Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:34:12 UTC

APT group: Sweed

Names	Sweed *(Talos)*	
Country	[Unknown]	
Motivation	Information theft and espionage	
First seen	2017	
Description	(Talos) Cisco Talos recently identified a large number of ongoing malware distribution campaigns linked to a threat actor we're calling "SWEED," including such notable malware as Formbook, Lokibot and Agent Tesla. Based on our research, SWEED — which has been operating since at least 2017 — primarily targets their victims with stealers and remote access trojans. SWEED remains consistent across most of their campaigns in their use of spear-phishing emails with malicious attachments. While these campaigns have featured a myriad of different types of malicious documents, the actor primarily tries to infect its victims with a packed version of Agent Tesla — an information stealer that's been around since at least 2014. The version of Agent Tesla that SWEED is using differs slightly from what we've seen in the past in the way that it is packed, as well as how it infects the system. In this post, we'll run down each campaign we're able to connect to SWEED, and talk about some of the actor's tactics, techniques and procedures (TTPs).	
Observed	Sectors: Defense, Energy, Financial, Shipping and Logistics, Manufacturing and Human Resources. Countries: Bosnia and Herzegovina, Canada, China, Djibouti, France, Germany, Hong Kong, India, Italy, Monaco, Russia, Qatar, Singapore, South Africa, South Korea, Switzerland, Taiwan, Turkey, UAE, UK, USA.	
Tools used	Agent Tesla, Formbook, LokiBot, RDP.	
Operations performed	2017	Steganography One of the earliest SWEED campaigns Talos identified dates back to 2017. In this attack, the actors placed droppers inside of ZIP archives, and then attached those ZIPs to emails. The attachments usually had file names similar to "Java_Updater.zip" or "P-O of Jun2017.zip".

	Jan 2018	In early 2018, we observed that SWEED began leveraging Java-based droppers. Similar to previous campaigns, the JAR was directly attached to emails and used file names such as “Order_2018.jar”. The purpose of the JAR was to obtain information about the infected system and facilitate the download of a packed version of Agent Tesla.
	Apr 2018	In April 2018, SWEED began making use of a previously disclosed Office exploit. One of the documents featured in these email campaigns was notable because it was a PowerPoint document (PPXS). Code contained inside one of the slides triggers an exploit for CVE-2017-8759, a remote code execution vulnerability in Microsoft .NET framework.
	May 2018	In May 2018, campaigns being conducted by SWEED began leveraging another vulnerability in Microsoft Office: CVE-2017-11882, a remote code execution bug in Microsoft Office that is commonly observed being leveraged in malicious documents used in commodity malware distribution.
	2019	Beginning in 2019, the campaigns associated with SWEED began leveraging malicious Office macros. As with previous attacks, they are leveraging spear-phishing emails and malicious attachments to initiate the infection process. <https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html>
Information	<https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
