Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:53:58 UTC

APT group: Cadelle

Names	Cadelle *(Symantec)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2011
Description	(Symantec) Symantec telemetry identified Cadelle and Chafer, APT 39 activity dating from as far back as July 2014, however, it's likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people. There is evidence to suggest that the two teams may be connected in some way, though we cannot confirm this. A number of computers experienced both Cadelspy and Remexi infections within a small time window. In one instance, a computer was compromised with Backdoor.Cadelspy just minutes after being infected with Backdoor.Remexi. The Cadelle and Chafer groups also keep the same working hours and focus on similar targets. However, no sharing of C&C infrastructure between the teams has been observed. If Cadelle and Chafer are not directly linked, then they may be separately working for a single entity. Their victim profile may be of interest to a nation state.
Observed	Countries: Germany, Iran, Iraq, Netherlands, Pakistan, Saudi Arabia, Singapore, Sudan, Tajikistan, Thailand, Turkey, UAE, UK, USA.
Tools used	Antak, Cadelspy.
Information	<https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets>

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format