📁 Incident Metadata

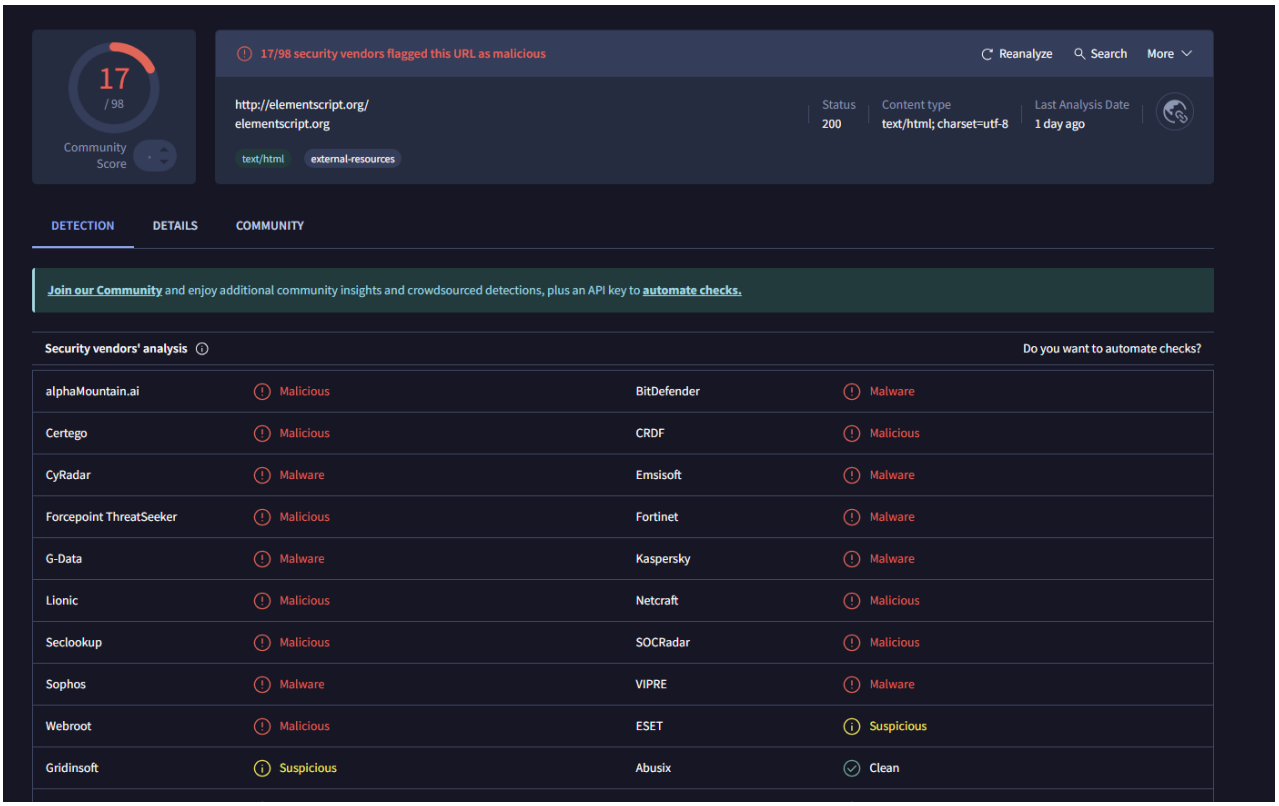
Case Type:	IOC Investigation - Data Exfiltration - DNS
Reported by:	False Negative Search
Analyst:	Haydar AKYÜREK
Date:	2025-10-25
Severity:	🔴 **High**
Status:	✅ Closed
Decision:	✅ **False Negative**

📜 Incident description:

We have an IOC value in the form of **http://elementscript.org/** and we're going to investigate it.

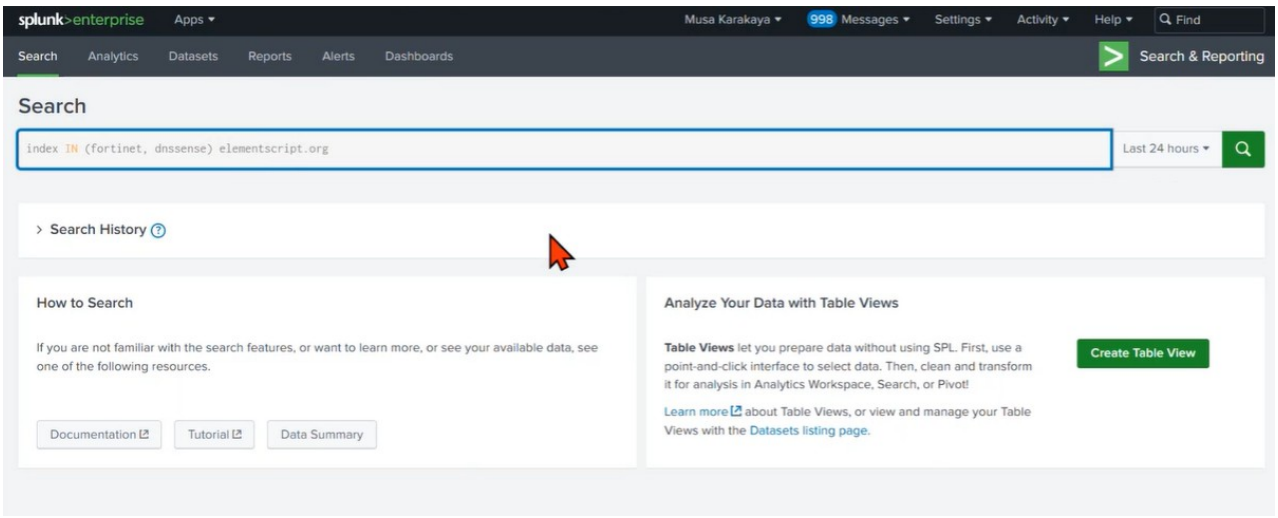
🔍 Analysis Notes

1. First, we check its reputation on VirusTotal. It appears to be flagged (malicious/suspicious).



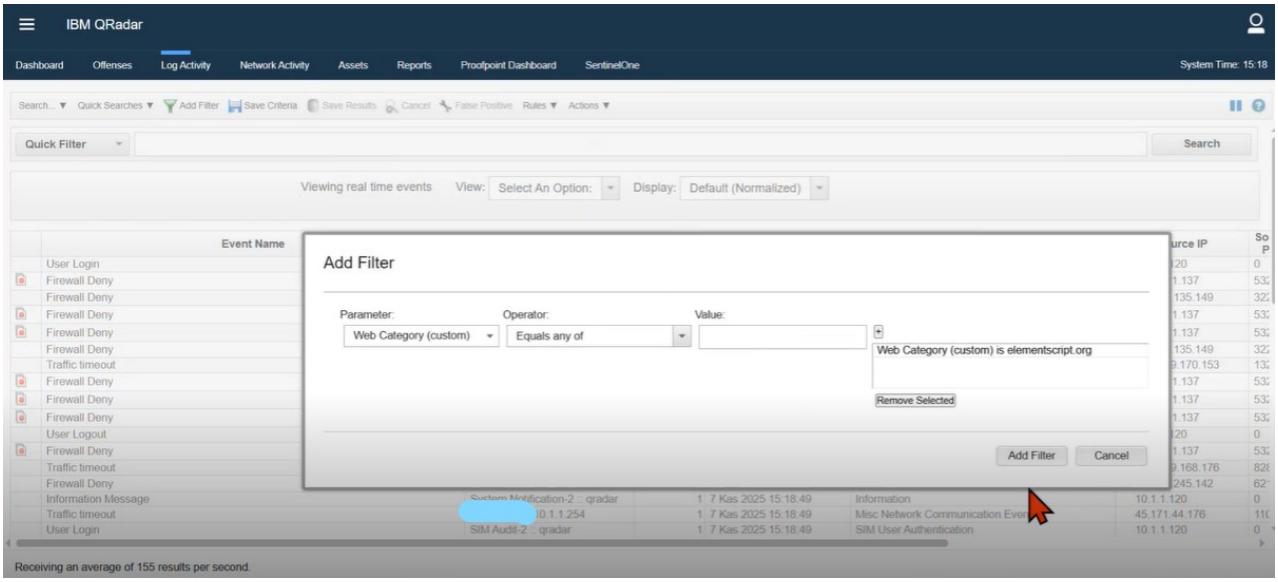
We saw that its creation date was 9 days ago, which is highly suspicious.

2. After that, we investigated it in Splunk.



No results were found.

3. We also searched for it in QRadar under the Web Category (custom).

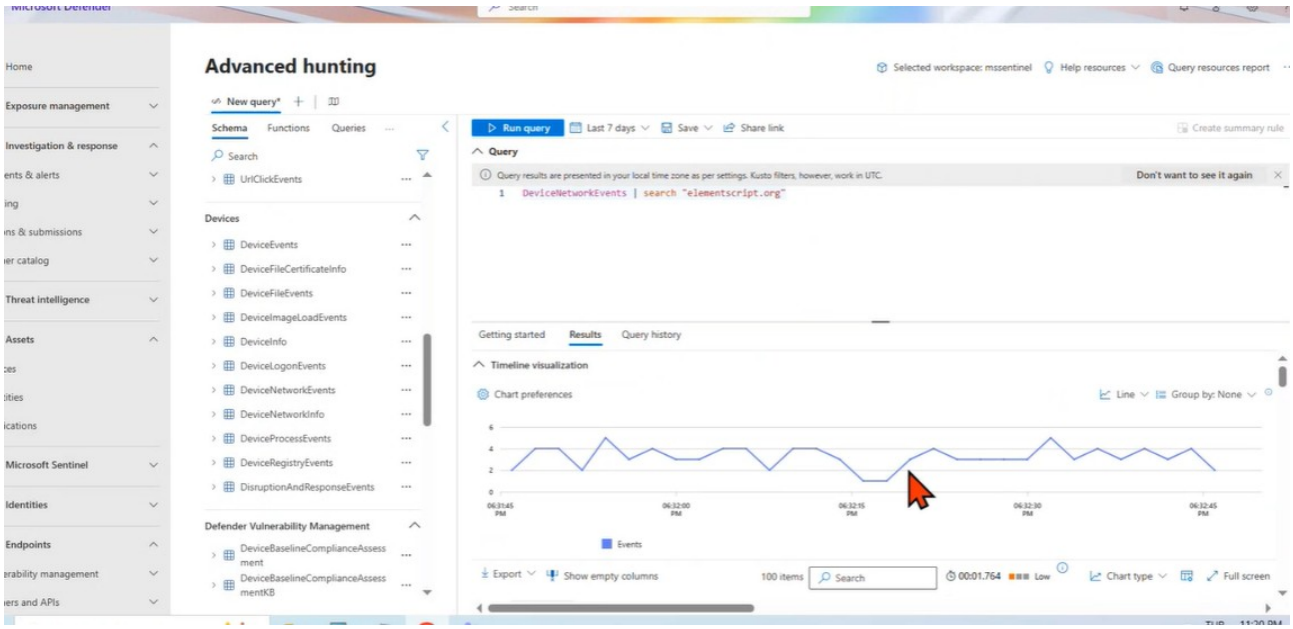


We also searched for it in DNSSense by adding a URL filter, but again found nothing.

4. Finally, we checked our EDR solution, Microsoft Defender. In the **Advanced Hunting** section, we selected **NetworkEvents** and ran the query:

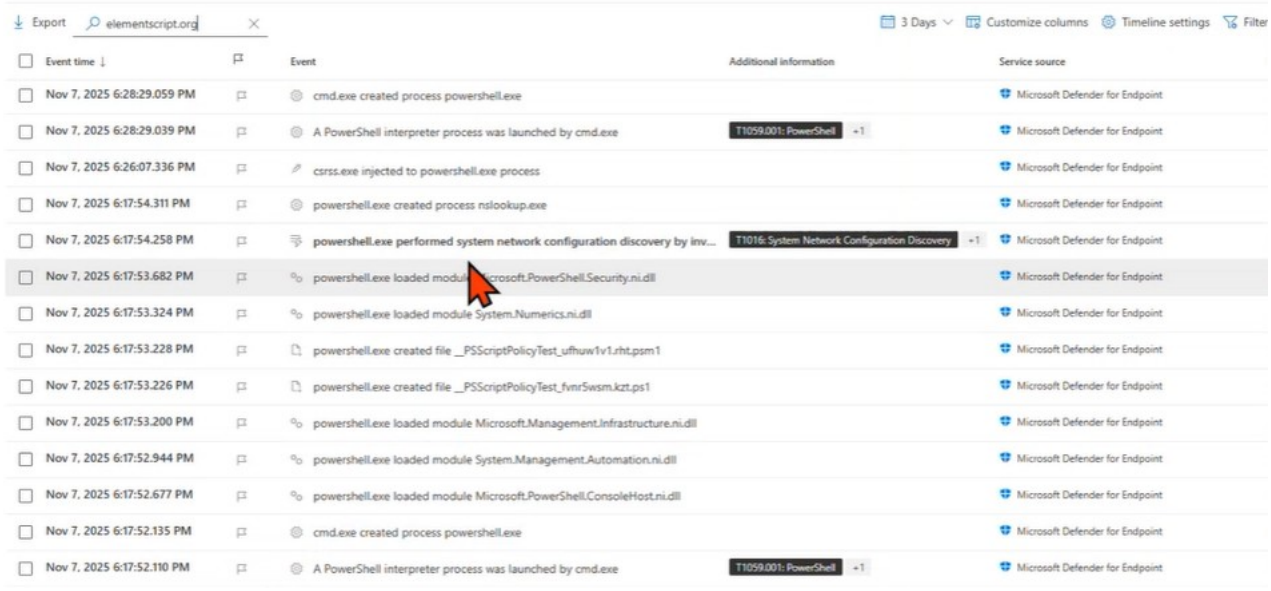
```
DeviceNetworkEvents | search "elementscript.org"
```

No results were returned.

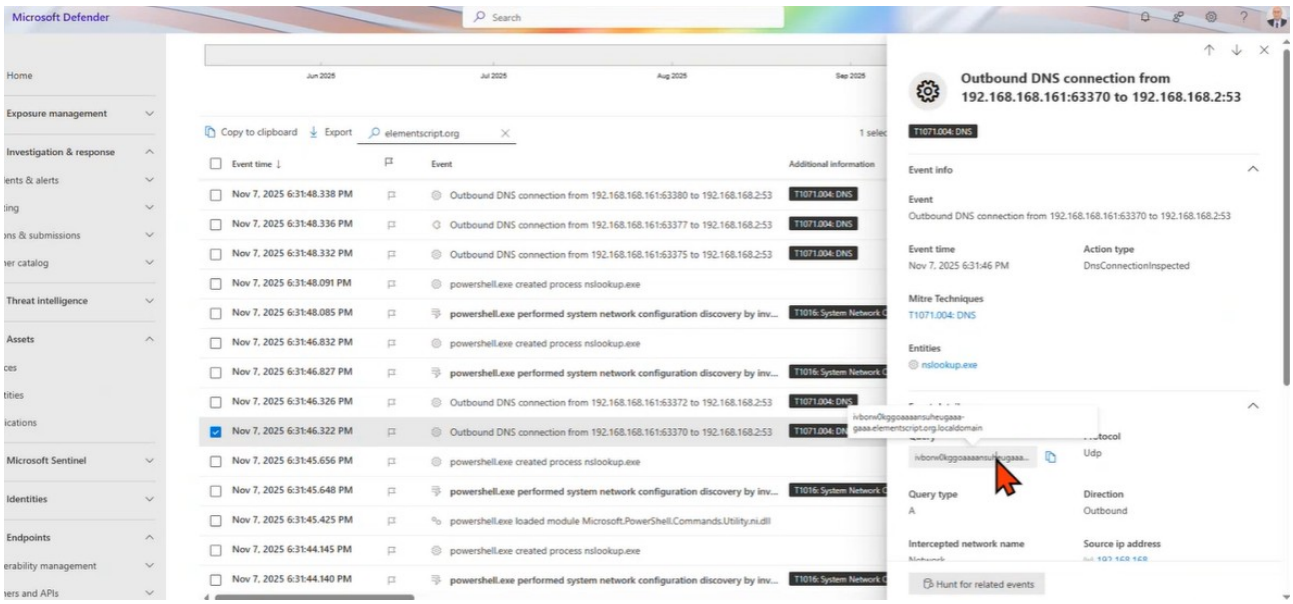


We saw a large number of results here, and the action field shows **DNSConnectionInspected**.

5. After noticing that all events were tied to the same **DeviceName**, we decided to review the timeline.



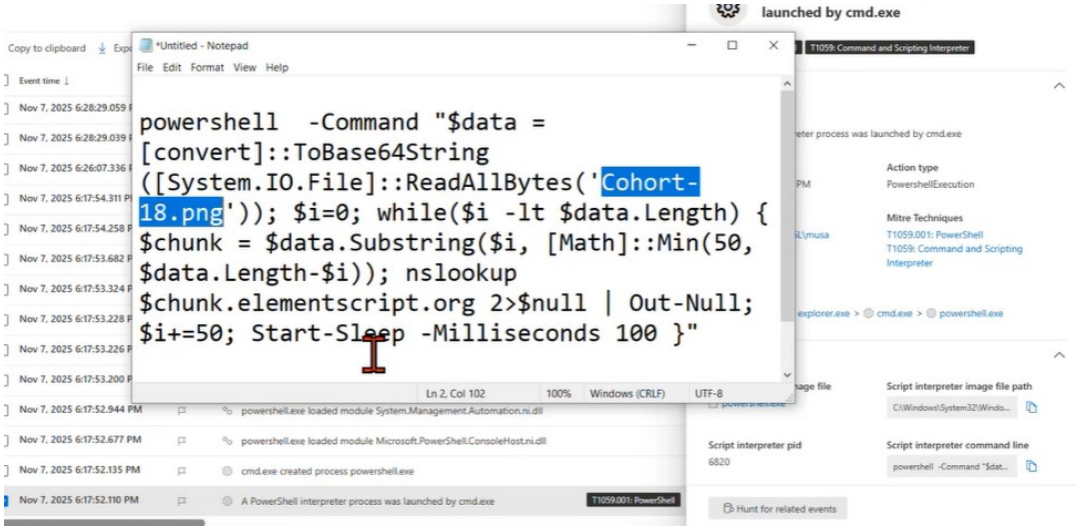
Here, we can see that after a process start, a PowerShell instance was created. When we opened one of the events, we observed **“nslookup”** being executed along with some query parameters.

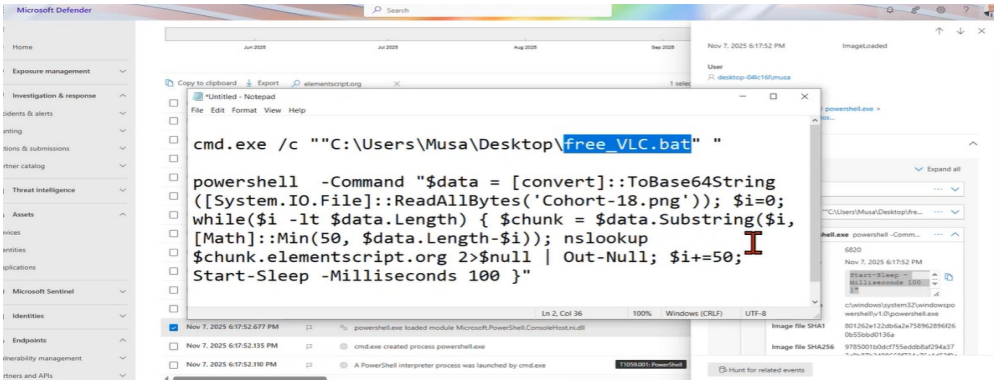


We noticed a meaningless subdomain in front, followed by the domain we were investigating. Reviewing them one by one, we saw that the subdomains kept changing while the main domain remained the same.

When we examined the script in detail, we found a command that converts this data into a PNG file.

Here, the subdomains continuously change to generate repeated queries. The activity is triggered by a file being executed through **cmd.exe**.

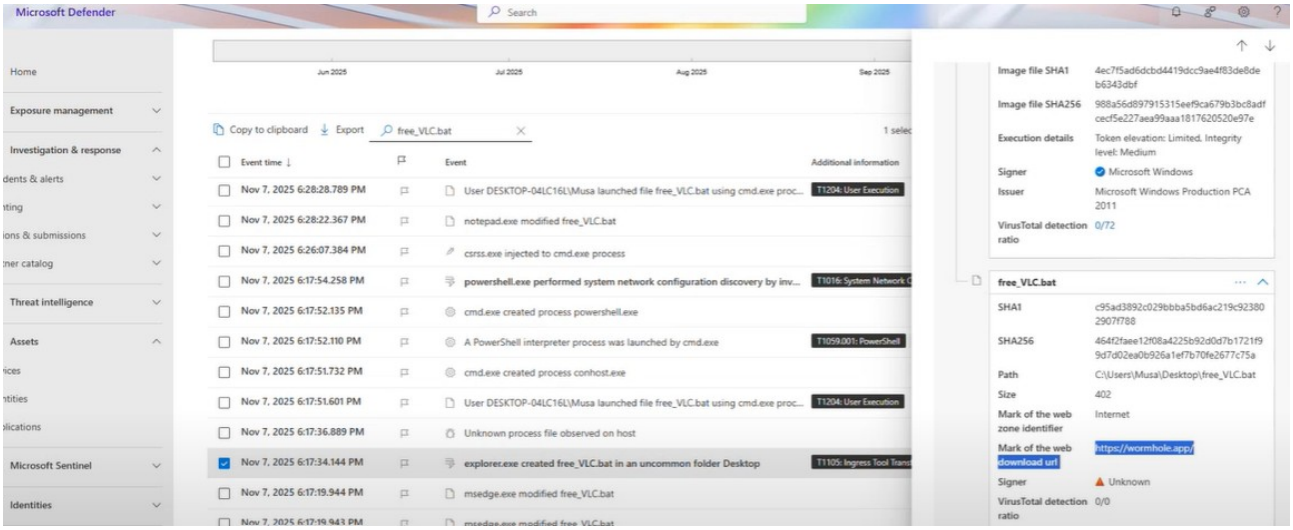


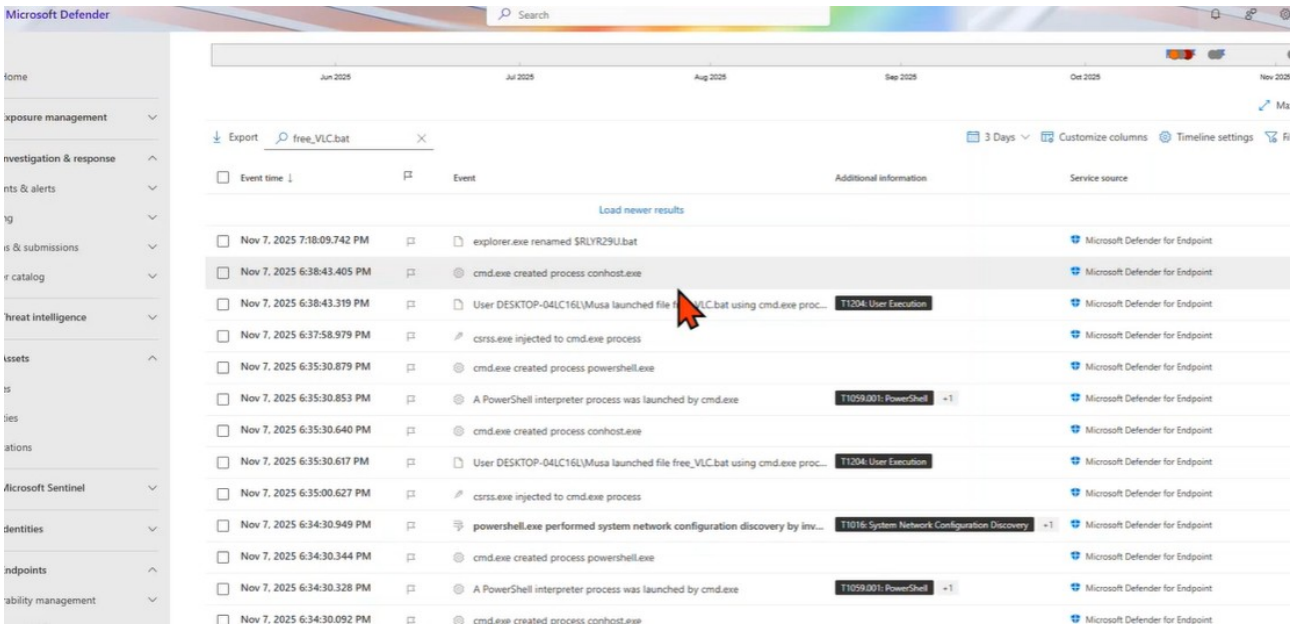


This is a case of **Data Exfiltration**, where data is being sent out using the DNS system. The pattern is that the main domain remains the same while the subdomains continuously change.

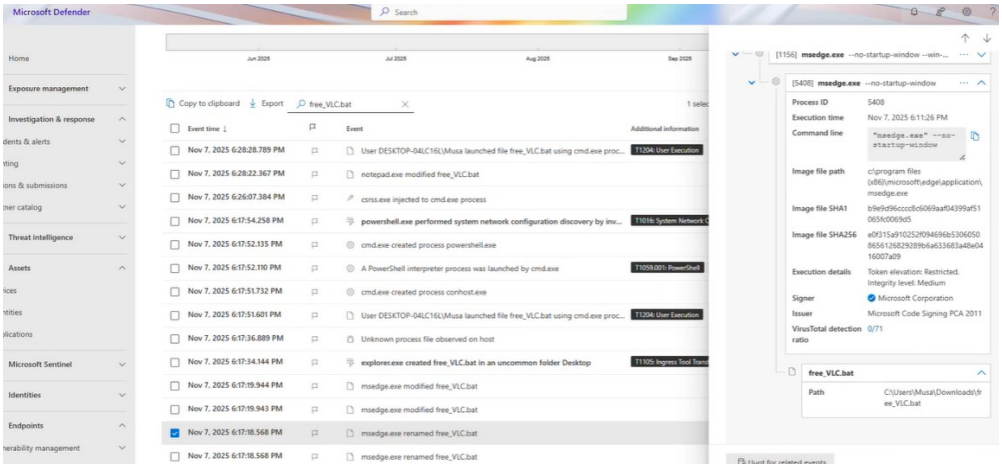
However, we do not see the DNS requests occurring. If they had, we would have observed them in Splunk and QRadar as well.

6. Now we will look into the root cause of the **free_VLC.bat** file that is triggering this query.

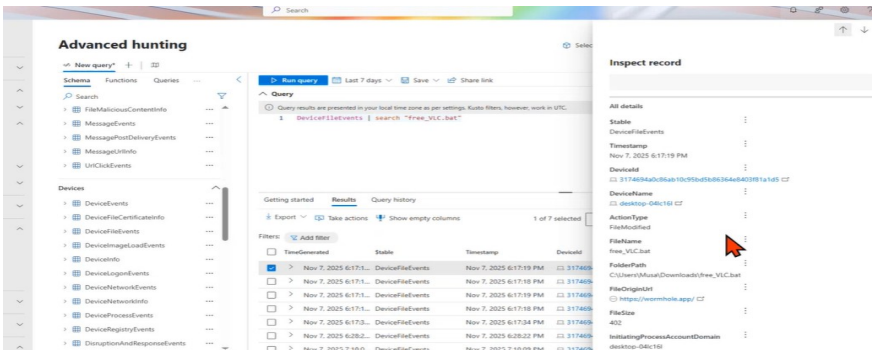




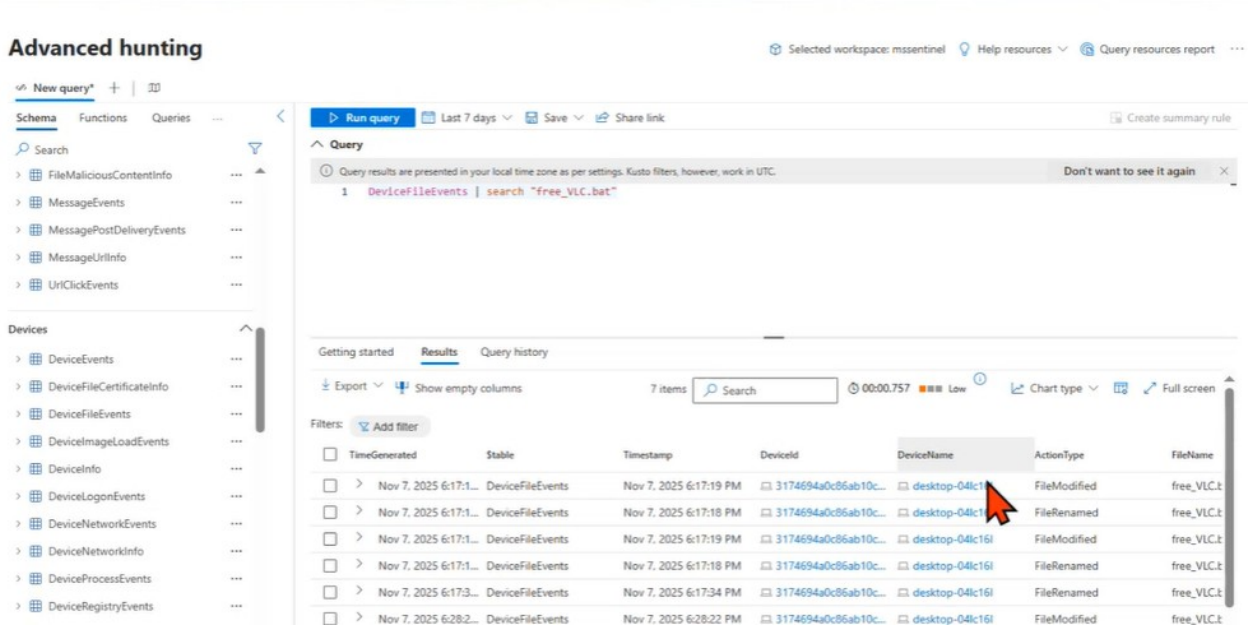
At this point, we could not identify any domain indicating where this BAT file originated from.



Then, by checking the log labeled **“created”**, we were able to identify the source domain.

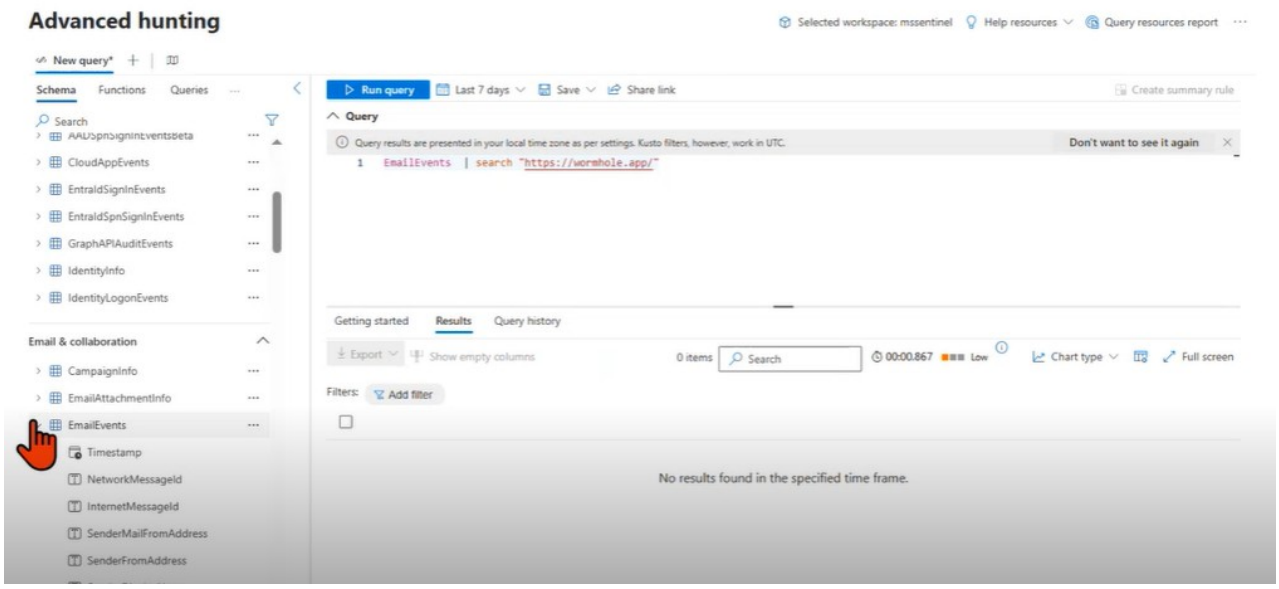


7. Next, we searched in Defender's **Hunting** section. While we could search under **DeviceNetworkEvents**, we chose to query **DeviceFileEvents** instead.

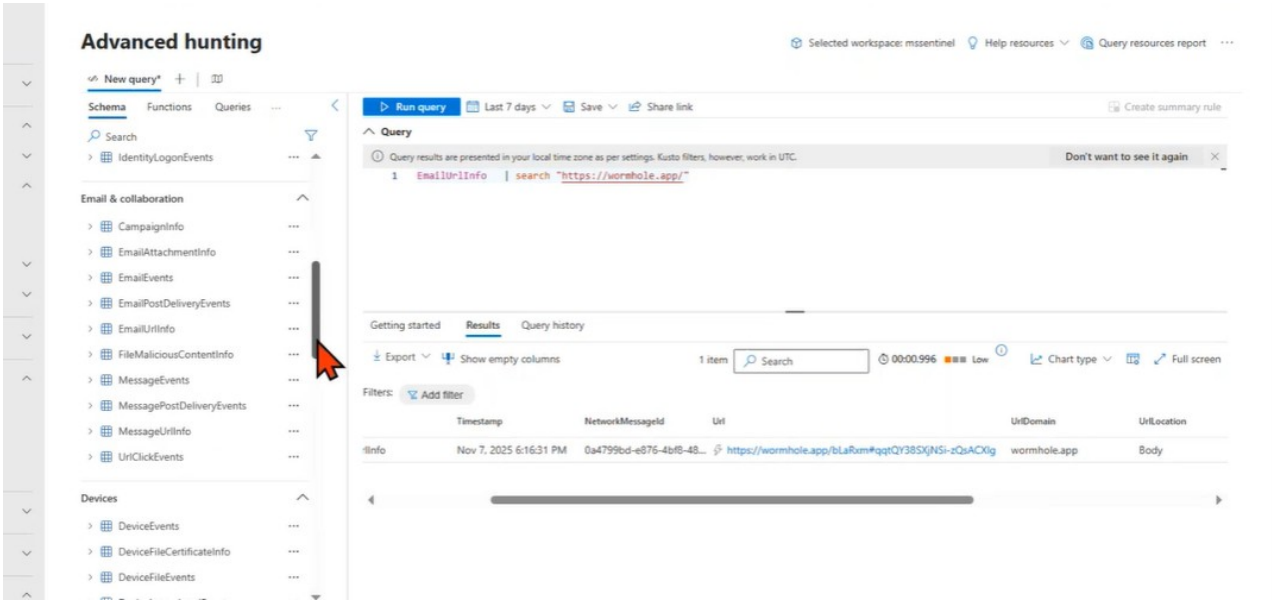


By clicking the first entry, we can identify the source it came from.

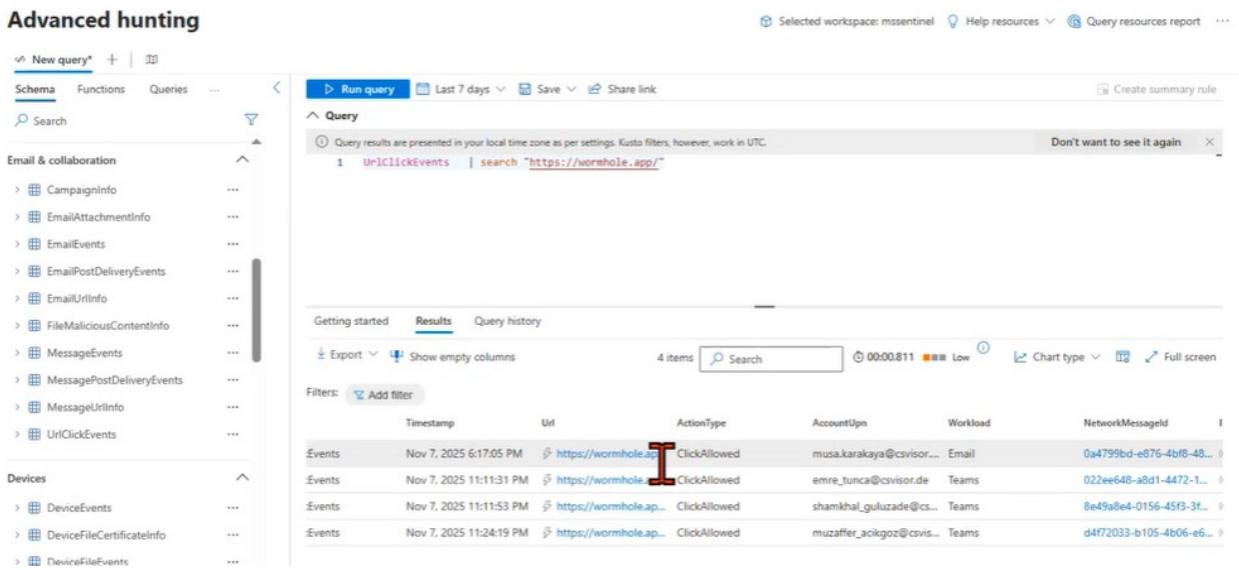
8. We searched for this address in **EmailEvents**, but no results were found.



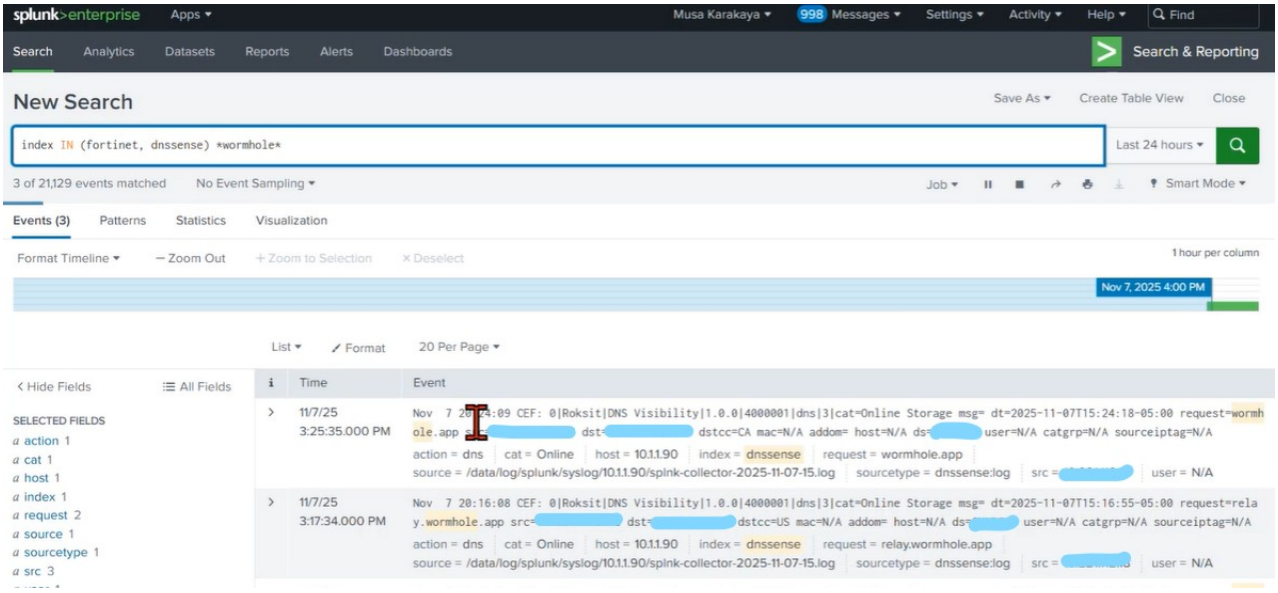
9. We found it in **EmailUrlInfo**.



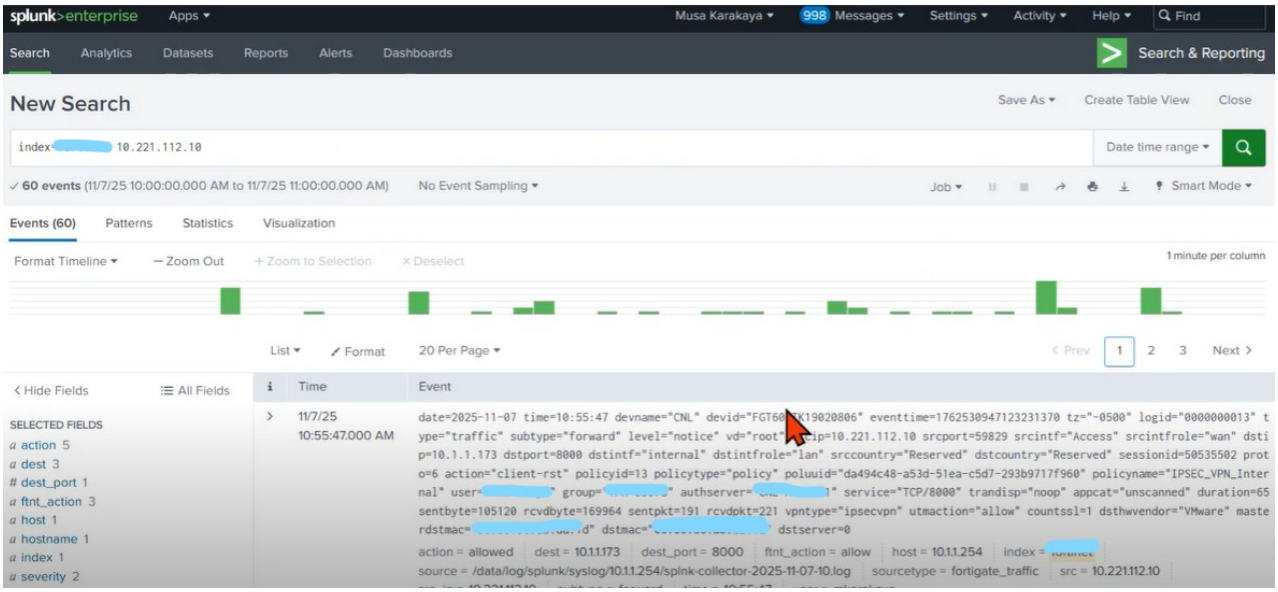
10. Next, we checked **UrlClickEvents** to see if it had been clicked. It shows **click allowed**.



11. This time, when we searched for **wormhole** in Splunk, we got results.



12. After that, we can search the IP address using the firewall index to identify the user.



Decision: ✅ **False Negative**

🔧 Recommended Actions (SOC Level)

- **Isolate the affected endpoint** to prevent further potential data exfiltration.
- **Perform a full malware scan** on the endpoint using the EDR solution.
- **Analyze the `free_VLC.bat` and related PowerShell scripts** to understand behavior and exfiltration method.
- **Block the identified malicious domain** (`elementscript.org`) at the firewall and DNS layers.
- **Monitor for unusual DNS queries** with changing subdomains to detect similar patterns.
- **Review EmailUrlInfo and UrlClickEvents logs** to identify any users who clicked the URL.
- **Check network logs and firewall indices** for associated IP addresses and users.
- **Update detection rules** in Splunk, QRadar, and EDR to capture this activity in the future. **Create a correlation rule in Splunk or QRadar** to trigger an alert if multiple subdomains are queried for the same domain within a 5-minute window, to detect potential DNS exfiltration.
- **Report the incident** to relevant teams and document the investigation steps.
- **Educate users** on suspicious emails and URLs to prevent phishing-related threats.