

Iran conflict drives heightened espionage activity against Middle East targets

 proofpoint.com/us/blog/threat-insight/iran-conflict-drives-heightened-espionage-activity-against-middle-east-targets

March 10, 2026

[Blog](#)

[Threat Insight](#)

Iran conflict drives heightened espionage activity against Middle East targets



The Proofpoint Threat Research Team

Analyst note: Proofpoint uses the UNK_ designator to define clusters of activity that are still developing and have not been observed for long enough to receive a numerical TA designation. This report reflects Proofpoint Threat Research's observations as of the date of publication and does not constitute geopolitical analysis or policy commentary.

What happened

On 28 February 2026, the US and Israel conducted strikes targeting assets inside Iran, in a campaign the US called Operation Epic Fury. According to public sourcing, the attacks targeted Iranian missiles and air defenses, other military infrastructure, and Iranian leadership. Iran responded with retaliatory missile and drone strikes in the region, targeting US embassies and military installations.

As the war continues into its second week, several Iranian hacktivist groups and personas have claimed responsibility for various disruptive operations. Iranian espionage-focused threat groups remain somewhat active despite the [Iranian government's shutdown of the internet](#) immediately following the initial US and Israeli attacks. For instance, on 8 March, Proofpoint observed the Iran-aligned threat actor TA453 (Charming Kitten, Mint Sandstorm, APT42) conduct a credential phishing attempt against a US thinktank target. The email correspondence culminating in this credential phishing attempt commenced prior to the beginning of the conflict, indicating that TA453 is continuing to prioritize intelligence collection against its traditional target set.

While it is unclear how wider Iranian cyber operations will continue, Proofpoint Threat Research has also observed an increase in campaigns from other state-sponsored threat actors targeting Middle East government organizations since the war began. These campaigns were conducted by both known groups and previously unobserved actors, with suspected attribution to China, Belarus, Pakistan, and Hamas. The campaigns heavily relied on aspects of the conflict as topical lure content to engage the targets and often used compromised accounts belonging to government organizations to send phishing emails. Proofpoint assesses that this activity reflects a mixture of threat actors opportunistically using the war as lure content to conduct routine operations and those with an increased focus on intelligence collection targeting Middle Eastern government and diplomatic entities.

Campaign #1: UNK_InnerAmbush

In early March 2026, the suspected China-aligned threat actor UNK_InnerAmbush conducted a phishing campaign targeting Middle Eastern government and diplomatic organizations. The emails were sent from a likely compromised email address "uzbembish@elcat[.]kg" and linked to a Google Drive URL. The initial wave began on March 1, one day after the conflict began. The theme of phishing emails observed in this initial wave was Ayatollah Khamenei's death with an attempt to share sensitive images from the US "Department of Foreign Affairs". Later waves purported to share evidence that "Israel prepares to attack Gulf oil and gas infrastructure to frame Iran."

Confirmed: Iran's Supreme Leader Ayatollah Ali Khamenei Died in missile attack

← ↶ ↷



○ uzbembish@elcat.kg <uzbembish@elcat.kg>

Sunday, 1 March 2026 at 14:53

To: ○ [REDACTED]

🔔 To protect your privacy, some external images in this message were not downloaded.

[Download external images](#)

[Go to Settings](#)

Be Careful With This Message

The sender may be an impostor.

Attached document

Confirmed: Iran's Supreme Leader Ayatollah Ali Khamenei Died in missile attack. Secret on-site images sent by the US Department of Foreign Affairs.

Hosted on Google Drive

[View and download file \[drive.google.com\]](#)

Attachment password: 2026

Figure 1. *UNK_InnerAmbush phishing email linking to archive hosted on Google Drive.*

The Google Drive URL hosted a password protected ZIP or RAR archive named "Photos from the scene.rar" or "Strike at Gulf oil and gas facilities.zip". These archives contained several Microsoft Shortcut (LNK) files disguised as JPG images, which run a loader executable stored within a hidden subfolder.

A decoy image is shown to the user, and the loader executes a benign signed executable vulnerable to DLL sideloading ("nvdaHelperRemoteLoader.exe"). Upon execution, "nvdaHelperRemoteLoader.exe" loads the malicious loader DLL "nvdaHelperRemote.dll" which decrypts a Cobalt Strike payload from WinHlp.hlp and loads it into memory. The Cobalt Strike payload uses a customized malleable C&C profile and communicates with the C&C domain "support.almersalstore[.]com".

