

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:49:36 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Gozi v2

↪ Tool: Gozi v2

Names	Gozi v2 Gozi Pranimalka Pranimalka-Gozi
Category	Malware
Type	Banking trojan , Credential stealer
Description	(IBM) RSA recently discovered a new malware variant it dubbed Pranimalka-Gozi, which reportedly will be used in a massive, coordinated attack on U.S. banks called Project Blitzkrieg. After analyzing Pranimalka-Gozi, IBM Security determined that it is a distant relative of the Gozi malware. According to our findings, the installation and HTML injection designation method it uses resembles Gozi. However, many implementation details such as the format of the HTML injection, certain configuration elements and the machine code injected into the browser process appear to be completely different than those of Gozi.
Information	< https://securityintelligence.com/project-blitzkrieg-how-to-block-the-planned-pranimalka-gozi-trojan-attack/ > < https://krebsonsecurity.com/tag/gozi-pranimalka/ > < https://lokalhost.pl/gozi_tree.txt >

Last change to this tool card: 24 May 2020

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

All groups using tool Gozi v2

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-da.or.th/cgi-bin/listgroups.cgi?u=9a68ee23-32e6-40bd-aac1-b620447a0c0f>