Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:33:38 UTC

Tool: Soraya

Names	Soraya
Category	Malware
Type	POS malware, Reconnaissance, Credential stealer
Description	(Trend Micro) Soraya is a Dexter-and-Zeus-inspired PoS RAM scraper variant first discovered in June 2014. It is custom-packed to obfuscate its code and to make it difficult for security researchers to reverse-engineer its binary. When first executed, Soraya injects its code into several running processes. It borrowed tricks from ZeuS and hooks the NtResumeThread API, which is called by Windows to execute new processes. It then injects its code into all newly created processes. It also copies itself to the %APPDATA% directory and adds itself to an Auto Start runkey to remain persistent.
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://www.codeandsec.com/Soraya-Malware-Analysis-Dropper> <https://www.arbornetworks.com/blog/asert/the-best-of-both-worlds-soraya/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.soraya>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool Soraya

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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