

# Libyan Oil Refinery Among Targets in Long-running Likely Espionage Campaign

✓ security.com/threat-intelligence/asyncrat-libya-oil-cyberattack



A series of attacks on Libyan organizations hit an oil refinery, a telecoms organization and a state institution between November 2025 and February 2026.

These attacks delivered the AsyncRAT backdoor, which is a publicly available backdoor that has previously been used by state-sponsored groups. This, and the organizations targeted, point to the possibility that this activity could be state sponsored.

While this activity dates from before U.S. and Israeli strikes on Iran led to conflict in the Gulf region and turmoil on the world's oil markets, the targeting of an oil refinery is notable. [Libyan oil production hit 1.37 million barrels a day last year, the highest in about 12 years](#). With so much disruption in the Middle East, it's possible that attacks against oil producers in other countries could ramp up as fears grow about global energy supplies.

## Attack chain

The initial infection vector in this campaign was likely a spear-phishing email, as we found lure documents on compromised networks that leverage interest in Libyan current affairs, with one lure document having the title *"Leaked CCTV footage - Saif al-Gaddafi's assassination.gz"*. Saif al-Gaddafi is the second son of former Libyan leader Muammar Gaddafi and was a major political figure in Libya. He was [assassinated by unknown gunmen at his home in Libya on February 3, 2026](#). The use of lure documents specific to Libya point to this campaign being purposely targeted, as opposed to these being victims that were targeted opportunistically.

A VBS downloader, which also has a topical filename, for example, *video\_saif\_gadafi\_2026.vbs*, was also found on targeted networks. This is downloaded from [https://hs8.krakenfiles\[.\]com/uploads/15-02-2026/JCaF7rrPQm/image.png](https://hs8.krakenfiles[.]com/uploads/15-02-2026/JCaF7rrPQm/image.png). Kraken Files is a

cloud-based file hosting and sharing platform. This downloads a PowerShell dropper (Filename: image.png). The PowerShell dropper creates the following scheduled task named 'devil' from 'C:\Users\Public\Music\Googless.xml'.

```
"C:\Windows\system32\schtasks.exe" /Create /XML C:\Users\Public\Music\Googless.xml /TN devil
```

```
"C:\Windows\system32\schtasks.exe" /run /tn devil
```

```
"C:\Windows\system32\schtasks.exe" /delete /tn devil /f
```

The dropper also downloads the AsyncRAT backdoor, which is the final payload. AsyncRAT is a remote access Trojan with a variety of capabilities, including keylogging, screen capture, and remote command execution capabilities, making it ideal for use in intelligence gathering and espionage attacks. It is also modular, meaning it can be updated and customized, which is attractive for attackers. AsyncRAT is publicly available so is not associated with one specific threat actor, and it has been used by both state-sponsored actors and ransomware actors in the past. This means we have not been able to attribute this activity to a named actor.

The earliest activity in this campaign occurred in November 2025, with the most recent activity occurring in mid-February 2026. There is evidence to suggest that the actor behind this activity has been on the networks of the oil company for all that time, with first activity on it occurring in November 2025, and further activity occurring in December 2025 and February 2026.

While the earliest activity our researchers uncovered dated from November 2025, files on VirusTotal related to this activity indicate that this attacker's campaign may have begun as far back as April 2025, with many of those files also having Libya-themed names, indicating a concentrated focus on organizations in that country. These additional files contain the same scheduled task that we saw on compromised machines. The names of these files include the following:

- Audio\_Libya\_algeria.vbs
- List\_name\_Libya\_israel.vbs
- Voice\_Egypt\_hafter\_Libya.vbs
- video\_saif\_eslam.vbs
- audio\_libya.vbs
- list\_name\_libya.vbs
- Libya\_Jordan\_File.vbs
- names\_libya444.vbs
- Libya\_voice2025.vbs

These files appear to also have been used in a phishing campaign that targeted Libya between November 2025 and February 2026, with the final payload also being AsyncRAT.

## Broader implications

---

The targeting of Libyan organizations shows how cyber threat actors are happy to take advantage of instability and major events in a country to try and gain a foothold on significant networks. Libya has been in a state of fluctuating stability since the Arab Spring of 2011 that toppled its long-time ruler Muammar Gaddafi. Attackers' willingness to take advantage of potential instability has relevance to the ongoing geopolitical situation in the world with the strikes and counterstrikes in the Gulf region leading to fears about what the ongoing situation may mean for the region and the wider global economy.

[Clashes in the Strait of Hormuz](#), through which around 20% of the world's oil travels, have led to claims that [oil costs could rise to more than \\$200 a barrel](#). This instability is likely to mean that interest in oil-producing nations and organizations outside of Iran is likely to peak - among both the general population and cyber actors too, who will always take advantage of emerging topical conflicts to capitalize on instability, or to use interest in them as part of lure documents and phishing emails.

Those operating in the energy sector should be aware that they could be the targets of unscrupulous threat actors in these tumultuous times. Meanwhile, organizations in all sectors should be aware of threat actors using interest in current events, including the conflict in Iran and rising oil prices, as lure topics in phishing campaigns.

## Protection/Mitigation

---

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

## Indicators of Compromise (IOCs)

---

12c65ac4e02313ed1aa2d32d56428f0a135b281604d536e5ae6ca08b6b4232c9 - AsyncRAT

0499152c6dd775491ce099eee4c382a94f72c07031081db164de921effa9664f - Executes AsyncRAT

39eade26c5680d20f5a8032a0d3996a29058e52c147e4b49a2072d2dcb353325 - VBS downloader - video\_saif\_gadafi\_2026.vbs

c03120163d9401d66d482899421d9dd68db63d34bac2b32e3090e8ad0b911d83 - VBS downloader - audio\_hafter\_saif\_eslam\_rusia.vbs, list\_names\_libya.vbs

cd7e16ca636f6e5cb86cd41561d57620a131a26b53c6e25a36edcbbcb2b5276a - VBS downloader - voice\_dbeibeh2025.vbs

3d5ada3b035e2adc8de1db24ab9d8e0e828eec1b7601ed9d064b41fa9d026a34 - VBS downloader - libya\_russia\_video2025.vbs

43c5d9a267742ee3c6c9bcf3e6f63ec397fbe0233a5d99bdb7dacbfa1a0f69d5 - VBS downloader -  
Audio\_Libya\_algeria.vbs

1d32f451d18c3dc8dbf00cd7df1200f83efa27cbaddeb9b2bed726e6d08ef5b1- VBS downloader -  
List\_name\_Libya\_israel.vbs

c2a2c2b26b235bad31a352e1fd475794167ec79928c52d98bccb3607e932c7b2

- VBS downloader - Voice\_Egypt\_hafter\_Libya.vbs

85e01e36b7b2b90af79642732a17dd566af0b10a85fd8a4cc85ea11583a0ff00

- VBS downloader - video\_saif\_eslam.vbs

d884a17046bbefd73f76f88533e1f2da40d5233b15caa48245de65d2c19c50dc

- VBS downloader - payload\_1.ps1

f8d2c5cb898cf92495fdb7e20f509603e1bdd62ba4b61bd7694a8e33a4c738f

- VBS downloader - payload\_1.ps1

3101cc378db2665eb2969b62e28efb9bfd5ca6f9bd3ebc27b422d5a29bfd1b17

- VBS downloader - audio\_libya.vbs

34ae832427b03df5f8cb90e78b5b174665c19602575b37fc7cad8100978898d2

- VBS downloader - list\_name\_libya.vbs

3ca93362559db4da9d44d614345cbdfdb81d882367af05651bb718e1cc57ab08

- VBS downloader - payload\_1.ps1

9843874eb6217a79ba5a51a6a886745169b1a1ad43f7ae12de6e610324e88ab7

- VBS downloader - Libya\_Jordan\_File.vbs

c3eef096073dd0873a821c35dd2e7eaf391863264ab72e1b91f2ca73218c2d04

- VBS downloader - image.png

ad4e27fe06fae2325faa2a00be7b41f40aa9c63fe79713597b3330ad7e583ca8

- VBS downloader - names\_libya444.vbs

22a1cf91fbac104e2dd374dd06e93488cfd216890088ef18318d90f440f00f6

- VBS downloader - image.png

b4a3f2f5091df7174e82283ed59cd557eea2e8ddd7a018dafc5e8151fd683429

- VBS downloader - Libya\_voice2025.vbs

0f3344e672d1ea6cde382b68b27063ed766fced717e9f5f2e15e6c79ce0737f7 - AsyncRAT

ad796fc0ac17b58e47dbadd42bf164790c18ac67aade8c6bf2251056ef68138d - AsyncRAT

946ae65e508acb4dbf6b29432889511a76636453cc04256230fbce25cef86b6a - AsyncRAT

ece81cdc6fc12a07a984b98df58e34c92998cdd957e1f45cabd925056bb0f92e - AsyncRAT

f307f8fa89b9f9eb8c2ae346055dff80c93f56034aa3abe7a8a25d6e5e680c6 - AsyncRAT

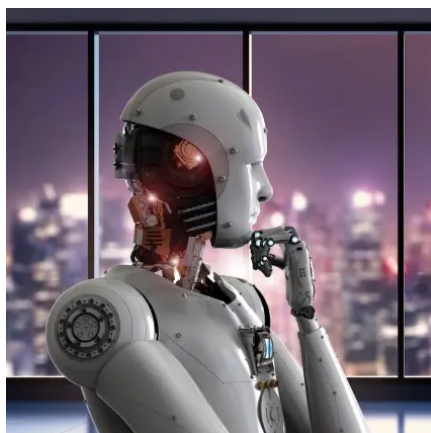
eb76f0797c27821635992ef23a570fe3a11c848998bc9f7735e968adc6b2f33c - AsyncRAT

5b573743306a2324608fdbd9c5ccea6bd5abfaccd1ea8b94c60f73da279e636 - AsyncRAT

f8b5a5429fb1da677ab8c09fc95b26e3b3d8bcd27521a56cc835fbf5878dbcd8 - AsyncRAT

## About the Author

---



Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.

You might also enjoy

---



### [Seedworm: Iranian APT on Networks of U.S. Bank, Airport, Software Company.](#)

---

- [5 Mar 2026](#)
- [23 Min Read](#)