📁 Incident Metadata

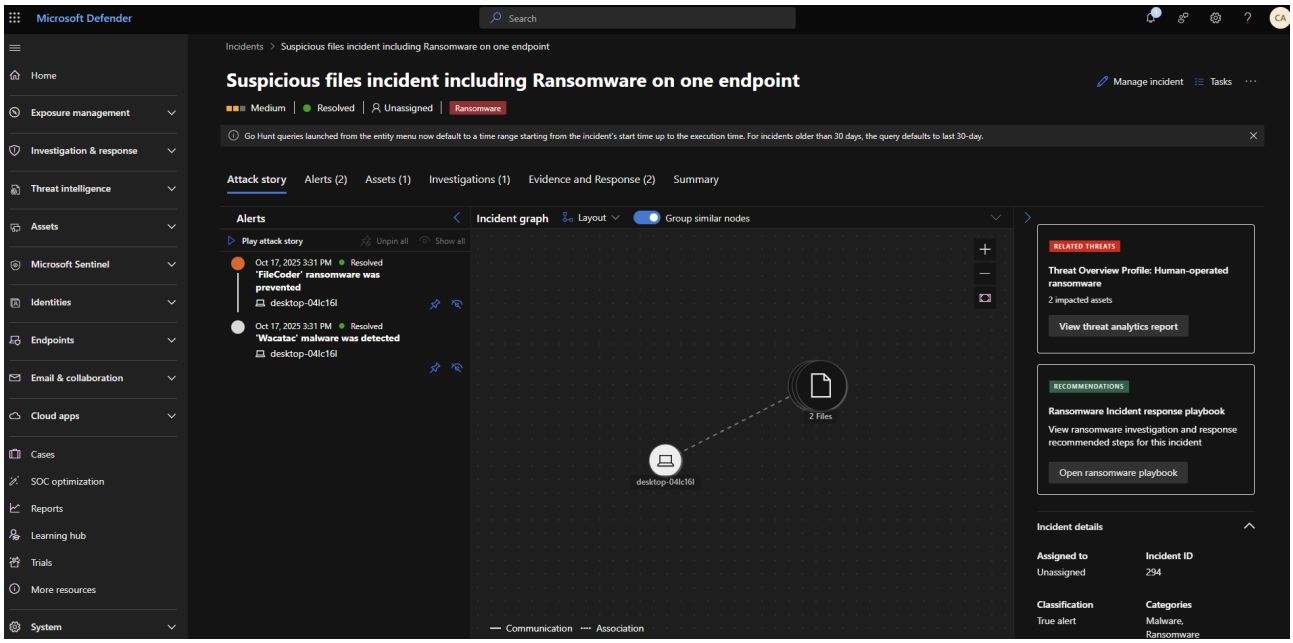
Case Type:	Ransomware
Reported by:	Microsoft Defender
Analyst:	Haydar AKYÜREK
Date:	2025-10-25
Severity:	🔴 **High**
Status:	✅ Closed
Decision:	✅ **True Positive**

📜 Incident description:

Ransomware use common methods to encrypt files using keys that are known only to attackers. As a result, victims are unable to access the contents of the encrypted files. Most ransomware display or drop a ransom note—an image or an HTML file that contains information about how to obtain the attacker-supplied decryption tool for a fee.

