Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:40:23 UTC

Tool: Qadars

Names	Qadars
Category	Malware
Type	Banking trojan, Backdoor, Credential stealer, Botnet
Description	(ESET) A new banking Trojan has been making its round in the past few months. First publicly discussed by LEXSI, this banking Trojan has been very active, infecting users throughout the world. Its modus operandi is banking fraud through web injection. While this approach has been present for a long time in various banking Trojan families, it is still effective. Win32/Qadars uses a wide variety of webinjects, some with Android mobile components, used to bypass online banking security and to gain access to user's bank account. Usually, banking Trojans either target a broad array of financial institutions or focus on a much smaller subset, usually institutions of which the user base is geographically close. Win32/Qadars fall in the second category: it pinpoints users in specific regions and uses webinject configuration files tailored to the banks most commonly used by the victims.
Information	<https://www.welivesecurity.com/2013/12/18/qadars-a-banking-trojan-with-the-netherlands-in-its-sights/> <https://securityintelligence.com/meanwhile-britain-qadars-v3-hardens-evasion-targets-18-uk-banks/> <https://info.phishlabs.com/blog/dissecting-the-qadars-banking-trojan> <https://pages.phishlabs.com/rs/130-BFB-942/images/Qadars%20-%20Final.pdf> <https://securityintelligence.com/an-analysis-of-the-qadars-trojan/> <https://www.johannesbader.ch/2016/04/the-dga-of-qadars/> <https://www.countercept.com/our-thinking/decrypting-qadars-banking-trojan-c2-traffic/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.qadars>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Qadars>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool Qadars

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=144de65c-7f10-4653-a970-eb3ea79e64e2