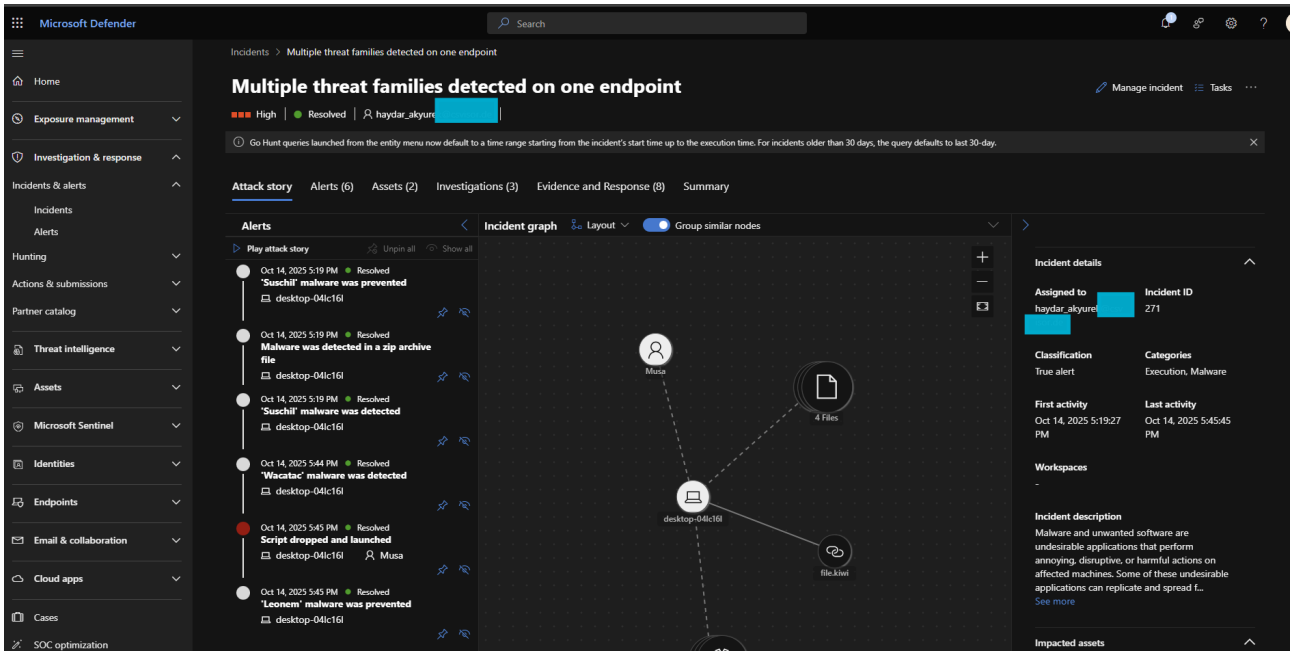
📁 Incident Metadata

Case Type:	Email and URL Threats
Reported by:	Microsoft Defender
Analyst:	Haydar AKYÜREK
Date:	2025-10-15
Severity:	🔴 **High**
Status:	✅ Closed
Decision:	✅ **True Positive**

📜 Incident description:

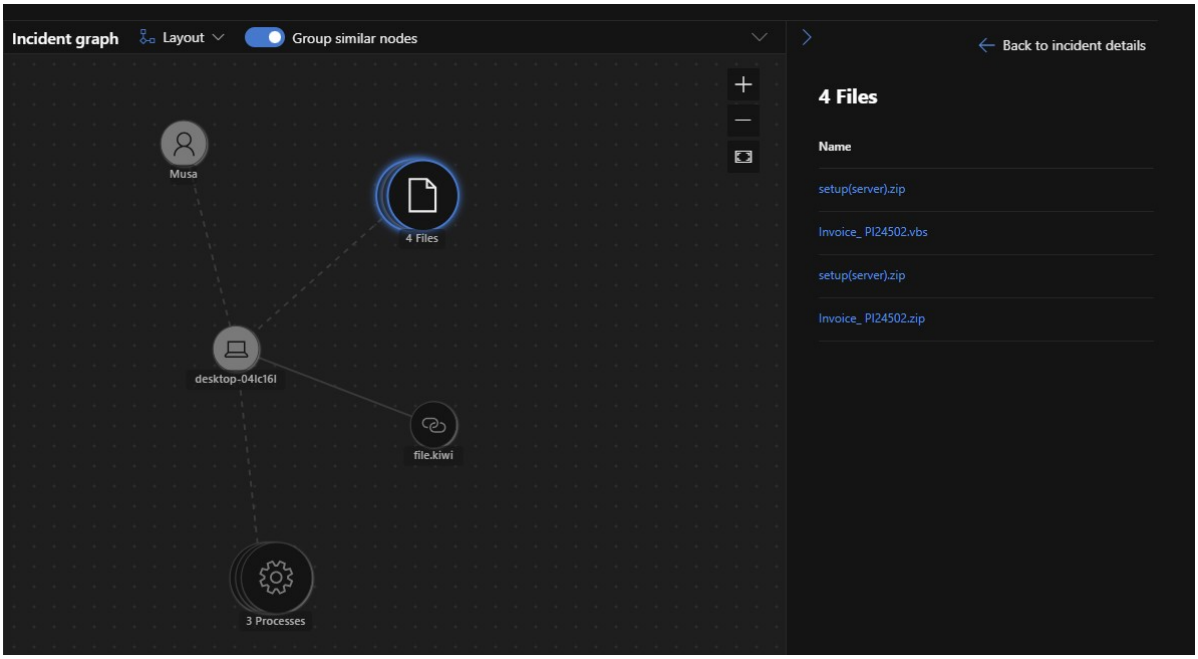
Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.

This detection might indicate that the malware was stopped from delivering its payload. However, it is prudent to check the machine for signs of infection.