The phishing emails also contained unique tracking pixels hosted on a likely compromised website to track target engagement. These were in the format:

"hxxps://deepdive.hypernas[.]com/hypernas/api/page.php?uid= <target-email-address>".

Campaign #2: TA402

In early March 2026, TA402 (Frankenstein, Cruel Jackal) targeted a Middle Eastern government entity with an email credential phishing campaign. The actor used a compromised Ministry of Foreign Affairs of Iraq sender account ("ban.ali@mofa.gov[.]iq") and an attacker-controlled

account ("nqandeel04@gmail[.]com") to send the phishing emails. The emails had conflict-themed subjects referencing a potential US ground operation in Iran and a Gulf military alliance to confront Iranian threats.

The emails contained a URL that selectively served either a decoy PDF or a credential harvesting page depending on the target's IP geolocation.

The actor-controlled site was designed to impersonate Microsoft Outlook Web Application (OWA):

"hxxps[:]//mail[.]iwsmailserver[.]com/owa/auth/logon.aspx?uid=<target_specific_uuid>"

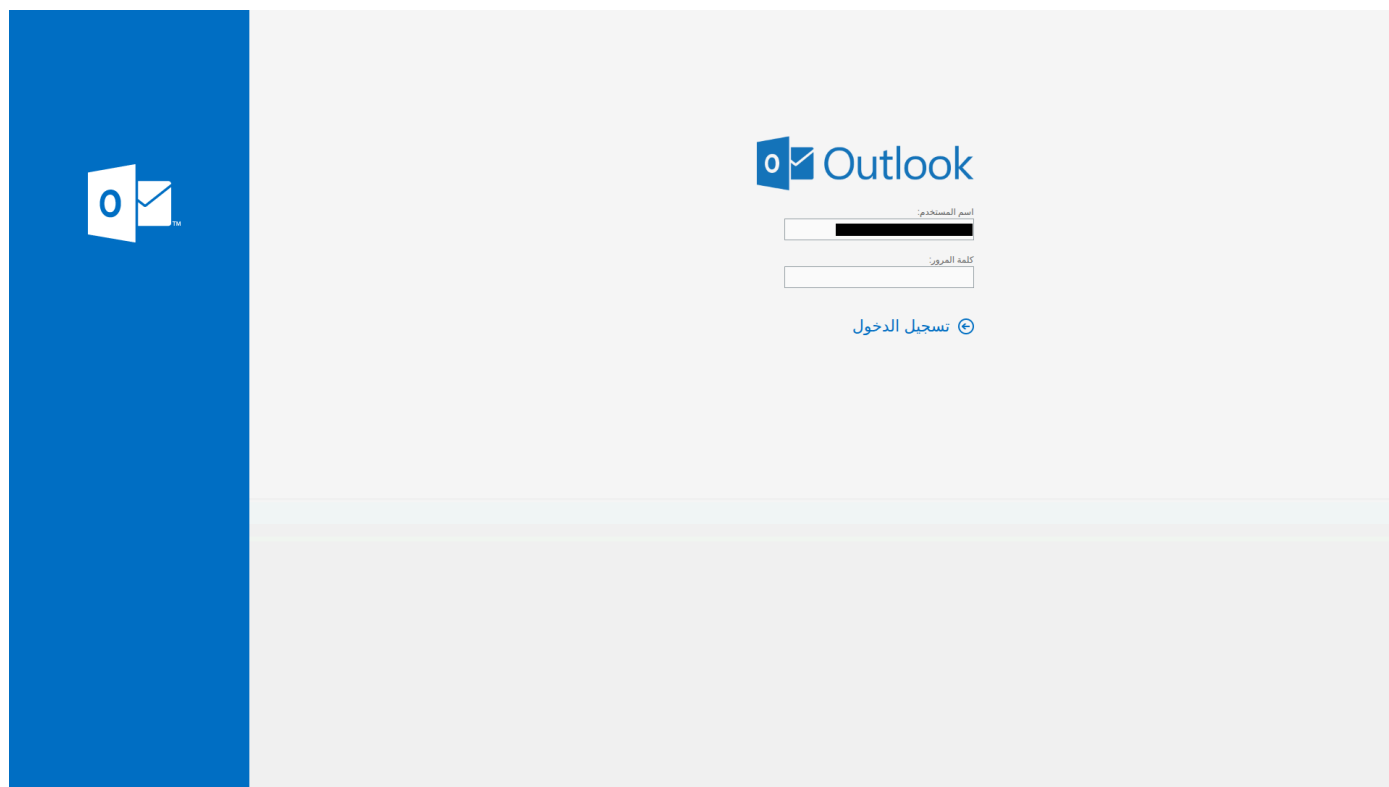


Figure 2. TA402 Outlook Web App (OWA) phish hosted on iwsmailserver[.]com.