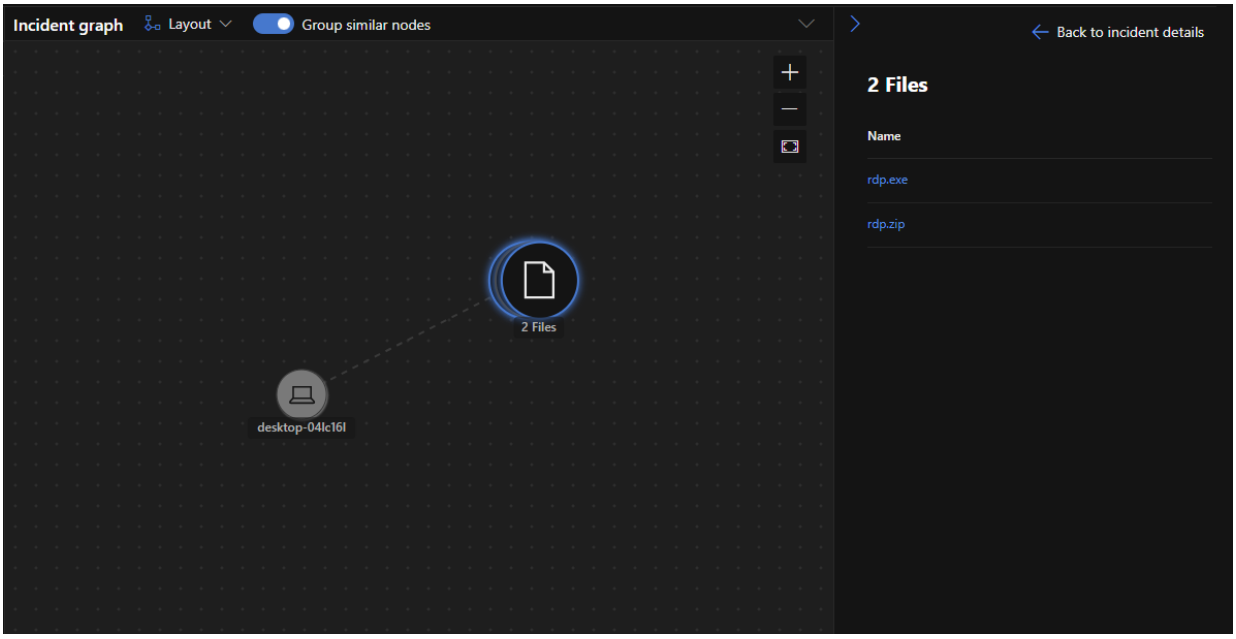
To target documents or other files that contain user data, some ransomware look for files in certain locations and files with certain extension names. It is also common for ransomware to rename encrypted files so that they all use the same extension name.

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.

