TA2552's O365 Third-Party Access Abuse | Proofpoint US

By September 29, 2020 The Proofpoint Threat Research Team

Published: 2020-09-29 · Archived: 2026-04-05 12:37:03 UTC

Since January 2020, Proofpoint researchers have tracked an actor abusing Microsoft Office 365 (O365) third-party application (3PA) access, with suspected activity dating back to August 2019. The actor, known as TA2552, uses well-crafted Spanish language lures that leverage a narrow range of themes and brands. The lures entice users to click a link in the message, taking them to the legitimate Microsoft third-party apps consent page. There they are prompted to grant a third-party application read-only user permissions to their O365 account via OAuth2 or other token-based authorization methods. TA2552 seeks access to specific account resources like the user's contacts and mail. Requesting read-only permissions for such account resources could be used to conduct account reconnaissance, silently steal data, or to intercept password reset messages from other accounts such as those at financial institutions. While organizations with global presence have received messages from this group, they appear to choose recipients who are likely Spanish speakers.

Attack Technique Overview

The campaigns from TA2552 follow a similar attack flow. Upon clicking the link in the message, the recipient is redirected to the authentic Microsoft third-party application consent page at login.microsoftonline.com and asked to grant or deny the requested permissions. If the browser is not already authenticated to O365, the user is prompted to authenticate. If consent is granted, the third-party application will be allowed to access the currently authenticated O365 account. The list of permissions we have observed in these campaigns allows read-only access to items such as the user's contacts, profile, and mail. Even if consent is denied, the browser is still redirected to an attacker-controlled page, giving the actor the opportunity to present more attack techniques to the visitor.

