What’s in an ASP? Creative Phishing Attack on Prominent Academics and Critics of Russia

By Google Threat Intelligence Group

Published: 2025-06-18 · Archived: 2026-04-05 16:20:25 UTC

Written by: Gabby Roncone, Wesley Shields

UPDATE (July 10)

In late June 2025, Google Threat Intelligence Group (GTIG) discovered continued UNC6293 operations that demonstrate an evolution in the group’s tradecraft. Using similar lure themes as previously observed activity, UNC6293 continued the ASP phishing campaign against prominent academics, critics of Russia, and journalists using different ASP names, potentially as a response to our publication of their tradecraft. In a different campaign, UNC6293 sought to convince targets to link an attacker-controlled device to their Microsoft 365 account through Microsoft’s device code authentication flow.

In an attempt to continue the ASP campaign, UNC6293 attempted to re-establish contact with specific individuals that had previously engaged with the initial phishing attempts. GTIG observed UNC6293 creating multiple new accounts with similar usernames to ones used previously and already disabled. UNC6293 also used different ASP names in this continuation wave of the campaign. Due to the engagement with their initial campaign, UNC6293 demonstrated a desire to keep the ruse of being State Department employees alive and re-engage with specific individual targets from the previous campaign.

UNC6293 also began to send tailored invitations to virtual meetings through calendar invites. These invitations included links to Zoom and Google Meet as well as a Microsoft authentication URL for an attacker controlled application.

```
 https://login.microsoft[.]com/<redacted>/oauth2/authorize?client_id=
fc45d3d0-d870-4c83-b3f7-08ebca61d3a0&prompt=
none&response_mode=form_post
```

Clicking the Microsoft authentication URL starts a redirect chain that includes an actor-controlled domain:

```
 https://rediruri[.]app/<redacted>
```

The attacker-controlled URL is only visible in the browser for a short period of time before it redirects the target to a Microsoft 365 authentication page (Figure 4).

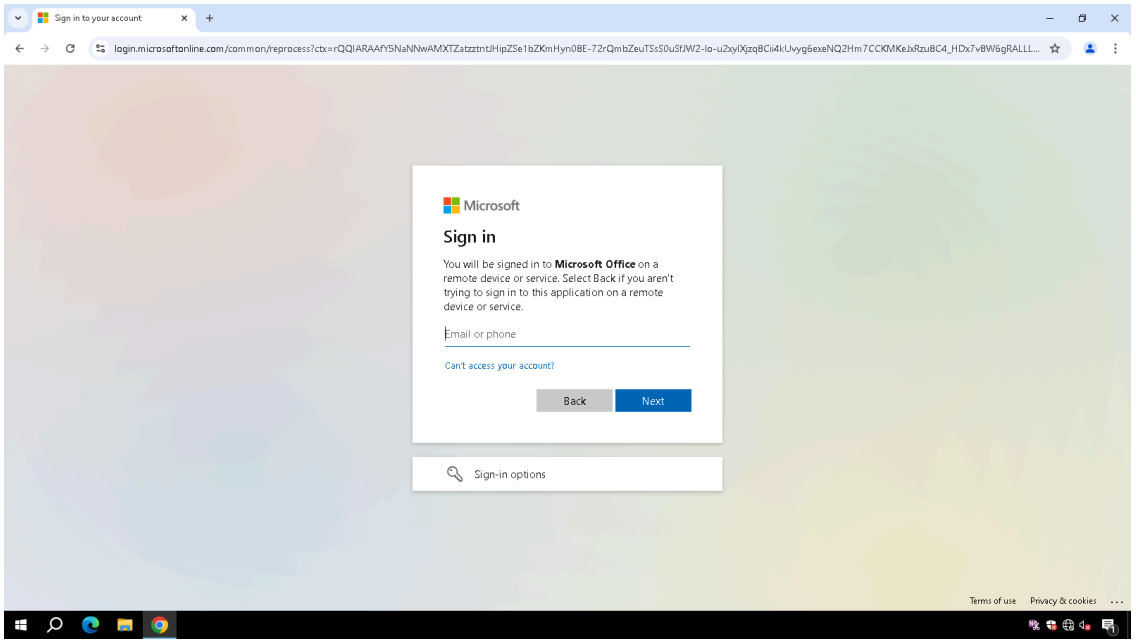


Figure 4: Microsoft 365 authentication page after redirect

Given the demonstrated patience, persistence and creativity of this threat actor, GTIG strongly recommends following the mitigations outlined in the initial version of this blog post to protect against any further ASP phishing campaigns from UNC6293 or other threat actors. Social engineering attacks abusing legitimate authentication features are difficult to defend against; as a result, we suggest individuals who may be targeted by this group use Google's enhanced security resources such as the Advanced Protection Program (APP).