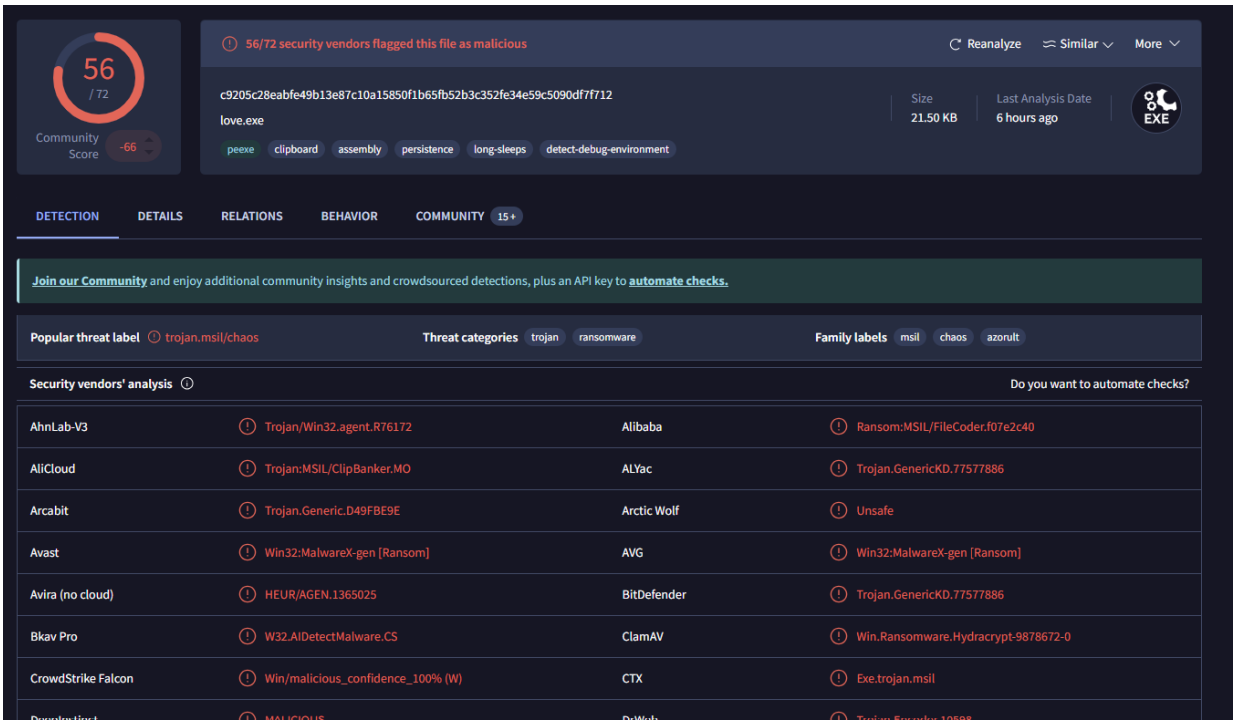


🔍 Microsoft Defender Incident Analysis Notes

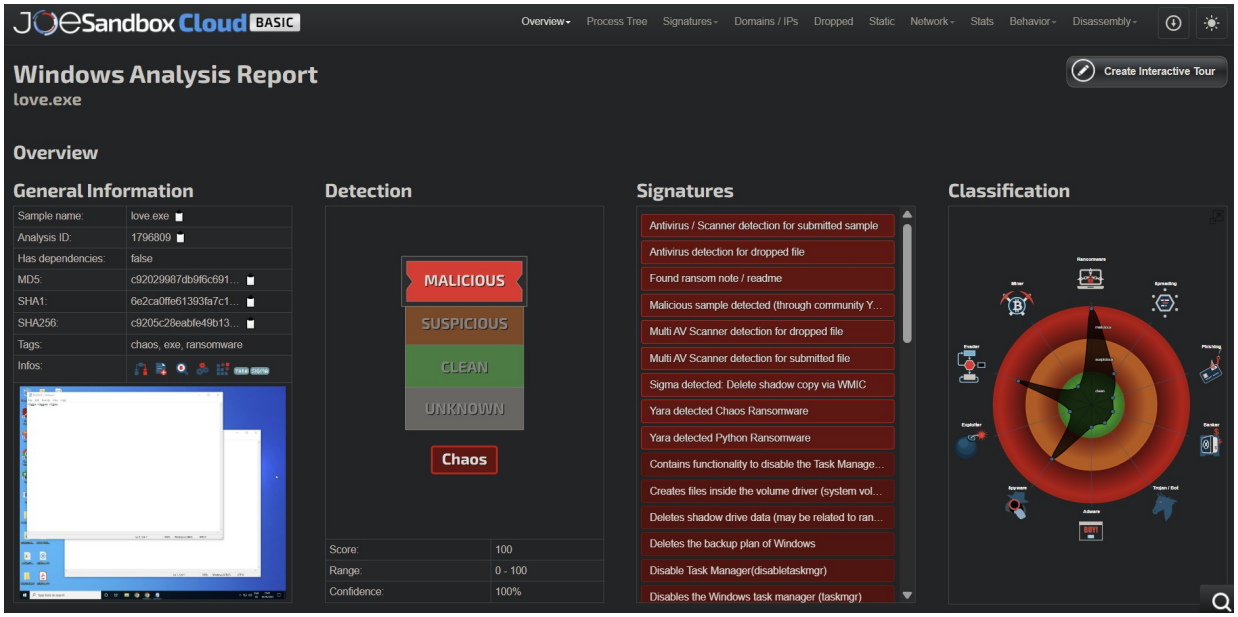
1. When we looked into it, there were two alerts. Defender usually reports *Wacatac* when it detects something malicious inside a zipped file. Indeed, there are two files — one executable (.exe) and one zipped file.



