3.0 Containment, Eradication, and Recovery

3.1.0 Incident Overview

This section outlines the containment, eradication, and recovery steps taken by the Incident Response Team (IRT) after confirming a compromise involving a crypto miner malware infection. The actions here directly follow the detection and analysis phase, where we discovered that the infection was triggered by a malicious Word document containing a macro that downloaded and executed a crypto mining malware file named **32th4ckm3.exe.**

3.1.1 Step 1: Containment Actions

To immediately stop the spread and prevent further impact across the organization, we acted fast. The first thing the IRT did was isolate the affected endpoint from the rest of the network. This helped contain the infection to a single system.

Next, we terminated the malicious process—**32th4ckm3.exe**—from the Windows Task Manager. This process had been using a large portion of CPU resources and maintaining outbound communication with a suspicious IP.

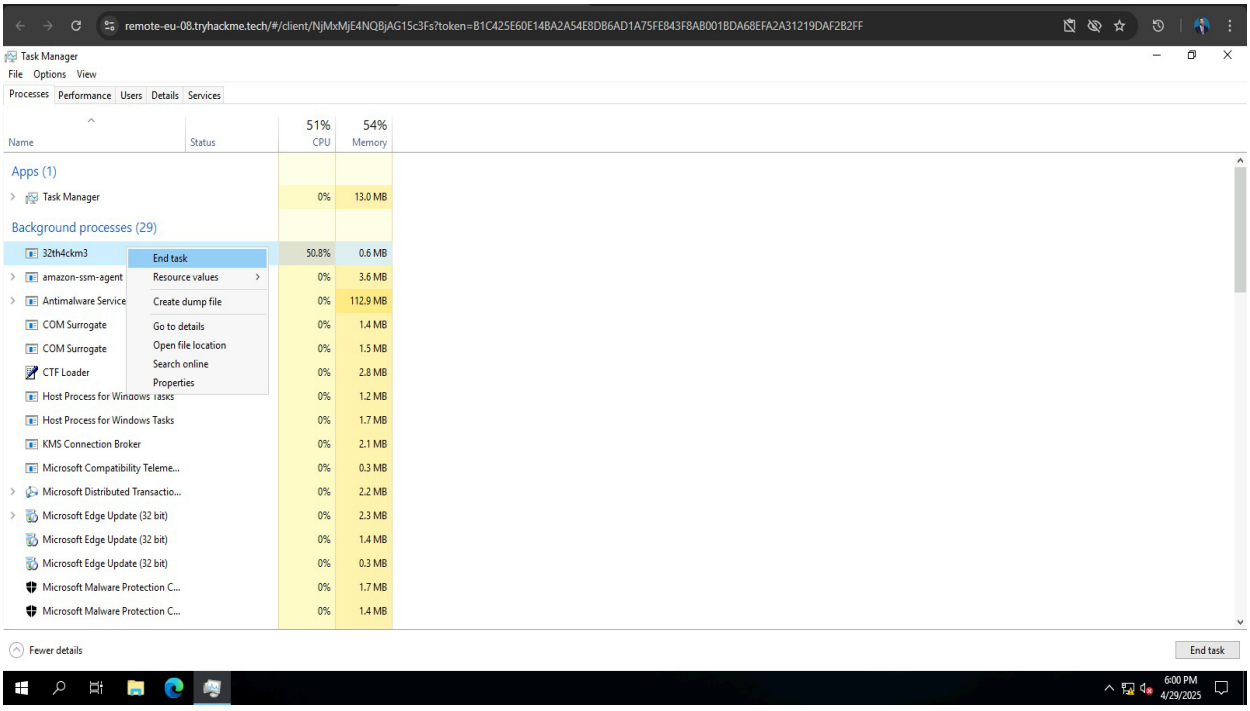

Fig 3.1: Ending Malware Process on Task Manager

After stopping the executable, we retrieved all Indicators of Compromise (IOCs) that were uncovered during the initial analysis. These included:

- The external IP address and port the malware was communicating with: 45.33.32.156:42424.
- The URL from which the macro downloaded the malware.
- The embedded URL found inside the malicious Word document titled "invoice n. 65748224.docm."

With this information, we performed a sweep across the organization's network using every detection and monitoring tool available—EDR, SIEM, IPS, and IDS—to check for any other traces of compromise or lateral movement by the malware.

3.1.2 Step 2: Eradication and Recovery

Once we confirmed the infection had not spread to other machines, we moved forward with cleaning the affected endpoint.

The first move was to delete the malware file located at:

C:\Users\TryCleanUser\AppData\Local\Temp\2\32th4ckm3.exe

This is the same temporary directory identified during the macro's execution path.

