

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:51:00 UTC

APT group: Sowbug

Names	Sowbug (<i>Symantec</i>) G0054 (<i>MITRE</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2015
Description	<p>(Symantec) Symantec has identified a previously unknown group called Sowbug that has been conducting highly targeted cyberattacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates.</p> <p>Symantec saw the first evidence of Sowbug-related activity with the discovery in March 2017 of an entirely new piece of malware called Felismus used against a target in Southeast Asia. We have subsequently identified further victims on both sides of the Pacific Ocean. While the Felismus tool was first identified in March of this year, its association with Sowbug was unknown until now. Symantec has also been able to connect earlier attack campaigns with Sowbug, demonstrating that it has been active since at least early-2015 and may have been operating even earlier.</p> <p>To date, Sowbug appears to be focused mainly on government entities in South America and Southeast Asia and has infiltrated organizations in Argentina, Brazil, Ecuador, Peru, Brunei and Malaysia. The group is well resourced, capable of infiltrating multiple targets simultaneously and will often operate outside the working hours of targeted organizations in order to maintain a low profile.</p>
Observed	Sectors: Government . Countries: Argentina , Brazil , Brunei , Ecuador , Malaysia , Peru .
Tools used	Felismus , StarLoader .
Information	< https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments >
MITRE ATT&CK	< https://attack.mitre.org/groups/G0054/ >

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.eta.or.th/cgi-bin/showcard.cgi?u=76db0506-25f4-4b80-90aa-032d0a8345fe>