

I'd come running back to EU again: TA416 resumes European government espionage campaigns

p proofpoint.com/us/blog/threat-insight/id-come-running-back-eu-again-ta416-resumes-european-government-espionage

March 26, 2026



Key findings

- From mid-2025 onwards, the China-aligned threat actor TA416 resumed observed targeting of European government and diplomatic organizations following a period of reduced EU-focused activity in our telemetry.
- This TA416 activity included multiple waves of web bug and malware delivery campaigns against diplomatic missions to the European Union and NATO across a range of European countries.
- In March 2026, Proofpoint also observed TA416 expand targeting to include diplomatic and government entities in the Middle East in the weeks following the outbreak of conflict in Iran.
- Throughout this period, TA416 regularly altered its infection chain, including abusing Cloudflare Turnstile challenge pages, abusing OAuth redirects, and using C# project files, as well as frequently updating its custom PlugX payload.
- TA416 most directly overlaps with public reporting on RedDelta, Red Lich, Vertigo Panda, SmugX, and DarkPeony.

Overview

In 2022, Proofpoint [reported](#) on high-volume TA416 activity targeting European governments, which increased sharply as Russian troops began amassing on the border of Ukraine. This high operational tempo of TA416 campaigns against European government targets continued until mid-2023, when the group shifted targeting away from Europe. From mid-2023 until mid-2025, Proofpoint observed minimal TA416 targeting within Europe, with the group [mostly active](#) across Southeast Asia, Taiwan, and Mongolia during this period.

Since mid-2025, TA416 resumed regular targeting of European government and diplomatic entities. This renewed focus most heavily targeted individuals or mailboxes associated with diplomatic missions and delegations to NATO and the EU. TA416's return to European government targeting occurred during heightened [EU–China tensions over trade, the Russia–Ukraine war, and rare earths exports](#), and commenced immediately following the [25th EU–China summit](#).

In March 2026, following the outbreak of the Iran war, TA416 conducted multiple campaigns targeting a wide range of diplomatic and government entities in the Middle East, a region not traditionally regularly targeted by this threat actor. This aligns with a [trend](#) observed by Proofpoint of some state-aligned threat actors shifting targeting toward Middle Eastern government and diplomatic entities in the aftermath of the war. This likely reflects an effort to gather regional intelligence on the status, trajectory, and broader geopolitical implications of the conflict.

From mid-2025 to early 2026, TA416 conducted both broad web bug and malware delivery campaigns. The TA416 web bug campaigns used freemail sender accounts and a range of thematic lures, such as Europe sending troops to Greenland, to perform delivery and engagement reconnaissance. A web bug (or tracking pixel) is a tiny invisible object embedded in an email that triggers an HTTP request to a remote server when opened, revealing the recipient's IP address, user agent, and time of access, allowing the threat actor to assess whether the email was opened by the intended target. Malware delivery campaigns used both attacker-controlled freemail accounts and compromised government and diplomatic mailboxes to send links to malicious archives hosted on Microsoft Azure Blob Storage, actor-controlled domains, Google Drive, and compromised SharePoint instances.

During this period, TA416 repeatedly altered its initial infection chains while maintaining a consistent goal of loading the group's customized PlugX backdoor via DLL sideloading triads. Initial access techniques evolved from using fake Cloudflare Turnstile challenge pages that gated access to ZIP archives, to abuse of Microsoft Entra ID third-party applications that redirected users to attacker-controlled malware delivery domains, and finally to archives containing a renamed Microsoft MSBuild executable and malicious C# project files. In each case, TA416 relied on either ZIP smuggling using Microsoft shortcut (LNK) files or CSPROJ-based downloaders to deliver a signed executable, malicious DLL, and encrypted payload triad that ultimately loaded PlugX into memory.

Delivery: widespread web bug campaigns targeting EU diplomatic entities

 Figure 1



Figure 1: TA416 “humanitarian concerns” web bug phishing email from July 2025.

TA416’s renewed targeting of European government entities commenced one day after the [25th EU–China summit](#) with a series of web bug campaigns targeting diplomatic missions to the EU across many European countries. In late July and early August 2025, TA416 sent over 100 phishing emails containing web bugs from the following Gmail email addresses:

- emmeline.voss@gmail[.]com
- kordula.wehrli@gmail[.]com
- kayden.beaufort@gmail[.]com

The group used multiple lure topics such as urgent humanitarian concerns, requests for interviews, and proposals for collaboration. These web bug campaigns were likely conducted for reconnaissance purposes to track delivery and engagement to inform follow-on malware delivery attempts. Proofpoint observed the following URL formats used in these campaigns, with each email including a unique image filename:

- hxxps://welnetsanda[.]org/images/upload/logo.png/{UniqueID}.png
- hxxps://phpthemes[.]net/images/upload/eu.png/{UniqueID}.png
- hxxps://phpthemes[.]net/images/upload/{UniqueID}.png

In January 2026, Proofpoint observed TA416 send another widespread wave of web bug phishing emails to European government entities, this time using an article taken from the London School of Economics [website](#) titled ‘*It is time for Europe to send “tripwire” troops to Greenland.*’ These emails also contained unique URLs that redirected to this news article if clicked. This was likely included as an additional method of reconnaissance, given many modern email clients and

applications disable external image download by default, diminishing the efficacy of web bugs. Both the web bug and link included in the email used the infrastructure associated with TA416 domain speedifynews[.]com.

