

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:52:22 UTC

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


## Tool: Neutrino

Names	Neutrino Neutrino Bot Neutrino Exploit Kit Kasidet
Category	<a href="#">Exploits</a>
Type	<a href="#">Backdoor</a> , <a href="#">Credential stealer</a>
Description	<a href="#">(Malwarebytes)</a> The Neutrino exploit kit is a malicious tool kit, which can be used by attackers who are not experts on computer security. Threat actors can have zero coding experience and still use exploit kits like Neutrino to conduct their illegal activity.
Information	<p>&lt;<a href="https://blog.malwarebytes.com/threats/neutrino/">https://blog.malwarebytes.com/threats/neutrino/</a>&gt;</p> <p>&lt;<a href="https://blog.malwarebytes.com/threat-analysis/2017/02/new-neutrino-bot-comes-in-a-protective-loader/">https://blog.malwarebytes.com/threat-analysis/2017/02/new-neutrino-bot-comes-in-a-protective-loader/</a>&gt;</p> <p>&lt;<a href="https://securityblog.switch.ch/2017/07/07/94-ch-li-domain-names-hijacked-and-used-for-drive-by/">https://securityblog.switch.ch/2017/07/07/94-ch-li-domain-names-hijacked-and-used-for-drive-by/</a>&gt;</p> <p>&lt;<a href="http://www.peppermalware.com/2019/01/analysis-of-neutrino-bot-sample-2018-08-27.html">http://www.peppermalware.com/2019/01/analysis-of-neutrino-bot-sample-2018-08-27.html</a>&gt;</p> <p>&lt;<a href="https://blog.malwarebytes.com/threat-analysis/2015/08/inside-neutrino-botnet-builder/">https://blog.malwarebytes.com/threat-analysis/2015/08/inside-neutrino-botnet-builder/</a>&gt;</p> <p>&lt;<a href="https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet">https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet</a>&gt;</p> <p>&lt;<a href="http://securitykitten.github.io/an-evening-with-n3utrino/">http://securitykitten.github.io/an-evening-with-n3utrino/</a>&gt;</p> <p>&lt;<a href="https://blog.malwarebytes.com/cybercrime/2017/01/post-holiday-spam-campaign-delivers-neutrino-bot/">https://blog.malwarebytes.com/cybercrime/2017/01/post-holiday-spam-campaign-delivers-neutrino-bot/</a>&gt;</p> <p>&lt;<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/">http://blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/</a>&gt;</p> <p>&lt;<a href="http://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html">http://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html</a>&gt;</p> <p>&lt;<a href="https://www.zscaler.com/blogs/research/malicious-office-files-dropping-kasidet-and-dridex">https://www.zscaler.com/blogs/research/malicious-office-files-dropping-kasidet-and-dridex</a>&gt;</p>
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino">https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino</a> >

Last change to this tool card: 14 May 2020

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

## All groups using tool Neutrino

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">OPERA1ER</a>	[Unknown]	2016-Jul 2023	●
	<a href="#">TA505, Graceful Spider, Gold Evergreen</a>		2006-Nov 2022	●

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

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=d8c25cb4-1fea-45b5-9838-03855d6c0daa>