Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

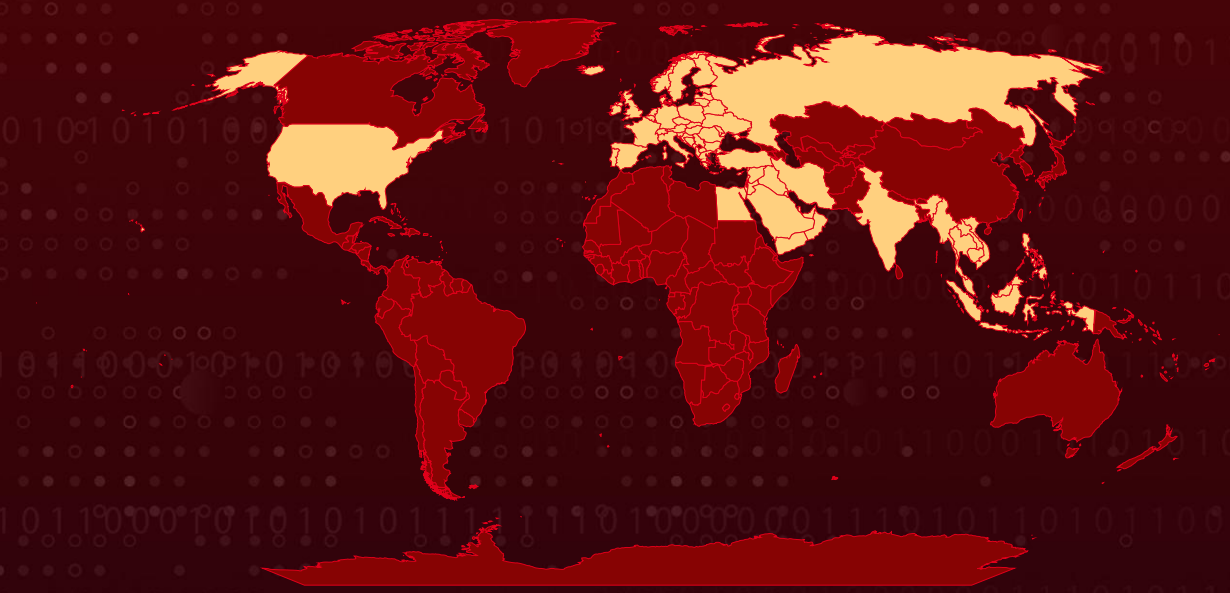
Phishing in the Fog of War: A Surge in State-Aligned Espionage Campaigns

Date of Publication	Admiralty Code	TA Number
March 17, 2026	A1	TA2026073

Summary

First Seen: Late February 2026
Targeted Regions: Middle East, Europe, United States, India, Southeast Asia
Targeted Platform: Windows
Targeted Products: Microsoft Outlook Web Application (OWA), Microsoft OneDrive, Adobe Reader, Google Drive, Domain Controllers, Web Servers, IT Workstations, Executive-Level Assets, C4I Systems
Targeted Industries: Government, Diplomatic Organizations, Think Tanks, Military, Defense
Malware: AppleChris, MemFun, Getpass
Threat Actor: UNK_InnerAmbush, **TA402** (aka Extreme Jackal, Molerats, Gaza Cybergang, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5, Frankenstein, Cruel Jackal), UNK_RobotDreams, UNK_NightOwl, **TA473** (aka Winter Vivern, UAC-0114, UNC4907, TAG-70), **TA453** (aka Charming Kitten, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm, Ballistic Bobcat, CharmingCypress), **CL-STA-1087**
Attack: Amid the escalating US-Israel-Iran conflict, multiple threat actors rapidly turned the crisis into a powerful social engineering lure, launching coordinated phishing and malware campaigns against Middle Eastern government, diplomatic, and military and defense targets in Southeast Asia. By exploiting fear-driven narratives, ranging from leadership deaths to military escalations, attackers delivered weaponized archives, credential-harvesting pages, and multi-stage malware loaders, using techniques such as DLL sideloading and geofenced payload delivery. These operations combined stealthy execution with highly targeted delivery, highlighting how geopolitical instability is being actively weaponized to accelerate cyber espionage.

