Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:32:52 UTC

Tool: SUPERNOVA

Names	SUPERNOVA
Category	Malware
Type	Backdoor
Description	(Palo Alto) In the analysis of the trojanized Orion artifacts, the .NET .dll app_web_logoimagehandler.ashx.b6031896.dll was dubbed SUPERNOVA, but little detail of its operation has been publicly explored. NOTE: The SUPERNOVA webshell's association with the SolarStorm actors is now questionable due to the aforementioned .dll not being digitally signed, unlike the SUNBURST .dll. This may indicate that the webshell was not implanted early in SolarWinds' software development pipeline as was SUNBURST, and was instead dropped by a third party. Additionally, Guidepoint Security conducted their own research into SUPERNOVA, with similar conclusions.
Information	<https://unit42.paloaltonetworks.com/solarstorm-supernova/> <https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/> <https://labs.sentinelone.com/solarwinds-understanding-detecting-the-supernova-webshell-trojan/> <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a> <https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group> <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112>
MITRE ATT&CK	<https://attack.mitre.org/software/S0578/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.supernova>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SUPERNOVA

Changed	Name	Country	Observed

APT groups

	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d066195c-0a56-41bc-9f4b-b2e8eeda540b