Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:43:58 UTC

Tool: Luminosity RAT

Names	Luminosity RAT LuminosityLink
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Downloader
Description	(Proofpoint) The stated purpose of LuminosityLink is ostensibly benign: 'LuminosityLink allows system administrators to manage a large amount of computers concurrently. Our product is ideal for business owners, educational institutions, and Windows system administrators.' Analysis upon install, however, reveals a very aggressive key logger that injects its code in almost every running process on the computer, and multiple attempts are made if not initially successful. This 'injection' behavior is aggressive even by the standard of the Zeus family: very few malware families exhibit such an aggressive behavior, and it is particularly unusual to observe this in key loggers, even commercial ones. We have observed LuminosityLink being used to download additional payloads. It is possible that the actors involved here are using LuminosityLink as a platform to collect information from the victim, and using that information to decide whether to deploy more sophisticated malware at high-value targets.
Information	<https://www.proofpoint.com/us/threat-insight/post/Light-After-Dark> <https://krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/> <http://malwarenailed.blogspot.com/2016/07/luminosity-rat-re-purposed.html> <https://researchcenter.paloaltonetworks.com/2018/02/unit42-rat-trapped-luminositylink-falls-foul-vermin-eradication-efforts/> <https://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/> <https://umbrella.cisco.com/blog/2017/01/18/finding-the-rats-nest/> <https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.luminosity_rat>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:luminositylink>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Luminosity RAT

Changed	Name	Country	Observed	
APT groups				
	LazyScripter	[Unknown]	2018	
	Sima		2016	
	TA2541	[Unknown]	2017	
	Transparent Tribe, APT 36		2013-Mar 2025	

4 groups listed (4 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b41e9810-7e30-4a2f-ac55-936b396b6b60