Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:46:34 UTC

Tool: Banatrix

Names	Banatrix
Category	Malware
Type	Banking trojan, Credential stealer
Description	(CERT.PL) Of all of the Polish malware families that we have seen last year, Banatrix seems to be the most technologically advanced one. This malware was used to replace the bank account number in the browser memory, however its implementation allowed an attacker to execute any arbitrary code on the victim's machine. This was used to extract passwords saved in the Mozilla Firefox browser.
Information	<https://www.cert.pl/en/news/single/banatrix-an-indepth-look/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.banatrix>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:banatrix>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool Banatrix

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

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