Smoke Loader - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:28:52 UTC

Tool: Smoke Loader

Names	Smoke Loader SmokeLoader Smoke Dofoil Sharik
Category	Malware
Type	Botnet, Downloader, Miner
Description	The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body. SmokeLoader, in addition to being used to download standalone coinminers, is available on underground markets with a built-in coinminer module for an additional fee.
Information	<https://unit42.paloaltonetworks.com/analysis-of-smoke-loader-in-new-tsunami-campaign/> <https://cloudblogs.microsoft.com/microsoftsecure/2018/04/04/hunting-down-dofoil-with-windows-defender-atp/> <https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet/> <https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html> <https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/> <https://info.phishlabs.com/blog/smoke-loader-adds-additional-obfuscation-methods-to-mitigate-analysis> <https://www.spamhaus.org/news/article/774/smoke-loader-improves-encryption-after-

	microsoft-spoils-its-campaign> <https://eternal-todo.com/blog/smokeloader-analysis-yulia-photo> <https://blog.malwarebytes.com/cybercrime/2018/01/fake-spectre-and-meltdown-patch-pushes-smoke-loader/> <https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/> <https://int0xcc.svbtle.com/a-taste-of-our-own-medicine-how-smokeloader-is-deceiving-dynamic-configuration-extraction-by-using-binary-code-as-bait> <https://www.cert.pl/en/news/single/dissecting-smoke-loader/> <https://blog.badtrace.com/post/anti-hooking-checks-of-smokeloader-2018/> <http://www.intel471.com/blog/cobalt-strike-cybercriminals-trickbot-qbot-hancitor> <https://www.fortinet.com/blog/threat-research/smokeloader-using-old-vulnerabilities> <https://www.secureworks.com/blog/smoke-loader-drops-whiffy-recon-wi-fi-scanning-and-geolocation-malware> <https://therecord.media/surge-in-smokeloader-malware-attacks-targeting-ukrainian-financial-gov-orgs> <https://asec.ahnlab.com/en/60703/> <https://unit42.paloaltonetworks.com/unit-42-scpc-ssscip-uncover-smoke-loader-phishing/> <https://www.fortinet.com/blog/threat-research/sophisticated-attack-targets-taiwan-with-smokeloader> <https://therecord.media/alleged-smokeloader-operator-charged-in-vermont>
MITRE ATT&CK	<https://attack.mitre.org/software/S0226/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Smoke%20Loader>

Last change to this tool card: 21 April 2025

Download this tool card in JSON format

All groups using tool Smoke Loader

Changed	Name	Country	Observed	
APT groups				
	TA530	[Unknown]	2016-Nov 2016	
Other groups				

	Bamboo Spider, TA544	[Unknown]	2016-Apr 2022	
	Smoky Spider	[Unknown]	2011-Apr 2019	
	TA516	[Unknown]	2016-Feb 2020	

4 groups listed (1 APT, 3 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c0fb51f1-5f2e-4efc-a59f-70ca9a5f0744