Introduction

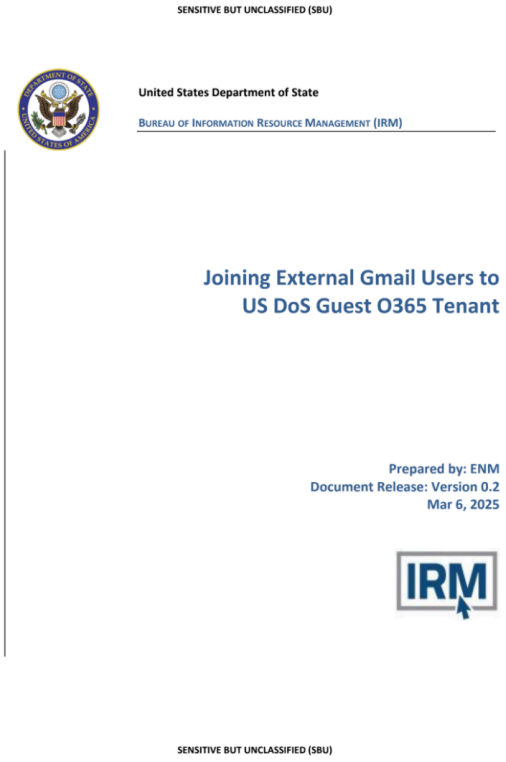
In cooperation with external partners, Google Threat Intelligence Group (GTIG) observed a Russia state-sponsored cyber threat actor impersonating the U.S. Department of State. From at least April through early June 2025, this actor targeted prominent academics and critics of Russia, often using extensive rapport building and tailored lures to convince the target to set up application specific passwords (ASPs). Once the target shares the ASP passcode, the attackers establish persistent access to the victim's mailbox. Two distinct campaigns are detailed in this post. This activity aligns with Citizen Lab's recent research on social engineering attacks against ASPs, another useful resource for high risk users.

GTIG tracks this activity as UNC6293, a likely Russia state-sponsored cyber actor we assess with low confidence is associated with APT29 / ICECAP. After establishing rapport, the attacker sent phishing lures disguised as meeting invitations, and added spoofed Department of State email addresses on the cc line of the initial outreach to increase the legitimacy of the contact attempt. The initial phishing email itself is not directly malicious, but encourages the victim to respond to set up a meeting.

---------- Forwarded message ---------
From: **Keir Giles** <keir.giles@conflictstudies.org.uk>
Date: Tue, Jun 3, 2025 at 11:44 PM
Subject: Re: Private Online Conversation Request
To: Weber Claudie S <WeberCS@state.gov>
Cc: Keir Giles <keir.giles@gmail.com>, Claudie S Weber <claudie.s.weber@gmail.com>, Schumm Leon <SchummL@state.gov>, Cailler Elliot T <CaillerET@state.gov>, Gonzalez Bénigne <GonzalezB@state.gov>

Figure 1: Keir Giles, a prominent British researcher on Russia, posted this screenshot of an email header with fake U.S. Department of State emails that was part of a UNC6293 campaign

Targets who responded received an email with a benign PDF lure attached. The State Department themed lure is customized to the target and contains instructions to securely access a fake Department of State cloud environment. This included directing victims to go to `https://account.google.com` and create an Application Specific Password (ASP) or "app passwords." ASPs are randomly generated 16-character passcodes that allow third-party applications to access your Google Account, intended for applications and devices that do not support features like 2-step verification (2SV). To use an ASP you must set it up and provide a name for the application.


SENSITIVE BUT UNCLASSIFIED (SBU)

United States Department of State

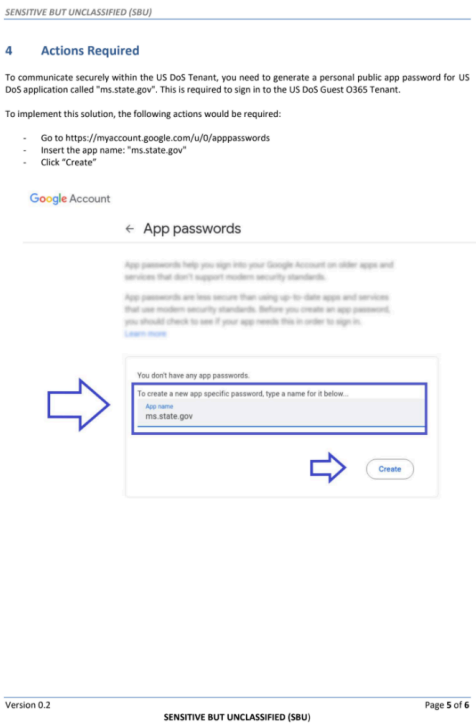
Bureau of Information Resource Management (IRM)

