Narwhal Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:48:11 UTC

Other threat group: Narwhal Spider

Names	Narwhal Spider *(CrowdStrike)* Gold Essex *(SecureWorks)* Storm-0302 *(Microsoft)*	
Country	[Unknown]	
Motivation	Financial gain	
First seen	2007	
Description	(CrowdStrike) CrowdStrike Falcon Intelligence has observed a new Cutwail spam campaign from NARWHAL SPIDER on 24 October 2018. NARWHAL SPIDER is the adversary name designated by Falcon Intelligence for the criminal operator of Cutwail version 2. NARWHAL SPIDER primarily provides spam services with a large customer base that has included malware operators such as Wizard Spider, Gold Blackburn (developer of TrickBot), affiliates of BAMBOO SPIDER (developer of Panda Zeus), and many others including URLZone, Nymaim and Gozi ISFB. The targets and payloads delivered through Cutwail spam campaigns are determined by the customers of NARWHAL SPIDER. Cutwail has been observed to distribute Dyre (Wizard Spider, Gold Blackburn), Zeus Panda (Bamboo Spider, TA544) and much of the malware from TA505, Graceful Spider, Gold Evergreen.	
Observed	Countries: Worldwide.	
Tools used	Cutwail.	
Operations performed	Aug 2011	Cutwail botnet resurfaces in major Facebook scam-paign <https://www.infosecurity-magazine.com/news/cutwail-botnet-resurfaces-in-major-facebook-scam/>
	Oct 2013	Without the Blackhole exploit kit around to inject malware such as the Zeus Trojan, keepers of the Cutwail spam bot have been forced to

		resort to some old-school methods of sending malware such as direct email attachments. <https://threatpost.com/cutwail-botnet-feeling-effects-of-blackhole-takedown/103228/> <https://www.secureworks.com/blog/cutwail-spam-swapping-blackhole-for-magnitude-exploit-kit>
	Oct 2018	The Japanese-language spam campaign uses a mixture of malicious PowerShell (PS) and steganography — a method of sending data in a concealed format — to distribute the eCrime malware family URLZone (a.k.a. Bebloh). <https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/>
Counter operations	Aug 2010	Security researchers have dealt a mighty blow to a spam botnet known as Pushdo, a massive grouping of hacked PCs that until recently was responsible for sending more than 10 percent of all junk e-mail worldwide. <https://krebsonsecurity.com/2010/08/researchers-kneecap-pushdo-spam-botnet/>
Information	<https://blog.malwaremustdie.org/2013/05/a-story-of-spambot-trojan-via-fake.html> <https://blog.avast.com/2013/06/25/15507/> <https://en.wikipedia.org/wiki/Cutwail_botnet>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
