkut-analysis/ > < https://en.wikipedia.org/wiki/CyberBerkut >

Last change to this card: 19 April 2020

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=c375b720-a3ec-464a-a81d-891c24f3e325>