

Incident Metadata

Email and URL Threats

Case Type:

Reported by:

Microsoft Defender

Analyst:

Haydar AKYÜREK

Date:

2025-10-15

Severity:

● High

Status:

✓ Closed

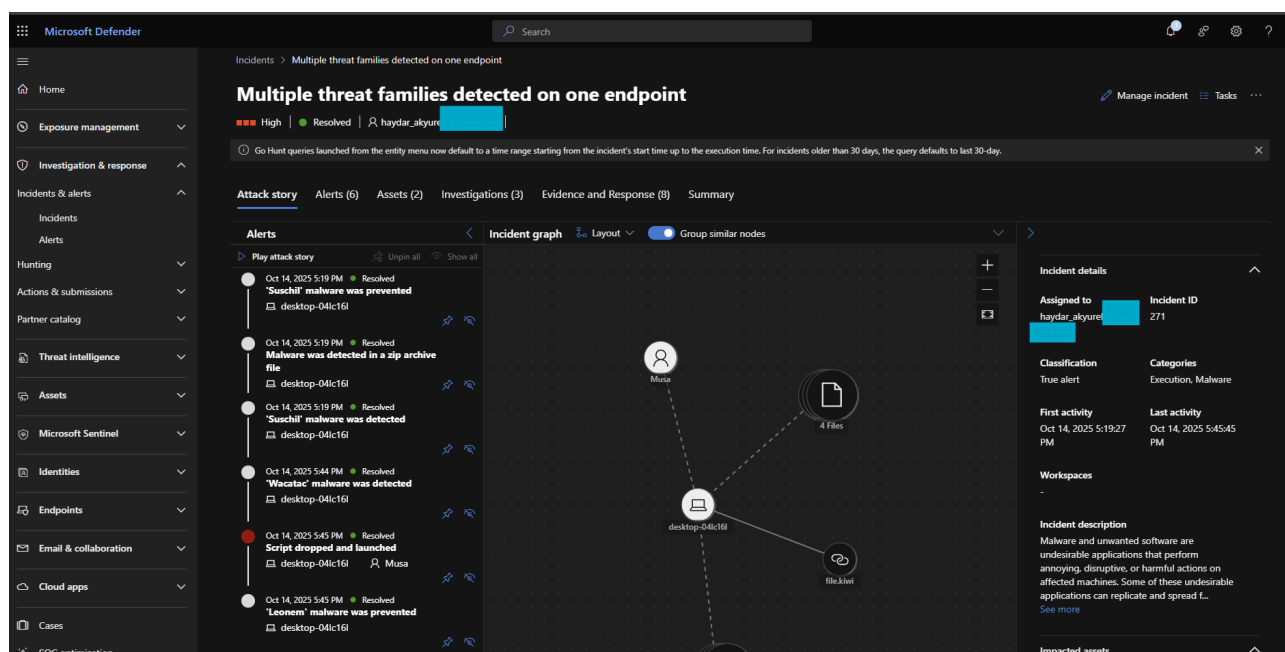
Decision:

✓ True Positive

Incident description:

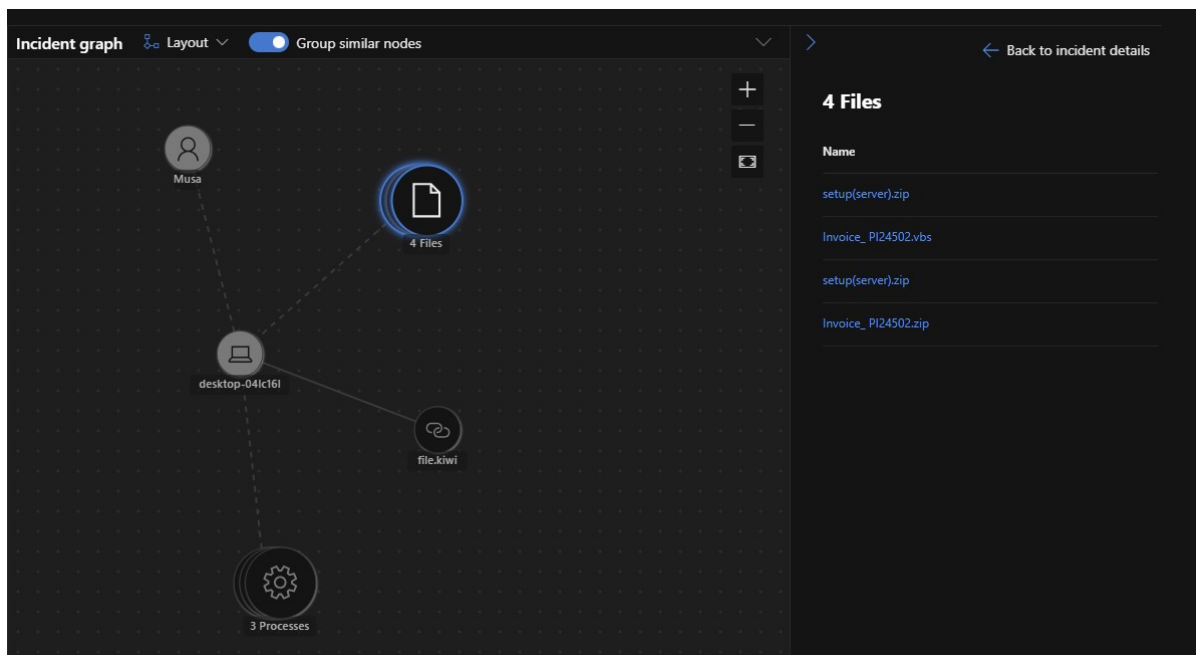
Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities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

The screenshot shows the details of an alert titled 'Suschi' malware was prevented. The main panel displays the file 'setup(server).zip' with the following metadata:

- SHA1: 6f0f1db89412b525bee0c1186e82160d41998
- Path: C:\Users\Musa\Downloads\setup(server).zip
- Size: 3 MB
- Is PE: False
- Mitre techniques: T1204.001: Malicious Link
- Signer: Unknown
- VirusTotal detection ratio: 35/63
- Mark of the web: https://file.kiwi/

The remediation details show: Defender detected 'Trojan:Win32/Suschi!trfn' in file 'setup(server).zip'. The status is 'Suschi' malware was prevented.

Below, the 'Additional related files' section shows the same file details. The right sidebar shows the 'Object details' for the file, including SHA1, SHA256, MD5, File size (4.07 MB), and Signer (Unsigned file). The 'File prevalence' section shows the following counts:

Category	Count
Organization devices	1
Organization cloud apps	0
Worldwide devices	1

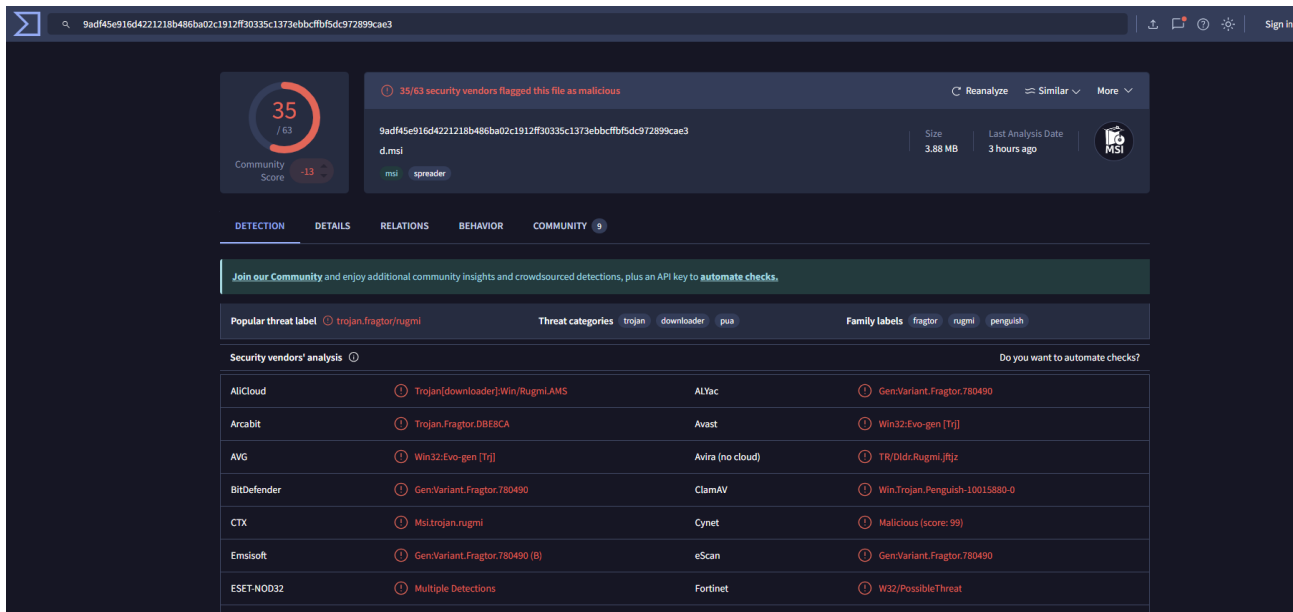
The 'Observed devices (last 30 days)' table shows the following data:

First seen	Last seen
Oct 14, 2025 5:19:27 PM	Oct 14, 2025 5:20:33 PM

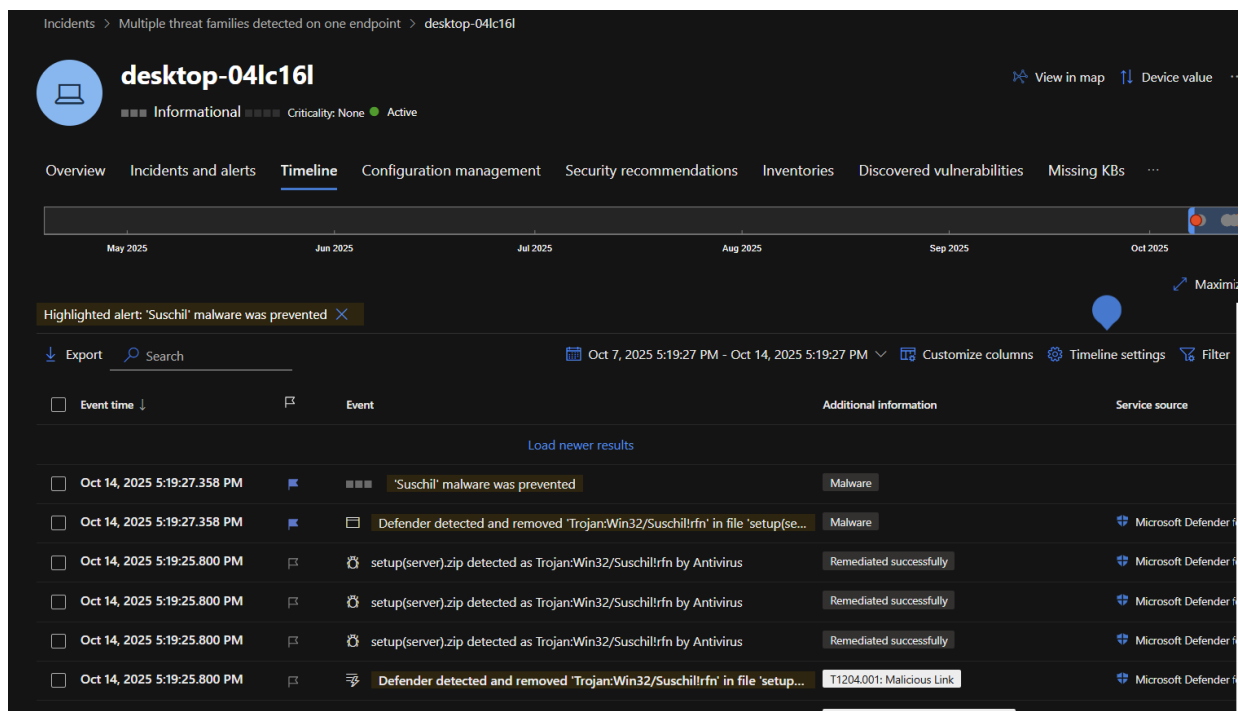
The 'Worldwide observed devices' table shows the following data:

First seen	Last seen
Oct 14, 2025 5:19:27 PM	Oct 14, 2025 5:20:33 PM

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.



- 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.

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

Advanced hunting

Selected workspace: mssentinel Help resources

Explore your content from Microsoft Sentinel
All data from Microsoft Sentinel, including tables, queries and functions is now available for you to explore.

Close

New query* X Intensive Tracking - Process* X +

Schema Functions Run query Custom time range Save Share link Create summary rule

Search

Favorites
Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"

Shared queries
Musabs Queries
Intensive Tracking - Process
Lolbin Activities
Process,URL,DNS,Port, File information
Zipped Files
Suggested

Query
Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.
1 search "kiwi"

Getting started Results Query history

Export Show empty columns 84 items Search 00:16.574 Low

Filters: Add filter

TimeGenerated	Stable	Type	Timestamp	AlertId	Title
> Oct 14, 2025 5:19:...	AlertEvidence	AlertEvidence	Oct 14, 2025 5:19:27 PM	daad6a0677-3018-4a...	'Suschil' m
> Oct 14, 2025 5:19:...	AlertEvidence	AlertEvidence	Oct 14, 2025 5:19:27 PM	daad6a0677-3018-4a...	'Suschil' m
> Oct 14, 2025 5:19:...	DeviceNetworkEvents	DeviceNetworkEvents	Oct 14, 2025 5:19:14 PM		

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.

Microsoft Defender Search

Advanced hunting

Explore your content from Microsoft Sentinel
All data from Microsoft Sentinel, including tables, queries and functions is now available for you to explore.

New query* X Intensive Tracking - Process* X +

Schema Functions Run query Custom time range Save Share link

Search

Favorites
Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"

Shared queries
Queries
Intensive Tracking - Process
Lolbin Activities
Process,URL,DNS,Port, File information
Zipped Files
Suggested

Query
Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.
1 search "kiwi"

Getting started Results Query history

Export 1 of 84 selected

TimeGenerated	Stable	Type
> Oct 14, 2025 7:33:...	MessageUrlInfo	MessageUrl
> Oct 14, 2025 5:19:...	UrlClickEvents	UrlClickEver
> Oct 14, 2025 7:33:...	UrlClickEvents	UrlClickEver

Inspect record

9ed8eede-9848-466e-5214-08de0b35021e

ReportId_string
0c7052cd-91b6-427a-056b-08de0b3507fc

ActionType
ClickAllowed

IdA-Address

Url
https://file.kiwi/4d5f197d#K6bDsZxoflQYxfLho3xwg

Workload

Email

IsClickedThrough
0

UrlChain

Value
https://file.kiwi/4d5f197d#K6bDsZxoflQYxfLho3xwg

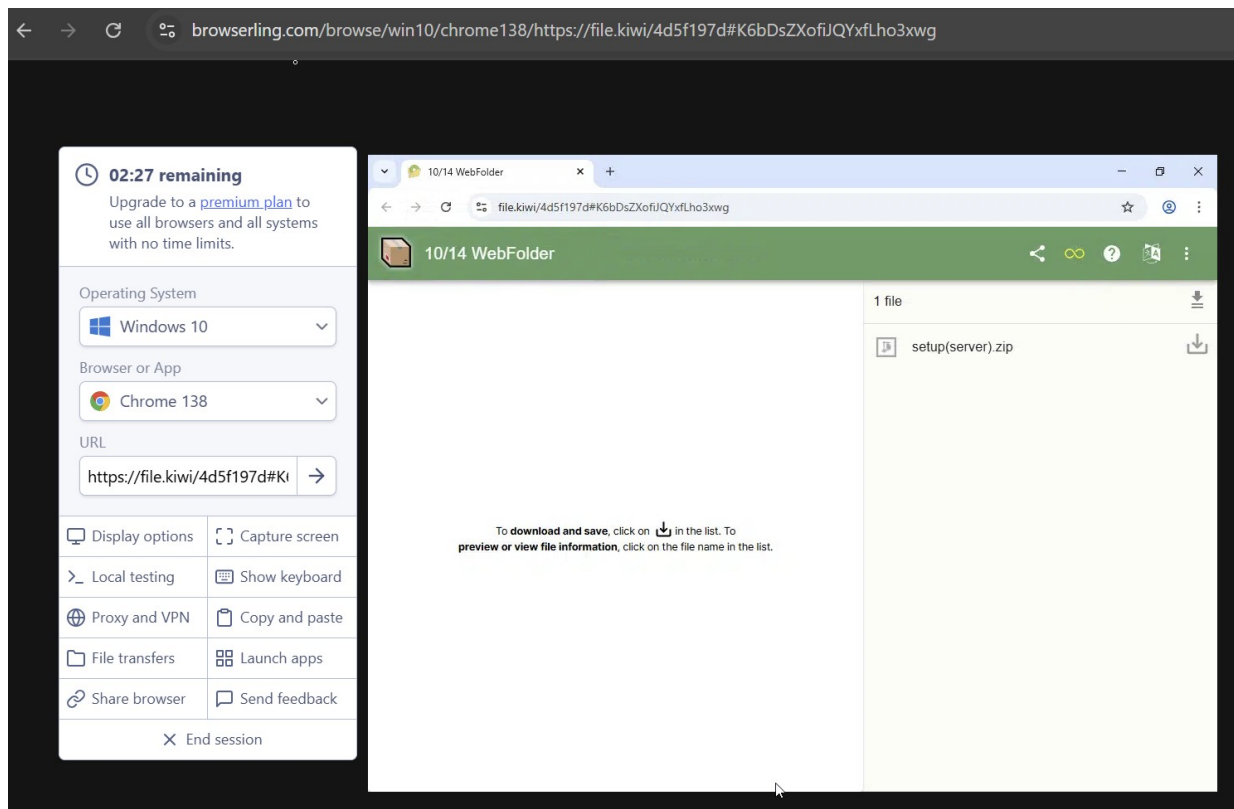
AppName

Mail

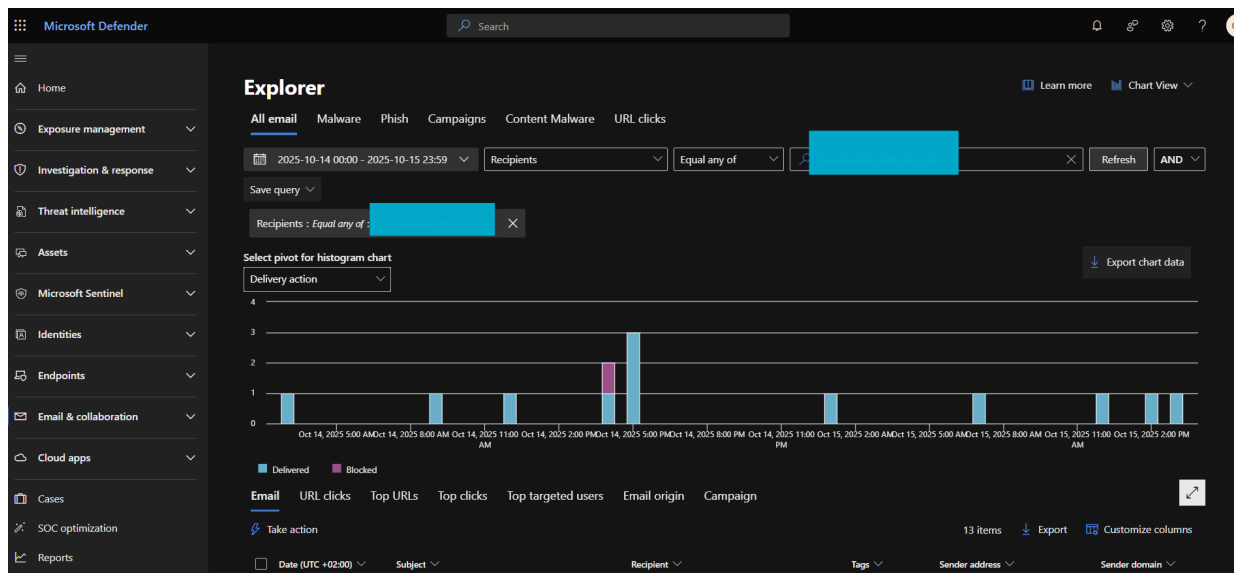
AppVersion
0.0.0000

SourceId
9ed8eede-9848-466e-5214-08de0b35021e

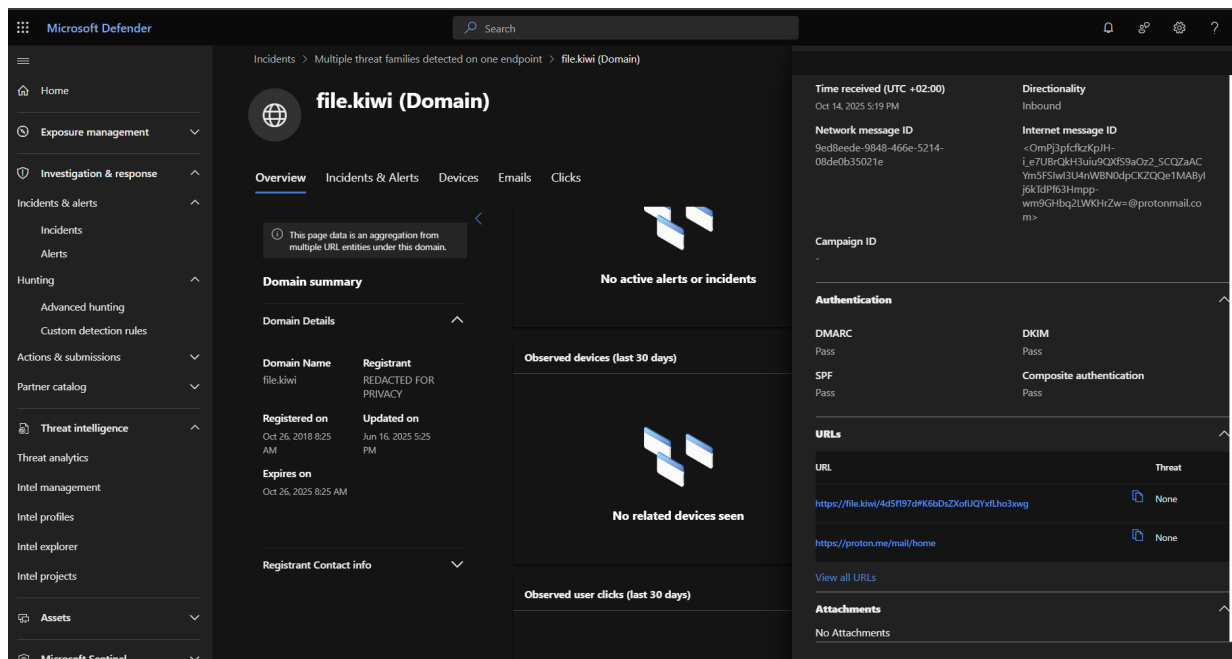
We looked in a sandbox environment to see if this was the file we were really looking for.



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.



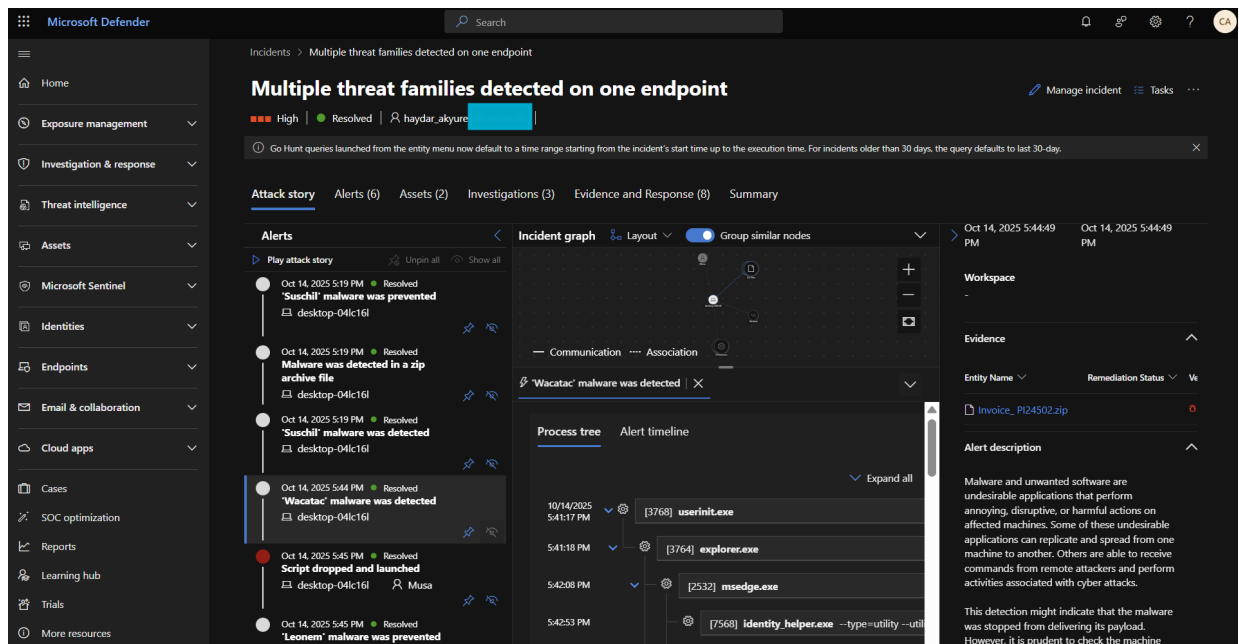
8. Finally, when we right-clicked and opened the Kiwi URL in the Incident Graph, we saw that we could access the URL information. Here, we also see that the email tab says "delivered."



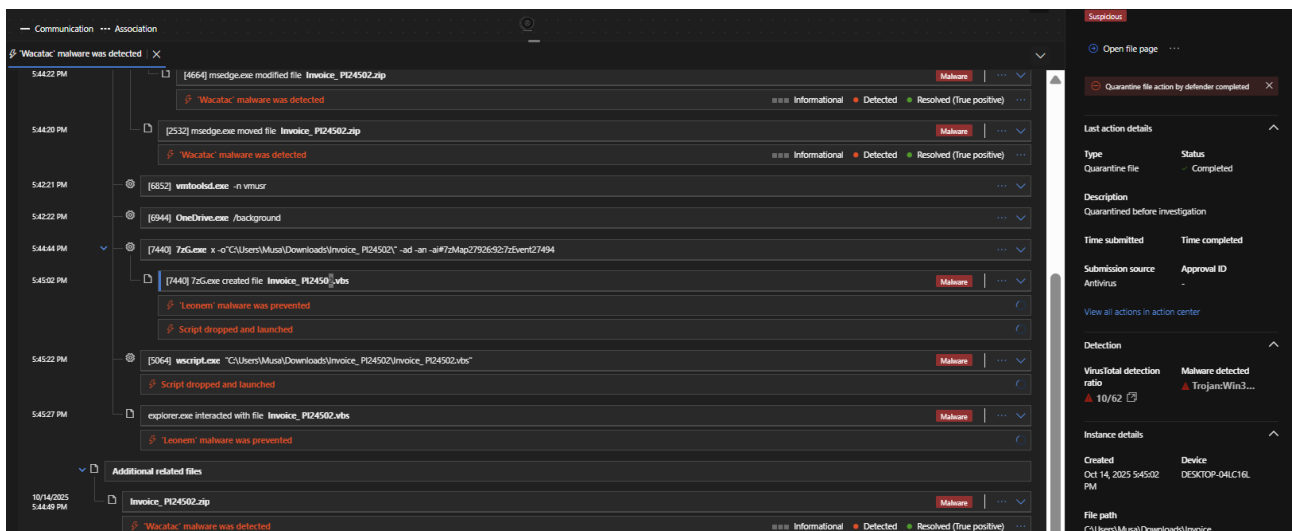
9. Here we also see the DMARC and DKIM records. They are all listed as Pass.