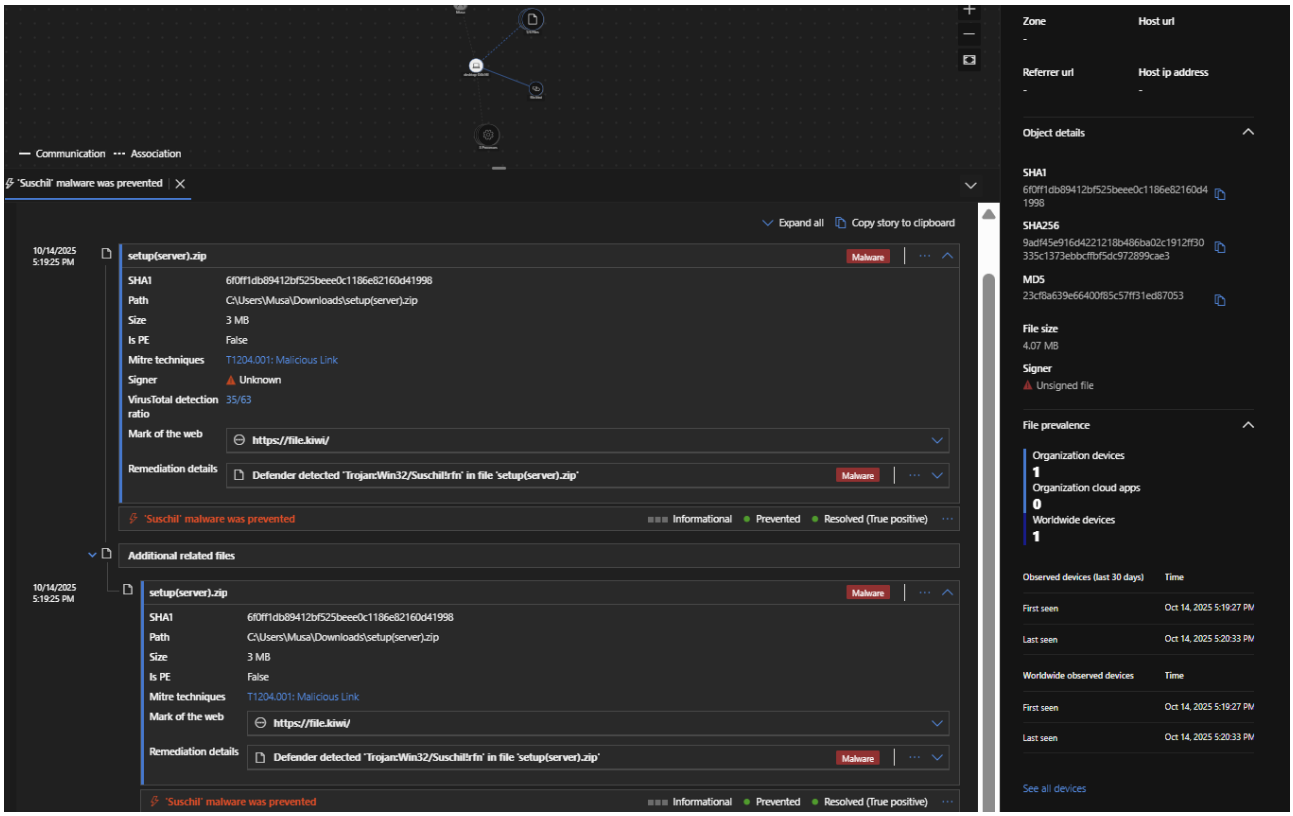


🔍 Microsoft Defender Incident Analysis Notes

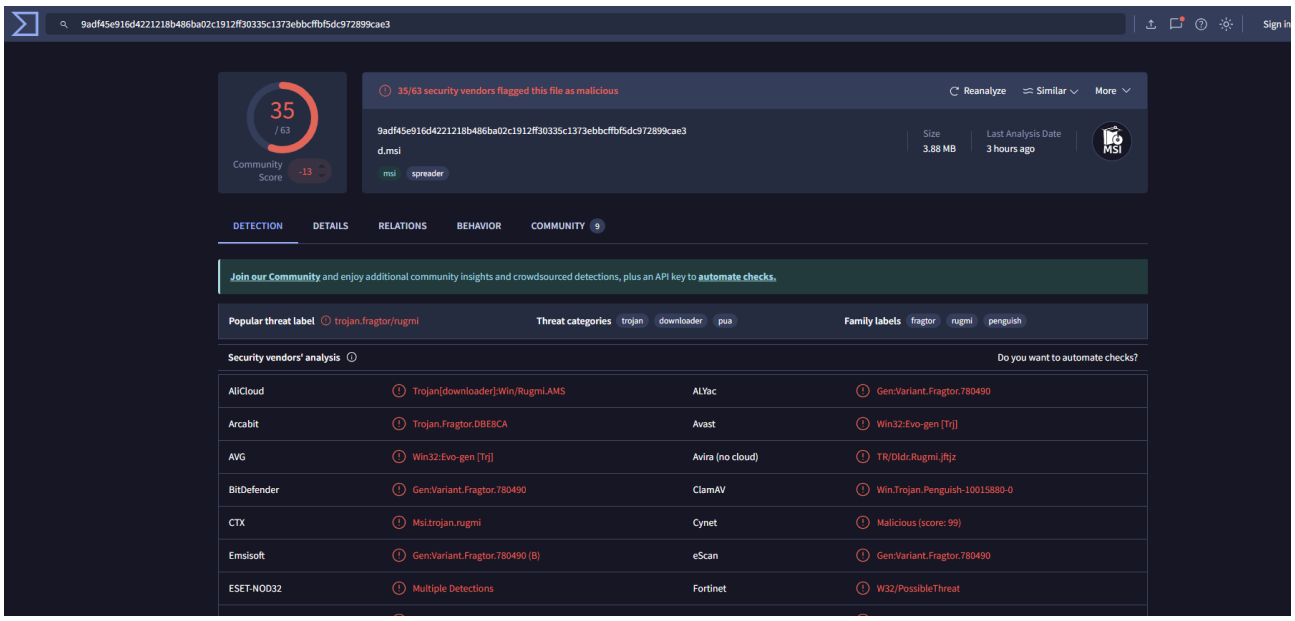
1. We select Incident and begin examining it. We see there are six alerts. Two of them are under the same "detected" and "prevented" headings.
2. There are a total of four files, three processes, and one domain. We select "View 4 Files" and look at the file names.