If the target enters credentials, the values are sent via HTTP POST to an authentication endpoint on the same host.

Campaign #3: UNK_RobotDreams

On 5 March 2026, a suspected Pakistan-aligned actor Proofpoint calls UNK_RobotDreams sent spearphishing emails to India-based offices of Middle East government organizations. The email was sent from an Outlook freemail address impersonating India's Ministry of External Affairs: "jscop.mea.gov.in@outlook[.]com". The email used the subject "Gulf Security Alert: Iran Retaliation Impacts" referencing the Iran war to increase credibility and urgency.

The emails delivered a PDF attachment containing a blurred decoy and a fake Adobe Reader button.

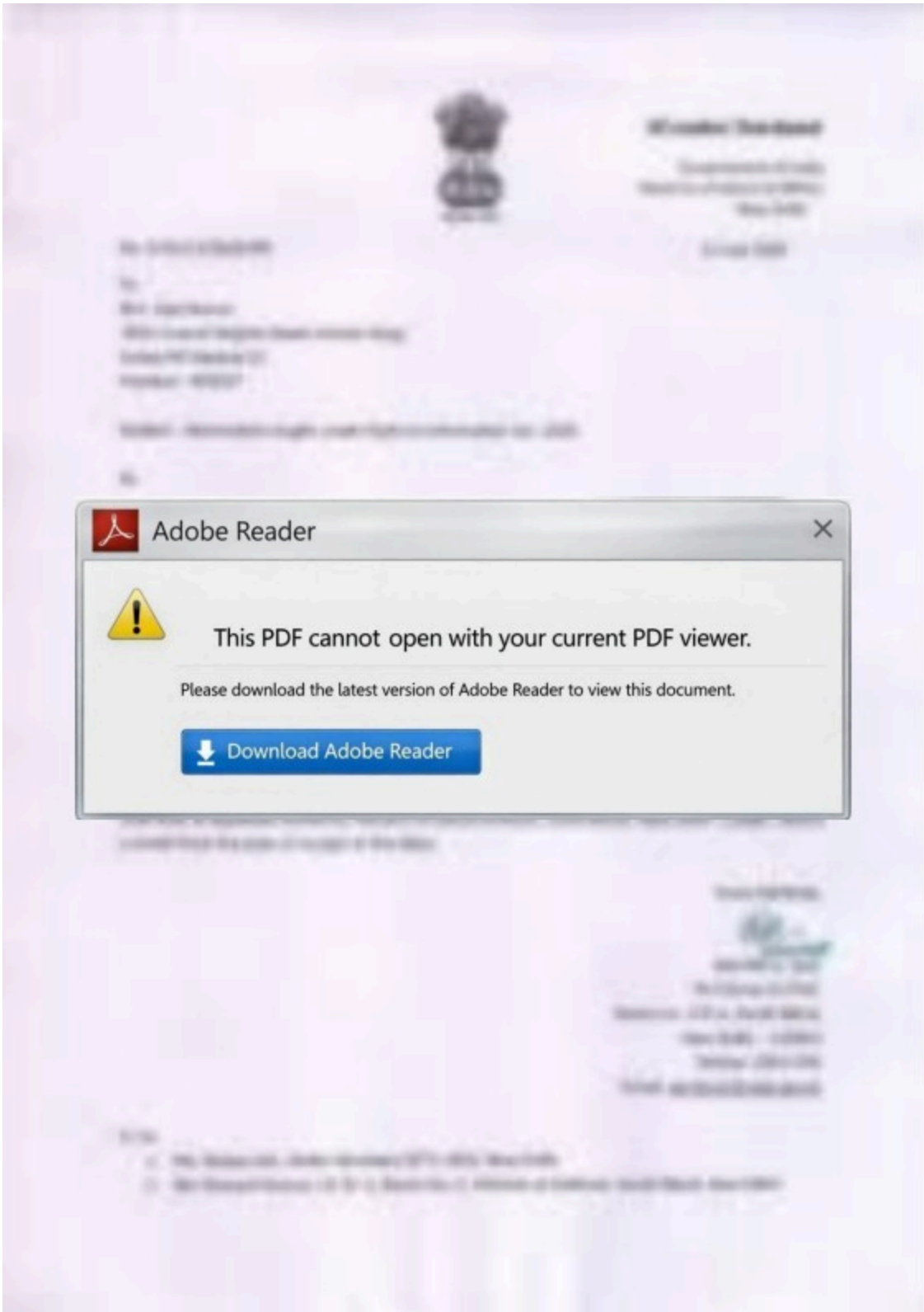


Figure 3. UNK_RobotDreams PDF attachment leading to executable hosted on defenceprodindia[.]site.

Clicking the button redirected the victim to an actor-controlled URL:

"hxxps://defenceprodindia[.]site/server.php?file=Reader_en_install". The URL implemented geofencing and served a decoy PDF to users outside the target region and an EXE payload to intended targets.

The downloaded executable ("Reader_en_install.exe") functioned as a .NET loader that used PowerShell (via "conhost.exe") to retrieve a Rust backdoor from the C&C host "endpoint1-b0ecetbuabcdg9cp[.]z01[.]azurefd[.]net", which was written to a file named "VLCMediaPlayer.exe". The Rust backdoor performed host fingerprinting and communicated with command and control using the same Azure Front Door hosted infrastructure.

This campaign and infrastructure overlapped with public reporting by [Bitdefender](#); however, Proofpoint does not currently track the activity as a named actor.

Campaign #4: UNK_NightOwl

On 2 March 2026, a suspected state-aligned actor that Proofpoint Threat Research calls UNK_NightOwl sent emails from both a likely compromised account and an attacker-owned freemail account to a government ministry in the Middle East. The compromised account appears to belong to the Ministry of Emergency and Disaster Management in Syria ("ali.mo@med.gov[.]sy"), and the freemail account was for a fake organization called War Analyse Ltd ("war.analyse.ltd@outlook[.]com"). The attackers targeted a government ministry in the Middle East and referred to the conflict in the Middle East as a lure topic with the subject "About Escalating Situation."

The emails included a domain that spoofed Microsoft OneDrive, but the URL led to a Microsoft Outlook Web Application (OWA)-themed credential harvesting page. The URL was target-specific with a client ID showing a fake session error and prompting the target to sign in again: "hxxps://iran.dashboard.1drvms[.]store/errors/sessionerrors/expire?client=<redacted>"

