Stealth Falcon, FruityArmor - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:04:19 UTC

APT group: Stealth Falcon, FruityArmor

Names	Stealth Falcon *(Citizen Lab)* FruityArmor *(Kaspersky)* Project Raven *(Reuters)* G0038 *(MITRE)*
Country	UAE
Motivation	Information theft and espionage
First seen	2012

Description	(Citizen Lab) This report describes a campaign of targeted spyware attacks carried out by a sophisticated operator, which we call Stealth Falcon. The attacks have been conducted from 2012 until the present, against Emirati journalists, activists, and dissidents. We discovered this campaign when an individual purporting to be from an apparently fictitious organization called “The Right to Fight” contacted Rori Donaghy. Donaghy, a UK-based journalist and founder of the Emirates Center for Human Rights, received a spyware-laden email in November 2015, purporting to offer him a position on a human rights panel. Donaghy has written critically of the United Arab Emirates (UAE) government in the past, and had recently published a series of articles based on leaked emails involving members of the UAE government. Circumstantial evidence suggests a link between Stealth Falcon and the UAE government. We traced digital artifacts used in this campaign to links sent from an activist’s Twitter account in December 2012, a period when it appears to have been under government control. We also identified other bait content employed by this threat actor. We found 31 public tweets sent by Stealth Falcon, 30 of which were directly targeted at one of 27 victims. Of the 27 targets, 24 were obviously linked to the UAE, based on their profile information (e.g., photos, “UAE” in account name, location), and at least six targets appeared to be operated by people who were arrested, sought for arrest, or convicted in absentia by the UAE government, in relation to their Twitter activity.	
Observed	Sectors: Civil society groups and Emirati journalists, activists and dissidents. Countries: Netherlands, Saudi Arabia, Thailand, UAE, UK.	
Tools used	Deadglyph, StealthFalcon and 0-day exploits.	
Operations performed	2014	Ex-NSA operatives reveal how they helped spy on targets for the Arab monarchy — dissidents, rival leaders and journalists. <https://www.reuters.com/investigates/special-report/usa-spying-raven/>
	Oct 2016	Windows zero-day exploit used in targeted attacks by FruityArmor APT <https://securelist.com/windows-zero-day-exploit-used-in-targeted-attacks-by-fruityarmor-apt/76396/>
	Oct 2018	Zero-day exploit (CVE-2018-8453) used in targeted attacks <https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/>
	Oct 2018	Zero-day in Windows Kernel Transaction Manager (CVE-2018-8611) <https://securelist.com/zero-day-in-windows-kernel-transaction-

		manager-cve-2018-8611/89253/>
	Sep 2019	ESET researchers discovered a backdoor linked to malware used by the Stealth Falcon group, an operator of targeted spyware attacks against journalists, activists and dissidents in the Middle East. <https://www.welivesecurity.com/2019/09/09/backdoor-stealth-falcon-group/>
	2023	Stealth Falcon preying over Middle Eastern skies with Deadglyph <https://www.welivesecurity.com/en/eset-research/stealth-falcon-preying-middle-eastern-skies-deadglyph/>
	Mar 2025	Inside Stealth Falcon’s Espionage Campaign Using a Microsoft Zero-Day <https://blog.checkpoint.com/research/inside-stealth-falcons-espionage-campaign-using-a-microsoft-zero-day/>
Information	<https://citizenlab.ca/2016/05/stealth-falcon/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0038/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