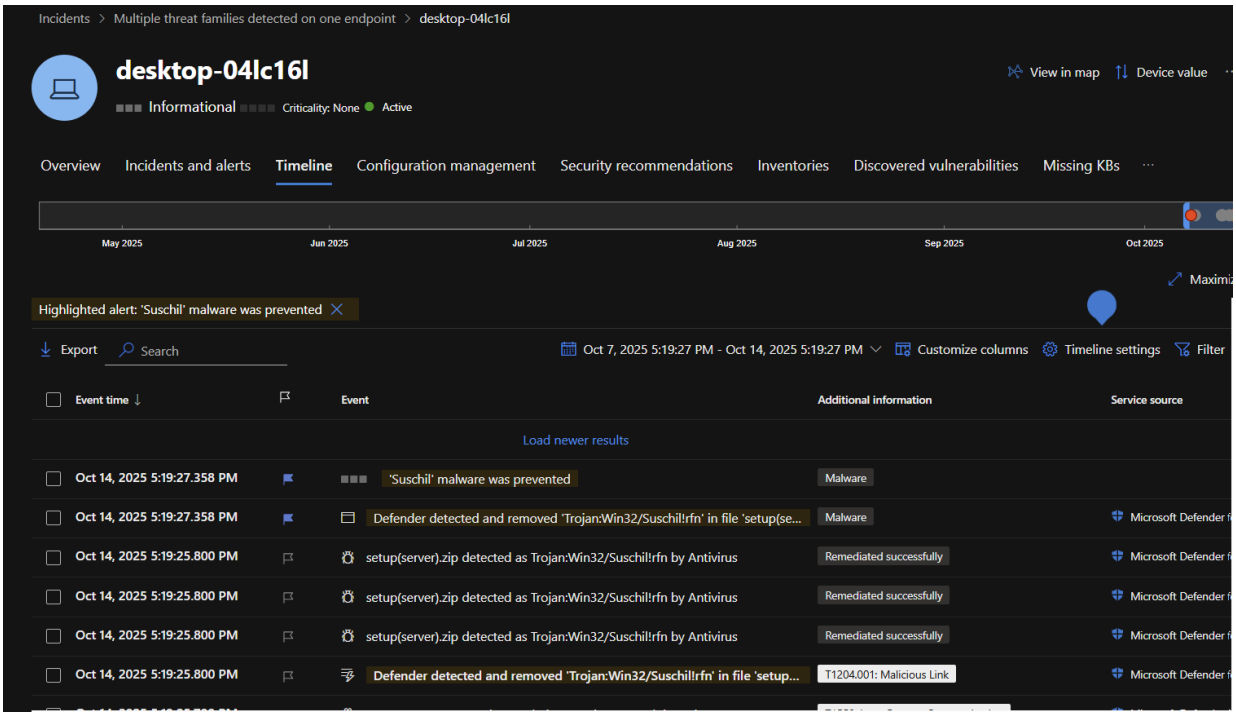
3. We also looked at the URL and processes. Then we clicked the first alert.



Similarly, we saw that this zip file came from Kiwi and checked its virustotal record. We also see that this zip file has been quarantined.