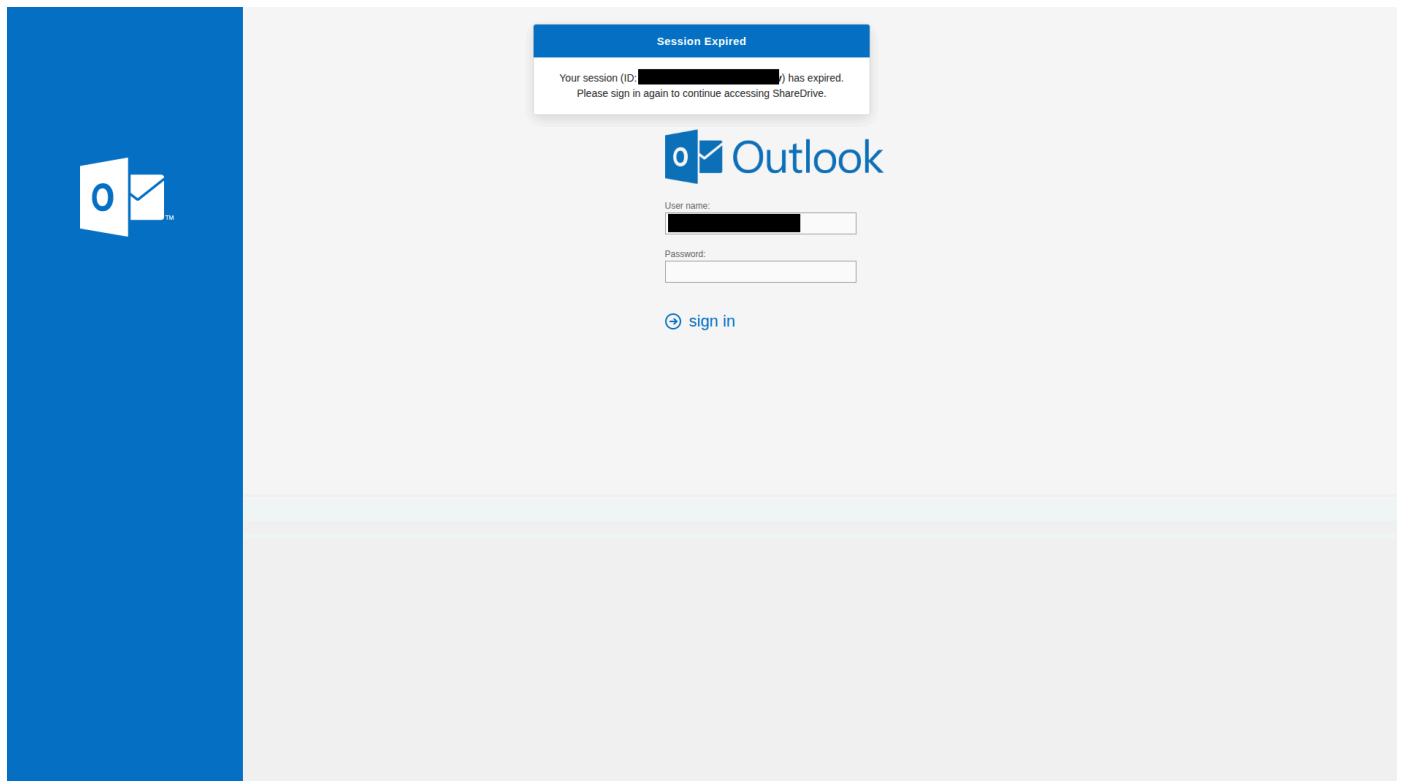


Figure 4. UNK_NightOwl OWA credential phishing site hosted on 1drvms[.]store.

If the user enters credentials and clicks the sign in button, the target is redirected to "hxxps://iran.liveuamap[.]com/", a legitimate open-source platform called Liveuamap with news updates on the Middle East conflict.



Figure 5. Redirection to iran.liveuamap[.]com after target enters credentials.

Proofpoint attributes this campaign to a new cluster called UNK_NightOwl as the observed activity does not align with any currently tracked actors.

Campaign # 5: TA473

Between 3-5 March 2026, the Belarus-aligned threat actor TA473 (Winter Vivern) sent emails to government organizations in Europe and the Middle East. These messages originated from likely compromised infrastructure and purported to be a European Council President spokesperson. The phishing emails contained a HTML attachment titled "european union statement on the situation in iran and the middle east.html". Notably, Proofpoint has not previously observed TA473 targeting Middle Eastern government organizations.

Mandatory reading of the European Union statement on the situation in Iran and the Middle East

⏪ ⏩ ↻

Today at 13:05



○ Maria Tomasik <maria.tomasik@denika.se>

To: ○ [REDACTED]



[Download All](#) • [Preview All](#)

Dear colleagues,

In light of recent events in Iran and the Middle East, I strongly urge all members of the diplomatic corps to familiarize themselves with the European Union's official statement. This statement outlines the EU's position on key issues such as the actions of the Iranian authorities regarding human rights, regional security, and Iran's nuclear and ballistic missile programs.

Given the gravity of the situation, I ask you to carefully review this document and be prepared for further discussions.

Best regards,

Maria Tomasik
Spokesperson for the European Council President
[+32470884535](tel:+32470884535)



Figure 6. TA473 phishing email spoofing spokesperson for the European Council President.

The HTML file, if opened, displays a decoy image to the user and conducts HTTP request to a URL of the format "hxxps://unityprogressall[.]org/imagecontent/getimgcontent.php?id=<target-email-address>". Proofpoint Threat Research was unable to retrieve any next-stage payloads at the time of analysis. Based on the HTML content, these HTTP requests were likely intended for tracking purposes rather than delivering follow-on malicious payloads.

Campaign #6: TA453

Proofpoint's tracking of known Iranian actors has surfaced only one campaign so far since the beginning of the war. In late February into early March, Iran-aligned actor TA453 (Charming Kitten, Mint Sandstorm, APT42) used an attacker-owned freemail account "McManus.Michael@hotmail[.]com" spoofing Michael McManus, the head of research at the Henry Jackson Society, to target an individual at a thinktank in the US.