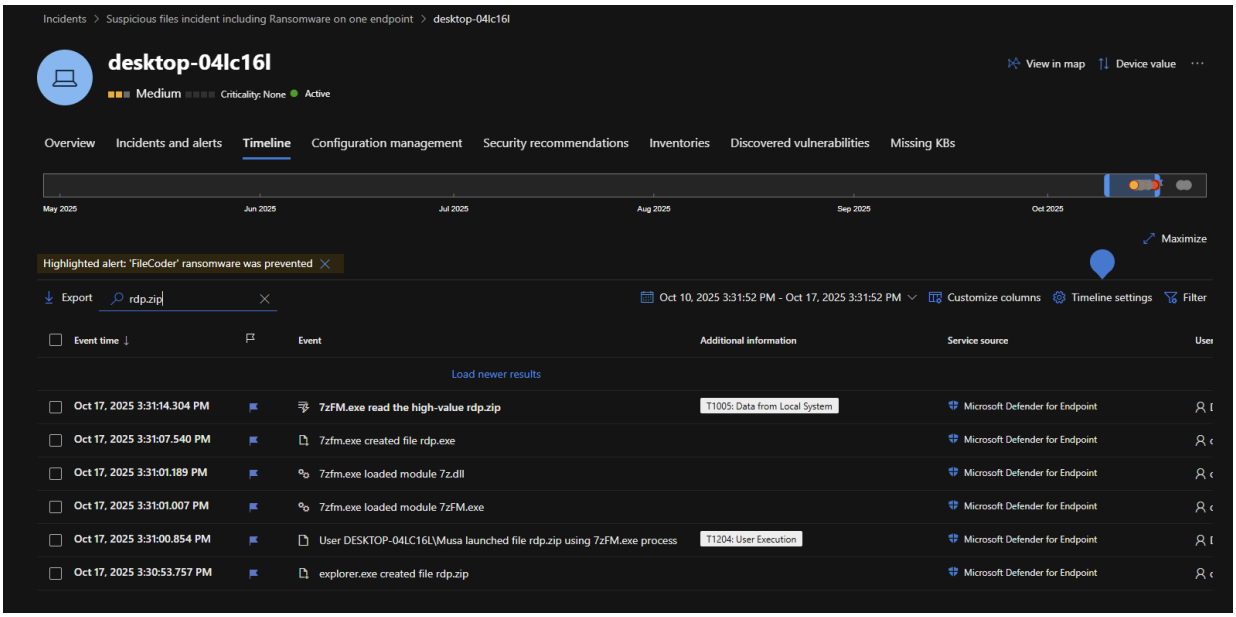
2. We checked the VirusTotal report for the **rdp.exe** file



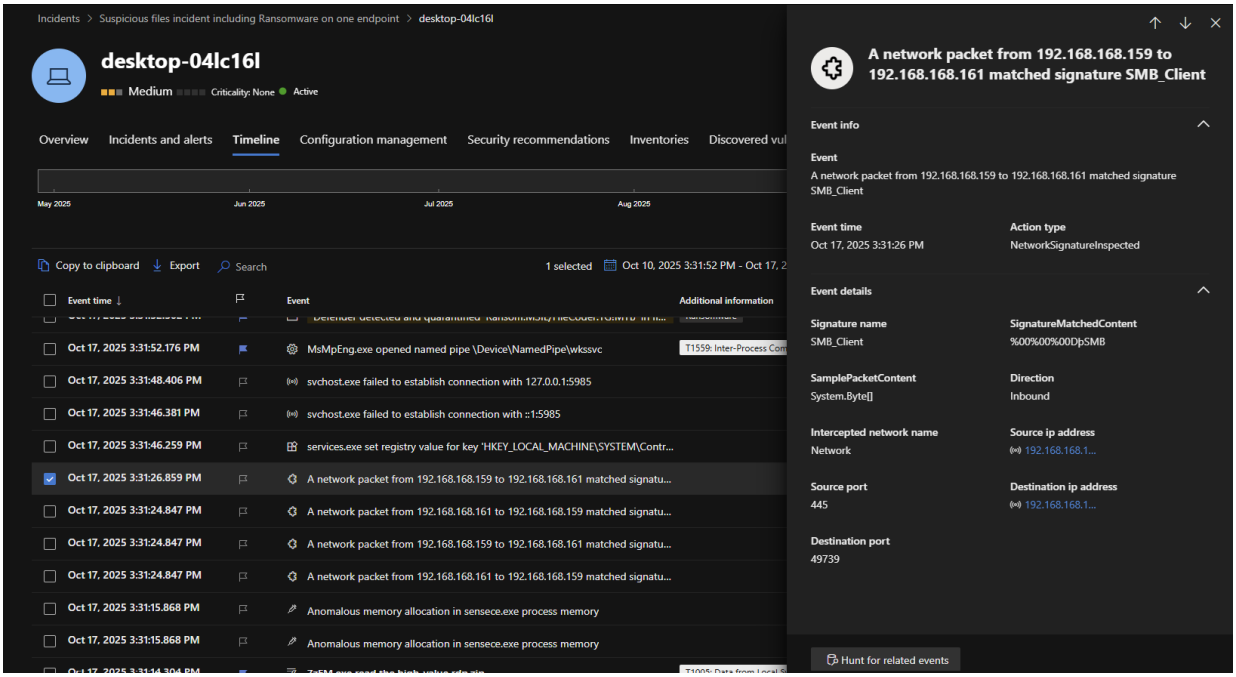
3. We also investigated it in a sandbox environment.



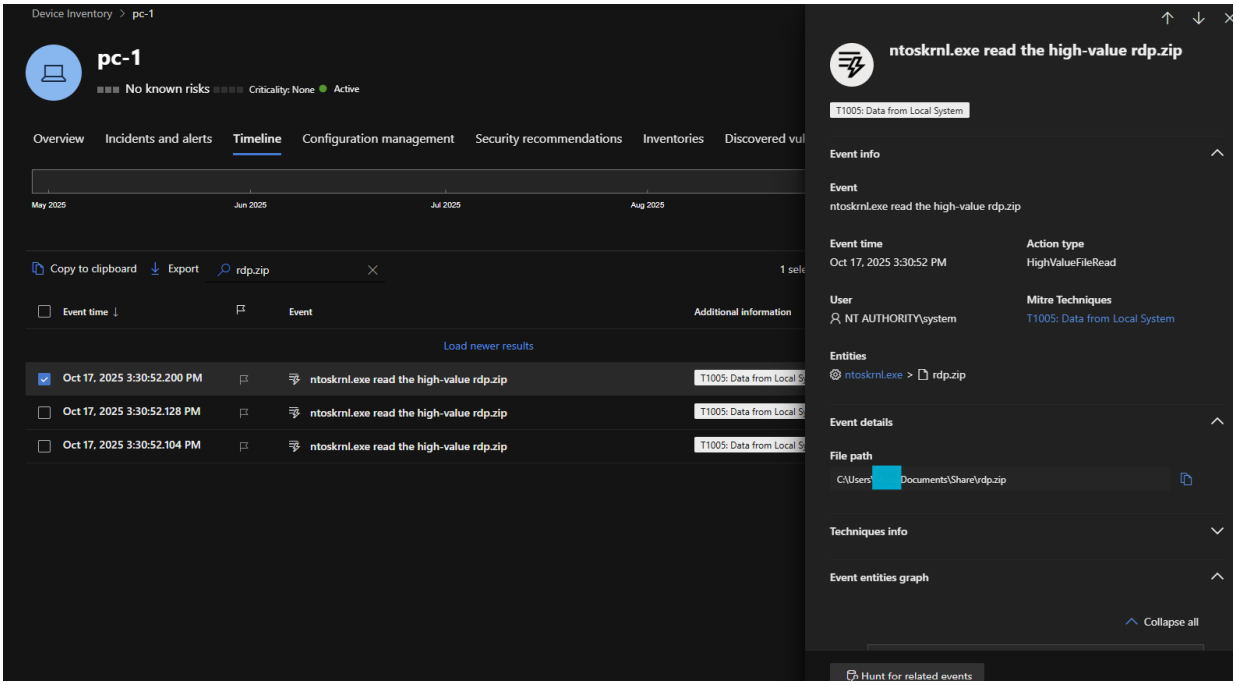
4. We clicked **“See in Timeline”** and started analyzing it.