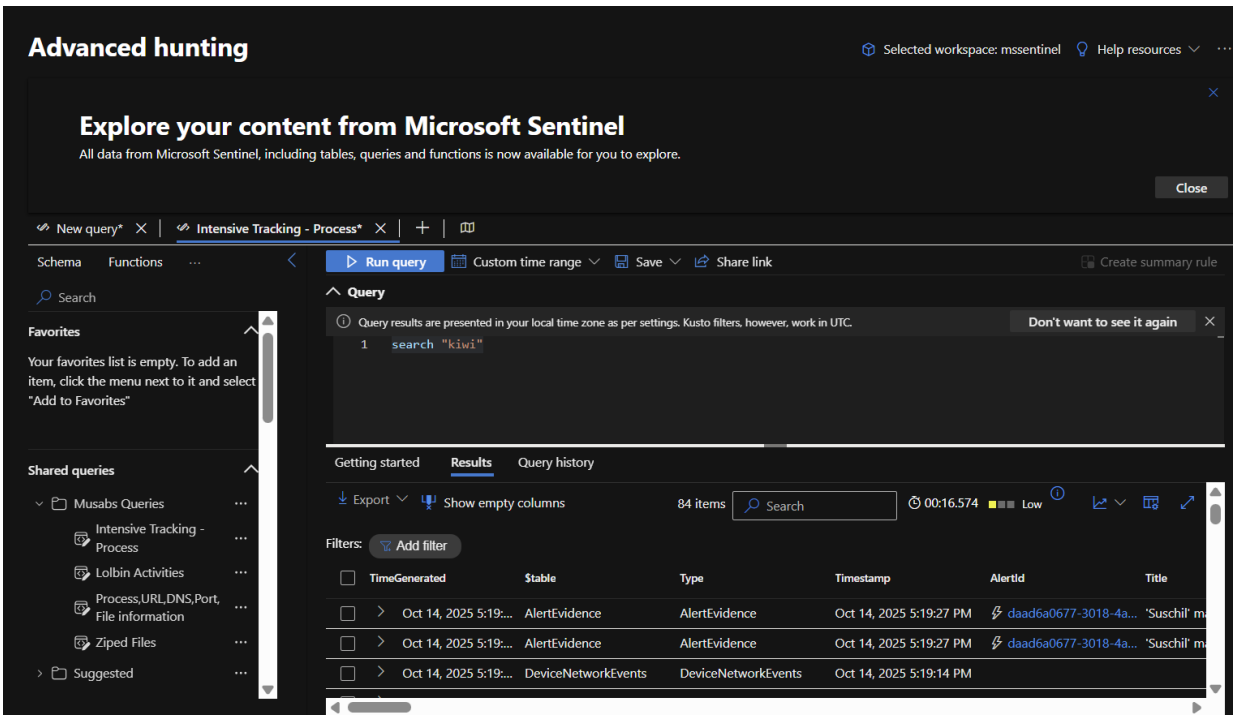


4. After clicking on the Alert, we pressed the three dots on the right side of the screen and clicked See in Timeline.



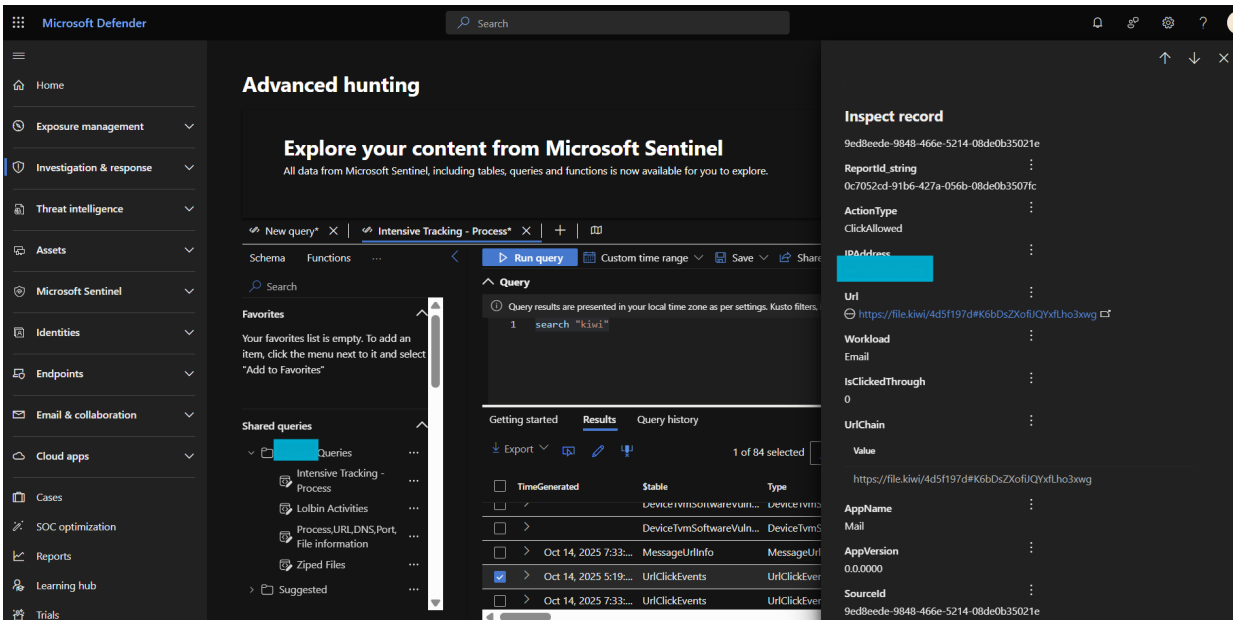
We adjusted the Timeline section and searched for "setup(server).zip." We couldn't find the exact domain record. Then we searched for "kiwi." But it still showed File/kiwi.

5. Then, to access this full domain information, we moved on to the Hunting section. We also found domain records here.

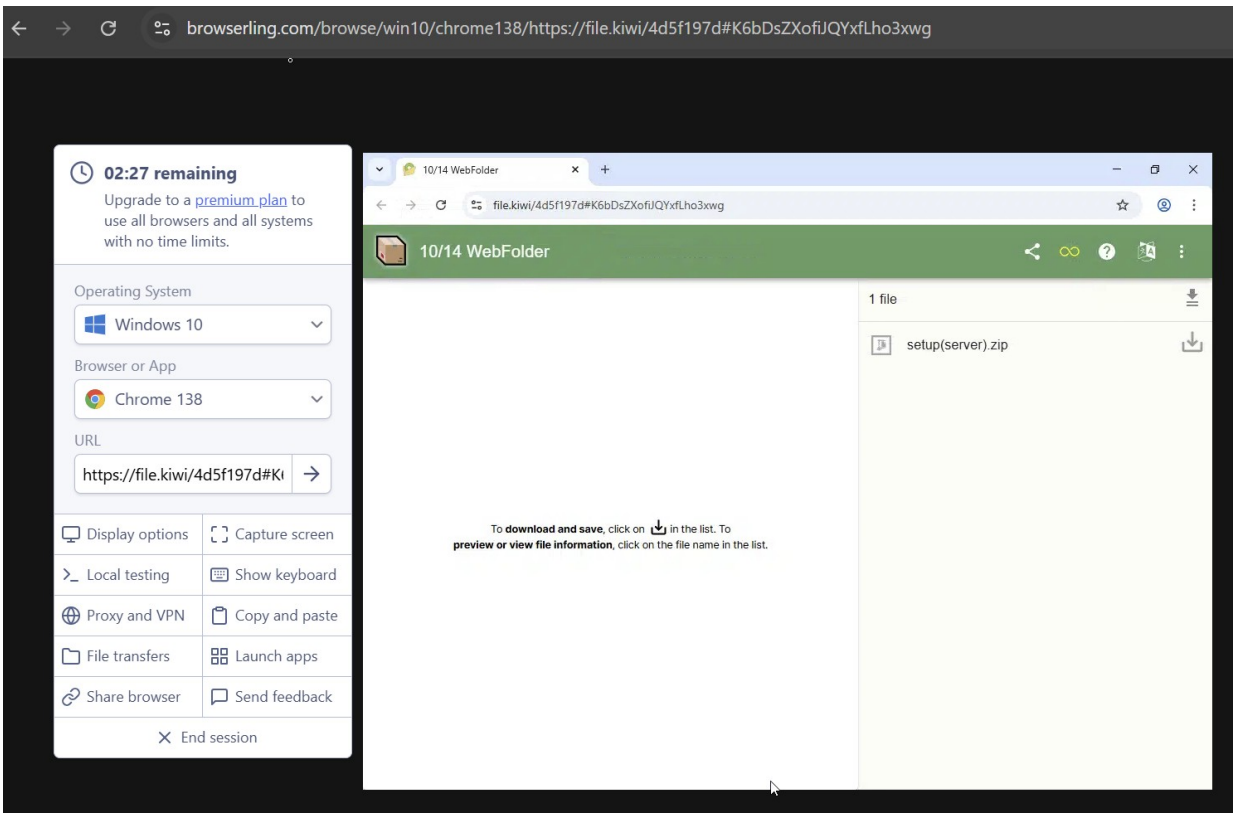


After reviewing, we saw email logs as URLClickEvents.