Attack Regions



Attack Details

#1

As tensions rapidly escalated into open conflict between the U.S., Israel, and Iran in late February 2026, a wave of opportunistic espionage campaigns quickly followed, turning geopolitical chaos into a highly effective lure. Within days, the suspected China-aligned actor UNK_InnerAmbush began spear-phishing operations targeting Middle Eastern government and diplomatic entities. Using a likely compromised Kyrgyzstan-based email account, the group crafted convincing narratives around sensitive developments, such as the rumored death of Ayatollah Khamenei and alleged Israeli plans to strike Gulf energy infrastructure. These emails directed recipients to Google Drive links hosting password-protected archives disguised as image collections. Around the same time, the Hamas-aligned group TA402 launched parallel credential harvesting campaigns, leveraging a hijacked Iraqi Ministry of Foreign Affairs account alongside attacker-controlled infrastructure to distribute lures centered on potential U.S. military operations in Iran and regional alliances.

#2

Behind the scenes, these campaigns relied on carefully staged infection chains designed to evade detection while maintaining credibility. In the UNK_InnerAmbush activity, victims who extracted the downloaded archives encountered LNK files masquerading as harmless images. Once executed, these shortcuts triggered a hidden loader that displayed a decoy image while silently abusing a legitimate, signed executable vulnerable to DLL sideloading. This ultimately led to the deployment of a Cobalt Strike payload, decrypted from a disguised file and injected directly into memory, communicating with attacker-controlled infrastructure via a tailored command-and-control profile. To further refine targeting and measure engagement, the phishing emails embedded tracking pixels hosted on compromised infrastructure.

#3

In parallel, a suspected Pakistan-aligned actor tracked as UNK_RobotDreams expanded the campaign landscape by targeting India-based offices of Middle Eastern government entities. Impersonating India's Ministry of External Affairs, the attackers distributed phishing emails containing weaponized PDF attachments. These files used blurred decoys and fake prompts to lure victims into clicking embedded links, which redirected to geofenced payload delivery infrastructure. Targets within the intended region received a .NET-based loader, which leveraged PowerShell execution through conhost.exe to retrieve a Rust-based backdoor from Azure-hosted infrastructure. Once deployed, the backdoor performed system reconnaissance and established persistent communication with its command-and-control servers.

#4 Simultaneously, multiple threat clusters, including TA402, UNK_NightOwl, and TA453, focused on credential harvesting through highly targeted, geolocation-aware phishing frameworks. These operations selectively served fake Microsoft OWA or OneDrive login pages only to intended victims, while diverting others to benign content to avoid scrutiny. In one instance, UNK_NightOwl abused a compromised Syrian government account and redirected victims to legitimate conflict-tracking websites after credential theft to maintain the illusion of authenticity. Meanwhile, TA473 (Winter Vivern) broadened its operational scope beyond Europe, delivering HTML-based lures that quietly tracked user interaction through background requests to attacker infrastructure.

#5 Notably, the Iranian-linked actor TA453 remained active despite domestic internet disruptions, continuing its long-standing focus on Western policy and research organizations. In a calculated, multi-stage social engineering effort, the group-initiated contact with a U.S. think tank by impersonating a senior figure from the Henry Jackson Society. After establishing credibility through benign communication and shared documents, the attackers transitioned to a phishing phase, delivering a malicious link that redirected the target to a credential-harvesting page pre-filled with their email address.

#6 A suspected China-based state-sponsored threat actor tracked as CL-STA-1087 has been conducting a persistent espionage campaign against military organizations in Southeast Asia since at least 2020. The operation employs custom-developed backdoors (AppleChris and MemFun) and a modified Mimikatz credential harvester (Getpass) to maintain long-term access, perform lateral movement, and selectively exfiltrate highly sensitive military intelligence, including organizational structures, joint military activities with Western armed forces, and C4I system documentation.

#7 Taken together, the diversity and coordination of these campaigns highlight how rapidly global threat actors adapt to geopolitical events. With actors spanning Chinese, Iranian, Hamas-aligned, Pakistani, and Belarusian affiliations, the conflict has not only intensified intelligence-gathering efforts but also provided a compelling narrative framework for large-scale, highly targeted social engineering operations against government, military, and diplomatic sectors.

Recommendations

Quarantine Conflict-Themed Phishing Emails: Configure email security gateways to flag and quarantine inbound messages referencing Iran conflict topics, particularly those containing archive attachments (RAR, ZIP), HTML attachments, or links to cloud storage services like Google Drive and OneDrive from unverified external senders.

Disable LNK File Execution from Archives: Deploy group policies or endpoint security rules to prevent the execution of Windows Shortcut (LNK) files extracted from downloaded archives, as this technique was central to the UNK_InnerAmbush Cobalt Strike delivery chain.

Detect DLL Sideloading Attempts: Implement endpoint detection rules to identify suspicious DLL loading by legitimate signed executables, specifically monitoring for "nvdaHelperRemoteLoader.exe" loading non-standard DLLs and any unsigned DLL loads from temporary or user-writable directories.