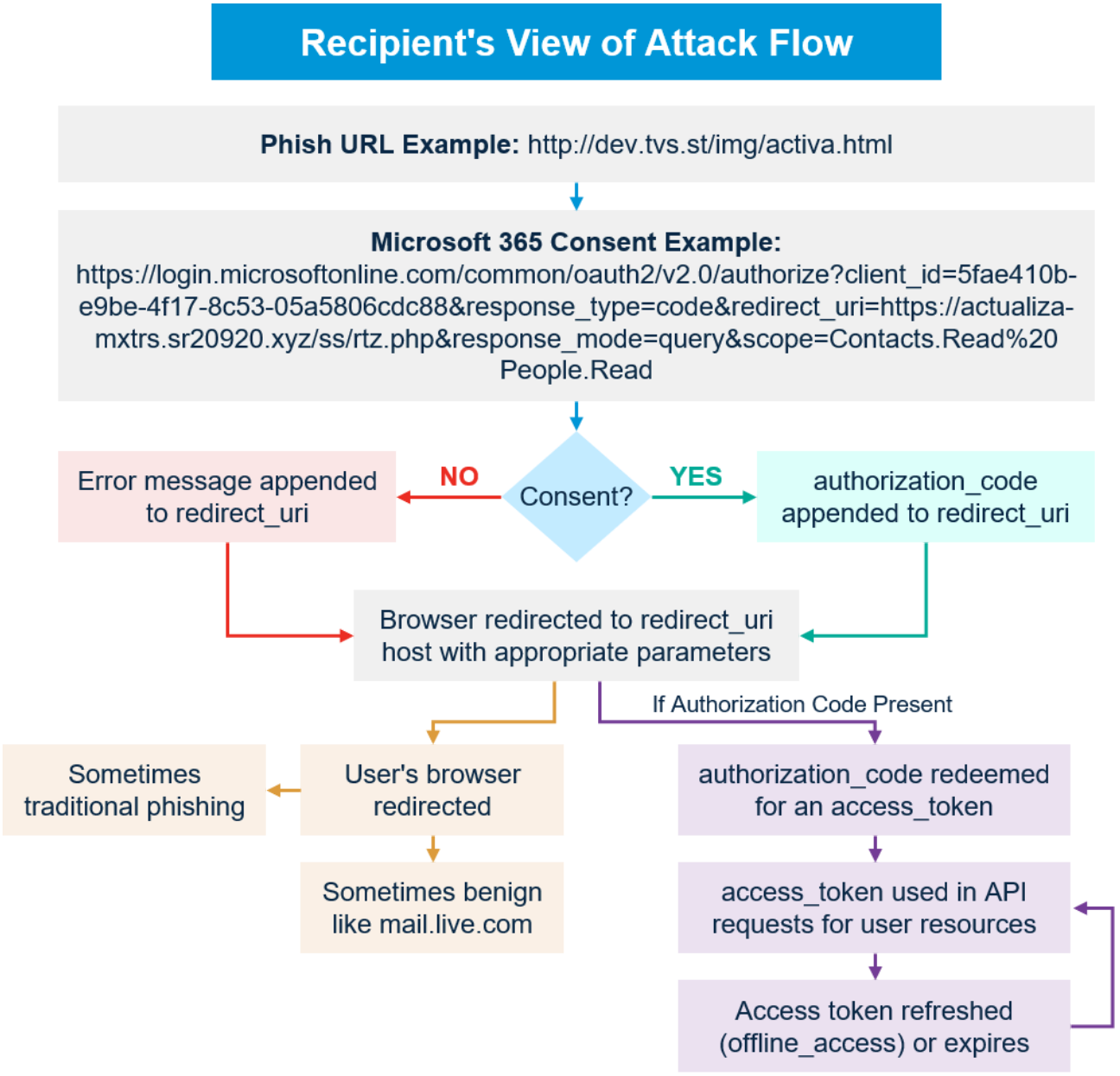

Figure 1: Overview of attack flow

The consent URL used during the OAuth authorization flow has a predictable structure. Values of interest are indicated in Figure 2.

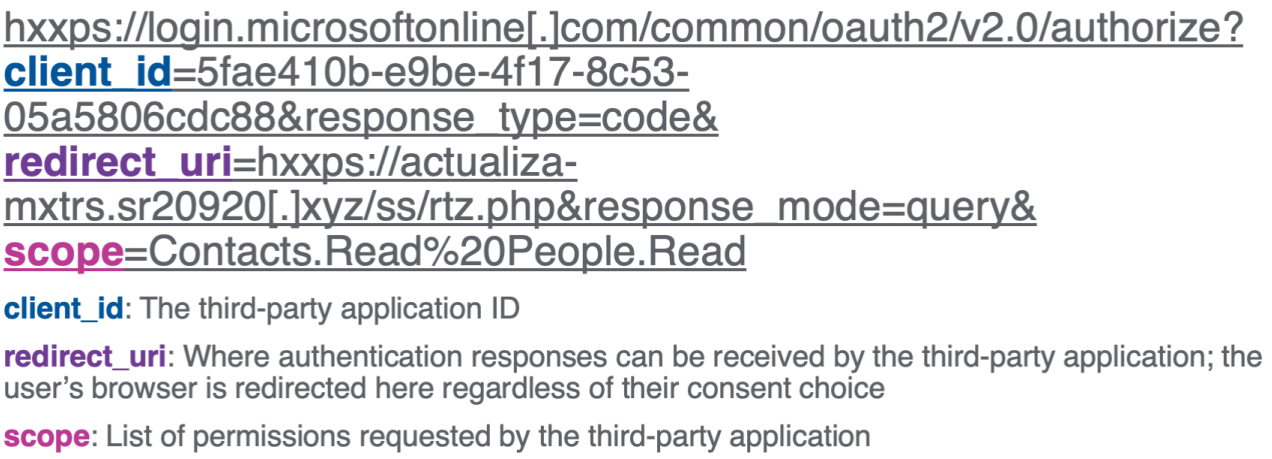

Figure 2: Relevant components of a consent URL

Through some campaigns, we have observed the same phish URLs leading to consent URLs with different values for client_id, redirect_uri, and scope options. Some campaigns have used multiple phish URLs. Samples listed below should not be considered representative of the complete list of 3PA IDs and URLs used by this actor over time.

Message Overview

In addition to the lures, there are several important components to the attacks described below. Below each message sample, we've included several relevant attributes:

- **OAuth Access Token Phish Lure Theme:** Branding or entity being impersonated.
- **OAuth Access Token Phish URL Sample:** Sample of the URL linked in the message body.
- **ClientID Sample:** Sample of the observed client_id value from consent URLs.
- **Consent redirect URL Sample:** A sample of the redirect_uri value from observed consent URLs where the user's browser is sent post-consent, regardless of the user's choice to consent or not. The request may contain an authorization code if the user chooses to consent, or an error code if the consent request was denied.
- **Scope values observed in consent URL:** A sample of the scope value from the consent URL. It describes the permissions requested by the third-party application

Impersonation of the Servicio de Administración Tributaria (SAT), Mexico's tax authority, is a common message theme for this actor. When SAT is used in the phish lure, the email suggests that the recipient needs to update their contact information and is presented with what appears to be a link to do so (Figures 3, 4). Some subjects, like "Acuse de Cita - Aclaraciones 2020. (Acknowledgment of Appointment – Clarifications 2020.)," make use of non-ASCII characters, possibly to evade simple spam filters (Figure 3).

