Microsoft Security

Solorigate Network Beacon

PDF file generated on Dec 30, 2025 1:29 AM Timestamps are generated in UTC+11

■■■ High | ● Active | Unassigned | Unclassified |

Last update time: Dec 30, 2025 12:55 AM

Contents

Overview

Incident details

Severity	High
Status	Active
Assigned to	-
Incident ID	5
Classification	Not set
Categories	Command and control
Time created	Dec 30, 2025 12:25 AM
First activity	Dec 30, 2025 12:25 AM
Last activity	Dec 30, 2025 12:25 AM
Description	Identifies a match across various data feeds for domains IOCs related to the Solorigate incident. References: https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html?1

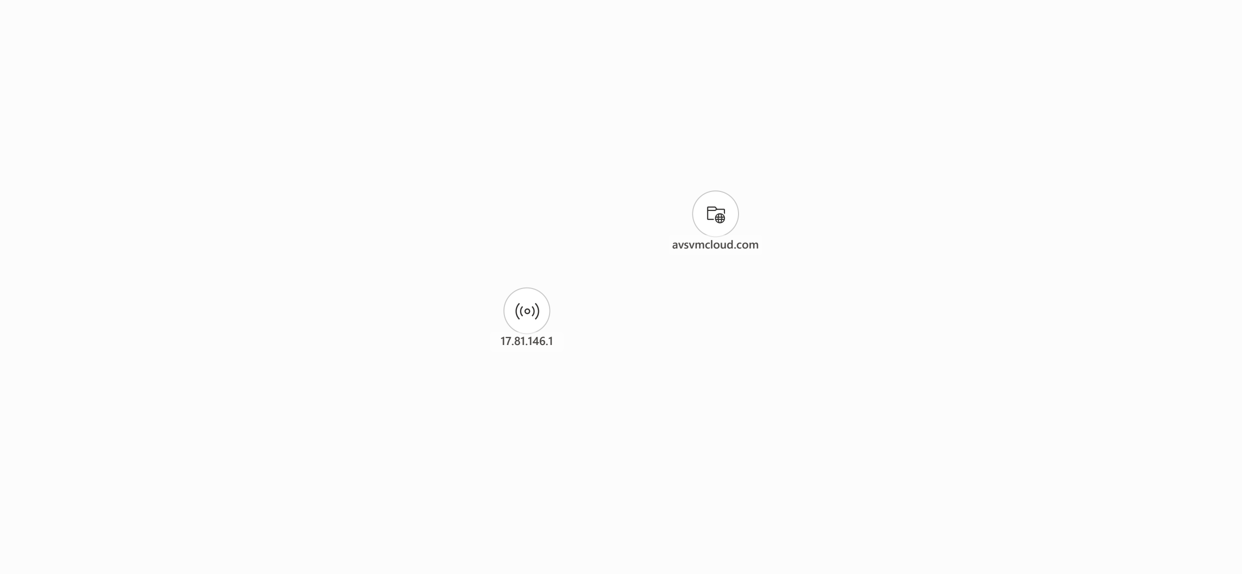
Attack story

Attack story graph

MITRE categories
1

Number of alerts
3

Evidence
2



Association
A relationship between two entities based on affiliation of one entity to another

Communication
Transmission of data between entities

Threat categories

1 threat categories

Alerts and categories

Active alerts
3/3

Tactics
1

Other categories
0

Command and control 3 / 3

MITRE ATT&CK tactics

Command and control

Other categories

No categories found

Scope

Impacted assets

There are no impacted assets to show for this incident.

Evidence and response

Evidence

2 evidence

DNS	IP Addresses
1	1

Top evidence

First seen↓	Entity	Entity type	Verdict	Remediation status	Impacted assets	Detection origin
Dec 30, 2025 12:25 AM	avsvmcloud.com	DNS	Suspicious			Solorigate Network Beacon,...
Dec 30, 2025 12:25 AM	17.81.146.1	IP Addresses	Suspicious			Solorigate Network Beacon,...

Supporting data

3 Active alerts

High
3

All alerts

Alert name	Severity	Status	Detection	Impacted assets	First activity	Last activity↓
Solorigate Network Beacon	High	New	ScheduledAlerts		Dec 30, 2025 12:25 AM	Dec 30, 2025 12:25 AM
Solorigate Network Beacon	High	New	ScheduledAlerts		Dec 30, 2025 12:25 AM	Dec 30, 2025 12:25 AM
Solorigate Network Beacon	High	New	ScheduledAlerts		Dec 30, 2025 12:25 AM	Dec 30, 2025 12:25 AM