

Incident Report

Rochester Institute of Technology ITS

**Date of Incident(s):** 04/11/22, 04/13,22, 04/18/22

**Date of Writing:** 04/18/22

**Authors:** Bradley Harker, Jeffrey Monaco, Dexter Delandro, Zachary Mangiaracina, Joseph Strozyk, Brayden Wachowiak

**Phone:** (585) 123-4567

**Fax:** (585) 455-8008

**Address:** 1 Lomb Memorial Dr. Rochester, NY, 14623

# Table of Contents

[**Table of Contents**](#_fs83tpml7hbt) **2**

[**Executive Summary**](#_bkdsxyqz0nsw) **3**

[**Disclaimer**](#_dngoiwiiysvr) **4**

[**Risk Matrix**](#_lonyn5l07aj) **5**

[**Sample Incident - <NAME>**](#_1m8fvzvw2omq) **6**

[General Information](#_nt425aiyny9f) 6

[Business Impact](#_4banobpp5qot) 6

[Detection](#_jla90g2bra7) 6

[Collected Information](#_90yhajjg1d29) 6

[Analysis](#_mqsfd1yl96x1) 6

[Containment](#_v9bcd2ftvuc0) 7

[Monitoring/Prevention](#_8w67s4n760gx) 7

## 

## 

# Executive Summary

# 

# Disclaimer

Just because an incident was not found on a machine does not mean that machine has had no

incidents or has no malware. It only means that the team did not discover any incidents on that

particular machine.

# Risk Matrix

# 

# Sample Incident - <NAME>

## General Information

| **Date of Incident:** | XX/XX/XX |
| --- | --- |
| **Impacted Machines:** | Box Name, Box Name, Box Name |
| **Risk Level:** | HIGH/MEDIUM/LOW |
| *Probability* | *HIGH/MEDIUM/LOW* |
| *Impact* | *HIGH/MEDIUM/LOW* |

## Business Impact

How can this interrupt business operations. Make some bs ab RIT up

## Detection

How you find it

## Collected Information

*<Screenshots here>*

*Desc
*

*Figure <incident number>.<screenshot number> - Lorem Ipsum Sit Dolor Amet*

## Analysis

Why is this bad

## Containment

What you do to fix it

## Monitoring/Prevention

How to prevent in future