Enforce Multi-Factor Authentication on All Email Platforms: Given that five of six campaigns targeted email credentials via OWA and OneDrive phishing pages, enforce phishing-resistant MFA (FIDO2/WebAuthn) across all Microsoft 365 and email platforms to neutralize harvested credentials.

Audit Compromised Government Email Accounts: Coordinate with partnering government entities, particularly those in Iraq and Syria, to investigate potentially compromised sender accounts identified in this advisory and revoke any unauthorized access.

Monitor Azure Front Door and Netlify for Suspicious Hosting: Implement monitoring for outbound connections to Azure Front Door endpoints and Netlify-hosted domains that are not associated with approved organizational services, as both were abused for payload staging and credential phishing in these campaigns.

Monitor Pastebin and Dropbox Connections: Implement monitoring and alerting for outbound connections to Pastebin and Dropbox from server infrastructure and critical endpoints, as these legitimate services are abused as Dead Drop Resolvers for C2 address retrieval.

Conduct Targeted Threat Hunting for Sensitive File Access: Proactively search for anomalous access patterns to military planning documents, organizational charts, C4I documentation, and files related to joint operations with allied forces, particularly from endpoints or accounts not typically associated with such access.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1583: Acquire Infrastructure	T1583.001: Domains
	T1585: Establish Accounts	T1585.001: Social Media Accounts
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
		T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
	T1047: Windows Management Instrumentation	
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
		T1574.001: DLL Search Order Hijacking
	T1055: Process Injection	T1055.012: Process Hollowing

Tactic	Technique	Sub-technique
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1620: Reflective Code Loading	
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
Credential Access	T1056: Input Capture	T1056.003: Web Portal Capture
	T1003: OS Credential Dumping	T1003.001: LSASS Memory
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1057: Process Discovery	
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.001: Dead Drop Resolver
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
	T1090: Proxy	T1090.001: Internal Proxy
Lateral Movement	T1021: Remote Services	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Reconnaissance	T1598: Phishing for Information	T1598.003: Spearphishing Link

Indicators of Compromise (IOCs)

TYPE	VALUE
Email Address	uzbembish[@]elcat[.]kg, ban.ali[@]mofa.gov[.]iq, nqandeel04[@]gmail[.]com, maria.Tomasik[@]denika[.]se, war.analyse[.]ltd[@]outlook[.]com, ali[.]mo[@]med[.]gov[.]sy, jscop[.]mea[.]gov[.]in[@]outlook[.]com, McManus[.]Michael[@]hotmail[.]com
SHA256	fed6ebb87f7388adf527076b07e81dfa432bac4e899b0d7af17b85cc0205ffad, a9de383c6a1b00c9bd5a09ef87440d72ec7fc4bcd781207b3cace2f246788d4d, dfaaaf75147afbd57844382c953ec7ef36f68a9c17c66a47a847279a6b1109c9, 4b9661092051839496c04169ccb52b659c0f65cefd14a990e23565a0c0e8eeaf, d518262dd687a48f273966853f3ed4eb7404eb918b165bb71ff83f75962c0104, b58ec14b0119182aef12d153280962ad76c30e3cd67533177d55481704eba705, 7b6d69a249fe2adf43eefc31cdeca62cf48ab428fcbf199322feeb99d24fb001, a8acb9864e6f64323ed75e69038ca9bfe76f7b1b0d24ec7df8ac07b6dbd641a3, 14efa1194cc4c6aa5585d63c032268794364123d41a01121cbd5e56f7c313399, 9477d9cd1435dc465b4047745e9c71103a114d65ed0d5f02ac3c97ac3f1dbf47, a9f4f4bc12896d0f0d2eeff02dd3e3e1c1406d8a6d22d59aa85f151d806ba390, ea1d98a41ad9343d017fa72f4baeeca0daa688bec6e0508e266c5e37e9d330de, 16db04b632668dae081359fc07c97e5a9b79dad61713642e48b494aa6b7828be, 9e44a460196cc92fa6c6c8a12d74fb73a55955045733719e3966a7b8ced6c500, 5a6ba08efcef32f5f38df544c319d1983adc35f3db64f77fa5b51b44d0e5052c, 0e255b4b04f5064ff97da214050da81a823b3d99bce60cdd9ee90d913cc4a952,

