Nitro, Covert Grove - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:32:32 UTC

APT group: Nitro, Covert Grove

Names	Nitro *(Symantec)* Covert Grove *(Symantec)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2011	
Description	(Symantec) The Nitro Attacks: Stealing Secrets from the Chemical Industry The attackers have changed their targets over time. From late April to early May, the attackers focused on hu rights related NGOs. They then moved on to the motor industry in late May. From June until mid-July no act was detected. At this point, the current attack campaign against the chemical industry began. This particular a has lasted much longer than previous attacks, spanning two and a half months. A total of 29 companies in the chemical sector were confirmed to be targeted in this attack wave and another various other sectors, primarily the defense sector, were seen to be affected as well. These 48 companies are t minimum number of companies targeted and likely other companies were also targeted. In a recent two week period, 101 unique IP addresses contacted a command and control server with traffic consistent with an infec machine. These Ips represented 52 different unique Internet Service Providers or organizations in 20 countrie Nitro may be related to APT 18, Dynamite Panda, Wekby.	
Observed	Sectors: Automotive, Chemical, NGOs, Technology. Countries: Argentina, Bangladesh, Canada, China, Czech, Finland, France, Germany, Hong Kong, India, Japa Netherlands, Norway, Russia, Singapore, South Korea, Sweden, Taiwan, UK, USA.	
Tools used	Gh0st RAT, PCClient, Poison Ivy, Spindest.	
Operations performed	Jul 2014	New Indicators of Compromise found Historically, Nitro is known for targeted spear phishing campaigns and using Poison Ivy malwa which was not seen in these attacks. Since at least 2013, Nitro appears to have somewhat modif their malware and delivery methods to include Spindest and legitimate compromised websites, a reported by Cyber Squared's TCIRT. <https://unit42.paloaltonetworks.com/new-indicators-compromise-apt-group-nitro-uncovered/>
Information	<https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks <https://blog.trendmicro.com/trendlabs-security-intelligence/the-significance-of-the-nitro-attacks/>	

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format