The initial thread had begun prior to the war as part of typical TA453 espionage activity with a benign email invitation sent to a target's personal account in February. The email exchange then continued with further targets' corporate accounts after the war, suggesting that TA453 is maintaining its intelligence collection efforts during the ongoing conflict.

The email was themed around an invitation to participate in a roundtable on air defense in the Middle East. Part of the benign outreach included a OneDrive link to a benign PDF ("Air Defense Depletion & Deterrence in the Middle East.pdf") with the proposal for the roundtable to support a credible lure.

"hxxps://1drv[.]ms/b/c/cbec61ab8028f986/IQDa9igU3D3BRqiyNtth76AzAbOM6jUpa8apnuRI-zKXKow?e=E8blfd"

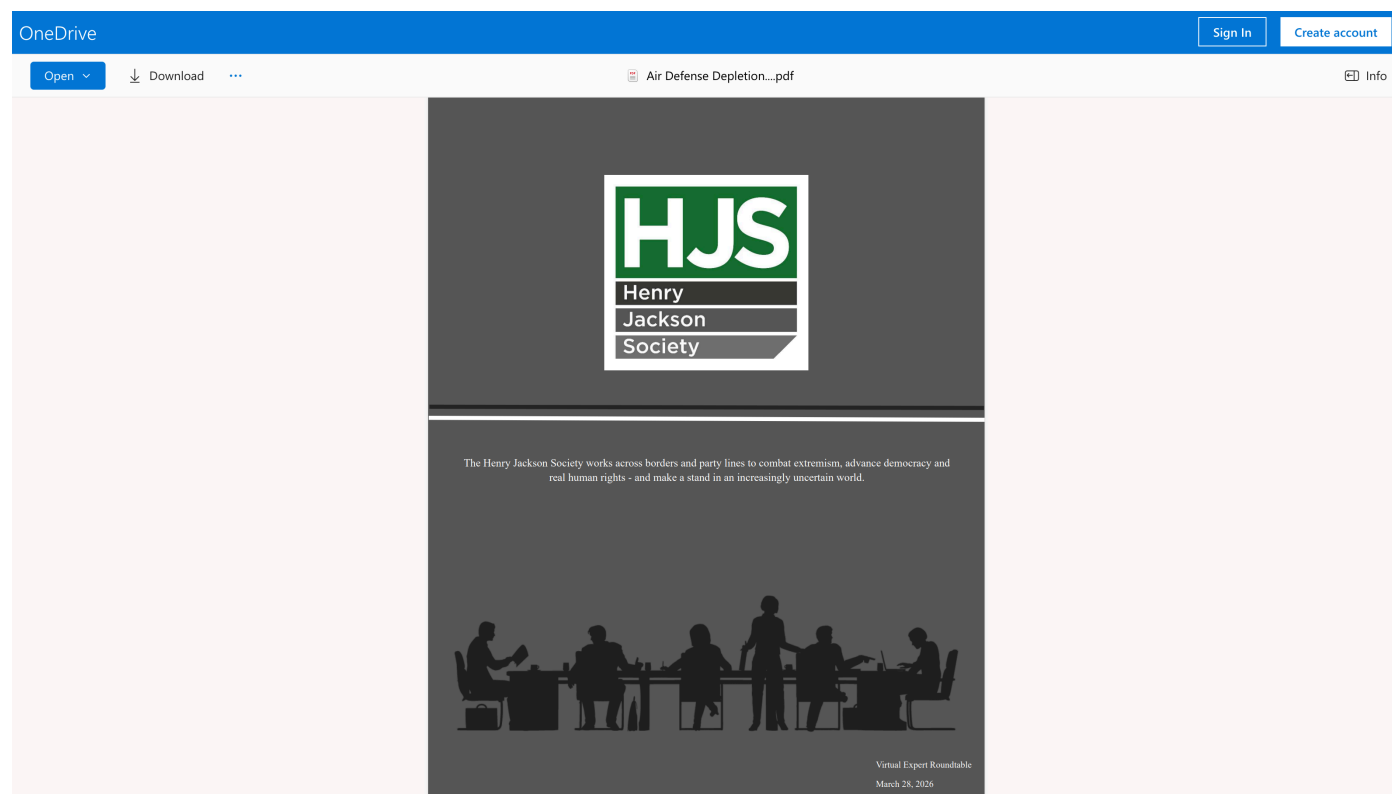


Figure 7. Benign OneDrive link hosting PDF proposal for Henry Jackson Society roundtable.

