Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:47:59 UTC

Tool: CloudDuke

Names	CloudDuke Cloud Duke MiniDionis CloudLook
Category	Malware
Type	Backdoor, Loader, Downloader
Description	(F-Secure) In the beginning of July 2015, the Dukes embarked on yet another large-scale phishing campaign. The malware toolset used for this campaign was the previously unseen CloudDuke and we believe that the July campaign marks the first time that this toolset was deployed by the Dukes, other than possible small-scale testing. The CloudDuke toolset consists of at least a loader, a downloader, and two backdoor variants. Both backdoors (internally referred to by their authors as “BastionSolution” and “OneDriveSolution”) essentially allow the operator to remotely execute commands on the compromised machine. The way in which each backdoor does so however is significantly different. While the BastionSolution variant simply retrieves commands from a hard-coded C&C server controlled by the Dukes, the OneDriveSolution utilizes Microsoft’s OneDrive cloud storage service for communicating with its masters, making it significantly harder for defenders to notice the traffic and block the communication channel. What is most significant about the July 2015 CloudDuke campaign is the timeline. The campaign appeared to consist of two distinct waves of spear-phishing, one during the first days of July and the other starting from the 20th of the month. Details of the first wave, including a thorough technical analysis of CloudDuke, was published by Palo Alto Networks on 14th July. This was followed by additional details from Kaspersky in a blog post published on 16th July.
Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0054/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cloud_duke>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:CloudDuke>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool CloudDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	
	Turla, Waterbug, Venomous Bear		1996-2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=806c8a75-8ce9-483d-8bbc-8c63978ed378