2.0 Detection and Analysis

2.1.0 Incident Overview

This report outlines the steps taken to detect and analyze the suspicious process that was discovered on the affected endpoint, resulting in significant system slowdowns. The incident began with a report from the Security Operations Center (SOC) team indicating that the user's machine was performing unusually slowly while browsing web pages. The following investigation and analysis were conducted to identify the cause of the issue and determine whether the system had been compromised.

2.1.1 Step 1: Initial Investigation

The first step was to check the Task Manager on the affected machine to identify any processes that could explain the observed system slowdown.

Observation: A process named 32th4ckm3 was found in the Task Manager, consuming an unusually high percentage of CPU resources—specifically, 52.3%.

Action: I examined the properties of this process and discovered that it was located in a temporary directory, which raised concerns about its legitimacy and potential malicious activity.

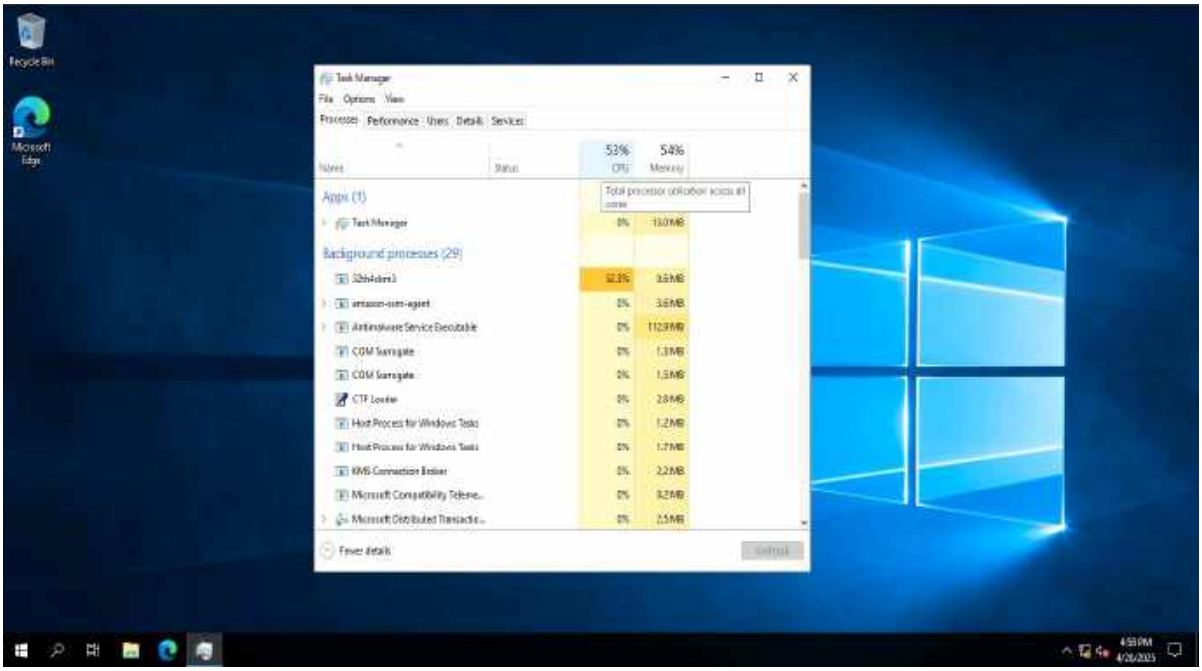


Fig 2.1: Task Manager showing malicious process running on User's PC

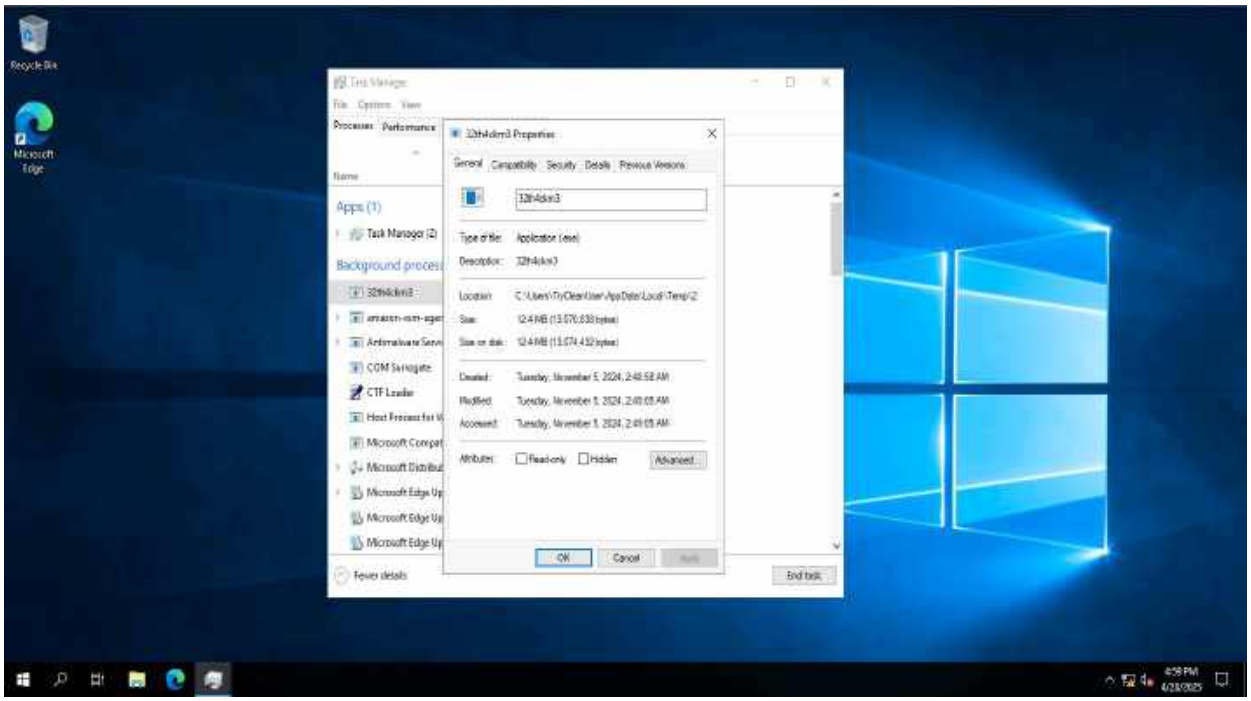


Fig 2.2: Malicious Process Properties

2.1.2 Step 2: Process Identification and Network Analysis

The next step was to further analyze the suspicious process to determine its behavior and network activity. The Process ID (PID) for the process was identified as 4500.

Action: I accessed the Command Prompt and ran the following command to check if the process was communicating with external servers:

netstat -aofn | find "4500"

Findings: The command revealed that the process was making outbound connections to an external IP address, 45.33.32.156, on port 42424. This was a key indication that the process was likely part of a remote command-and-control communication channel.