Once a rapport had been established with the target, the following email in the exchange included a malicious URL disguised as a link to another PDF called "Air Defense Depletion & Deterrence in the Middle East-Event Overview.pdf".

The URL used an attacker-owned domain ("transfergocompany[.]com") that then redirected to a OneDrive-themed credential phishing page hosted on the cloud-hosting service Netlify ("fileportalshare.netlify[.]app") pre-filled with the target's email.

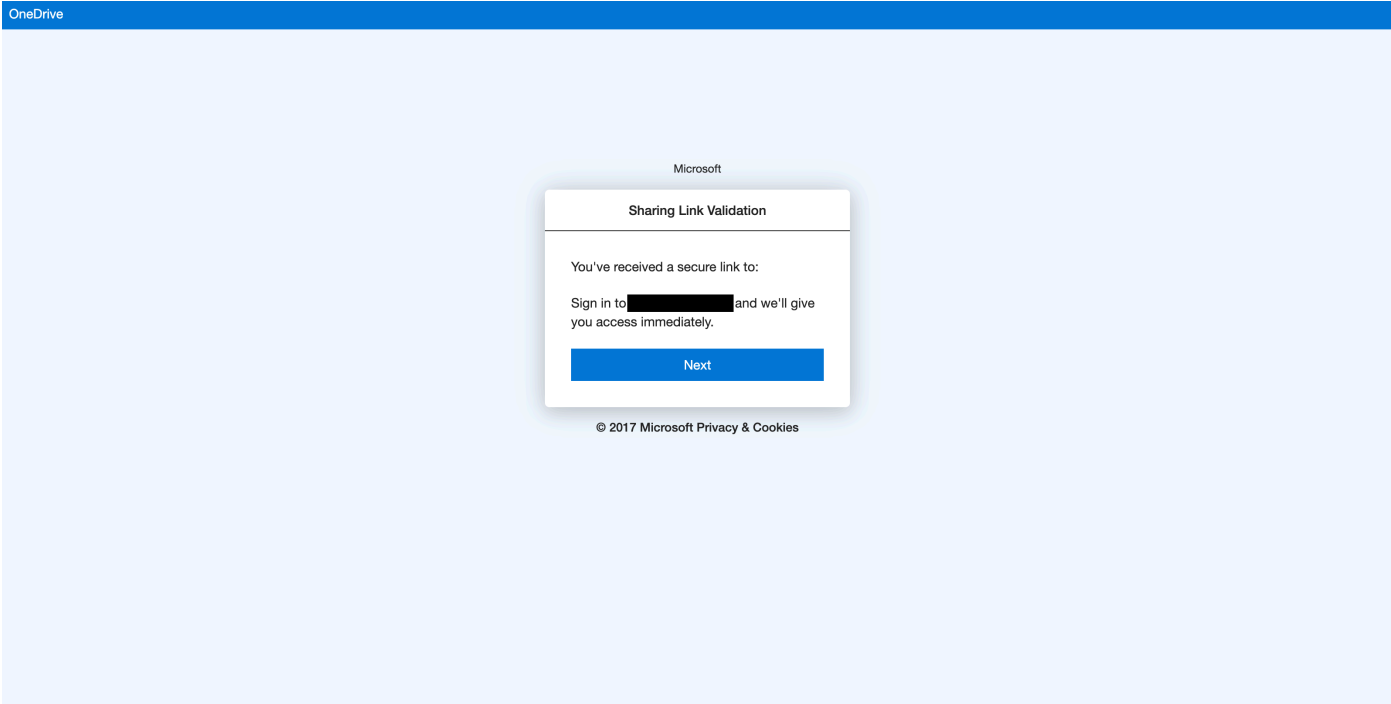


Figure 8. OneDrive spoofing credential phishing landing page.