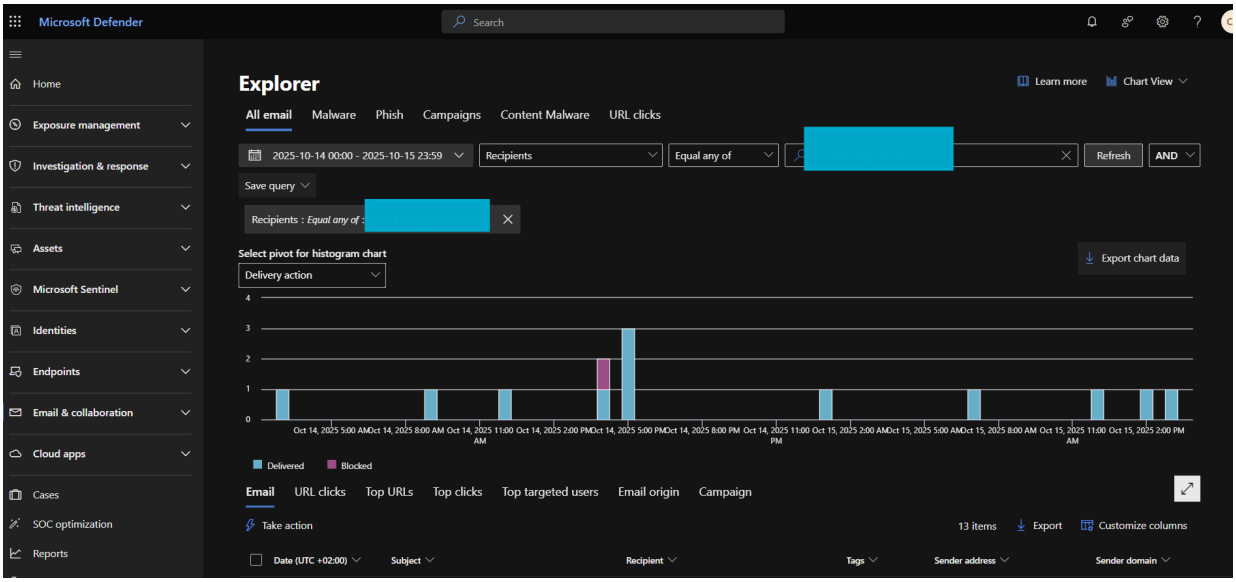
6. When we clicked on one of these logs, we saw that it gave us full URL information.



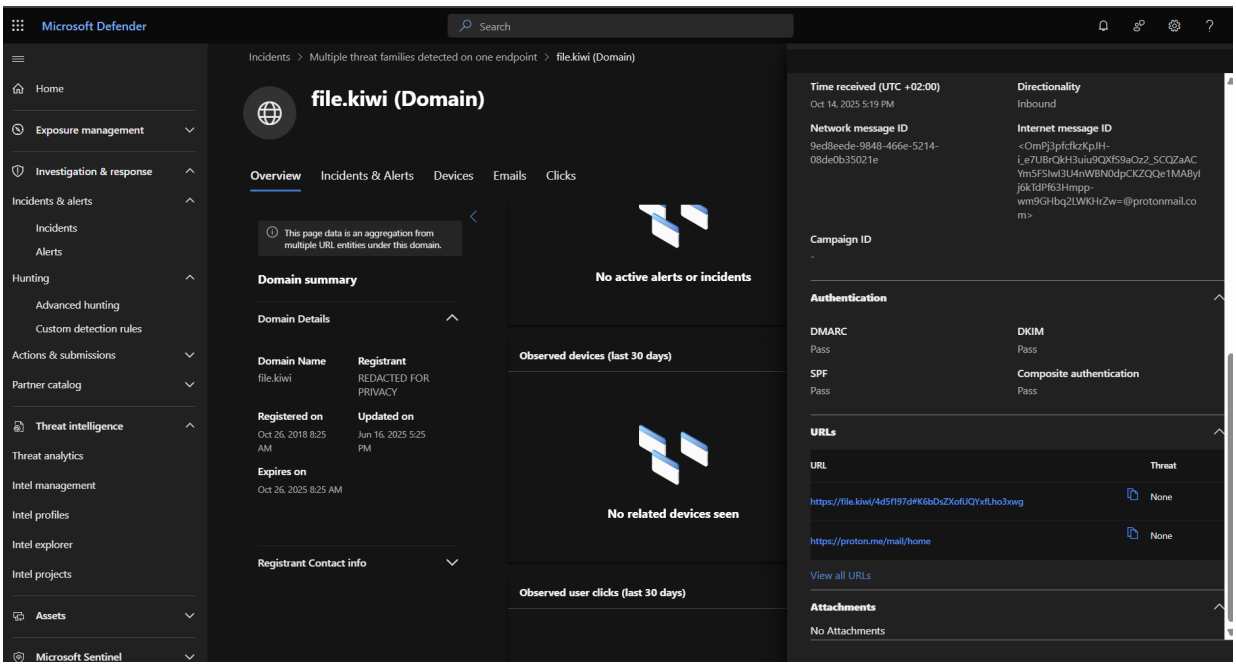
We looked in a sandbox environment to see if this was the file we were really looking for.



7. We went to the Explore section from the Email & Collaboration section. Here, we can also access the full URL information on the events. Here, we see that the user has landed in their inbox and clicked.



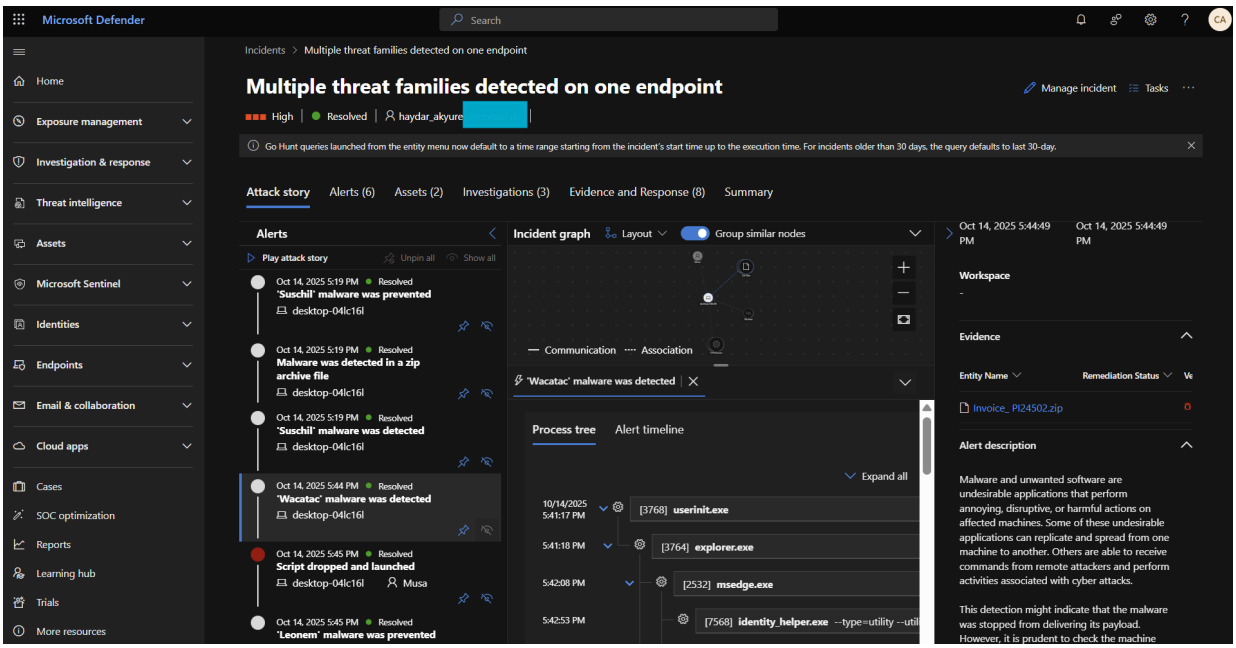
8. Finally, when we right-clicked and opened the Kiwi URL in the Incident Graph, we saw that we could access the URL information. Here, we also see that the email tab says "delivered."



