Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:35:34 UTC

Tool: Slingshot

Names	Slingshot
Category	Malware
Type	Loader
Description	(Kaspersky) While analysing 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. The initial loader replaces the victim´s legitimate Windows library ‘scesrv.dll’ with a malicious one of exactly the same size. Not only that, it interacts with several other modules including a ring-0 loader, kernel-mode network sniffer, own base-independent packer, and virtual filesystem, among others. Following infection, Slingshot would load a number of modules onto the victim device, including two huge and powerful ones: Cahnadr, the kernel mode module, and GollumApp, a user mode module. The two modules are connected and able to support each other in information gathering, persistence and data exfiltration.
Information	<https://securelist.com/apt-slingshot/84312/> <https://s3-eu-west-1.amazonaws.com/khub-media/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.slingshot>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Slingshot

Changed	Name	Country	Observed

APT groups

	Slingshot	[Unknown]	2012	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=24bf0029-00d6-4eb3-9410-922221a07e36