

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:56:39 UTC

Tool: BetaBot

Names	BetaBot Neurevt
Category	Malware
Type	Banking trojan , Backdoor , Info stealer , Credential stealer , DDoS , Downloader
Description	<p>(Cybereason) Betabot's main features include:</p> <ul style="list-style-type: none">• Browsers Form Grabber• FTP and mail client stealer• Banker module• Running DDOS attacks• USB infection module• Robust Userland Rootkit (x86/x64)• Arbitrary command execution via shell• The ability to download additional malware• Persistence• Crypto-currency miner module (added 2017)
Information	<p><https://www.cybereason.com/blog/betabot-banking-trojan-neurevt> <https://medium.com/@woj_ciech/betabot-still-alive-with-multi-stage-packing-fbe8ef211d39> <http://www.xylibox.com/2015/04/betabot-retrospective.html> <https://asert.arbornetworks.com/beta-bot-a-code-review/> <http://resources.infosecinstitute.com/beta-bot-analysis-part-1/> <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/BetaBot.pdf> <http://www.malwaredigger.com/2013/09/how-to-extract-betabot-config-info.html> <https://blog.talosintelligence.com/2021/08/neurevt-trojan-takes-aim-at-mexican.html></p>
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.betabot >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:betabot >

Last change to this tool card: 01 November 2021

Download this tool card in [JSON](#) format

All groups using tool BetaBot

Changed	Name	Country	Observed
APT groups			
	RATicate	[Unknown]	2019

1 group listed (1 APT, 0 other, 0 unknown)

[↑](#)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b9940a31-3e91-424f-81f5-e5b36c6b6056