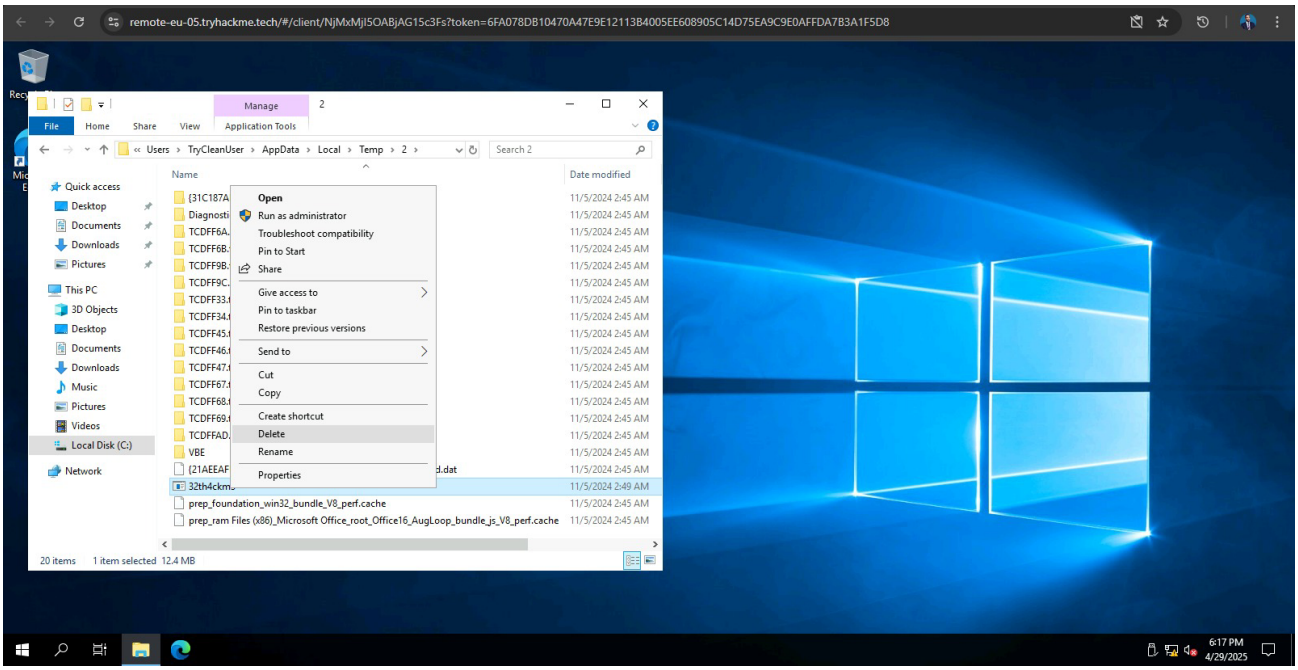

Fig 3.2: Deleting malicious executable file from temporary directory

Next, we removed the malicious Word document that had been downloaded via the browser. The file—"invoice n. 65748224.docm"—was deleted from the system and its download record was cleared from the browser history to prevent future accidental access.

