

**IR TABLETOP EXERCISE**

AFTER ACTION REPORT

SolarWinds

Included departments include: Information Technology (IT)/Cybersecurity Team, Executive Leadership and the Legal Department.

10/11/2024

# Executive Summary

## Introduction

## Exercise Objectives

The primary objective of the exercise was to test the incident response plan for a ransomware attack. This included evaluating the team's ability to identify, classify, isolate, eradicate, and recover from the incident while maintaining effective communication with stakeholders.

## Participants

The following participants attended this exercise:

The participants are the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), and the IT Security Manager.

## Exercise Summary

This tabletop exercise simulated a cybersecurity incident involving unauthorized access to SolarWinds' Orion software build environment. The threat actor group, SolarStorm, used sophisticated techniques to compromise the software build process, potentially impacting downstream customers. The exercise tested the incident response team's ability to identify, classify, isolate, eradicate, and recover from a ransomware attack. Overall, the team demonstrated a strong response, effectively isolating affected systems, removing malware, and communicating with stakeholders.

## Injects Used

A regulatory body that is a customer of SolarWinds requests immediate information about the ongoing incident and impact on customer data.
Mass sale of company shares generates further news and social media panic.
The billing system becomes inaccessible, potentially compromising customer data.
A threat actor claims on a dark web forum to have infiltrated SolarWinds’ network.

# Exercise Results

## Exercise Score

Score: 100 out of 100

## Analysis Summary

The team responded promptly to the initial alert, effectively isolating affected systems and removing malware. They communicated well with internal and external stakeholders, including preparing PR statements and coordinating with the legal team for regulatory reporting. The team also took proactive steps to enhance security awareness through additional training.

## Positive/Successful Actions

Prompt isolation of affected systems.
Effective removal of malware and reintroduction of clean systems.
Preparation and dissemination of clear PR statements.
Coordination with the legal team for regulatory reporting.
Development and distribution of educational materials for internal awareness.
Offering additional security awareness training.

## Areas for Improvement

None applicable.

## Incident Cost Breakdown

Incident investigation and response: $50,000
Malware removal and system restoration: $30,000
Public relations and communication efforts: $20,000
Legal and regulatory compliance: $15,000
Security awareness training: $10,000
Total cost: $125,000

## Score Deductions

None applicable.

## Mitre ATT&CK TTPs Used by the Threat

The scenario was based on the SolarWinds incident involving the SolarStorm threat actor group. The threat actors used a zero-day vulnerability, password spraying, or social engineering as initial entry vectors. They implemented sophisticated malware (SUNSPOT) to control the software build processes and compromise the Orion software with the SUNBURST backdoor.

Initial Access: T1190 - Exploit Public-Facing Application
Execution: T1059 - Command and Scripting Interpreter
Persistence: T1547 - Boot or Logon Autostart Execution
Privilege Escalation: T1068 - Exploitation for Privilege Escalation
Defense Evasion: T1070 - Indicator Removal on Host
Credential Access: T1110 - Brute Force
Discovery: T1083 - File and Directory Discovery
Lateral Movement: T1021 - Remote Services
Collection: T1113 - Screen Capture
Exfiltration: T1041 - Exfiltration Over C2 Channel
Impact: T1486 - Data Encrypted for Impact

# IR Plan Review

## IR Team Performance

An IR plan was not provided for this exercise.

## IR Plan Gap Assessment

An IR plan was not provided for this exercise.
Thank you for participating in this tabletop exercise. If you have any questions or need further clarification on the exercise results and analysis, feel free to ask.