Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:39:23 UTC

APT group: Suckfly

Names	Suckfly *(Symantec)* G0039 *(MITRE)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2014	
Description	(Symantec) In March 2016, Symantec published a blog on Suckfly, an advanced cyberespionage group that conducted attacks against a number of South Korean organizations to steal digital certificates. Since then we have identified a number of attacks over a two-year period, beginning in April 2014, which we attribute to Suckfly. The attacks targeted high-profile targets, including government and commercial organizations. These attacks occurred in several different countries, but our investigation revealed that the primary targets were individuals and organizations primarily located in India. While there have been several Suckfly campaigns that infected organizations with the group's custom malware Backdoor.Nidiran, the Indian targets show a greater amount of post-infection activity than targets in other regions. This suggests that these attacks were part of a planned operation against specific targets in India.	
Observed	Sectors: Entertainment, Financial, Government, Healthcare, Media, Shipping and Logistics and E-commerce, Software development and Video game development. Countries: India.	
Tools used	gsecdump, Nidiran, smbscan, Windows Credentials Editor.	
Operations performed	Apr 2014	The first known Suckfly campaign began in April of 2014. During our investigation of the campaign, we identified a number of global targets across several industries who were attacked in 2015. Many of the targets we identified were well known commercial organizations located in India. <https://www.symantec.com/connect/blogs/indian-organizations-targeted-suckfly-attacks>

	Late 2015	We discovered Suckfly, an advanced threat group, conducting targeted attacks using multiple stolen certificates, as well as hacktools and custom malware. The group had obtained the certificates through pre-attack operations before commencing targeted attacks against a number of government and commercial organizations spread across multiple continents over a two-year period. This type of activity and the malicious use of stolen certificates emphasizes the importance of safeguarding certificates to prevent them from being used maliciously. <https://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0039/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
