

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:42:03 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Matrix Banker

Tool: Matrix Banker

Names	Matrix Banker RediModiUpd
Category	Malware
Type	Banking trojan , Credential stealer
Description	<p>(Arbor) This post takes a look at a new banking malware that has, so far, been targeting financial institutions in Latin America—specifically, Mexico and Peru. Initially, we’ve called it “Matrix Banker” based on its command and control (C2) login panel, but it seems that “Matrix Admin” is a template available for the Bootstrap web framework. Proofpoint calls it “Win32/RediModiUpd” based on a debugging string from an earlier sample.</p> <p>The malware is under active development, but as with some of the other banking trojans we’ve analyzed, it’s difficult to assess how far and wide this threat will go while it’s still so new.</p>
Information	< https://www.netscout.com/blog/asert/another-banker-enters-matrix >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.matrix_banker >

Last change to this tool card: 22 May 2020

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

All groups using tool Matrix Banker

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.eta.or.th/cgi-bin/listgroups.cgi?u=5990b482-f24a-4c94-988a-93153a27cbc1>