 Figure 2



Figure 2: TA416 Greenland-themed web bug phishing email campaign from January 2026.

Delivery: malware campaigns targeting EU diplomatic entities

In late September 2025, Proofpoint observed TA416 conduct multiple malware delivery campaigns targeting European ministries of defense and ministries of foreign affairs. This targeting predominantly focused on individuals assigned to NATO missions and delegations. In one instance, TA416 used a likely compromised account belonging to a European armed forces organization to send the phishing emails. In another, the group used a compromised email address from a Southeast Asian diplomatic entity. Proofpoint has observed TA416 abusing compromised accounts from this same Southeast Asian entity to conduct phishing campaigns on multiple occasions throughout 2025 and 2026. The infection chains observed in these campaigns have been covered extensively in public reporting by [StrikeReady](#) and [Arctic Wolf](#).

 Figure 3



Figure 3: TA416 February 2026 spearphishing email spoofing Icelandic Ministry of Foreign Affairs.

In January and February 2026, TA416 again conducted a series of malware delivery campaigns targeting numerous European government organizations, with later campaigns focusing on targeting individuals or mailboxes associated with diplomatic missions to the EU and Taiwan. Most of these phishing emails were sent via the Gmail accounts `office2000005@gmail[.]com` and `hsuhalingaye26@gmail[.]com` and spoofed various diplomatic entities. A smaller subset was sent via likely compromised accounts associated with the interior ministry of a European country and a Southeast Asian ministry of foreign affairs.

Delivery: post-conflict expansion to Middle East targeting

In mid-March 2026, Proofpoint observed TA416 conduct multiple campaigns targeting government and diplomatic entities within the Middle East. Historically, this region has not been regularly targeted by TA416, and this expansion in targeting was very likely driven by the outbreak of the war in Iran. One campaign conducted on 16 March 2026 used a compromised Syrian Ministry of Foreign Affairs and Expatriates account to send a phishing email concerning energy infrastructure in Iran, which was sent to a wide range of embassies located across multiple Middle Eastern countries.

 Figure 4



Figure 4: TA416 March 2026 spearphishing email using Iranian energy infrastructure lure.

Shifting infection chains: all roads lead to PlugX

The following section examines how TA416's infection chains have evolved over recent months while maintaining core elements of the group's longstanding tradecraft.

 Figure 5



Figure 5: Evolving TA416 infection chain from September 2025 to March 2026.

Some components of TA416's Tactics, Techniques, and Procedures (TTPs) remain consistent after many years. This includes the continued use of compromised diplomatic email accounts, web bug reconnaissance campaigns, and DLL sideloading triads to deploy a custom PlugX variant, all of which align with previous Proofpoint [reporting](#) on this threat actor in 2022. Despite this, TA416 continues to regularly evolve and innovate. The group regularly adapts the early stages of its infection chains and integrates new defense evasion and anti-analysis features into a custom PlugX variant. Between September 2025 and March 2026, Proofpoint observed TA416 employing multiple different initial infection chains that all ultimately lead to this customized PlugX variant.

September 2025 – January 2026: Fake Cloudflare Turnstile challenge pages

Beginning in September 2025, TA416 began employing fake Cloudflare Turnstile challenge pages impersonating login.microsoftonline[.]com hosted on Microsoft Azure Blob Storage sites. Early variations used a real Turnstile widget, which is used to redirect the target to a ZIP archive hosted on the same Microsoft Azure Blob Storage site when the checkbox is clicked and a Turnstile token is returned, though this token is not validated at any point. The user is redirected to a payload URL that is obfuscated within the page source code using character code arrays, as noted in StrikeReady [reporting](#).

 Figure 6



Figure 6: Fake Cloudflare Turnstile challenge landing page used by TA416.

Later variations instead redirected the user from the fake Cloudflare Turnstile challenge page to an attacker-controlled domain, with the returned Turnstile token appended as a URL parameter. This allows the threat actor to validate the Turnstile token server-side to impede automated analysis, before redirecting to a direct download of a ZIP archive, again hosted using Microsoft Azure Blob Storage.

 Figure 7



Figure 7: Redirection logic employed in later variations of fake Cloudflare Turnstile challenge landing page used by TA416.

