Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:45:31 UTC

Tool: LokiBot

Names	LokiBot Loki LokiPWS Loki.Rat ForeIT
Category	Malware
Type	Banking trojan, Backdoor, Keylogger, Info stealer, Credential stealer, Loader
Description	(Accenture) Loki Bot is a resident loader, and password and cryptocurrency wallet stealer. Loki Bot captures passwords from browsers, as well as e-mail, FTP, SSH and poker clients.
Information	<https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf> <https://www.threatfabric.com/blogs/lokibot_the_first_hybrid_android_malware.html> <https://isc.sans.edu/diary/24372> <https://github.com/R3MRUM/loki-parse> <http://www.malware-traffic-analysis.net/2017/06/12/index.html> <https://www.lastline.com/blog/password-stealing-malware-loki-bot/> <https://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file> <http://blog.fernandodominguez.me/lokis-antis-analysis/> <https://phishme.com/loki-bot-malware/> <https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/> <https://r3mrum.wordpress.com/2017/05/07/loki-bot-atrifacts/> <https://securelist.com/loki-bot-stealing-corporate-passwords/87595/> <https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/> <https://github.com/d00rt/hijacked_lokibot_version/blob/master/doc/LokiBot_hijacked_2018.pdf> <https://www.sans.org/reading-room/whitepapers/malicious/loki-bot-information-stealer-keylogger-more-37850> <https://us-cert.cisa.gov/ncas/alerts/aa20-266a> <https://blog.talosintelligence.com/2021/01/a-deep-dive-into-lokibot-infection-chain.html> <https://www.trendmicro.com/en_us/research/21/h/new-campaign-sees-lokibot-delivered-via-multiple-methods.html> <https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros> <https://cofense.com/blog/lokibot-phishing-malware-baseline/>

	<https://blog.sonicwall.com/en-us/2024/03/lokibot-is-being-distributed-by-windows-shortcut-files/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0447/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.lokibot> <https://malpedia.caad.fkie.fraunhofer.de/details/apk.loki> <https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:LokiBot>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=lokibot>

Last change to this tool card: 14 March 2024

Download this tool card in JSON format

All groups using tool LokiBot

Changed	Name	Country	Observed	
APT groups				
	El Machete	[Unknown]	2010-Mar 2022	
	Gorgon Group		2017-Jul 2020	
	Patchwork, Dropping Elephant		2013-Jun 2025	
	RATicate	[Unknown]	2019	
	Sweed	[Unknown]	2017-2019	

5 groups listed (5 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f37100e9-04b8-40ff-a39c-fe1d24a814cc