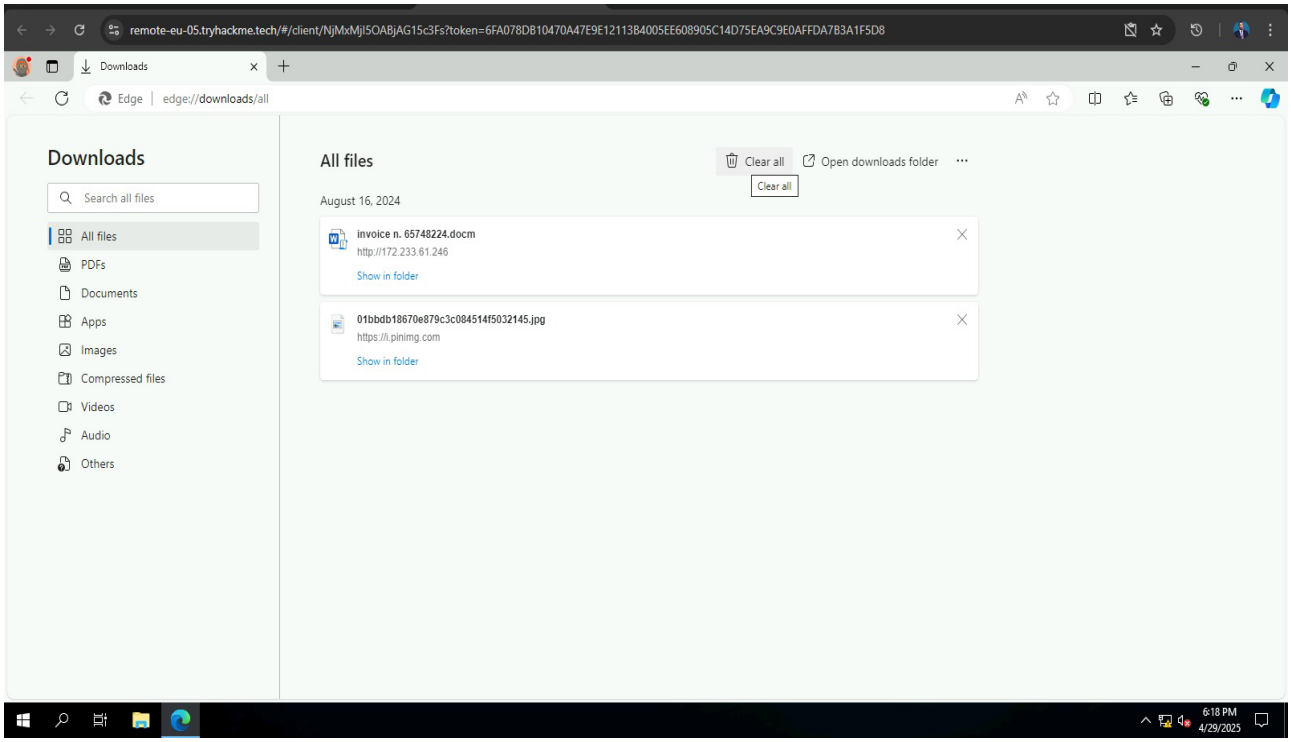

Fig 3.3: Deleting Downloads History

To ensure complete eradication and eliminate the malware's persistence mechanism, we also checked and cleaned the system registry. The malicious macro had created a registry entry under the Run key, which would automatically execute the malware every time the system booted or the user logged in. To remove it, we launched the Registry Editor and navigated to:

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

There, we found a suspicious entry titled "Default app"—the key responsible for launching the malware executable on startup. We carefully deleted this key to prevent any automatic re-infection or execution during user logins.

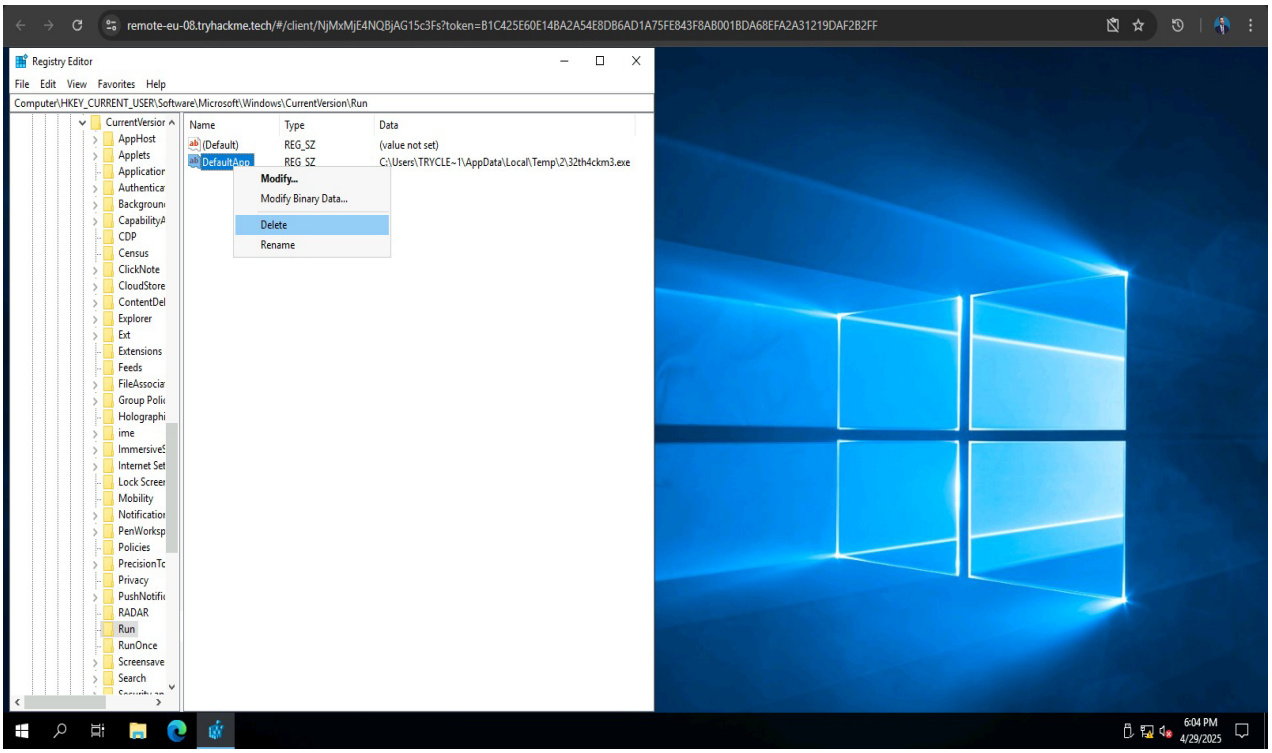

Fig 3.4: Deleting the Registry Run Key named Default App added by the Macro

These steps ensured the malware payload and its initial dropper were completely removed. Afterward, we performed a final scan using our antivirus, EDR, and registry monitoring tools to confirm that:

- No persistence mechanism (like registry keys) remained.
- No additional malicious processes were running.
- System performance had returned to normal.