The downloaded archives in these infection chains all use a [ZIP smuggling](#) technique to hide the next stage file within the ZIP structure. The ZIP files contain a single Microsoft shortcut (LNK) file that runs an embedded PowerShell command to search for the parent ZIP, then carve an MSI or TAR file from the ZIP using either a byte marker or hardcoded offset, and execute either the MSI or a DLL sideloading executable contained within the TAR. In all cases, this leads to a DLL sideloading triad loading PlugX.

While Proofpoint has not observed the use of these fake Cloudflare Turnstile pages in our telemetry since November 2025, submissions to third-party malware repositories in January 2026 suggest the group is continuing to use this technique selectively.

December 2025 – January 2026: Microsoft OAuth redirect abuse

In December 2025, TA416 began abusing third-party Microsoft Entra ID cloud applications to trigger redirects leading to direct downloads of malicious archives. In this infection chain, the group registers a third-party application in Entra ID and configures its redirect URI to point to an attacker-controlled domain hosting the malicious payload. TA416 phishing emails using this technique contain a link to Microsoft's legitimate OAuth authorization endpoint, crafted with parameters that suppress user interaction and force an authorization failure. When clicked, the user is redirected to the application's registered redirect URI, resulting in a direct download of the malicious archive with no user interaction. Proofpoint has previously [reported](#) on similar techniques used to perform redirection, which allow threat actors to bypass URL reputation checks and email security filters by ensuring the initial link points to a trusted Microsoft domain. The inclusion of a trusted Microsoft URL is also more likely to appear legitimate to targeted users.

 Figure 8



Figure 8: Example of Microsoft OAuth redirect technique employed by TA416.

An example of a URL observed in a TA416 phishing email is shown above. In this case, the `client_id` refers to the attacker-controlled third-party application, the scope is set to a nonexistent value (`scope=invalid`) to deliberately trigger an authorization failure, and `prompt=none` is set to suppress user interaction. As the URL does not include a `redirect_uri` value, it defaults to the redirect URI configured on the application registration. This deliberately triggers an `interaction_required` error, and the user is redirected to a predetermined URL where TA416 has staged a direct download of a malicious ZIP archive. Proofpoint observed TA416 using a different state value for each target, likely to allow the use of unique URLs within each email and to easily correlate payload downloads with targets. The downloaded ZIP archives delivered through these infection chains use the same previously described ZIP smuggling technique to load PlugX. Microsoft published a [report](#) in March 2026 on the use of this redirection technique by TA416 and other threat actors.

February 2026: use of MSBuild and C# project files

Beginning in February 2026, Proofpoint observed TA416 adapt its initial infection chain once again in campaigns linking to archives hosted on Google Drive or a compromised SharePoint instance. In this case, the downloaded archives contained a legitimate Microsoft MSBuild executable renamed as a lure filename, alongside a malicious C# project (CSPROJ) file.

 Figure 9



Figure 9: Archive containing renamed MSBuild executable and malicious C# project file.

When the MSBuild executable is run, it searches the current directory for a project file and automatically builds it. In the observed TA416 activity, the CSPROJ file acts as a downloader, decoding three Base64-encoded URLs to fetch a DLL sideloading triad from a TA416-controlled domain, saving them to the user's temp directory, and executing a legitimate executable to load PlugX via the group's typical DLL sideloading chain.

The CSPROJ samples observed by Proofpoint were highly similar, with only the Base64-encoded URLs swapped out. The presence of slightly modified comments before these encoded URL variables within each sample, such as Base64-encoded URLs with separate endpoints and Base64-encoded URLs with new endpoints, suggests that these CSPROJ files may have been created or altered with the assistance of an LLM.

 Figure 10



Figure 10: Excerpt of C# project file showing example of comments preceding Base64-encoded URL variables.

TA416 tweaks PlugX sideloading chain

While the overall DLL sideloading triad delivery mechanism has remained consistent for several years, TA416 regularly changes the PlugX payload loading chain, in particular the DLL loader, payload obfuscation, and sideloading executable used. Between September 2025 and March 2026, Proofpoint observed the following signed executables being abused by TA416 to load PlugX.

Filename	SHA256
cnmpaui.exe	4ed76fa68ef9e1a7705a849d47b3d9dcdf969e332bd5bcb68138579c288a16
steam_monitor.exe	8c0051a83b3611ff2b669b670aa005633f3d9e844454a112b31d2a4bc944a2
ABRemove.exe	6b363e0f16fc5a612bd98631e7cdc4f68a95329e92c21ef0495c9117b8b8f36
Avk.exe	8421e7995778faf1f2a902fb2c51d85ae39481f443b7b3186068d5c33c472d9
ErsChk.exe	bc8b022c10bcab39da302446b0a50988de94607c7e724f2051578e8ed2f8b
CNMNSST2.exe	53086e3b557a1d21cf7f4ffc73d92c39b08872334a8cdb09dda0a06bd060cfe

Figure 11: Signed executables vulnerable to DLL sideloading abused by TA416 between September 2025 – March 2026.