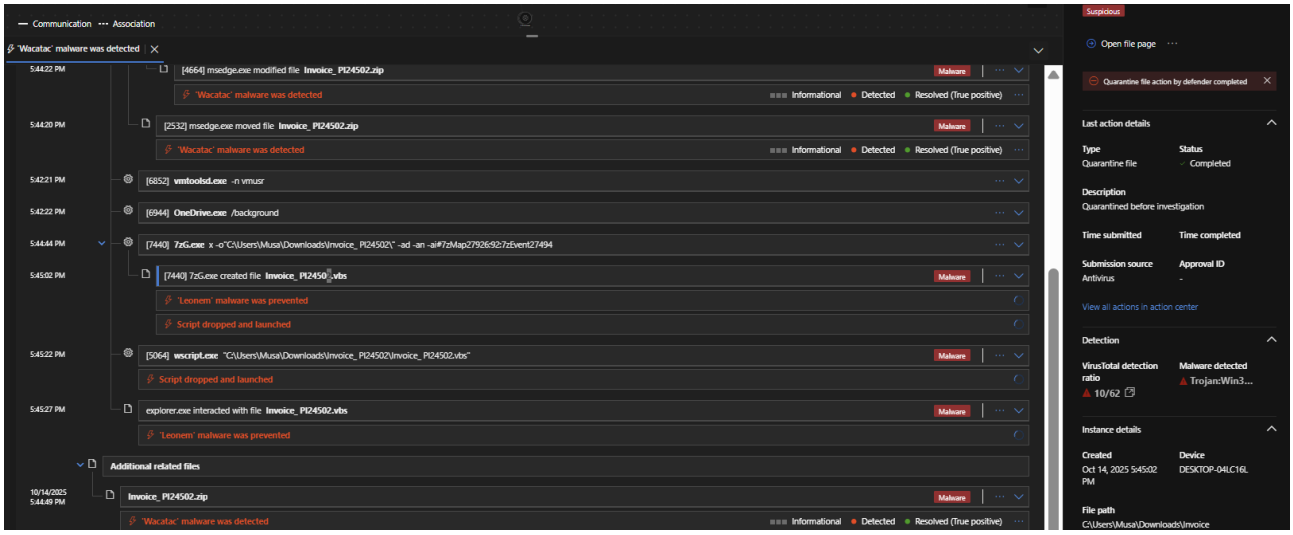
9. Here we also see the DMARC and DKIM records. They are all listed as Pass.

- **SPF (Sender Policy Framework):** Tells which mail servers are allowed to send emails for your domain.
  👉 *"Who is allowed to send?"*
- **DKIM (DomainKeys Identified Mail):** Adds a digital signature to emails so the receiver can verify they weren't changed.
  👉 *"Was it changed?"*
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** Uses SPF and DKIM to decide what to do with suspicious emails (accept, quarantine, or reject).
  👉 *"What should happen if it fails?"*

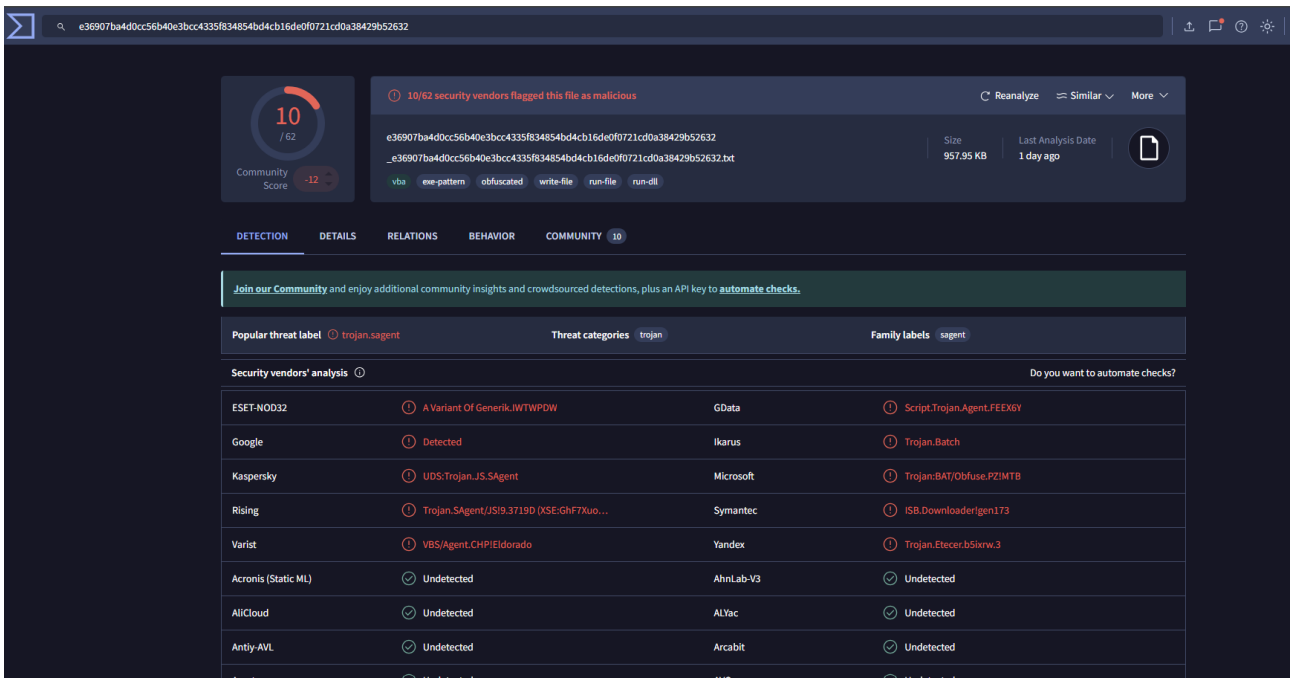
10. Now let's move on to the next alert. There's a file named invoice. Looking at the processes here, the user has opened the machine. Explorer.exe has run. The invoice... zip file has arrived via msdedge.exe. Here, on the right, we see the source of the "Referer Url."