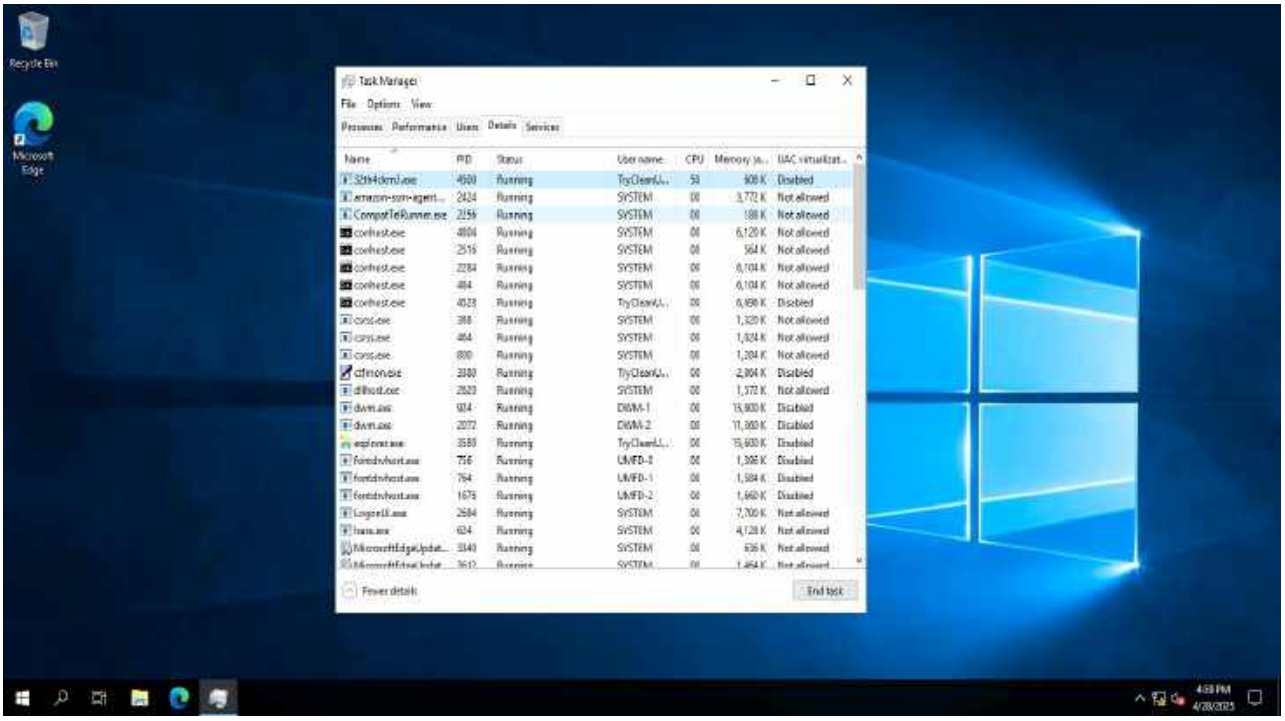


Fig 2.3: Malicious Process PID

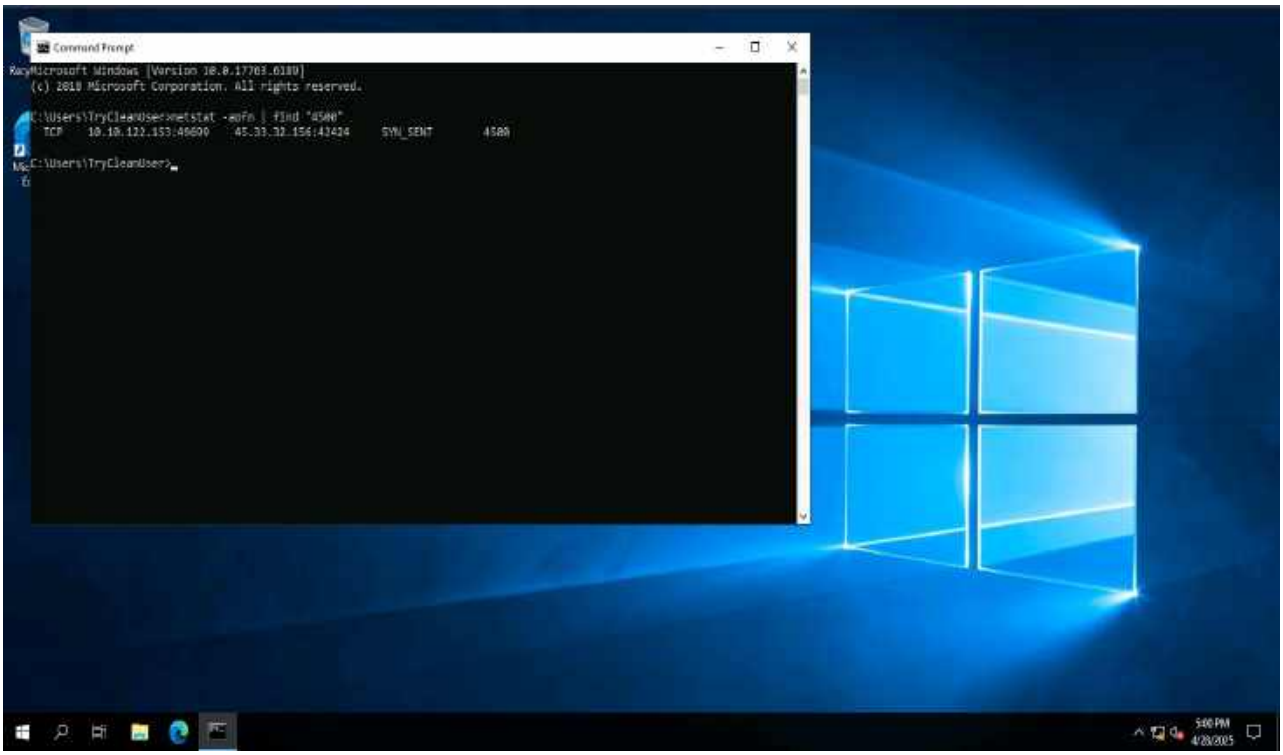


Fig 2.4: Command Window showing destination IP address of suspicious outbound communication