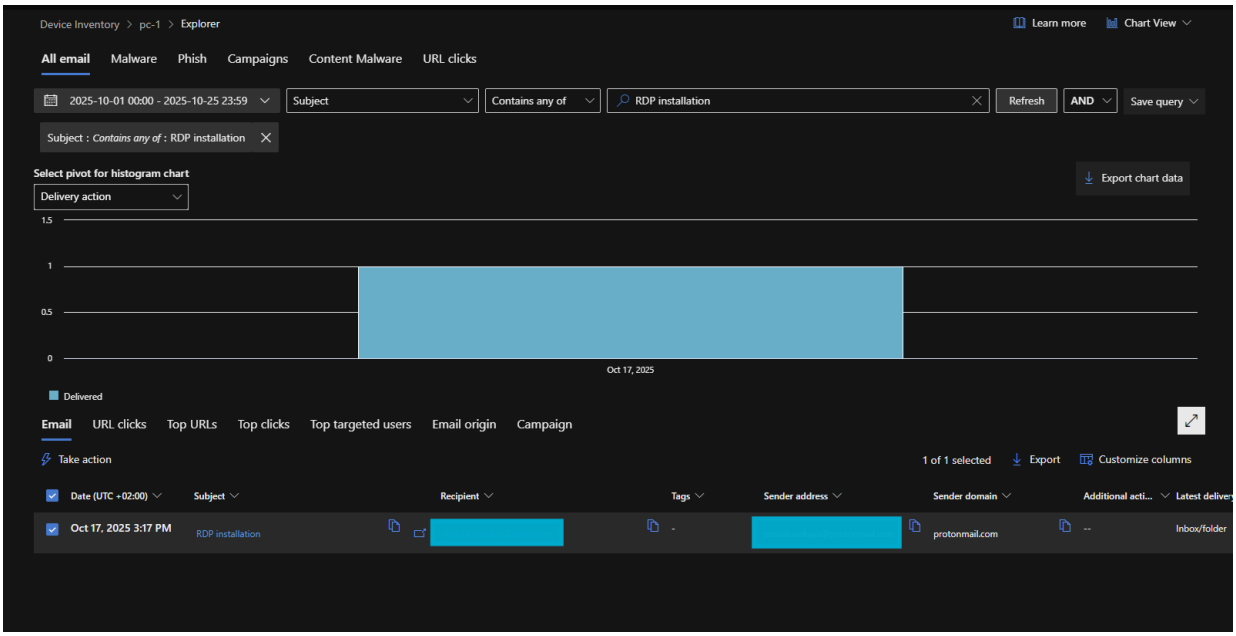
5. We observed an **SMB connection** here.



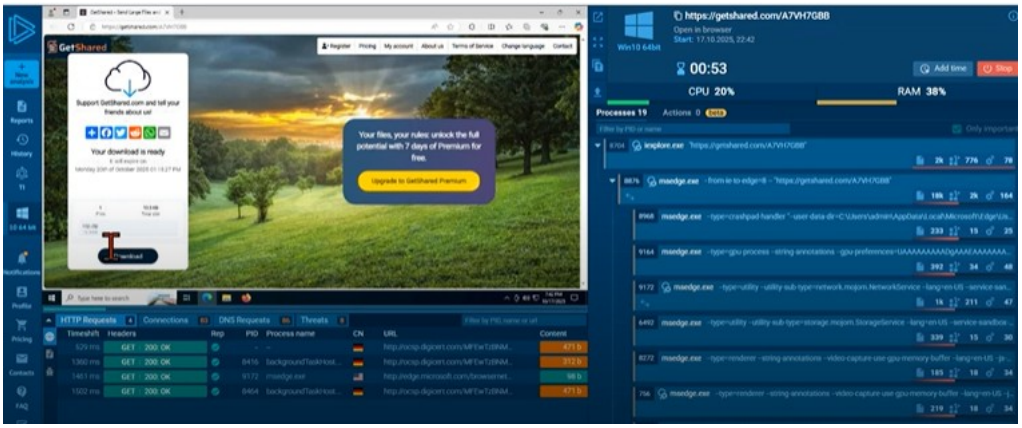
6. Next, we decided to investigate where the file came from via **Email**. In the “recipients” field, we entered this user and discovered that the root cause of the incident was a malicious file delivered through email.



7. Next, we decided to investigate where the file came from via **Email**. In the “recipients” field, we entered this user and discovered that the root cause of the incident was a malicious file delivered through email.



8. When we clicked the subject line, a URL link appeared in the right panel. We submitted this link to **AnyRun** for sandbox analysis and confirmed it was the same **rdp.zip** file.



9. In conclusion, a file was doswloaded from email and executed from that machine. The affected machines needs to be re-imaged. We resolved the root cause on our own machine.

Decision: ✅ **True Positive**

🔧 **Recommended Actions (SOC Level)**

- Re-image the affected machine.
- Block or isolate the source host (\PC-1).
- Review SMB share permissions and disable unnecessary shares.
- Investigate how the ransomware file was transferred to \PC-1.
- Check for similar indicators across the network.
- Update endpoint protection and run full scans.
- Document the incident and update detection rules.