Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:57:41 UTC

Tool: Andromeda

Names	Andromeda Gamarue B106-Gamarue B67-SS-Gamarue b66
Category	Malware
Type	Botnet, Downloader
Description	(Avast) Andromeda is one of the longest running and most prevalent malware families to have existed. Andromeda was first discovered in late 2011 and it probably evolved from ngrBot/DorkBot. Throughout its existence, the groups behind Andromeda have used various methods to spread the malware and infect users.
Information	<https://blog.avast.com/andromeda-under-the-microscope> <https://blog.fortinet.com/2014/04/16/a-good-look-at-the-andromeda-botnet> <https://blog.fortinet.com/2014/05/19/new-anti-analysis-tricks-in-andromeda-2-08> <http://blog.morphisec.com/andromeda-tactics-analyzed> <https://eternal-todo.com/blog/yet-another-andromeda-gamarue-analysis> <http://resources.infosecinstitute.com/andromeda-bot-analysis/> <https://blog.fortinet.com/2014/04/23/andromeda-2-7-features> <http://www.0xebfe.net/blog/2013/03/30/fooled-by-andromeda/> <https://eternal-todo.com/blog/andromeda-gamarue-loves-json> <http://resources.infosecinstitute.com/andromeda-bot-analysis-part-two/> <https://byte-atlas.blogspot.ch/2015/04/kf-andromeda-bruteforcing.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S1074>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.andromeda>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool Andromeda

Changed	Name	Country	Observed	
Other groups				
	Andromeda Spider		2011-Nov 2017	

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

↑

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=67a1d20f-99b7-44ce-bb05-2464d2819fb6