2.1.3 Step 3: Investigating User Activity

According to the SOC team, the user's system slowed down while browsing web pages. To understand the potential cause of the issue, I investigated the user's browser history, specifically the download history, to determine if any suspicious files were involved.

Action: I accessed the browser's download history in Microsoft Edge by navigating to the following URL:

edge://downloads/all

Findings: I discovered that the user had recently downloaded a suspicious Word document titled "invoice n. 65748224.docm". This document appeared to be the potential source of the issue.

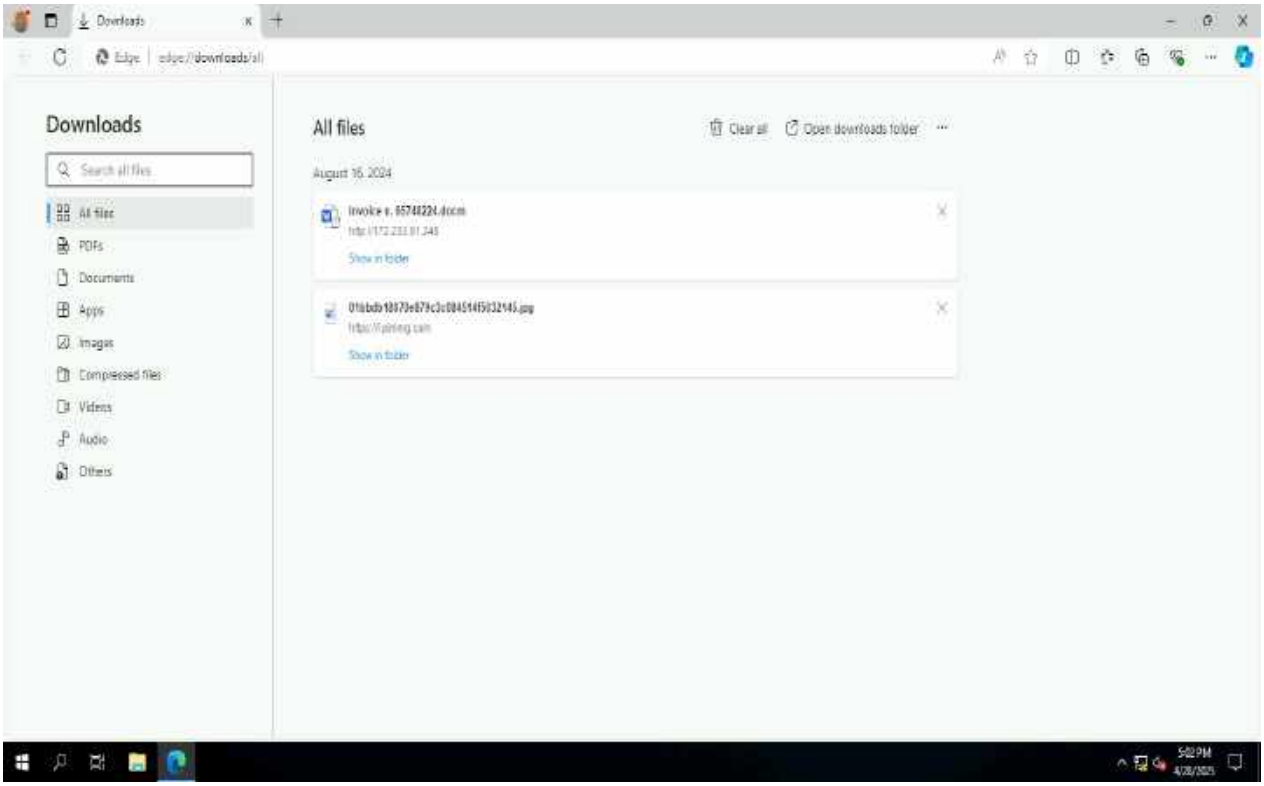


Fig 2.5: Suspicious word document found in web browser's downloads history

2.1.4 Step 4: Malicious Document Analysis

The next step was to open the suspicious document and analyze its contents. Upon inspection, I found that the document contained a suspicious hyperlink and an embedded macro defined as AutoOpen.

