REPORT

CloudVector Provides the Only Effective Security Solution Against SolarWinds SUPERNOVA Malware

Protect Against Shadow API Vulnerabilities of Your Third-Party Applications

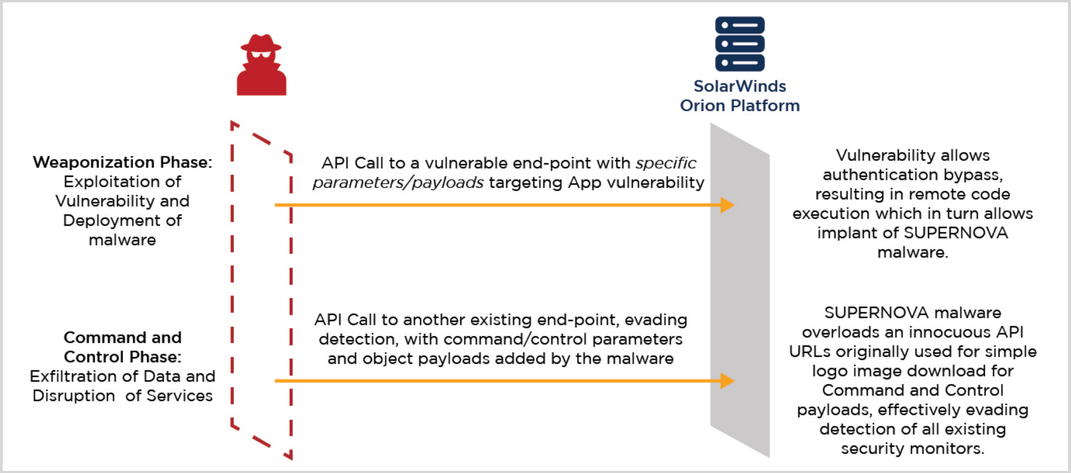
SOLARWINDS SUPERNOVA MALWARE BREACH: WHAT HAPPENED?

The digital world was recently rocked by a major supply chain attack in the SolarWinds Orion platform, exploiting a vulnerability called SunBurst. Analysis of the SunBurst vulnerability and its related artifacts led to the discovery of an even stealthier malware called SUPERNOVA. SUPERNOVA is the most recent example in a long line of covert malware leveraging API vulnerabilities through all phases of the attack lifecycle:

Weaponization: In the first phase, an API vulnerability of the SolarWinds Orion platform is leveraged by a malicious actor to execute remote code, which bypasses authentication, to deploy the SUPERNOVA malware. The attack is virtually undetectable because it leverages a vulnerable API, which blends in with normal API traffic, to compromise the Orion API endpoint. These Shadow APIs evade detection because existing security solutions were not designed to monitor them.

Command and Control: Once deployed, the SUPERNOVA malware turns an existing API endpoint of the Orion platform into a command/control interface, enabling it to further evade detection as a Shadow API. Attack actors then leverage these Shadow API calls to send commands inside the altered data object payloads to control the malware.

> “CloudVector is a superior solution for detecting Shadow APIs because its API inspection is deep down to the data layer (instead of signature-based detection). This makes it effective against existing, future and zero-day Shadow API attacks.”



Weaponization Phase: Exploitation of Vulnerability and Deployment of malware

API Call to a vulnerable end-point with *specific parameters/payloads* targeting App vulnerability

Vulnerability allows authentication bypass, resulting in remote code execution which in turn allows implant of SUPERNOVA malware.

Command and Control Phase: Exfiltration of Data and Disruption of Services

API Call to another existing end-point, evading detection, with command/control parameters and object payloads added by the malware

SUPERNOVA malware overloads an innocuous API URLs originally used for simple logo image download for Command and Control payloads, effectively evading detection of all existing security monitors.

Figure 1: Two Phases of the SUPERNOVA Malware Attack

The fact that this attack was discovered in SolarWinds should be no comfort to security operators, especially since it went unnoticed by so many organizations. API attack vectors could very well be in use against other third-party software systems, especially since Web APIs are such a common communication method. What enterprises need is a security solution that can help detect zero-day API vulnerability exploits against 3rd party applications that are not developed in house.

WHY EXISTING SECURITY SOLUTIONS FAILED TO DETECT SUCH ATTACKS?

Existing security solutions are unable to prevent these attacks because they were not designed to detect Shadow API vulnerabilities.

