Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:46:45 UTC

Tool: LightNeuron

Names	LightNeuron NETTRANS XTRANS
Category	Malware
Type	Info stealer
Description	(ESET) Turla is believed to have used LightNeuron since at least 2014. • LightNeuron is the first publicly known malware to use a malicious Microsoft Exchange Transport Agent. • LightNeuron can spy on all emails going through the compromised mail server. • LightNeuron can modify or block any email going through the compromised mail server. • LightNeuron can execute commands sent by email. • Commands are hidden in specially crafted PDF or JPG attachments using steganography. • LightNeuron is hard to detect at the network level because it does not use standard HTTP(S) communications.
Information	<https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0395/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.lightneuron>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool LightNeuron

Changed	Name	Country	Observed

APT groups

	Turla, Waterbug, Venomous Bear		1996-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d1283603-7f97-4f89-8591-103d90aa9389