


Strider, ProjectSauron - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:40:23 UTC

[Home](#) > [List all groups](#) > Strider, ProjectSauron

APT group: Strider, ProjectSauron

Names	Strider (<i>Symantec</i>) ProjectSauron (<i>Kaspersky</i>) G0041 (<i>MITRE</i>)
Country	 USA
Motivation	Information theft and espionage
First seen	2011
Description	<p>(Symantec) Strider has been active since at least October 2011. The group has maintained a low profile until now and its targets have been mainly organizations and individuals that would be of interest to a nation state's intelligence services. Symantec obtained a sample of the group's Remsec malware from a customer who submitted it following its detection by our behavioral engine.</p> <p>Remsec is primarily designed to spy on targets. It opens a back door on an infected computer, can log keystrokes, and steal files.</p> <p>Strider has been highly selective in its choice of targets and, to date, Symantec has found evidence of infections in 36 computers across seven separate organizations. The group's targets include a number of organizations and individuals located in Russia, an airline in China, an organization in Sweden, and an embassy in Belgium.</p>
Observed	<p>Sectors: Defense, Embassies, Financial, Government, Telecommunications and Scientific research centers.</p> <p>Countries: Belgium, China, Iran, Russia, Rwanda, Sweden.</p>
Tools used	Remsec .
Information	<p><https://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets></p> <p><https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf></p>

MITRE ATT&CK

<<https://attack.mitre.org/groups/G0041/>>

Last change to this card: 16 August 2025

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

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=d7d99de3-c515-4117-b40c-7696babb69c1>