Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:55:14 UTC

Tool: Nymaim

Names	Nymaim nymain
Category	Malware
Type	Banking trojan, Downloader
Description	(Digital Forensics Corp) Nymaim was discovered in 2013 and is a downloader. It recently teamed up with the banking trojan Gozi ISFB, so there was a new family of malware called GozNym. However, the original version Nymaim still continues to be used as the boot various other threats.
Information	<https://www.digitalforensics.com/blog/nymaim-the-banker-trojan-advanced-analysis/> <https://www.proofpoint.com/us/threat-insight/post/nymaim-config-decoded> <https://www.cert.pl/en/news/single/nymaim-revisited/> <https://bitbucket.org/daniel_plohmann/idapatchwork> <https://arielkoren.com/blog/2016/11/02/nymaim-deep-technical-dive-adventures-in-evasive-malware/> <https://public.gdatasoftware.com/Web/Landingpages/DE/GI-Spring2014/slides/004_plohmann.pdf> <https://github.com/coldshell/Malware-Scripts/tree/master/Nymaim>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:nymaim>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Nymaim

Changed	Name	Country	Observed
APT groups			

	TA530	[Unknown]	2016-Nov 2016	
Other groups				
	Bamboo Spider, TA544	[Unknown]	2016-Apr 2022	

2 groups listed (1 APT, 1 other, 0 unknown)

↑