Joining External Gmail Users to US DoS Guest O365 Tenant

Prepared by: ENM
Document Release: Version 0.2
Mar 6, 2025

IRM

SENSITIVE BUT UNCLASSIFIED (SBU)


SENSITIVE BUT UNCLASSIFIED (SBU)

4 Actions Required

To communicate securely within the US DoS Tenant, you need to generate a personal public app password for US DoS application called "ms.state.gov". This is required to sign in to the US DoS Guest O365 Tenant.

To implement this solution, the following actions would be required:

- Go to https://myaccount.google.com/u/0/apppasswords
- Insert the app name: "ms.state.gov"
- Click "Create"

Google Account

← App passwords

You don't have any app passwords.

To create a new app specific password, type a name for it below...

App name

ms.state.gov

Create

Version 0.2 Page 5 of 6

SENSITIVE BUT UNCLASSIFIED (SBU)

In campaign one, the ASP name suggested in the lure PDF was "ms.state.gov" and in campaign two, we observed a Ukrainian and Microsoft themed ASP name. After creating the ASP, the attackers directed the target to send them the 16-character code. The attackers then set up a mail client to use the ASP, likely with the end goal of

accessing and reading the victim's email correspondence. This method also allows the attackers to have persistent access to accounts.

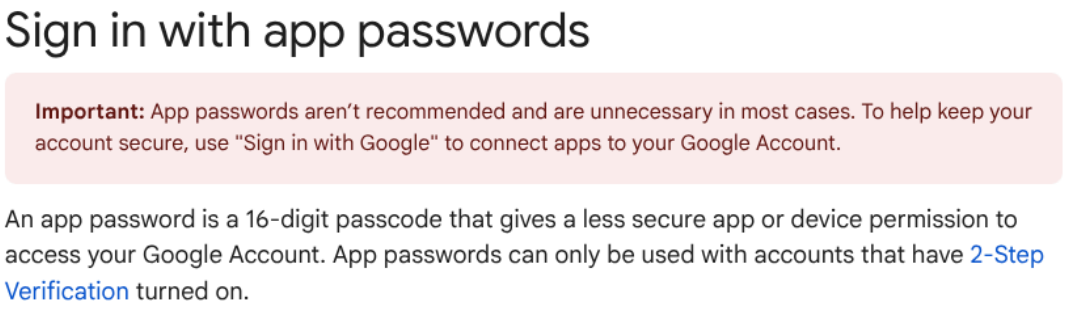
Campaign	Sender Theme	ASP Name	Attacker Infrastructure Used
Campaign 1	State Department	ms.state.gov	91.190.191.117 - Residential proxy
Campaign 2	Unknown	Ukrainian and Microsoft-themed ASP	91.190.191.117 - Residential proxy

Attackers logged into victim accounts primarily using residential proxies and VPS servers, in some cases re-using infrastructure to access different victim or attacker accounts. As a result, we were able to connect the two distinct campaigns we observed to the same cluster. We have re-secured the Gmail accounts compromised by these campaigns.

Mitigations

GTIG is committed to our mission of understanding and countering advanced threats. We use the results of our research to ensure that Google's products are secure and to protect our users and enterprise customers.

Users have complete control over their ASPs and may create or revoke them on demand. Upon creation, Google sends a notification to the corresponding account Gmail, recovery email address, and any device signed in with that Google account to ensure the user intended to enable this form of authentication.



Google provides enhanced security resources such as the Advanced Protection Program (APP), intended for individuals at high risk of targeted attacks and exposure to other serious threats. Opting to use the APP prevents an account from creating an ASP due to the program's heightened security requirements.

We are committed to sharing our findings with the security community and with companies and individuals that may have been targeted by these activities, and we hope that improved understanding of tactics and techniques will enhance threat hunting capabilities and lead to stronger user protections across the industry.

Lure PDF Document

SHA256: 329fda9939930e504f47d30834d769b30ebeaced7d73f3c1aadd0e48320d6b39

Posted in

- Threat Intelligence

Source: https://cloud.google.com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia