

Incident Metadata

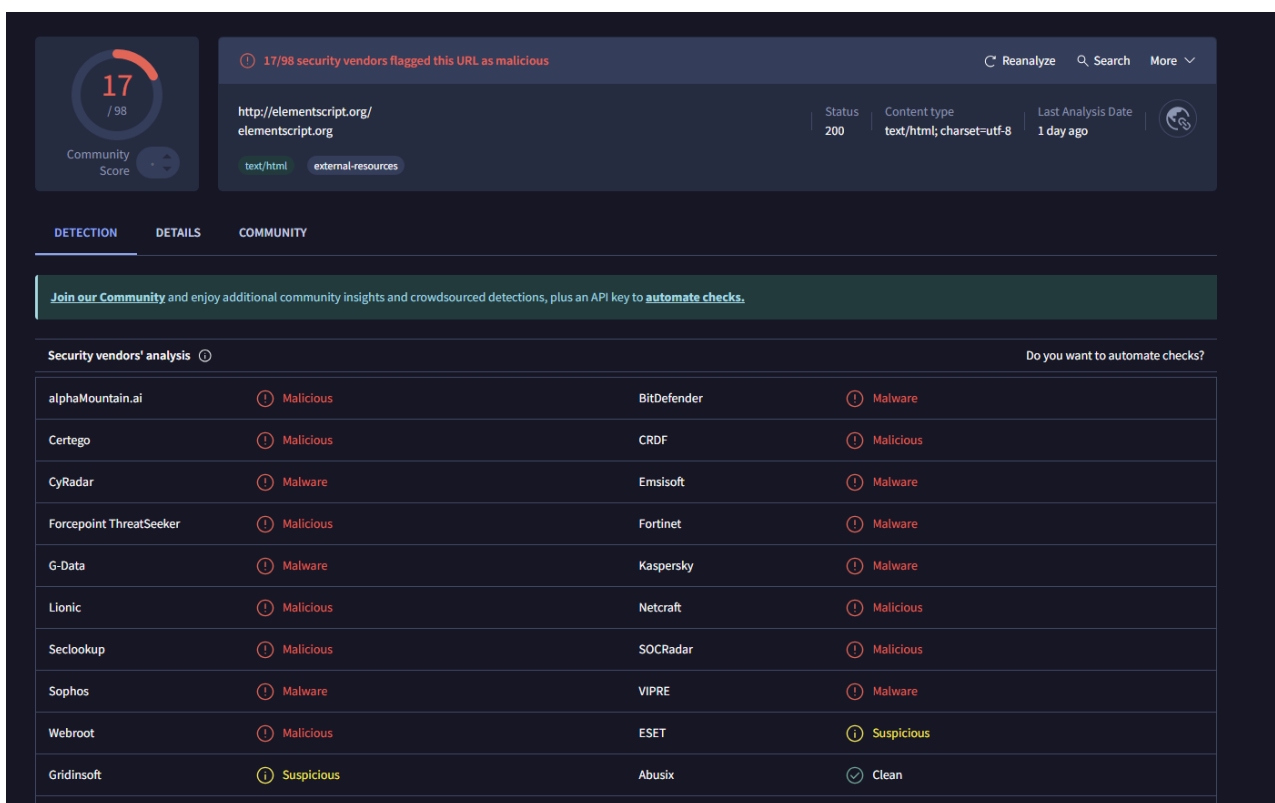
Case Type:	IOC Investigation - Data Exfiltration - DNS
Reported by:	False Negative Search
Analyst:	Haydar AKYÜREK
Date:	2025-10-25
Severity:	● High
Status:	✓ Closed
Decision:	✓ False Negative

Incident description:

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

Analysis Notes

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

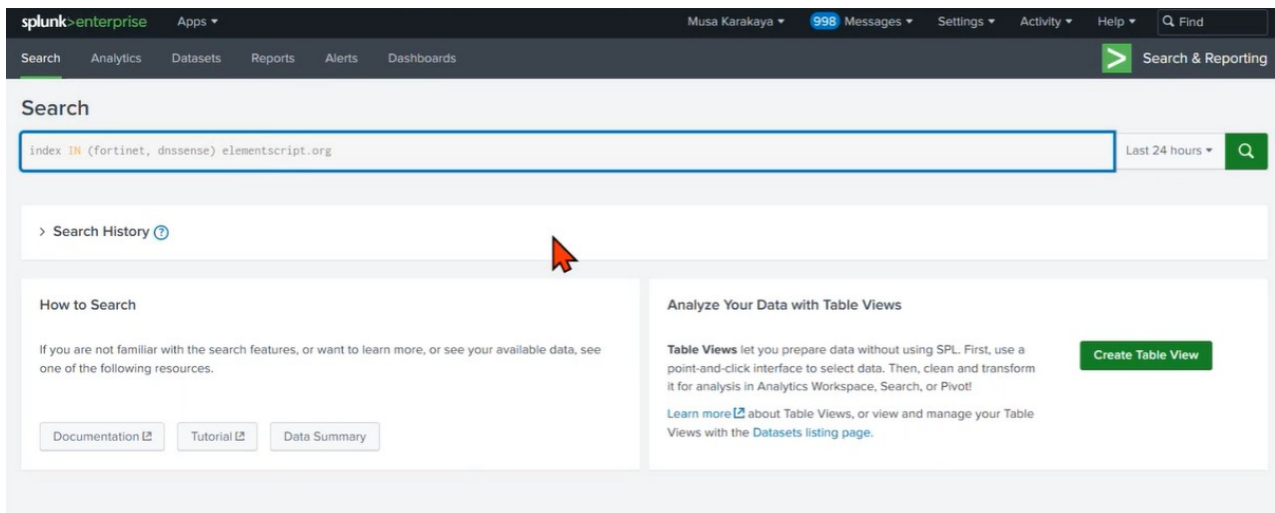


The screenshot shows the VirusTotal interface for the URL <http://elementscript.org/>. The community score is 17/98. A banner indicates that 17/98 security vendors flagged this URL as malicious. The status is 200, content type is text/html; charset=utf-8, and the last analysis date is 1 day ago. Below the tabs (DETECTION, DETAILS, COMMUNITY), there is a link to join the community. The 'Security vendors' analysis' section shows a table of results from various vendors.

Security vendors' analysis		Do you want to automate checks?	
alphaMountain.ai	Malicious	BitDefender	Malware
Certego	Malicious	CRDF	Malicious
CyRadar	Malware	Emsisoft	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malicious	Netcraft	Malicious
Seclookup	Malicious	SOCRadar	Malicious
Sophos	Malware	VIPRE	Malware
Webroot	Malicious	ESET	Suspicious
Gridinsoft	Suspicious	Abusix	Clean

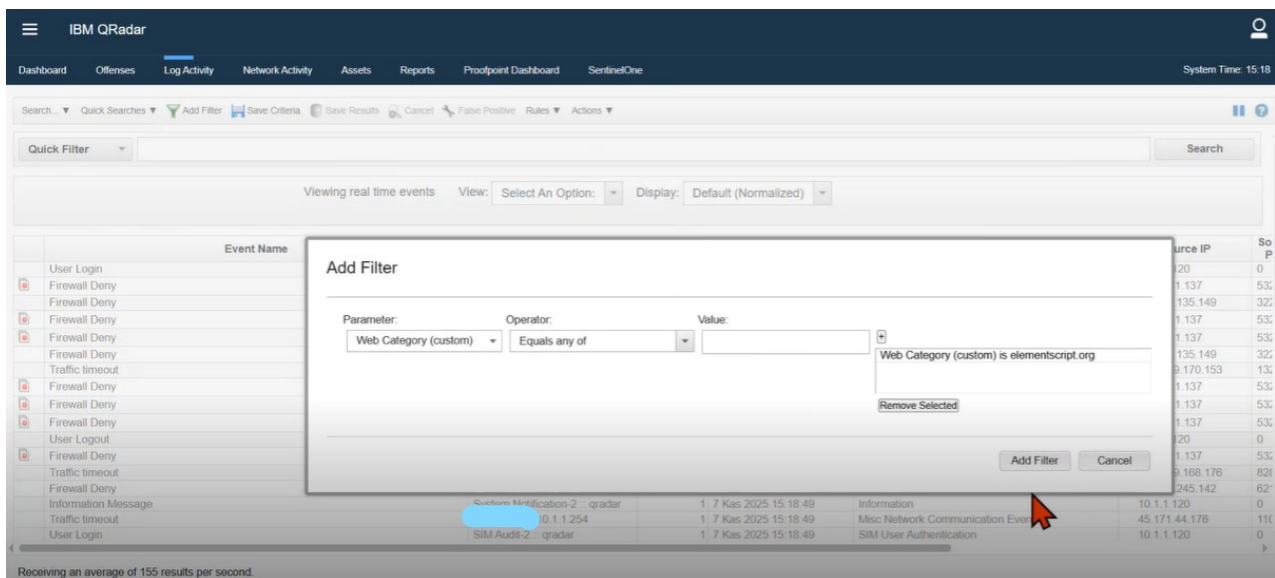
We saw that its creation date was 9 days ago, which is highly suspicious.

- After that, we investigated it in Splunk.



No results were found.

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

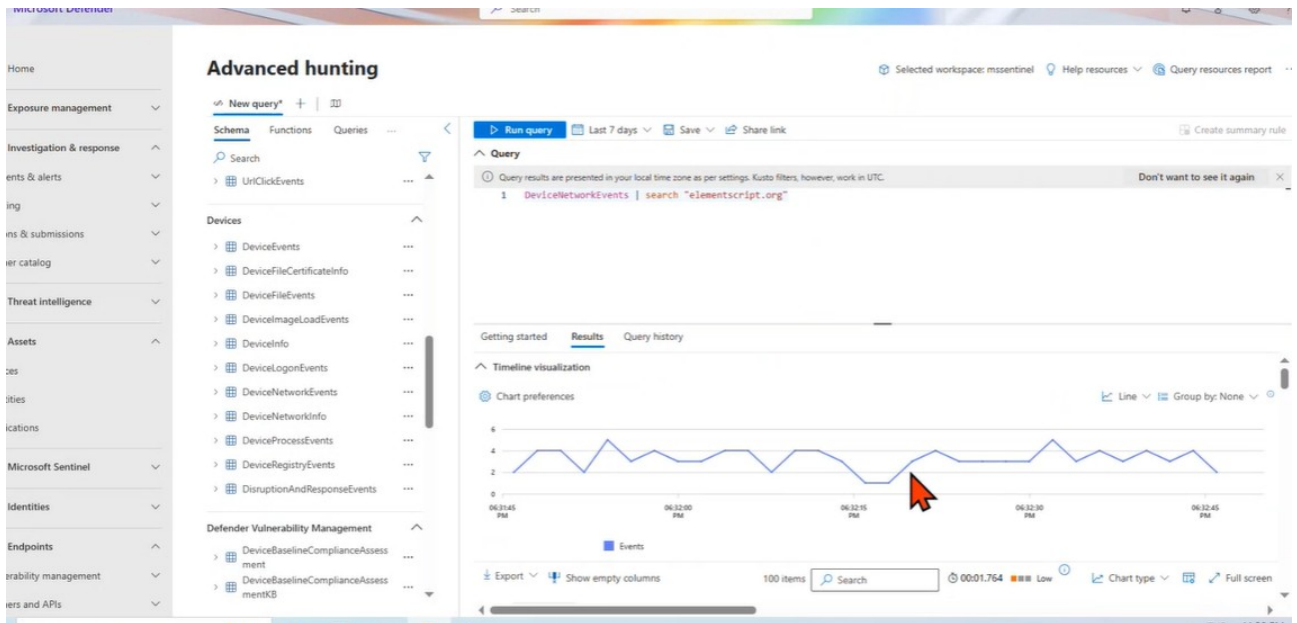


We also searched for it in DNSSense by adding a URL filter, but again found nothing.

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

`DeviceNetworkEvents | search "elementsript.org"`

No results were returned.

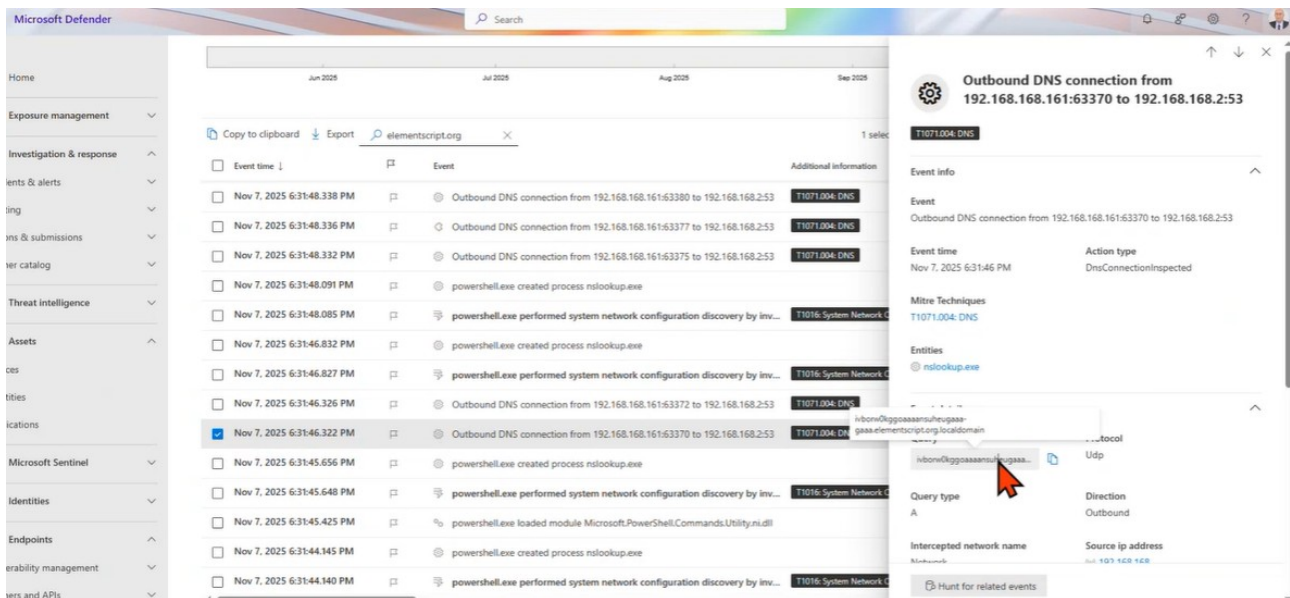


We saw a large number of results here, and the action field shows **DNSConnectionInspected**.

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

Event time	Event	Additional information	Service source
Nov 7, 2025 6:28:29.059 PM	cmd.exe created process powershell.exe		Microsoft Defender for Endpoint
Nov 7, 2025 6:28:29.039 PM	A PowerShell interpreter process was launched by cmd.exe	T1059.001: PowerShell +1	Microsoft Defender for Endpoint
Nov 7, 2025 6:26:07.336 PM	csrss.exe injected to powershell.exe process		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:54.311 PM	powershell.exe created process nslookup.exe		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:54.258 PM	powershell.exe performed system network configuration discovery by inv...	T1016: System Network Configuration Discovery +1	Microsoft Defender for Endpoint
Nov 7, 2025 6:17:53.682 PM	powershell.exe loaded module Microsoft.PowerShell.Security.ni.dll		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:53.324 PM	powershell.exe loaded module System.Numerics.ni.dll		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:53.228 PM	powershell.exe created file __PSScriptPolicyTest_uhuw1v1.rht.psm1		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:53.226 PM	powershell.exe created file __PSScriptPolicyTest_fmvr5wsm.kzt.ps1		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:53.200 PM	powershell.exe loaded module Microsoft.Management.Infrastructure.ni.dll		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:52.944 PM	powershell.exe loaded module System.Management.Automation.ni.dll		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:52.677 PM	powershell.exe loaded module Microsoft.PowerShell.ConsoleHost.ni.dll		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:52.135 PM	cmd.exe created process powershell.exe		Microsoft Defender for Endpoint
Nov 7, 2025 6:17:52.110 PM	A PowerShell interpreter process was launched by cmd.exe	T1059.001: PowerShell +1	Microsoft Defender for Endpoint

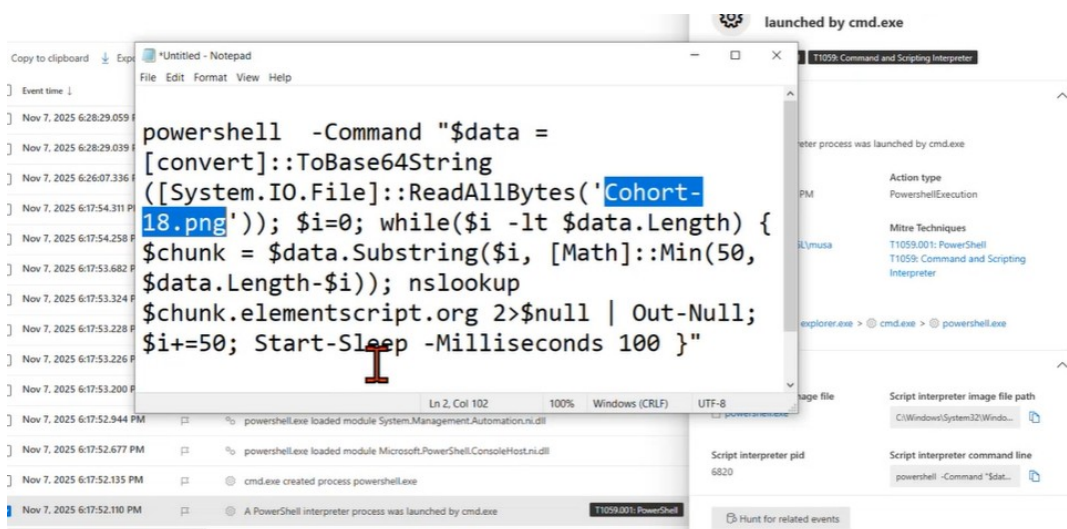
Here, we can see that after a process start, a PowerShell instance was created. When we opened one of the events, we observed **“nslookup”** being executed along with some query parameters.

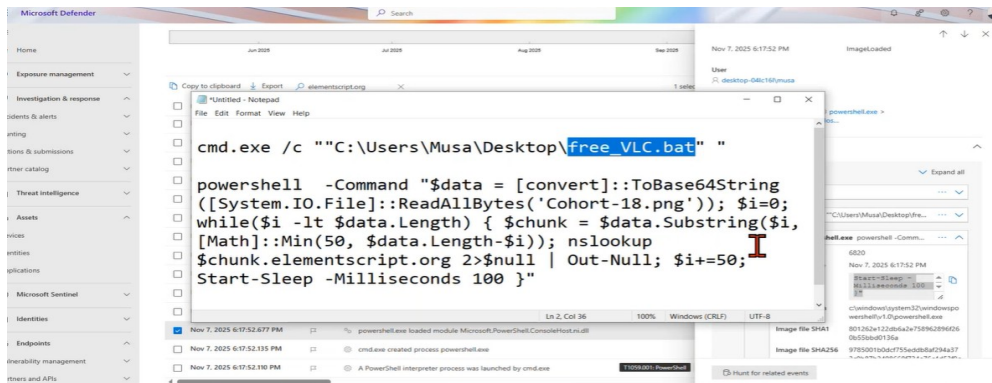


We noticed a meaningless subdomain in front, followed by the domain we were investigating. Reviewing them one by one, we saw that the subdomains kept changing while the main domain remained the same.

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**.

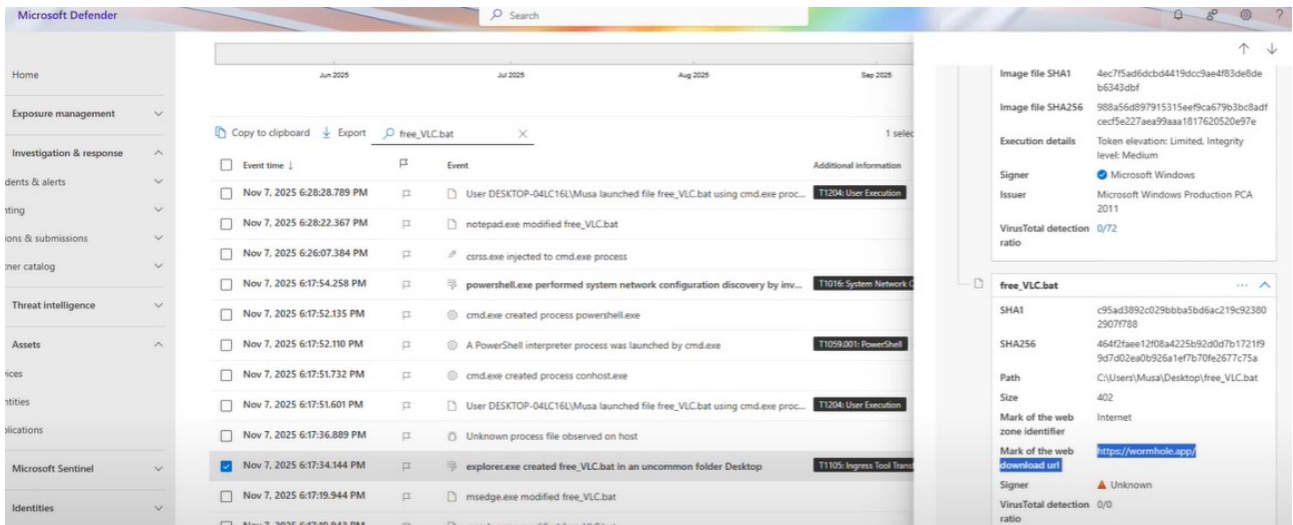


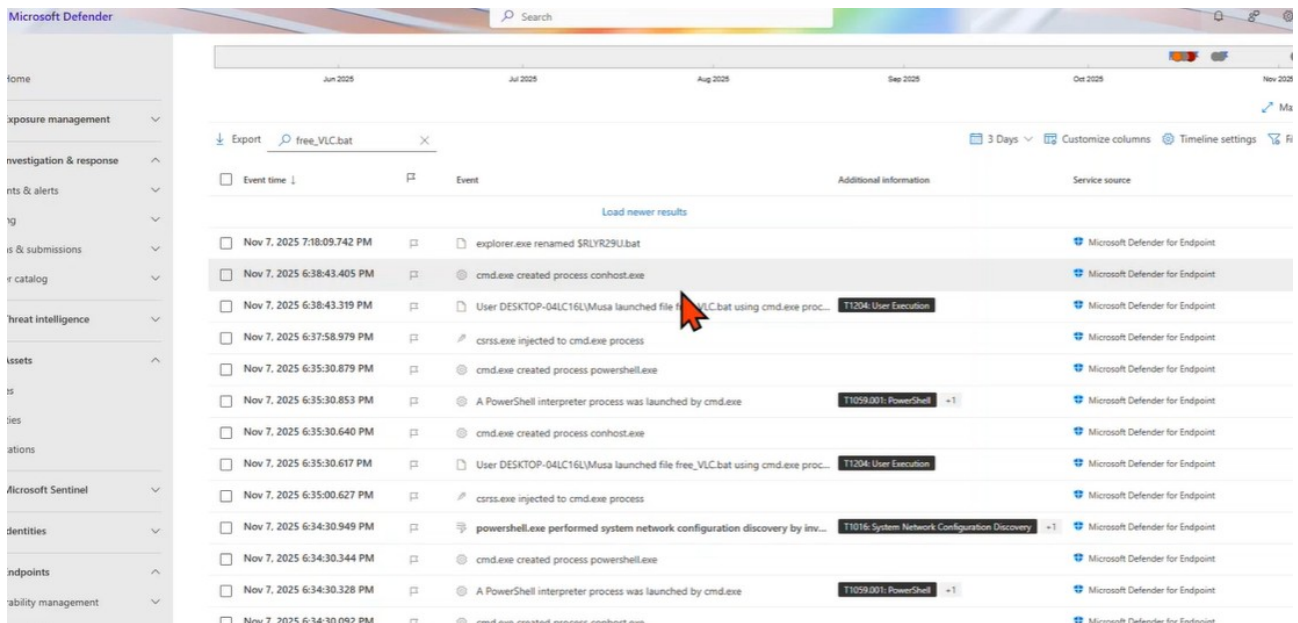


This is a case of **Data Exfiltration**, where data is being sent out using the DNS system. The pattern is that the main domain remains the same while the subdomains continuously change.

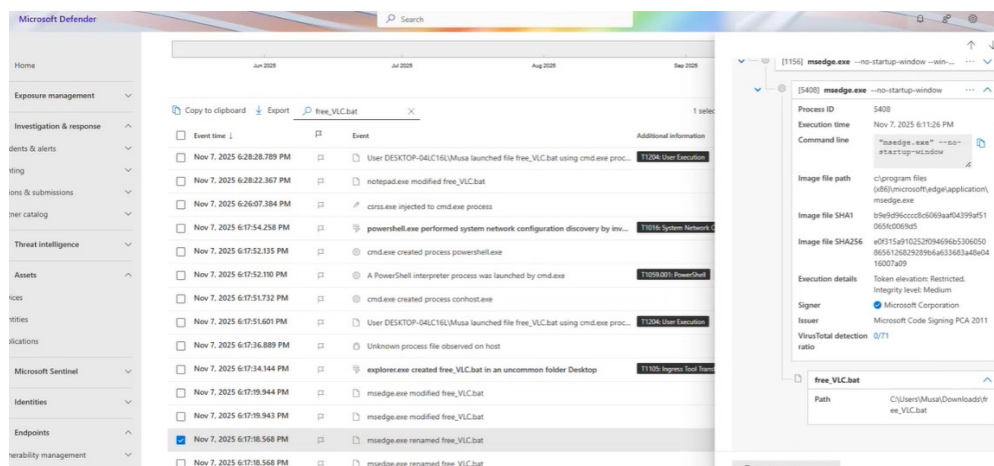
However, we do not see the DNS requests occurring. If they had, we would have observed them in Splunk and QRadar as well.

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

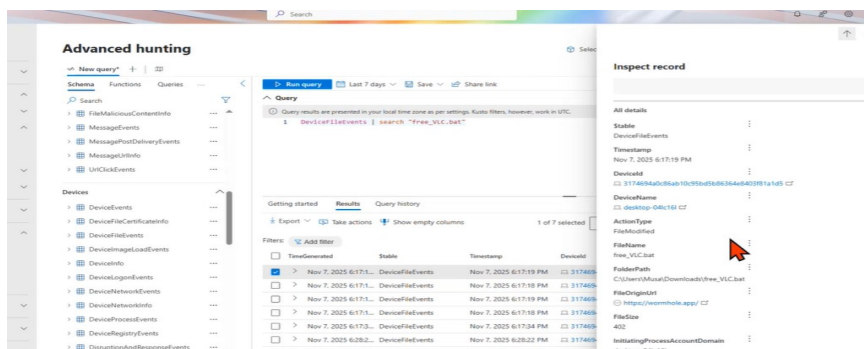




At this point, we could not identify any domain indicating where this BAT file originated from.



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.

Advanced hunting

Selected workspace: ms Sentinel | Help resources | Query resources report

New query + | 20

Schema Functions Queries

Search

- FileMaliciousContentInfo
- MessageEvents
- MessagePostDeliveryEvents
- MessageUrlInfo
- UrlClickEvents

Devices

- DeviceEvents
- DeviceFileCertificateInfo
- DeviceFileEvents
- DeviceImageLoadEvents
- DeviceInfo
- DeviceLogonEvents
- DeviceNetworkEvents
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceRegistryEvents

Run query Last 7 days Save Share link Create summary rule

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC. Don't want to see it again

1 DeviceFileEvents | search "free_VLC.bat"

Getting started Results Query history

Export Show empty columns 7 items Search 00:00.757 Low Chart type Full screen

Filters: Add filter

	TimeGenerated	Stable	Timestamp	DeviceId	DeviceName	ActionType	FileName	
<input type="checkbox"/>	>	Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:19 PM	3174694a0c86ab10c...	desktop-04lc16i	FileModified	free_VLC.t
<input type="checkbox"/>	>	Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:18 PM	3174694a0c86ab10c...	desktop-04lc16i	FileRenamed	free_VLC.t
<input type="checkbox"/>	>	Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:19 PM	3174694a0c86ab10c...	desktop-04lc16i	FileModified	free_VLC.t
<input type="checkbox"/>	>	Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:18 PM	3174694a0c86ab10c...	desktop-04lc16i	FileRenamed	free_VLC.t
<input type="checkbox"/>	>	Nov 7, 2025 6:17:3...	DeviceFileEvents	Nov 7, 2025 6:17:34 PM	3174694a0c86ab10c...	desktop-04lc16i	FileRenamed	free_VLC.t
<input type="checkbox"/>	>	Nov 7, 2025 6:28:2...	DeviceFileEvents	Nov 7, 2025 6:28:22 PM	3174694a0c86ab10c...	desktop-04lc16i	FileModified	free_VLC.t

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.

The screenshot shows the Microsoft Sentinel Advanced Hunting interface. On the left, the 'Schema' pane is open, and 'EmailEvents' is selected under the 'Email & collaboration' category. The main query editor shows a query: `1 EmailEvents | search "https://wormhole.app/"`. The 'Results' tab is active, displaying '0 items' and the message 'No results found in the specified time frame.'

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

The screenshot shows the Microsoft Sentinel Advanced Hunting interface. On the left, the 'Schema' pane is open, and 'EmailUrlInfo' is selected under the 'Email & collaboration' category. The main query editor shows a query: `1 EmailUrlInfo | search "https://wormhole.app/"`. The 'Results' tab is active, displaying '1 item'. The results table is as follows:

	Timestamp	NetworkMessageId	Url	UrlDomain	UrlLocation
1	Nov 7, 2025 6:16:31 PM	0a4799bd-e676-4b68-48...	https://wormhole.app/bLaRxm#qqtQY38SXNSi-zQuACXlg	wormhole.app	Body

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

Advanced hunting

Selected workspace: mssentinel Help resources Query resources report

New query* | |

Schema Functions Queries

Search

Email & collaboration

- CampaignInfo
- EmailAttachmentInfo
- EmailEvents
- EmailPostDeliveryEvents
- EmailUrlInfo
- FileMaliciousContentInfo
- MessageEvents
- MessagePostDeliveryEvents
- MessageUrlInfo
- UrlClickEvents

Devices

- DeviceEvents
- DeviceFileCertificateInfo
- DeviceFileEvents

Run query Last 7 days Save Share link Create summary rule

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC. Don't want to see it again

1 UrlClickEvents | search "https://wormhole.app/"

Getting started Results Query history

Export Show empty columns 4 items Search 00:00.811 Low Chart type Full screen

Filters: Add filter

	Timestamp	Url	ActionType	AccountUpn	Workload	NetworkMessageId
Events	Nov 7, 2025 6:17:05 PM	https://wormhole.app	ClickAllowed	musa.karakaya@csvisor...	Email	0a4799bd-e876-4b08-48...
Events	Nov 7, 2025 11:11:31 PM	https://wormhole.app	ClickAllowed	emre_tunca@csvisor.de	Teams	022ee648-a8d1-4472-1...
Events	Nov 7, 2025 11:11:53 PM	https://wormhole.ap...	ClickAllowed	shamkhal_guluzade@cs...	Teams	8e49a8e4-0156-45f3-3f...
Events	Nov 7, 2025 11:24:19 PM	https://wormhole.ap...	ClickAllowed	muzaffer_acikgoz@csvis...	Teams	d4f72033-b105-4b06-e6...

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

splunk enterprise Apps Musa Karakaya 998 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

index IN (fortinet, dnssense) *wormhole* Last 24 hours

3 of 21,129 events matched No Event Sampling Job Smart Mode

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- a action 1
- a cat 1
- a host 1
- a index 1
- a request 2
- a source 1
- a sourcetype 1
- a src 3

i	Time	Event
>	11/7/25 3:25:35.000 PM	Nov 7 25:34:09 CEF: 0 Roksit DNS Visibility 1.0.0 4000001 dns 3 cat=Online Storage msg= dt=2025-11-07T15:24:18-05:00 request=wormhole.app dst= dstcc=CA mac=N/A addom= host=N/A ds= user=N/A catgrp=N/A sourceiptag=N/A action = dns cat = Online host = 10.11.90 index = dnssense request = wormhole.app source = /data/log/splunk/syslog/10.11.90/splunk-collector-2025-11-07-15.log sourcetype = dnssense:log src = user = N/A
>	11/7/25 3:17:34.000 PM	Nov 7 20:16:08 CEF: 0 Roksit DNS Visibility 1.0.0 4000001 dns 3 cat=Online Storage msg= dt=2025-11-07T15:16:55-05:00 request=relay.wormhole.app src= dst= dstcc=US mac=N/A addom= host=N/A ds= user=N/A catgrp=N/A sourceiptag=N/A action = dns cat = Online host = 10.11.90 index = dnssense request = relay.wormhole.app source = /data/log/splunk/syslog/10.11.90/splunk-collector-2025-11-07-15.log sourcetype = dnssense:log src = user = N/A

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

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. Below this, a 'New Search' bar contains the query 'index= 10.221.112.10'. The search results show 60 events. A timeline visualization is displayed above a table of events. The table shows a single event at 11/7/25 10:55:47 AM. The event details include a client-rst action, policyid=13, and a destination IP of 10.11.173. The event is categorized as 'allowed' and 'dest = 10.11.173'.

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.