TYPE	VALUE
SHA256	413daa580db74a38397d09979090b291f916f0bb26a68e7e0b03b4390c1b472f, 2ee667c0ddd4aa341adf8d85b54fbb2fce8cc14aa88967a5cb99babb08a10fae, ad25b40315dad0bda5916854e1925c1514f8f8b94e4ee09a43375cc1e77422ad, ee4d4b7340b3fa70387050cd139b43ecc65d0cfd9e3c7dcb94562f5c9c91f58f
Domains	almersalstore[.]com, iwsmailserver[.]com, unityprogressall[.]org, defenceprodindia[.]site, transfergocompany[.]com, fileportalshare.netlify[.]app
Hostname	support[.]almersalstore[.]com, endpoint1-b0ecetbuabcdg9cp[.]z01[.]azurefd[.]net
URL	hxxps[:]//mail[.]iwsmailserver[.]com/owa/auth/logon[.]aspx?uid=<target_specific_uuid>, hxxps[:]//unityprogressall[.]org/imagecontent/getimgcontent[.]php?id=<target-email-address>, hxxps[:]//iran[.]dashboard[.]1drvms[.]store/errors/sessionerrors/expire?client=[redacted], hxxps[:]//defenceprodindia[.]site/server[.]php?file=Reader_en_install, hxxps[:]//endpoint1-b0ecetbuabcdg9cp[.]z01[.]azurefd[.]net[:]443/download[.]php?file=cnVzdHVwaW5pdA, hxxps[:]//1drv[.]ms/b/c/cbec61ab8028f986/IQDa9igU3D3BRqiyNtth76AzAbOM6jUpa8apnuRl-zKXKow?e=E8bIfd
IPv4	72[.]60[.]90[.]32, 8[.]212[.]169[.]27, 8[.]220[.]135[.]151, 8[.]220[.]177[.]252, 8[.]220[.]184[.]177, 116[.]63[.]177[.]49, 118[.]194[.]238[.]51, 154[.]39[.]142[.]177, 154[.]39[.]137[.]203, 109[.]248[.]24[.]177
Mutex	0XFEXYCDAPPLE05CHRIS, GOOGLE

TYPE	VALUE
Filenames	swrpv.sys, swprv32.sys, update.exe, Googleupdate.exe, WinSAT.db

References

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

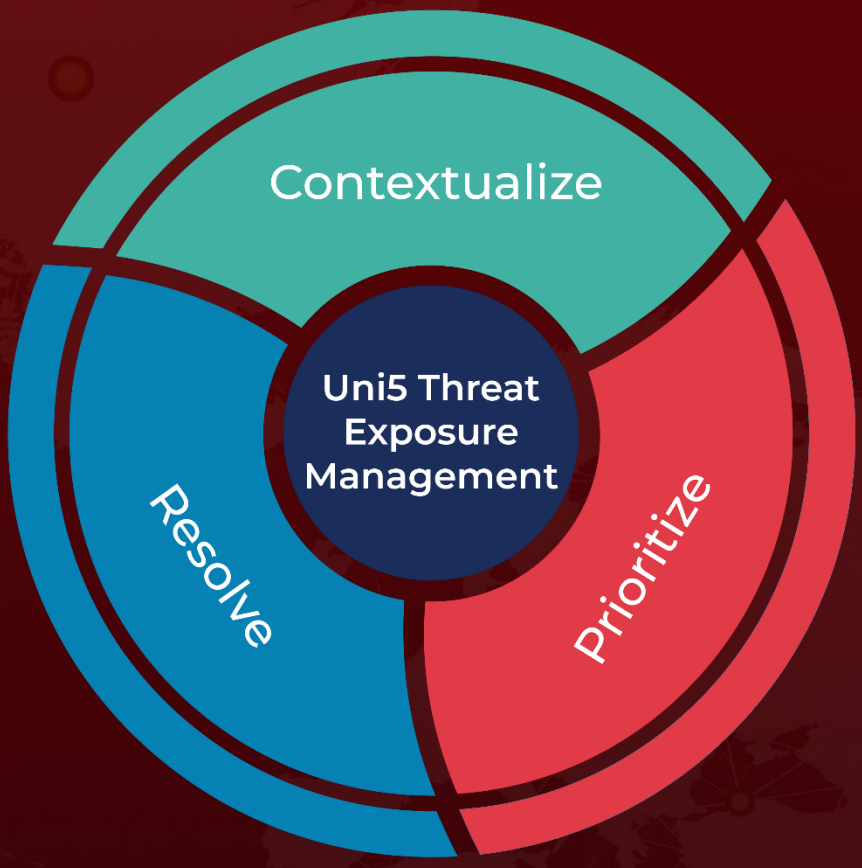
https://unit42.paloaltonetworks.com/espionage-campaign-against-military-targets/

https://www.recordedfuture.com/blog/the-iran-war-what-you-need-to-know

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 17, 2026 • 10:00 AM

More at www.hivepro.com