Why it matters

As the conflict involving Iran and regional actors continues, the operations of Iranian threat actors remain a mix of traditional espionage and disruptive campaigns in support of war efforts. Proofpoint also observed a range of non-Iranian threat groups targeting Middle Eastern governments with conflict-themed social engineering. While several of these groups incorporated the war-themed lure content in operations that are largely consistent with typical targeting remits, others demonstrated a shift toward intelligence collection against Middle Eastern government and diplomatic entities. This likely reflects an effort to gather regional intelligence on the standing, trajectory, and broader geopolitical implications of the conflict. This suggests the conflict is being used both as a topical social engineering pretext and a driver of collection priorities for a range of state-aligned threat actors.

Indicators of compromise

UNK_InnerAmbush		
Indicator	Type	D
uzbembish@elcat[.]kg	Email address	S C

fed6ebb87f7388adf527076b07e81dfa432bac4e899b0d7af17b85cc0205ffad	SHA256	P
a9de383c6a1b00c9bd5a09ef87440d72ec7fc4bcd781207b3cace2f246788d4d	SHA256	S f
dfaaaf75147afbd57844382c953ec7ef36f68a9c17c66a47a847279a6b1109c9	SHA256	9 3
4b9661092051839496c04169ccb52b659c0f65cefd14a990e23565a0c0e8eeaf	SHA256	2
d518262dd687a48f273966853f3ed4eb7404eb918b165bb71ff83f75962c0104	SHA256	L
b58ec14b0119182aef12d153280962ad76c30e3cd67533177d55481704eba705	SHA256	C
7b6d69a249fe2adf43eefc31cdeca62cf48ab428fcfb199322feeb99d24fb001	SHA256	n
a8acb9864e6f64323ed75e69038ca9bfe76f7b1b0d24ec7df8ac07b6dbd641a3	SHA256	n
14efa1194cc4c6aa5585d63c032268794364123d41a01121cbd5e56f7c313399	SHA256	V
support.almersalstore[.]com	Hostname	C
almersalstore[.]com	Domain	C

TA402			
Indicator	Type	Description	First Seen

ban.ali@mofa.gov[.]iq	Email address	Sender email (likely compromised)	March 2026
nqandeel04@gmail[.]com	Email address	Sender email	March 2026
hxxps://mail.iwsmailserver[.]com/owa/auth/logon.aspx?uid=<target_specific_uuid>	URL	OWA credential phishing URL format	March 2026
iwsmailserver[.]com	Domain	TA402-controlled domain	March 2026

TA473		
Indicator	Type	Description
maria.tomasik@denika[.]se	Email address	Sender email compromised
hxxps://unityprogressall[.]org/imagecontent/getimgcontent.php?id=<target-email-address>	URL	URL format cc HTML attachm
unityprogressall[.]org	Domain	TA473-control
72.60.90[.]32	IP address	Hosting IP add for unityprogre

UNK_NightOwl		
Indicator	Type	Description

war.analyse.ltd@outlook[.]com	Email address	Sender email
ali.mo@med.gov[.]sy	Email address	Sender email (likely compromised)
hxxps://iran.dashboard.1drvms[.]store/errors/sessionerrors/expire?client=[redacted]	URL	Credential harvesting page

UNK_RobotDreams	
Indicator	Type
jscop.mea.gov.in@outlook[.]com	Email address
hxxps://defenceprodindia[.]site/server.php?file=Reader_en_install	URL
defenceprodindia[.]site	Domain
hxxps://endpoint1-b0ecetbuabcdg9cp.z01.azurefd[.]net:443/download.php?file=cnVzdHVwaW5pdA	URL
endpoint1-b0ecetbuabcdg9cp[.]z01[.]azurefd[.]net	Hostname
9477d9cd1435dc465b4047745e9c71103a114d65ed0d5f02ac3c97ac3f1dbf47	SHA256
a9f4f4bc12896d0f0d2eeff02dd3e3e1c1406d8a6d22d59aa85f151d806ba390	SHA256

ea1d98a41ad9343d017fa72f4baeeca0daa688bec6e0508e266c5e37e9d330de	SHA256
--	--------

TA453	
Indicator	Ty
McManus.Michael@hotmail[.]com	En ad
hxxps://1drv[.]ms/b/c/cbec61ab8028f986/IQDa9igU3D3BRqiyNtth76AzAbOM6jUpa8apnuRI-zKXKow?e=E8blfd	UF
16db04b632668dae081359fc07c97e5a9b79dad61713642e48b494aa6b7828be	PC
transfergocompany[.]com	Dc

[Previous Blog Post](#)

Subscribe to the Proofpoint Blog

Business Email: