Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:11:53 UTC

APT group: Slingshot

Names	Slingshot *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2012
Description	(Kaspersky) While nalyzing an incident which involved a suspected keylogger, we identified a malicious library able to interact with a virtual file system, which is usually the sign of an advanced APT actor. This turned out to be a malicious loader internally named 'Slingshot', part of a new, and highly sophisticated attack platform that rivals Project Sauron and Regin in complexity. While for most victims the infection vector for Slingshot remains unknown, we were able to find several cases where the attackers got access to MikroTik routers and placed a component downloaded by Winbox Loader, a management suite for MikroTik routers. In turn, this infected the administrator of the router. We believe this cluster of activity started in at least 2012 and was still active at the time of this analysis (February 2018).
Observed	Countries: Afghanistan, Congo, Iraq, Jordan, Kenya, Libya, Somalia, Sudan, Tanzania, Turkey, Yemen.
Tools used	Cahnadr, GollumApp, Slingshot and WinBox (a utility used for MikroTik router configuration).
Information	<https://securelist.com/apt-slingshot/84312/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format