- **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?"

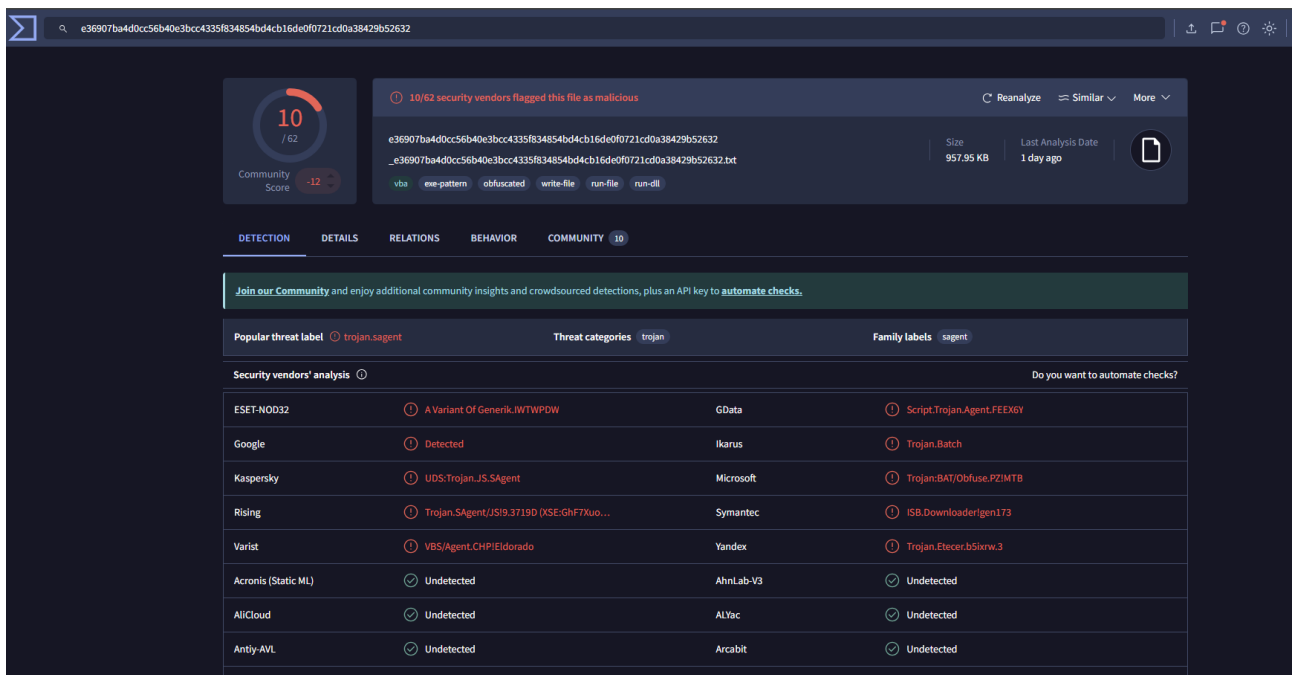
10. Now let's move on to the next alert. There's a file named invoice. Looking at the processes here, the user has opened the machine. Explorer.exe has run. The invoice... zip file has arrived via msdedge.exe. Here, on the right, we see the source of the "Referer Url."



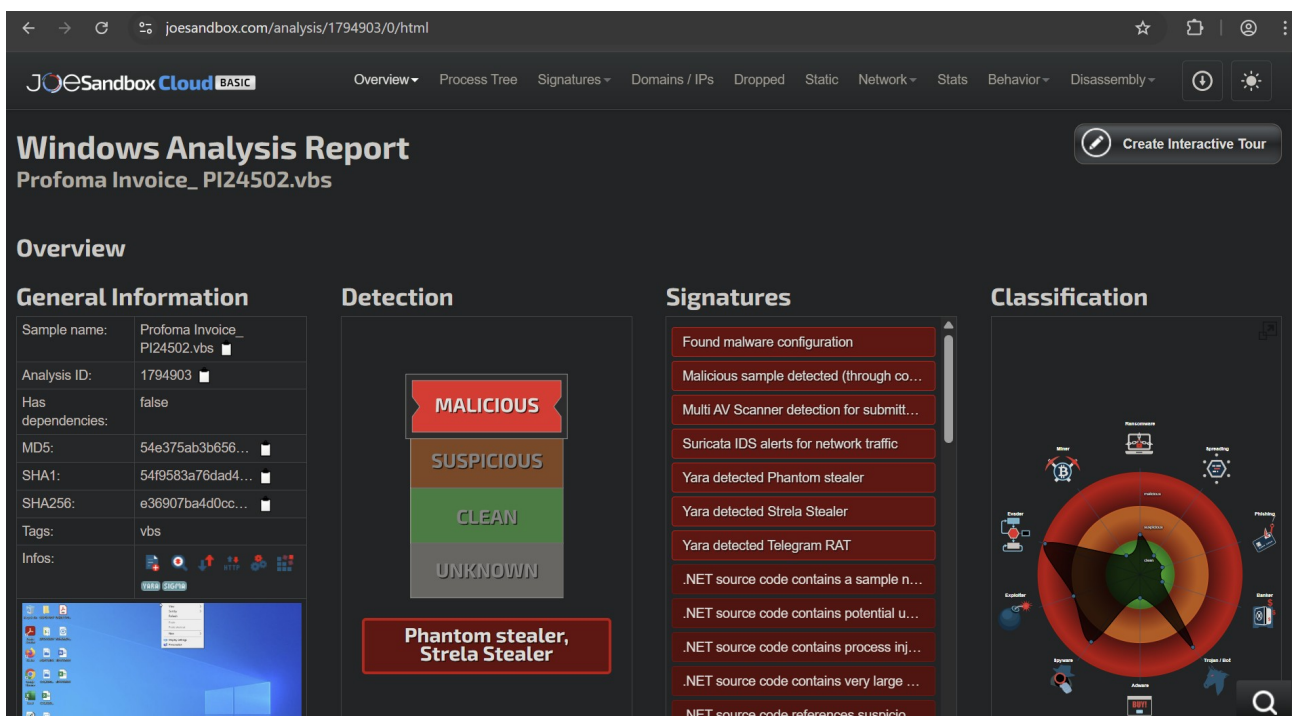
11. When this zip file was first downloaded, we saw that it was only detected. However, when opened with 7zip.exe, we found that it was immediately blocked.



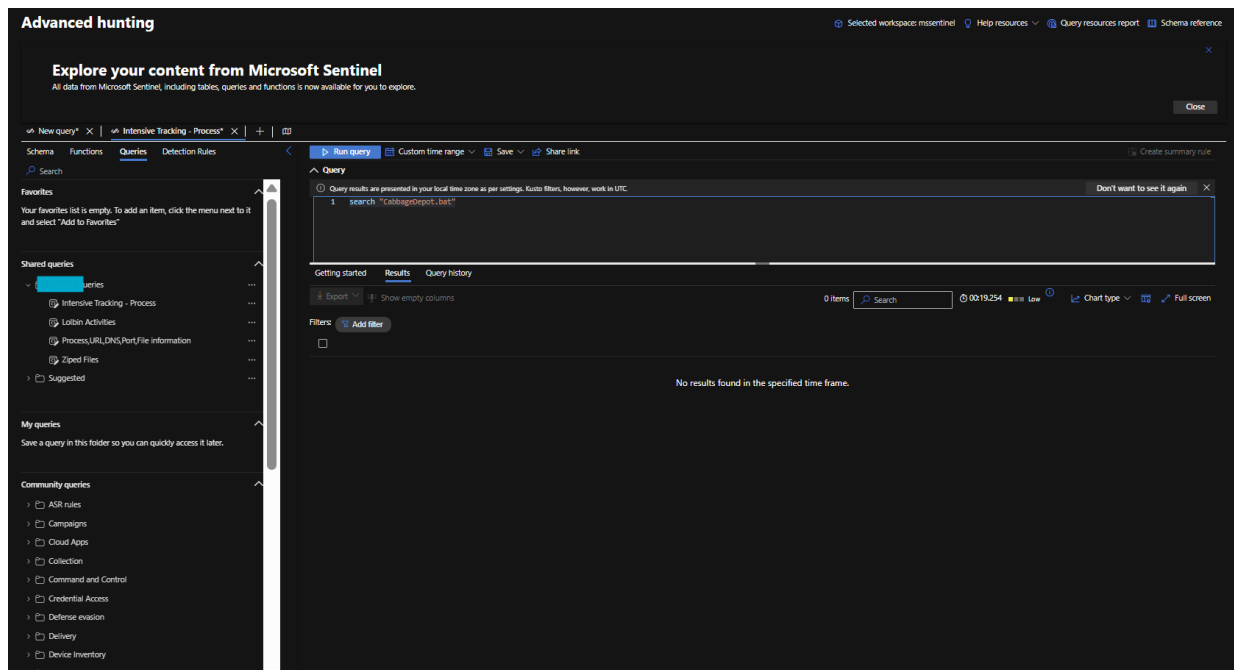
We looked at the file on Virustotal:



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



- 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".



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.