Salty Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:05:29 UTC

Other threat group: Salty Spider

Names	Salty Spider *(CrowdStrike)*	
Country	Russia	
Motivation	Financial gain	
First seen	2003	
Description	(CrowdStrike) The pervasiveness of Salty Spider's attacks has resulted in a long list of victims across the globe. While it seems, for the most part, that this adversary doesn't single out particular nations and industries, there do appear to be a few pockets where SALTY SPIDER may be more prevalent. In 2017, SALTY SPIDER ceased propagation of traditional proxy and spambot payloads, and shifted its sights towards the mining and theft of cryptocurrencies. This shift is likely an indicator that the cryptocurrency industry has proven to be a more lucrative area for monetizing Sality.	
Observed	Countries: Worldwide.	
Tools used	Sality.	
Operations performed	Apr 2014	DNS hijacking is still going strong and the Win32/Sality operators have added this technique to their long-lasting botnet. This blog post describes how the malware guesses router passwords as part of its campaign to misdirect users, send spam and infect new victims. <https://www.welivesecurity.com/2014/04/02/win32sality-newest-component-a-routers-primary-dns-changer-named-win32rbrute/>
	Dec 2018	Sality has terrorized computer users since 2003, a year when personal digital assistants (PDAs) made tech headlines and office PCs ran Windows XP. Over the intervening years users traded their PDAs for smartphones and desktops migrated to newer operating systems and digital workplace solutions. Sality, however, survived the breakneck pace of technological innovation and continues to threaten organizations today.

		<https://threatvector.cylance.com/en_us/home/cylance-vs-sality-malware.html>
Information	<https://www.crowdstrike.com/blog/who-is-salty-spider/> <https://en.wikipedia.org/wiki/Sality>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