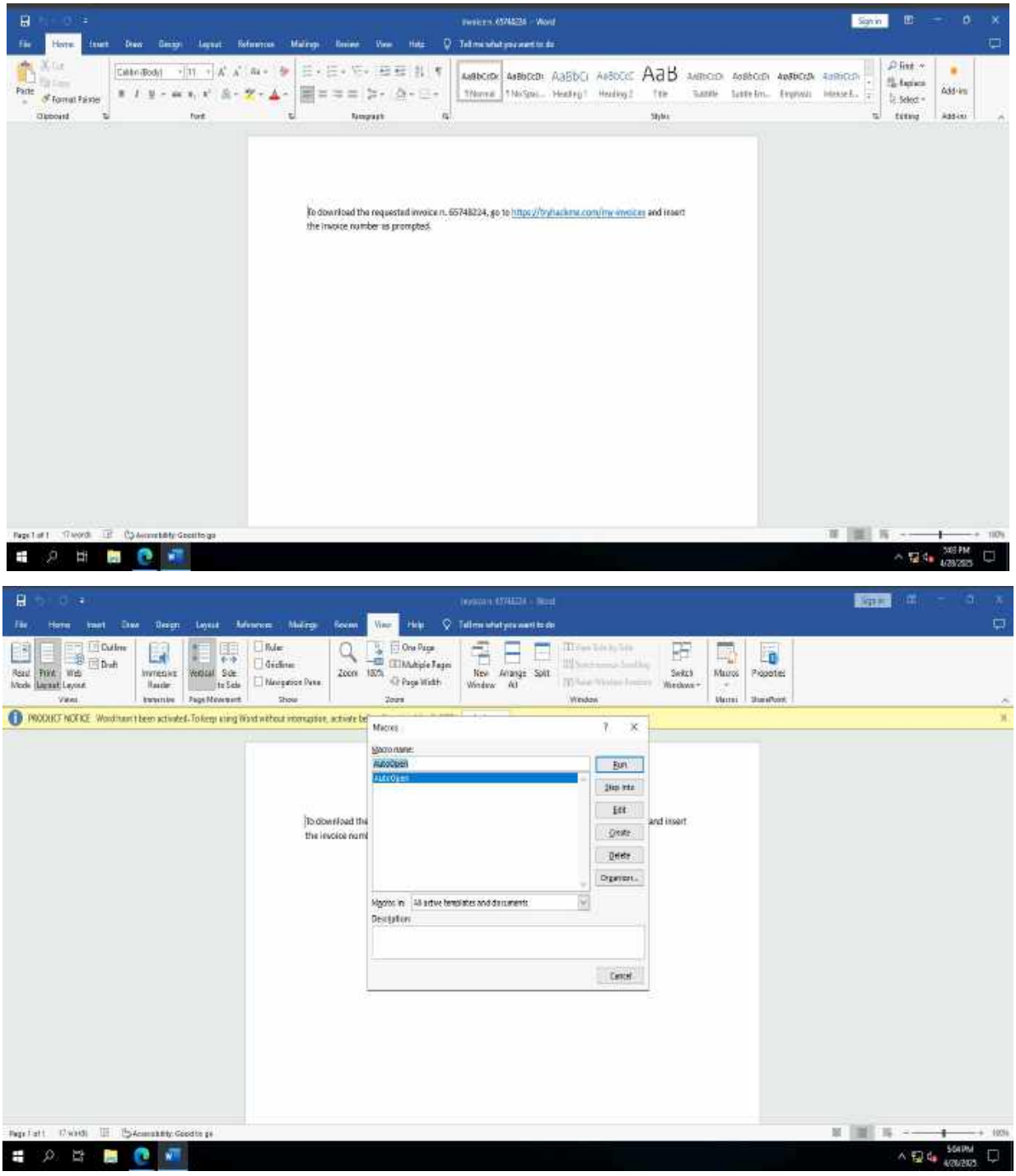
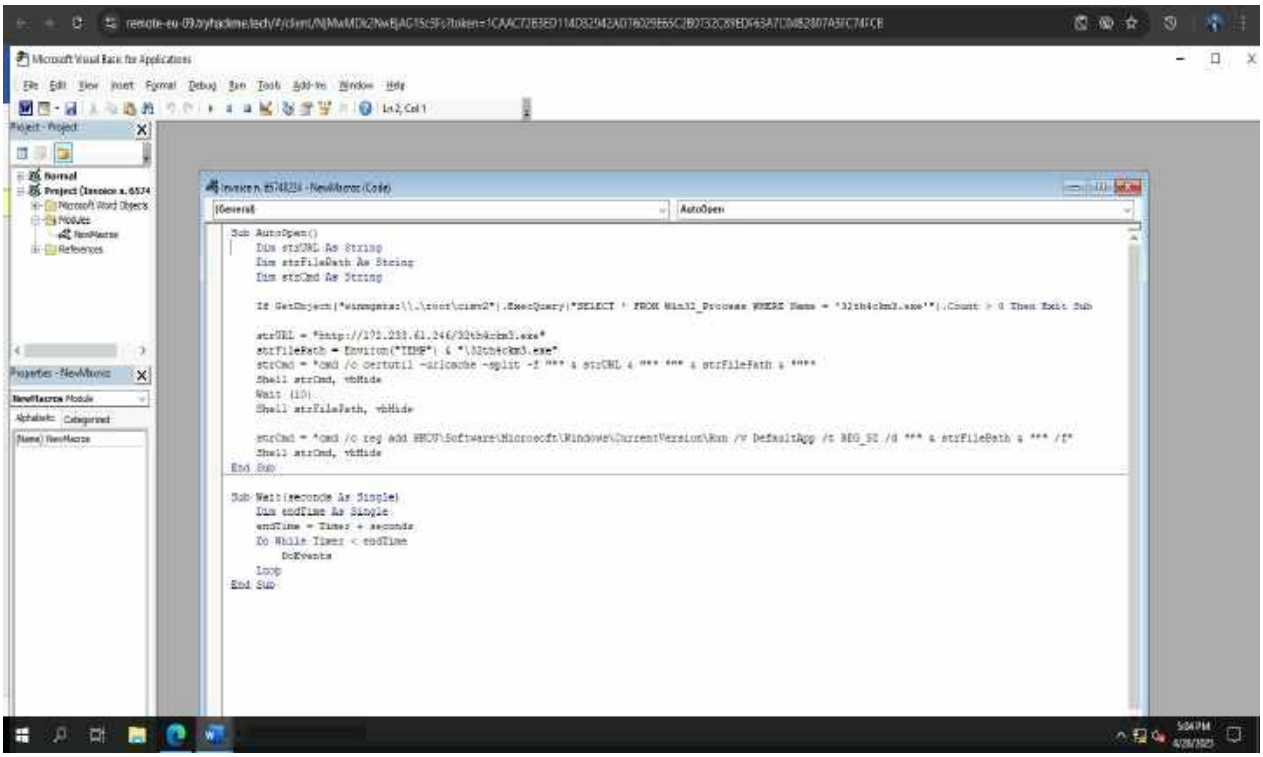


Fig 2.6 (a) & (b): Embedded hyperlink and macro in suspicious word document



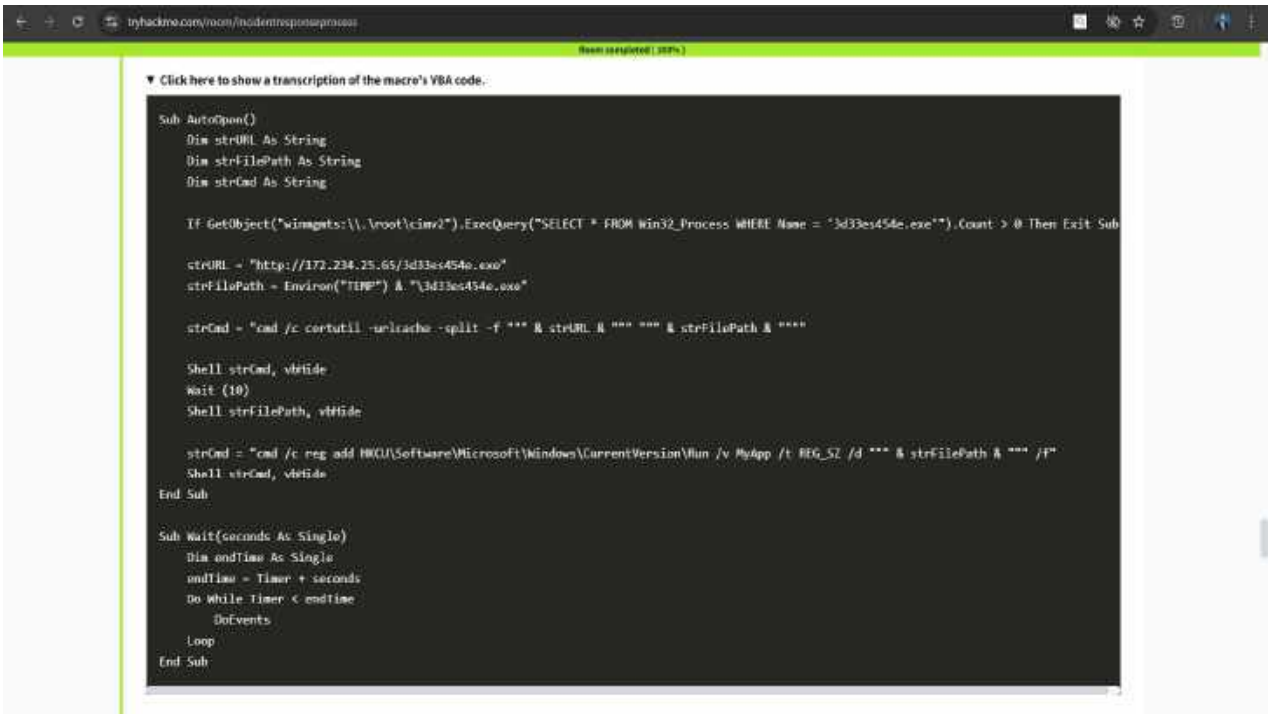


Fig 2.7 (a) & (b): AutoOpen VBA Macro code and its transcription

Macro Analysis: The macro was written in VBA (Visual Basic for Applications) code. Key findings from the macro analysis are as follows:

a. AutoOpen Definition: The macro was defined as AutoOpen, meaning it would execute automatically whenever the document was opened.

b. Variables Defined: The macro defined three variables:

strURL: The URL from which the malware (a crypto miner) would be downloaded.

strFilePath: The location on the system where the malware would be saved, pointing to a temporary directory.

strCmd: A command string for downloading the malware using certutil, a legitimate Windows utility, allowing the malware to be stealthily downloaded without triggering antivirus alerts.

c. Process Check: The macro included code to check if the process was already running. If the process was already active, the macro would terminate to prevent multiple instances of the process from executing simultaneously.

d. Downloading the Malware: The macro set strURL to the location of the crypto miner malware and strFilePath to a temporary directory. The strCmd command used certutil to silently download the malware to the system.

e. Stealthy Execution: The macro executed the strCmd command in a hidden window to download the malware, then waited for 10 seconds before executing the downloaded malware in another hidden window.

f. Persistence Mechanism: The macro added a registry entry in HKCU\Software\Microsoft\Windows\CurrentVersion\Run, ensuring that the downloaded malware would execute every time the user logged into the system. This provided persistence for the malware, explaining the slow performance even after the user rebooted the system, as reported by the SOC team.

2.1.5 Step 5: Conclusion

The analysis confirmed that the suspicious process, 32th4ckm3, was part of a crypto mining attack. The infection was triggered by a malicious Word document containing an AutoOpen macro. The macro used certutil to download the malware to a temporary directory, running it in a hidden window and ensuring its persistence through registry modifications.

The external communication observed earlier, along with the download history and macro analysis, confirmed that the system had been compromised via the downloaded document. The system slowdown was a direct result of the crypto miner consuming significant resources.