Conventional Web Application Firewalls (WAF) and/or API Gateways can only detect certain anomalous access patterns or protect against already known attacks. Even an advanced Web Application and API Protection (WAAP) solution is dependent on known API specifications for API data layer validation. In the case of third-party application APIs, these sort of gateway solutions are ineffective because they lack access to the up-to-date API specifications they need to operate.

Code and configuration scanning tools cannot scan a third-party application, making it impossible for them to detect such a vulnerability or attack. Likewise, API testing tools are unable to test third-party application APIs.

HOW CLOUDVECTOR'S SOLUTION CAN HELP

CloudVector delivers two unique capabilities that make all the difference in protecting your critical infrastructure and data from third-party API threats like the SolarWinds SUPERNOVA:

1. CloudVector's non-intrusive API sensors can be deployed in a low impact out-of-band manner to monitor **all runtime API calls** without any change of code, any agent in the platform, or any additional inline device. The API sensor is light-weight and highly efficient, capable of processing and filtering a large number of API calls with inspection deep into the object/parameter level.
2. CloudVector ingests data from these smart sensors into an AI/ML engine that automatically learns the API data layer structure from its live API calls to produce an accurate API blueprint (of its expected behavior), even without an API specification. This continuously updated blueprint enables CloudVector to detect and respond to data-level anomalies with high accuracy, protecting the third party applications from advanced API attacks.

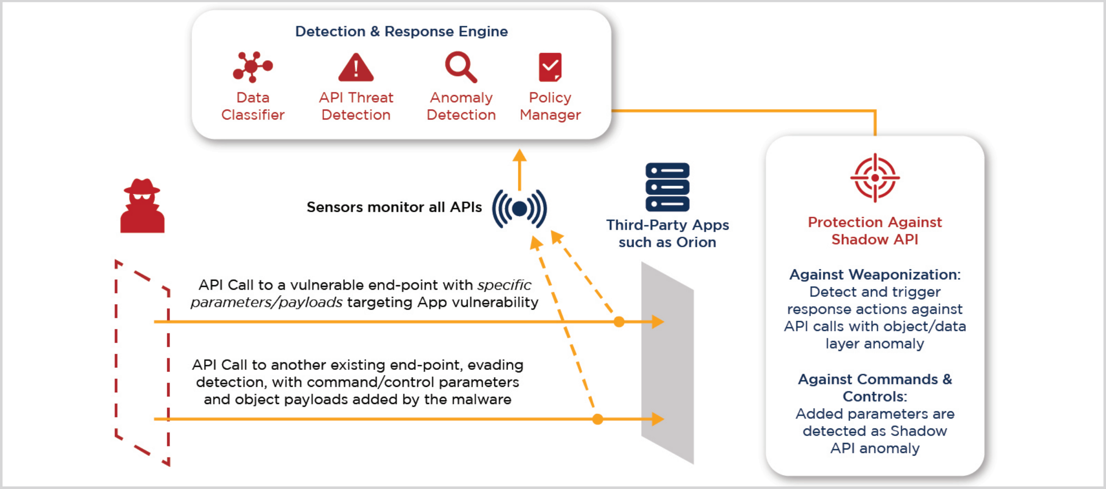

Detection & Response Engine
Data Classifier
API Threat Detection
Anomaly Detection
Policy Manager
Sensors monitor all APIs
Third-Party Apps such as Orion
Protection Against Shadow API
Against Weaponization:
Detect and trigger response actions against API calls with object/data layer anomaly
Against Commands & Controls:
Added parameters are detected as Shadow API anomaly
API Call to a vulnerable end-point with *specific parameters/payloads* targeting App vulnerability
API Call to another existing end-point, evading detection, with command/control parameters and object payloads added by the malware

Figure 2: CloudVector API Detection/Response Against SUPERNOVA Malware Attack

In the case of Shadow API calls, CloudVector can identify out-of-the-ordinary API calls, even within individual parameter values during the weaponization phases. CloudVector applies granular controls and a targeted response to automatically terminate the API session of an attack, which would have prevented the deployment of SUPERNOVA. Or in the case of an existing SUPERNOVA compromise, CloudVector would detect the command and control calls as an anomaly in the parameters of the Shadow API. The reason CloudVector is so effective at detecting Shadow APIs is that its API inspection is deep down to the data layer (instead of signature-based detection), making it effective against existing, future and zero-day Shadow API attacks.

To learn more about how CloudVector's API security solution can help, email us at contact@cloudvector.com, request a meeting, or join us for our next live demo.