A Very Important Incident

## Date: 2024-11-28

## Handler: Duc K.

# Executive Summary

On 2021-02-10 at 10:00AM PST department X notified the SOC about unusual behavior on one of their servers, server-a. On investigation Information Security found that a malware strain known as BadStuff was present on the system. While BadStuff is known to steal credentials investigations into network traffic did not reveal any evidence indicating that information was breached before the system was shut down. On 2017-03-28 at 09:00AM PST department X was authorized to reimage the system and resume normal operations. Total financial impact to the organization is $50,000.

Unless the Incident is specifically about an account, accounts should likely not be mentioned here. In addition, please note that the notifying entity was a department and not a person. It’s best to use department names and titles, and not the names of individuals involved in the incident or the investigation.

The executives will always want to see what the financial and operational impact was in this section of the document.

# Background

This section includes background on what systems, services, and accounts were involved and what they normally do. It also includes how and when Cyber Security was notified of the incident. This information is intended to help your readers understand the details of what you write in the rest of the report by having some background information on the systems involved and their business functions. The reader should be able to ascertain the potential impact to business operations after having read this section of the report.

# Timeline

2017-03-24 at 8:00AM PST – Something bad happened

2017-03-27 at 10:00AM PST – Department X notified SOC

2017-03-28 at 8:00PM PST – Something else happened

2017-03-29 at 9:00AM PST – This should include all important events of the incident

2017-03-29 at 10:00AM PST – Document each significant step that the attacker took in your environment

2017-03-29 at 11:00AM PST – Document each significant step that your team took as incident responders to detect, analyze, contain, eradicate, and recover from the incident

2017-03-29 at 3:00PM PST – The timeline should conclude at the point which major incident response activities have concluded. This could be when systems have been recovered or when breach response activities have concluded.

2017-03-29 at 4:00PM PST – The timeline is not the same as your investigation log. If you are unclear about the difference between the two, please review lectures and ask questions during office hours or in Piazza.

# Findings

This is an outline of what happened. It is not a restatement of your investigative log or timeline. It is intended to convey to management and technical leadership what we believe happened to the system. It frequently makes sense to present this chronologically, though it does not have to be if some other ordering conveys the information more succinctly. In some cases, a bulleted timeline may work, but frequently paragraphs work better. If you choose to use chronological paragraphs the time, as closely as you can derive it, should be close to the beginning of each paragraph.

# Actions Taken

This is a statement of what actions were taken in response to the incident. This informs management of how the incident has been contained and what effort has been taken to restore service.

# Financial Impact

|  |  |
| --- | --- |
| Item | Cost |
| This section documents the financial impact of the incident | $10 |
| It must NOT include new technologies or fixes identified within the lessons learned | $100,000 |
| It should include both direct costs and investigative costs1 | $25,000 |
| Labor2 | $50,000 |
| Total | $175,010 |

1. Include footnotes to document how costs were calculated. For example, 25 investigative hours x $1,000 per investigative hour = $25,000
2. Labor cost should always be included. Your organization may include a standard way to compute this, but if not you should assume that all time spent on the incident multiplied by the employee’s hourly rate is attributable to the incident.

# Lessons Learned

This section is not optional.

## Successes

* Outline where things worked
* This includes controls that helped you find it
* Make sure you include other departments who performed well

## Opportunities for Improvement

**Issue:** An item that could have been better including security controls as well as investigative procedures. It is recommended you follow the attack lifecycle and identify control weaknesses at each step of the lifecycle.

**Recommendation:** How it could be improved. It helps to talk this through with other parts of the organization if it affects them.

**Action Item Owner:** Who should be responsible for fixing it