Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:27:59 UTC

Home > List all groups > List all tools > List all groups using tool Neuron

Tool: Neuron

Names	Neuron
Category	Malware
Type	Backdoor
Description	Neuron consists of both client and server components. The Neuron client and Neuron service are written using the .NET framework with some codebase overlaps. The Neuron client is used to infect victim endpoints and extract sensitive information from local client machines. The Neuron server is used to infect network infrastructure such as mail and web servers, and acts as local Command & Control (C2) for the client component. Establishing a local C2 limits interaction with the target network and remote hosts. It also reduces the log footprint of actor infrastructure and enables client interaction to appear more convincing as the traffic is contained within the target network.
Information	<https://threatpost.com/turla-compromises-iranian-apt/149375/> <https://www.ncsc.gov.uk/alerts/turla-group-malware>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.neuron>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Neuron

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	
	Turla, Waterbug, Venomous Bear		1996-2024	

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