In the latest observed variants in March 2026, TA416 used a signed Canon executable CNMNSST.exe to sideload a malicious loader DLL named CNCLID.dll. The loader DLL uses DJB2 API hashing to dynamically resolve Windows API functions and execute a payload file Canon.dat as shellcode, which decodes the PlugX payload. The loader and payload code and data are obfuscated using techniques such as API hashing, junk code, and control-flow flattening. For persistence, the DLL sideloading triad is copied to the directory C:\Users\Public\Canon and a Run registry key Canon is created to run CNMNSST.exe upon startup.

Overview and updates in C&C protocol

The PlugX payload establishes C&C communications over HTTP using an RC4-encrypted binary protocol. Prior to initiating network activity, the malware performs several initialization steps to generate host identifiers and applies anti-analysis checks.

The client initiates communication to the C&C server by sending an HTTP GET request. The server responds with application/octet-stream data that serves as the RC4 encryption key for the subsequent exchange. The client creates a SYSINFO structure containing information on the infected host; RC4 encrypts it using the key received in the previous step; and sends it to the server inside an HTTP POST request body. The SYSINFO structure is as follows:

Field	Description
is64bit	Whether the host runs a 64-bit OS
dwMajorVersion	OS major version
dwMinorVersion	OS minor version
dwBuildNumber	OS build number
wServicePackMajor	Service pack major version
wServicePackMinor	Service pack minor version
wSuiteMask	OS suite mask
user_name	Current username
computer_name	Computer name
id	Campaign/victim identifier
ip_address	Host IP address

Figure 12: PlugX SYSINFO system reconnaissance structure.

The server then replies with RC4 encrypted data that contains the command and its parameters. Currently, the following list of commands are available:

Command	Description
0x00000002	Outgoing system information beacon (SYSINFO structure)
0x00001005	Uninstall — deletes autorun registry keys and drops a self-delete batch file
0x00001007	Adjusts reconnect_interval and connection_timeout parameters
0x00003004	Downloads a new payload set (EXE, DLL, DAT) and executes the sideloading binary
0x00007002	Opens a reverse command shell

Figure 13: List of available PlugX commands.

In older variations seen prior to December 2025, the C&C HTTP requests include four custom headers that mimic the Fetch metadata specification:

Sec-Fetch-Dest: <random_string>

If-None-Match: <system_token>

Sec-Fetch-Site: none

Sec-Fetch-Mode: cors

The If-None-Match header carries a host-generated hex token, while the Sec-Fetch-Dest value is randomized per request. In this older C&C protocol, the HTTP URI used the following predictable pattern:

- A base endpoint selected randomly from a fixed set:
- /upload
- /download
- /developer
- /help/?
- /api/v1/resource
- /user/profile
- /settings

- /i/bookmark
- A timestamp parameter appended: ?t=<unix_timestamp>
- A variable number of randomly generated key-value pairs

This led to URI values such as /api/v1/resource?

t=1760970011&1Tr=askZVyeahfE00bt4&d9=e8cAQ4T&vE8=uUIMYYuJ&S=zMLY3z.

 Figure 14



Figure 14: Older PlugX variant HTTP C&C traffic.

In the updated variants first seen in December 2025, the group updated this C&C protocol, likely to evade network-based detections. In the new variation, the Sec-Fetch-Dest, If-None-Match, Sec-Fetch-Site, and Sec-Fetch-Mode custom headers are no longer sent. Instead, a 16-character host token is embedded within a Cookie header, surrounded by randomly generated cookie key-value pairs. Additionally, the use of hardcoded base URI endpoints is removed, with the full URI path now randomly generated.

 Figure 15



Figure 15: Newer PlugX variant HTTP C&C traffic.

Updates in config encryption

The PlugX payload C&C parameters (C&C domains or IP addresses, campaign identifiers, mutex names, install paths, and decoy document metadata) are stored in an embedded configuration blob that is RC4-encrypted. The encryption scheme and internal structure of this configuration have evolved in more recent variations such as those seen in February 2026, with the newer variant introducing additional hardening to the configuration encryption and now employing two layers of obfuscation. After RC4 decryption of the outer blob, individual string fields such as C&C domains, mutex names, and campaign identifiers are then independently decoded using a rolling XOR.

Variable	Value
RC4 key	anMgFtsFCvA
Decoy Size	41671
Decoy Filename	Meeting invitation.pdf
Mutex Name	dGcEuQhKT
Campaign ID	msbuild

Install Directory	%public%\GData
Decoy Directory	%temp%
C&C	ombut[.]com:443, ombut[.]com:443, ombut[.]com:443

Figure 16: Example of decrypted PlugX configuration from February 2026 campaign.

Infrastructure analysis

In recent years, TA416 has shifted its infrastructure procurement TTPs and now almost exclusively uses a steady supply of re-registered, formerly legitimate domains for C&C, malware delivery, and web bugs, often first using domains within days after re-registering them. This tactic of purchasing previously legitimately used domains is likely an effort to evade domain reputation-based heuristics. The group typically also uses the Cloudflare Content Delivery Network (CDN) to obscure backend hosting IP addresses used for malware delivery and C&C.

 Figure 17



Figure 17: Timeline of TA416 C&C domain first sightings (July 2025-March 2026).

TA416 has heavily favored use of the virtual private server (VPS) providers Evoxt Enterprise (AS149440), XNNET LLC (AS6134), and Kaopu Cloud HK Limited (AS138915) throughout 2025 and 2026. The group also typically deploys minimal fake websites on its C&C domains, likely to hinder signaturing and tracking efforts and to make these domains appear legitimate.

 Figure 18



Figure 18: Example of fake websites hosted on TA416 C&C domains (example shown is ombut[.]com).

Attribution – what even is Mustang Panda anyway?

In recent years, the Mustang Panda moniker within public threat intelligence reporting has become increasingly opaque and difficult to disentangle. Generally, Proofpoint tracks what is commonly publicly referred to as Mustang Panda under two primary clusters: TA416 (covered within this report) and a second group tracked under the temporary designator UNK_SteadySplit.

Within Proofpoint’s visibility, UNK_SteadySplit has been active since at least 2022, with related open-source activity dating back to at least 2019. UNK_SteadySplit is a user of the custom TONESHELL and PUBLOAD malware families, alongside multiple other first-stage malware families delivered in phishing campaigns. Since the beginning of 2025, Proofpoint has predominantly observed UNK_SteadySplit targeting government, hospitality, and technology organizations in South and Southeast Asia, with a particular focus on Myanmar and Thailand. Within Proofpoint's telemetry, the group exclusively uses freemail senders and typically employs much more simplistic infection chains than TA416, most often delivering an archive containing a DLL sideloading pair downloaded from a cloud storage service. The table below highlights some of the key similarities and differences between the two clusters, as observed within Proofpoint’s visibility.

	TA416	UNK_SteadySplit
--	-------	-----------------

Targeting	• European government and diplomatic entities • Southeast Asian and Mongolian government and healthcare organizations • Five Poisons targeting	Government, insurance, hospitality, technology, and energy organizations in South and Southeast Asia
Capabilities	• Customized PlugX variant • Heavy obfuscation and use of control flow flattening	• PUBLOAD • TONESHELL • Various custom first stage loaders • Minimal obfuscation • Regular inclusion of Easter egg strings and recurring PDB path patterns • Recurring use of FakeTLS C&C protocols
Infection Chain	• Use of both freemail and compromised government sender email addresses • Varied infection chains, including use of: • MSC files • HTA files • LNK files with Zip Smuggling • Fake Cloudflare Turnstile challenge pages • CSPROJ files • Microsoft OAuth redirection abuse • DLL sideloading triads • Updates DLL sideloading executable every 1-2 months	• Exclusive use of freemail sender email addresses • Archive download from cloud hosting site (e.g. Google Drive) • Archive typically contains a DLL sideloading pair with lure filename • More frequent rotation of DLL sideloading executable than TA416, with minimal overlap in sideloading executables
Infrastructure	• Mostly uses domains for C&C • Heavy usage of Cloudflare CDN • Re-registers former legitimate domains • Favors Evoxt Enterprise (AS149440), XNNET LLC (AS6134), and Kaopu Cloud HK Limited (AS138915)	• Mostly uses raw IP addresses for C&C • Varied hosting providers, no overlaps in providers favored by TA416

Lure themes	• Geopolitical events and diplomatic communications • Meeting invitations • Conference invitations	• Geopolitical events and diplomatic communications • Fake job promotions • Hotel room bookings • Hotel association and lifestyle benefits offers • Meeting minutes and notes
--------------------	--	---

Figure 19: Similarities and differences between TA416 and UNK_SteadySplit clusters.

As noted in previous [reporting](#) by Trend Micro in 2022, there are historical technical overlaps between TA416 and UNK_SteadySplit activity, most directly via the presence of a UNK_SteadySplit TONESHELL C&C IP address within a filepath seen in two LNK files used in TA416 campaigns. It is therefore likely that some form of organizational, personnel, or hierarchical link exists or existed between TA416 and UNK_SteadySplit. However, currently Proofpoint is unable to assess the nature of this relationship, and we have not observed similar overlaps in recent years. From Proofpoint’s perspective, both clusters appear operationally distinct and use different tooling, TTPs, and infrastructure to conduct different targeting.

Based on an analysis of public research and discussions with industry partners, Proofpoint believes the following most accurately reflects the clustering overlaps between TA416, UNK_SteadySplit, and related groups tracked by other vendors:

TA416	UNK_SteadySplit	TA416 and UNK_SteadySplit combined
--------------	------------------------	---

Figure 20: Overlaps between TA416, UNK_SteadySplit, and related groups tracked by other vendors.

Conclusion

TA416's shift back to European government targeting in mid-2025, following two years of focus on Southeast Asia and Mongolia, is consistent with a renewed intelligence-collection focus against EU and NATO-affiliated diplomacy entities. In addition, TA416's expansion to Middle Eastern government targeting in March 2026 further highlights how the group’s tasking prioritization is likely influenced by geopolitical flashpoints and escalations. Throughout this period, the group has shown a willingness to iterate on infection chains, cycling through using fake Cloudflare Turnstile pages, OAuth redirect abuse, and MSBuild-based delivery, while continuing to update its customized PlugX backdoor.

These TA416 operations suggest the group will likely continue to prioritize targeting European diplomatic networks and, as the conflict continues, Middle Eastern diplomatic entities, while maintaining parallel activity across Southeast Asia. Organizations in scope for this targeting

should expect continued experimentation with initial access vectors delivered via spearphishing campaigns alongside continually updated PlugX payloads.

ET rules

- [2068412 - ET MALWARE TA416 PlugX CnC Activity \(GET\)](#)
- [2068413 - ET MALWARE TA416 PlugX CnC Activity \(GET\)](#)
- [2068414 - ET MALWARE TA416 PlugX CnC Activity \(POST\)](#)

Indicators

Note: indicators encompass a range of TA416 activity observed since July 2025, not just campaigns targeting European government.

Indicator
cnrelojes[.]com
hnk-capljina[.]com
harrietmwelch[.]com
theprmummy[.]com
ecolnomy[.]com
mettayoga[.]org
it-evenement[.]nl
welnetsanda[.]org

thecamco[.]net

paquimetro[.]net

fuyuju[.]com

nvofficespace[.]com

premegalithic[.]com

phpthemes[.]net

supplementsoftheyear[.]com

colorflee[.]org

atravelingwitch[.]com

napasbdc[.]org

buzzurro[.]net

racineupci[.]org

cubukluescort[.]com

cseconline[.]org

ecomputers[.]org

designehair[.]com

loumuenz[.]com

ronnybush[.]net

hayabusamt[.]com

rondabusco[.]com

doorforum[.]com

portabalbufe[.]com

papermoonweddings[.]com

hoplitellc[.]com

mongolianews[.]info

devredin[.]com

famisu[.]com

espacebus[.]com

dnzapping[.]com

buddhismnewsdaily[.]org

buywownow[.]com

goodmedsx[.]com

anbusivam[.]com

phbusiness[.]net

bobbush[.]org

majicbus[.]org

busopps[.]org

turileco[.]net

basecampbox[.]com

adimagemarketing[.]com

ecoafrique[.]net

speedifynews[.]com

creatday[.]com

fruitbrat[.]com

dalerocks[.]com

aatile[.]com

ombut[.]com

gestationsdiabetes[.]com

gynecocuk[.]net

decoraat[.]net

embwishes[.]com

carhirechicago[.]com

ytsonline[.]net

coastallasercompany[.]com

shalomrav[.]org

rhonline[.]net

winesnmore[.]net

alpinemfg[.]net

amblecote[.]net

stuypa[.]org

buscacnpj[.]org

subbusiness[.]org

florarevival[.]com

bushidomma[.]net

devlyrics[.]com

softhunts[.]com
gesecole[.]net
meritsoftwebportals[.]com
foxmediagency[.]com
ghonline[.]net
hxxps://mydownload.z29.web.core.windows[.]net/nv2199_update_on_situation_of_cambodia-thai
hxxps://mydownload.z29.web.core.windows[.]net/nv2230_update_of_situation_on_cambodia-thai
hxxps://mydownload.z29.web.core.windows[.]net/naju_plan_obuka_oktobar_2025.html
hxxps://mydownload.z29.web.core.windows[.]net/epc_invitation_letter_copenhagen_1-2_october_
hxxps://mydownloadfile.z7.web.core.windows[.]net/jatec_workshop_on_wartime_defence_procur
hxxps://mydownfile.z11.web.core.windows[.]net/agenda_meeting_26_sep_brussels.html
hxxps://filesdownld.z13.web.core.windows[.]net/a9t3zb7l1qx5.html
hxxps://filestoretome.z23.web.core.windows[.]net/filelocate.html

hxxps://attd.z23.web.core.windows[.]net/attd.html
hxxps://gooledives.z48.web.core.windows[.]net/election_2026.html
hxxps://gooledives.z48.web.core.windows[.]net/%e0%a6%a8%e0%a6%bf%e0%a6%b0%e0%a7'
mydownload.z29.web.core.windows[.]net
mydownloadfile.z7.web.core.windows[.]net
mydownfile.z11.web.core.windows[.]net
filesdownld.z13.web.core.windows[.]net
attd.z23.web.core.windows[.]net
filestoretome.z23.web.core.windows[.]net
gooledives.z48.web.core.windows[.]net
reloadsite.z13.web.core.windows[.]net
hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?client_id=607bb911-0f5a-4180
hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?client_id=5e6b7cf5-69b7-4f85

hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?client_id=8d015a9c-f912-4450
hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?client_id=684d7892-c993-41d
hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?client_id=a9785a2d-445e-4ffa
hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?state=149&x_client_ver=1.0.0 c39b958e5743&nonce=ab93f2c1&prompt=none&scope=invalid&ui_locales=en-us
hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?state=6&x_client_ver=1.0.0&r 7a7aa08f4bb2&nonce=ab93f2c1&prompt=none&scope=invalid&ui_locales=en-us
hxxps://login.windows[.]net/common/oauth2/v2.0/authorize?client_id=7d980c52-31e5-4554-9e20-
hxxps://login.microsoftonline[.]com/common/oauth2/v2.0/authorize?utm_source=portal&utm_med c1fe4c86f073&response_type=code&scope=invalid&prompt=none&utm_campaign=login&state=c
hxxps://web.florarevival[.]com:443/download/a6d6u9ff13?error=interaction_required&error_descri
hxxps://www.bushidomma[.]net/download/l7o9afe?error=interaction_required&error_description=s
hxxps://www.buscacnpj[.]org/download/we7823bn?error=interaction_required&error_description=
hxxps://www.subbusiness[.]org/download/aetce17ge?error=interaction_required&error_description
hxxps://www.foxmediagency[.]com/download/qqa36sa0d6fq066?error=interaction_required&error
hxxps://dash.ghonline[.]net:443/download/jyebbtg?error=interaction_required&error_description=s

607bb911-0f5a-4186-9d48-ecff8e094280
5e6b7cf5-69b7-4f85-87d1-8b4cb6df8aa2
8d015a9c-f912-445d-8b3c-4f3b3201ded1
684d7892-c993-41d7-b6c1-07613c43cd61
a9785a2d-445e-4ffa-a770-bec734911841
3c7bf1a4-927f-40a1-97b0-7a7aa08f4bb2
b004ab26-f57b-439d-ae54-c39b958e5743
7d980c52-31e5-4554-9e20-b89c4617102f
c47683e4-16a3-4b8a-a3d3-c1fe4c86f073
262a1003a2cd04993b29e687686eba573d6202fea8611c437ecbd6312802677a
7c96d08f5ce46d1a857184490a7e68ca2b02e9cbe9d188742f184f21bc9c62d9
ae8d2cef8eac099f892e37cc50825d329459baa9625b71fb6f4b7e8f33c6ccce
36e516182b4c8aa48ea3e50b7dc353f32d3412f59fb0cb1c7b3590aa4d821c57

30475ff5b32776e554433ff00e7c18590253521024662c267abaefd24f1b9bbe
28a8bdaee803d9cf9186ff4756e15b0fb491fd3b65bde002361615f27e5ca92d
c96338533d0ab4de8201ce1f793e9ea18d30c6179daf1e312e0f01aff8f50415
56f0247049be8b9dc1da7c55957d2fb4f7177965ba62789c512f3e2b4c0c5c26
e036e2ba402d808adbb7982ec8d7a207849ff40456633b2b372bc7916d9dc22f
e1e597852d684bd6d0395d5094e58831f13635f668e7cf66ba71b8b66be0ce6c
795ad4789a185c3abc35b3ad82117db6b60a7b8ab857e41080873f070d4a06f0
79e0ab17e761a00ad12b9848f1f07b507f57db532fa2df8c722693e14feb17c3
784a914bd1878ad68a6cf3f693da5ddcc2f04b794204333098ad749b7e372fd4
e31eafb49dbcad079ff177703b5a033f3e0365991cf28492339eccfe0fdf812c
2c3708a103b257fa75fcb34948c817fd564d4479f1e267b33c5b08f0d4c7634f
e9d8f28fd0aef3bc3f5b28a41b3f342165b371db9aefd7d03f2aba4292009d3e
50746ddd81a5dbc5cec793209ab552125fff9c7184aa5bcfe22d6c3b267f67f1

d0576b39bb6c05ea0a24d3a3d5d7cb234454fefc65860f21a97757582adc7650
84d6a8b47edadf5725d9937d8928a90d190e0c98b5b4d1a4c58e97cddcd36768
f988d58e4a32b908ff7a557d740c6860c59807832c7626774330dcaed65ead14
31f3606433e95bfbb047d31c885e56a70111e130f3d2da0580644c01323b46d1
29cd44aa2a51a200d82cca578d97dc13241bc906ea6a33b132c6ca567dc8f3ad
7d2b6c48cbd6cef05ea2bdae7dfc001504ccdda99dd89eb7fe6646e96c1d5515
3e7478d3854eaeed487230ba9299c87d5a5d70e4fbeac841555327c76b7b405e
c8a6302adf92353556c600a0afa9146fbc04663fffe8be90808df2bf04ec5703
de8ddc2451fb1305d76ab20661725d11c77625aeaa1447faf3fbf56706c87f1
f333bc5238e39790fb7560de067a852e9a99df2bb783cf08738d8a0d424b9658
06a70c54c580ec4c362bfbc94147a0f1ac9020c421933ccf494a8d553b114260
46314092c8d00ab93cbbdc824b9fc39dec9303169163b9625bae3b1717d70ebc
e7ed0cd4115f3ff35c38d36cc50c6a13eba2d845554439a36108789cd1e05b17

a3f9e20315663e4e8feb13e77563e3cb0f2f4844734987e51e14bd172b9a04fd
5c3208c5217933e16c5119e7baf78f85fd409e8822d1cd7a8ef2d52a5bd511c1
42c3b9cad6c8383699eba4f82d51908c0d61e9ea454bc40447cf20475ce20ff0
64bae6a215ad9e956d1028603438228003d832bdd5e586ad4988f5c7ad1c54f0
843b22df66f87a587be77145da163f9615fe8164a5ea17f9e33562ff43894fbf
eb10443a2f0b9a25d01a84426a6a8532b0e7c9157abda55b94c98a1fd2d45562
b1606ca49aa15eadb039f33d438697973b203693d0003e467e1f33b36d10a530
87929c8f53341a5e413950d33c7946c64e1d4b2eba6d1a8b2d08ef56f7065052
6788365386ccd34d1db681c61ef07ef4d2faea5672571b77a76dc48f327afaa9
2712f4ac5ad422bcf749699389cb1a0111a1b11e298efb0cffeabc2e2f0becb5f
4d528842c7fe73681dfe569d38a39f8d38ca5548dbc8b6ac02df096713a92efd
45d8d4f04eb44dc5d10290038825194b0ffc38048a786b4a8b81bb796afc58a3
a82c8845587a87010eab52ef8c35d45eaea8eb8102aae77ec96e222197b7db66

16e258b7b712b747a6037d56ee8d2cc99f8f8139da4a3a59c24af0887531ace0
29a70241660ff3234f1c5e8c01878ee01adb4a289262bd37403e1a323129ea86
c73050860c8aaa0f79c03781519cdcee133832805e2e3e778fef3cb0e917efb1
9d61c4e21bbbddde5bb780ea0c5238a3538a84b9afe98d62d08845b47fb5caa9
b394e7a3b350b2104b73e29a04e48e5ede5078b9a811abae58d842ce3442c6b3
0b916d2b4a02d01b42c2b04e281d786a05cc7974d2c4a272b01e8060fa713403
965894996e2cb9be1e0ccc509e079e7eca072cbc4e68945beb00ff5979dda19c
69b685fadce4f34bc4964b3d78d43694a428ae1ee4d2fe0ce4ed26fad07847fa
30c71d644bc72e0d55d46bed753ab3f72dc77b7f1be0e34693c957939a779507
e79d19d68d307c12413f8549aafa4a56776002dd04601e36e0125b2e6d56ff94
44cfba85aa27265779b01f6eb8b69718462b1ca8078b21066061e8d1622dff7a
774841a2bfb07b61a8be3de8ae31e9847f987de652eef179761dc3d1b34c42ff
3c065947461df428b0d29e401e2a28a0d2560943e96d3ac8b9ed71858fbceec38

7be77e6166aae9a89b16b64b593f35afc7424926047635f2230a4e364c6a46d8
b6d866054dedf7a882dd1fa405a066de1278e35acf639b3a0e850a637d27c4bc
9e67f72bfbc8772ce10633430e1277fd8374e99877ddedb598b4f6717c799eeb
de13e4b4368fbe8030622f747aed107d5f6c5fec6e11c31060821a12ed2d6ccd
a95e3857e2f32c2a9c23accadebc1ad6aabf73fed9d63c792d69122d9ec6726d
3021f4d365a641722748c5e60d983a080db17bef8f0a1dbe624ffe63cd544cc1
c5267fefaac1764eba5f42681eb216f146b7d18fcbf546275d33e70cb36fdfba
bcd30f2116f5ba6731c628483d597b2ba3620ed464c63875855906306beb102a
1df74ce45aa9320c48858eddce3f46f5687fbfdcf497d92a1e17476e7a2951e
93e9402af72b355554f9ba93c64871b1bae5be498e3b8a10e61ebdd10ab0d050
2261c7640fe2f3c2385de61c546b5020ec8a486ad5bad64c31bc9268f6b36a2c
kordula.wehrli@gmail[.]com
kayden.beaufort@gmail[.]com

emmeline.voss@gmail[.]com

epc.copenhagen2025.dm@gmail[.]com

galinaburl76@gmail[.]com

office2000005@gmail[.]com

hsuhalingaye26@gmail[.]com