Smoky Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:56:55 UTC

Other threat group: Smoky Spider

Names	Smoky Spider *(CrowdStrike)*	
Country	[Unknown]	
Motivation	Financial gain	
First seen	2011	
Description	(IBM) According to 360 NetLab, the (relatively) ancient malware downloader has enjoyed a slow burn on the black market, where malicious actors can pick up a customized copy for $850. While other researchers have identified various aspects of the threat, 360 NetLab took aim at the malware's admin panel, which offers support for multiple plugins and functions — such as FORM GRAB, BOT LIST, KEYLOGGER and more — designed to help attackers successfully infiltrate targeted devices. The flexibility of Smoke Loader remains its biggest appeal; it was among the top 10 malware threats detected by Check Point in December 2018. It's the first time a second-stage downloader has made the list, and may indicate a coming shift in the threat profiles of typical malware attacks. Smoke Loader has been observed to distribute DoppelPaymer (Doppel Spider), TinyLoader (Tiny Spider), DanaBot (Scully Spider, TA547), BokBot (Lunar Spider), Zeus Panda (Bamboo Spider, TA544) and TrickBot (Wizard Spider, Gold Blackburn).	
Observed	Countries: Worldwide.	
Tools used	Smoke Loader, Sasfis.	
Operations performed	2015	Smoke Loader – downloader with a smokescreen still alive <https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/>
	Apr 2018	Smoke Loader malware improves after Microsoft spoils its Campaign <https://www.spamhaus.org/news/article/774/smoke-loader-malware-improves-after-microsoft-spoils-its-campaign>

	Jun 2018	Smoking Guns - Smoke Loader learned new tricks <https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html>
	Jul 2018	The Cylance Threat Research team recently dissected a resurgent form of Smoke Loader. Our investigation uncovered two other samples of malware working with Smoke Loader: a document packed with malicious macros, and Trickbot, a banking Trojan. <https://threatvector.cylance.com/en_us/home/threat-spotlight-resurgent-smoke-loader-malware-dissected.html>
	Nov 2018	Analysis of Smoke Loader in New Tsunami Campaign <https://unit42.paloaltonetworks.com/analysis-of-smoke-loader-in-new-tsunami-campaign/>
	Apr 2019	Proofpoint observed that the malware returned to regular attacks against German and Swiss users in April 2019 after taking a hiatus in 2018. These campaigns helped reveal several new techniques now employed by the banking Trojan. One geographically targeted campaign against Switzerland, for instance, used an Object Linking and Embedding (OLE) package to deliver Smoke Loader. This threat, in turn, downloaded Retefe two hours after infection. <https://securityintelligence.com/news/retefe-banking-trojan-returns-with-smoke-loader-as-its-intermediate-loader/>
Counter operations	Mar 2018	Behavior monitoring combined with machine learning spoils a massive Dofoil coin mining campaign <https://www.microsoft.com/security/blog/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/>
Information	<https://www.webroot.com/blog/2012/02/03/a-peek-inside-the-smoke-malware-loader/> <https://www.cert.pl/en/news/single/dissecting-smoke-loader/> <https://blog.netlab.360.com/smoke-loader-the-core-files-the-admin-panel-the-plugins-and-the-3rd-party-patch/> <https://securityintelligence.com/news/smoke-loader-botnet-still-active-on-black-market-after-8-years/>	

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