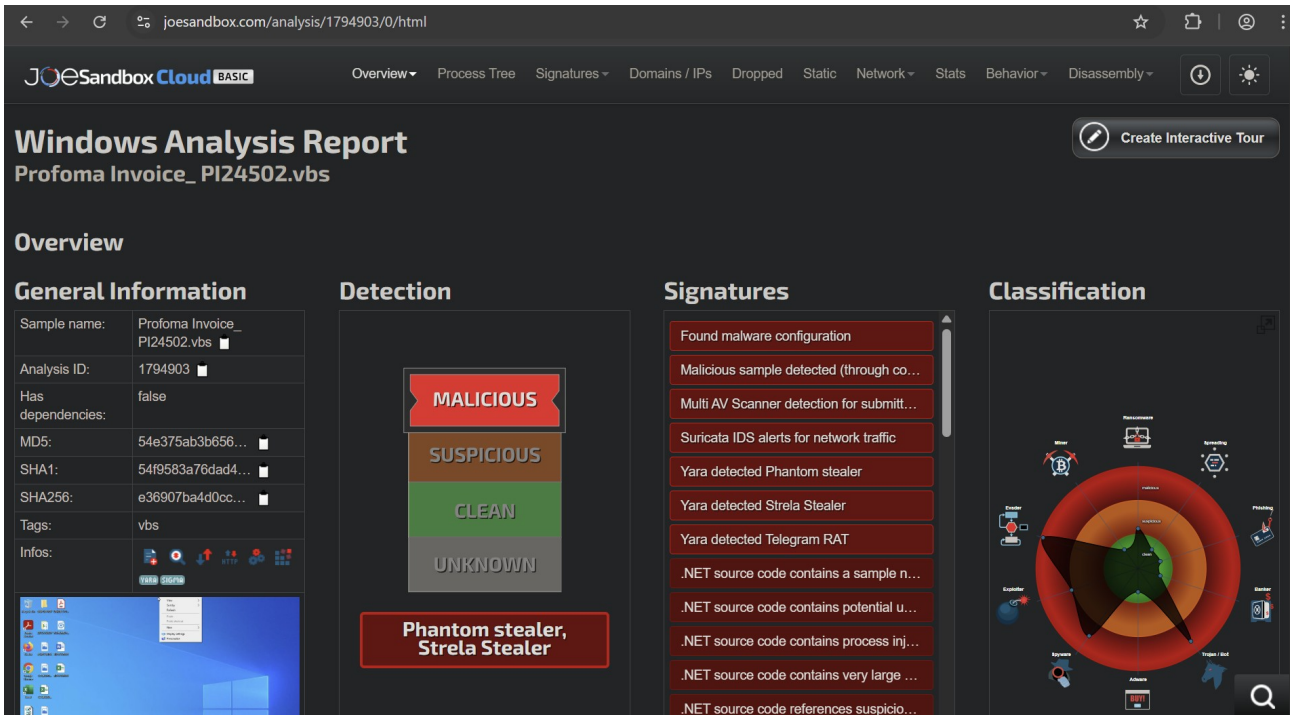
11. When this zip file was first downloaded, we saw that it was only detected. However, when opened with 7zip.exe, we found that it was immediately blocked.



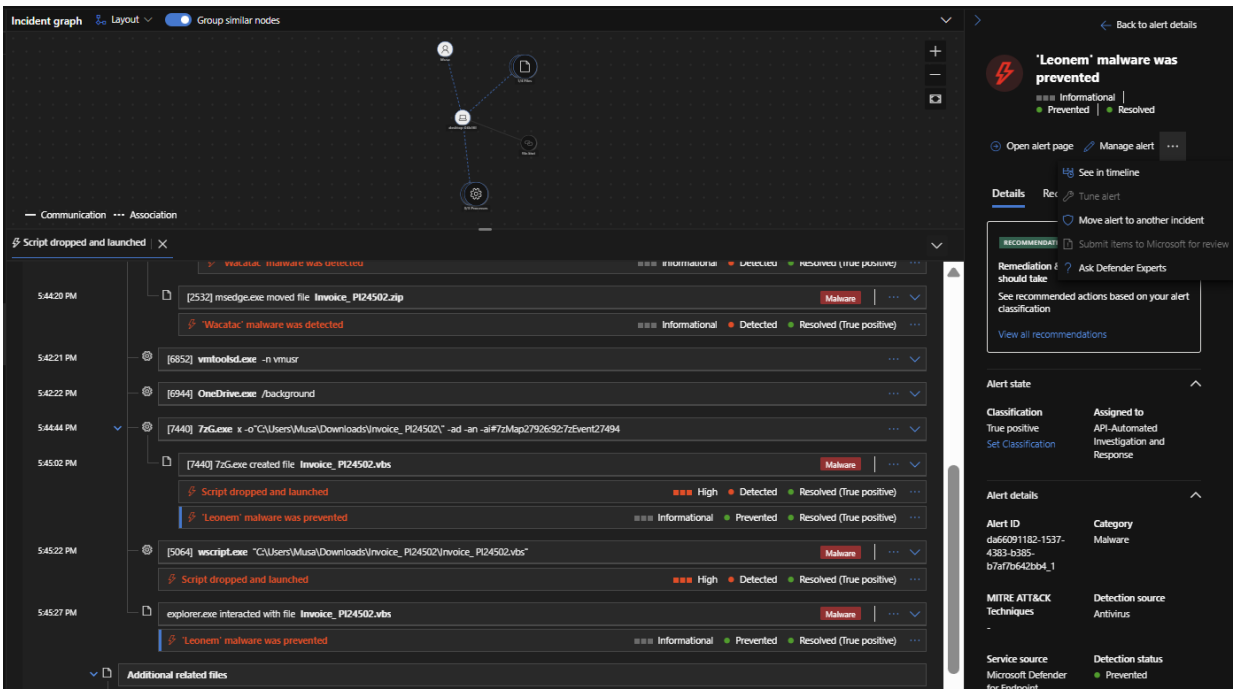
We looked at the file on Virustotal:



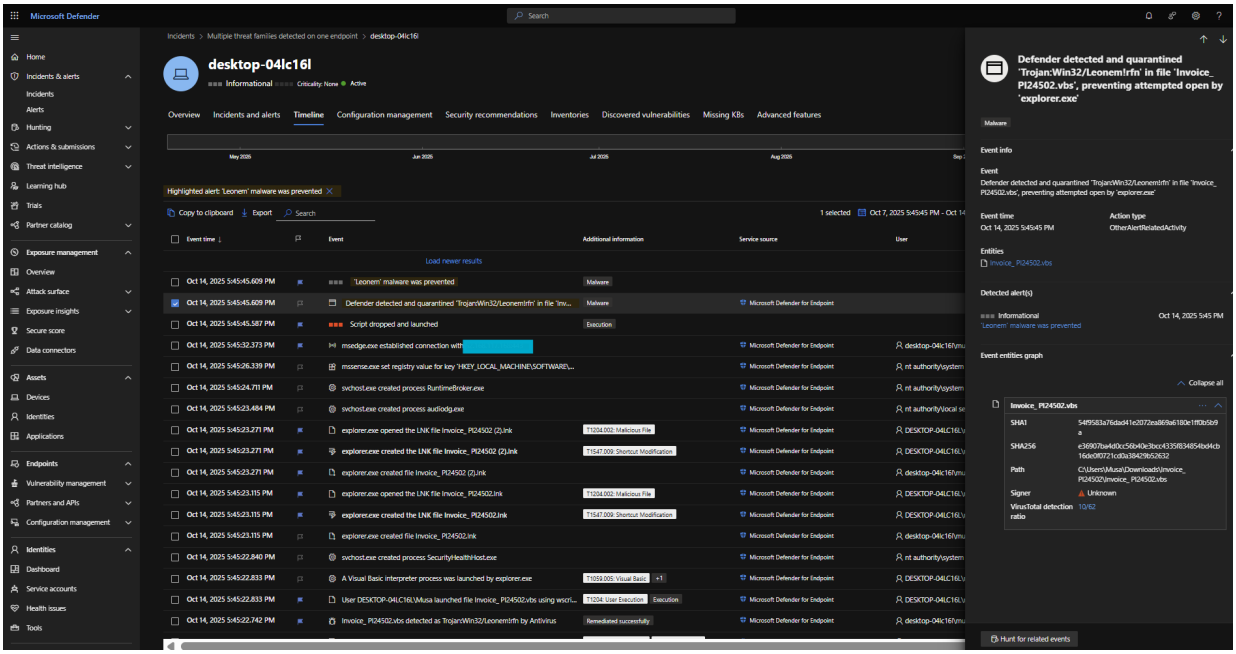
Next, we wanted to look at the sabdbox report. It might have worked on our machine as well. We'll see if it performed the same operations.



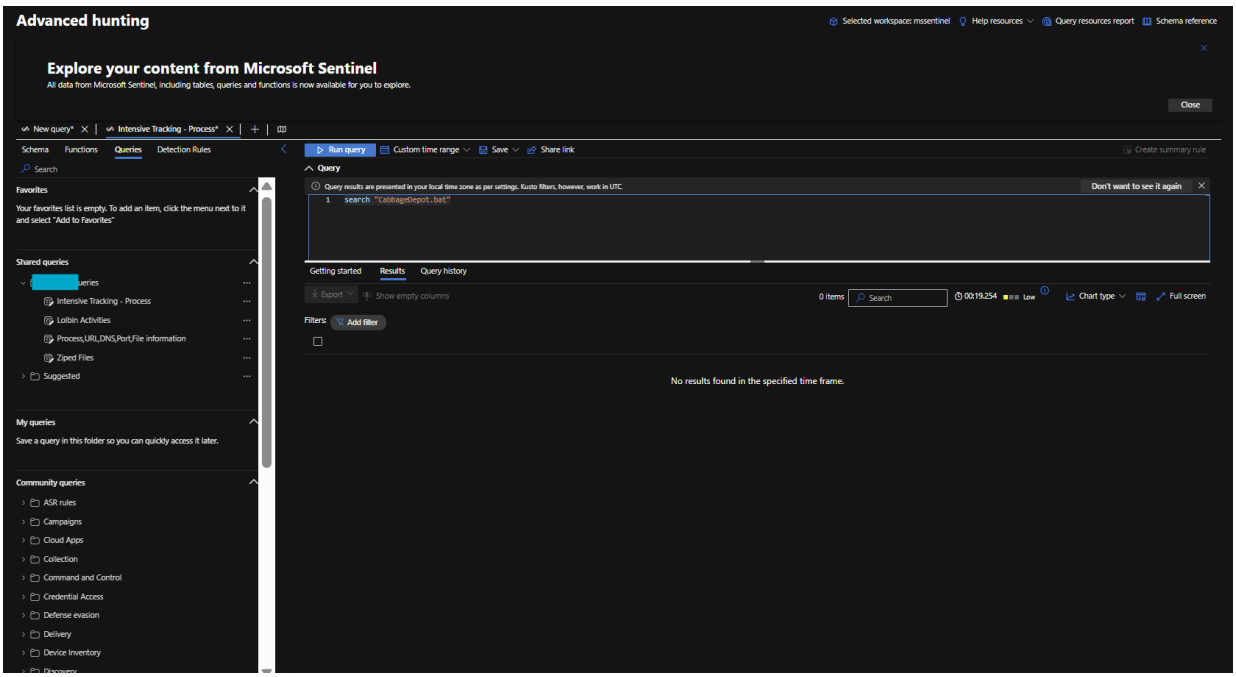
12. Afterwards, while we were researching these possible side effects on our computer, we clicked on the alert, clicked on the 3 dots on the screen that opened on the right, and said "See in Timeline".



13. Now, using this opened timeline, we checked whether any of the processes in joesandbox were running. We didn't see any problems.



14. To be completely sure, we searched the file named “CabbageDepot.bat” in the sandbox with Advanced Hunting.



We saw that it didn't work. We also ran IP scans for network connections, etc. There were no problems.

15. Finally, we searched for the file named "Invoice_PI24502.zip" in the Hunting section and reconfirmed its source in the FileOriginUrl section. We also checked whether this link was only in the device logs or whether there was an email address. Then, we ran an advanced search to see if any other emails had been sent from these senders.

Decision: ✅ **True Positive**

🔧 Recommended Actions (SOC Level)

- Quarantine and preserve evidence: collect memory, full disk image and relevant logs before remediation.
- Perform eradication and recovery on the host; ensure malicious artifacts, files, and persistence are removed.
- Provide security awareness training to the user.
- Document findings, update detection rules, and run tabletop/lessons-learned to close gaps.