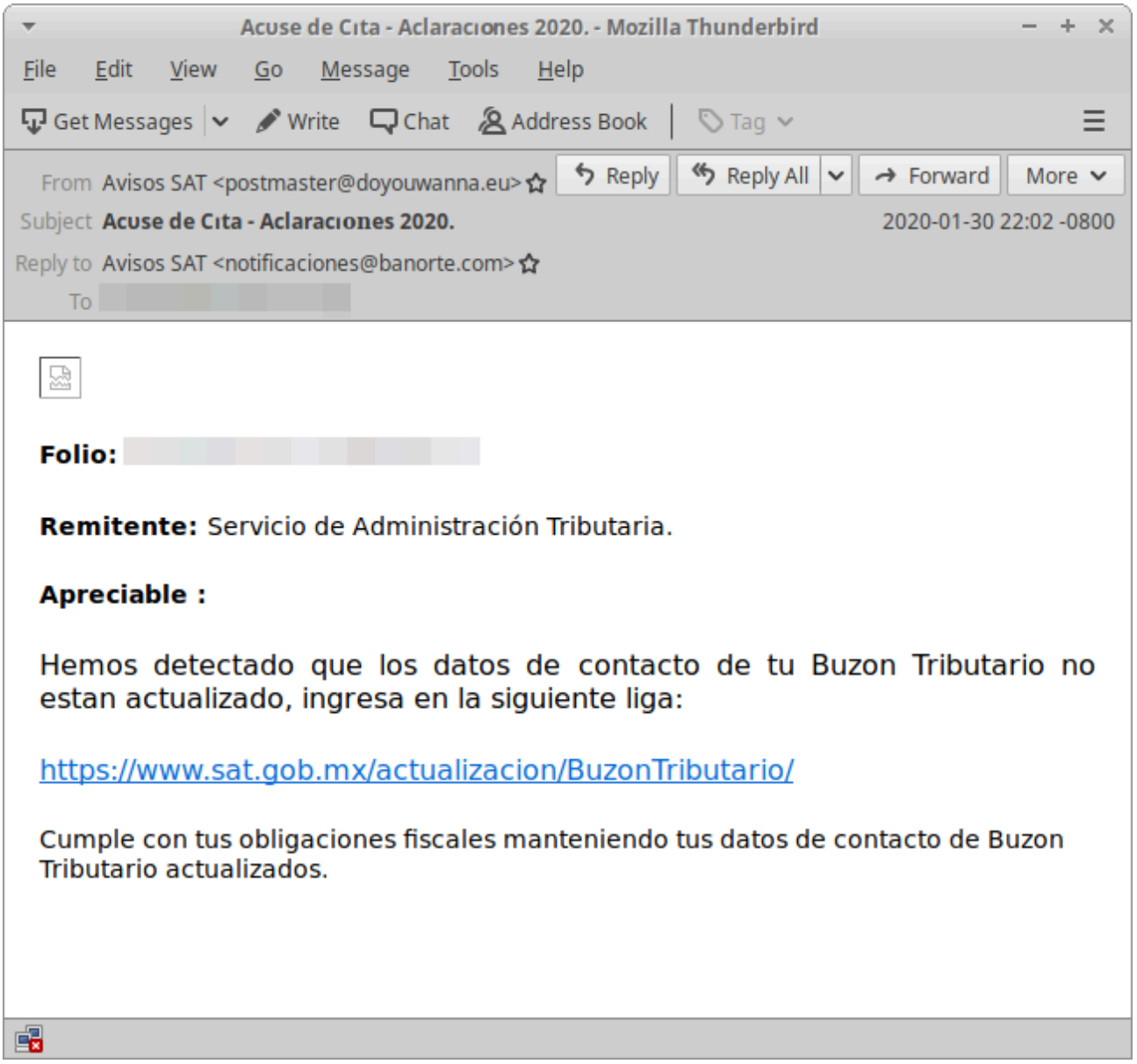

Figure 3: Mexican tax authority lure

- OAuth Access Token Phish Lure Theme: update your information with SAT of Mexico
- OAuth Access Token Phish URL Sample: hxxp://akglass[.]in/menu/redirect.php
- ClientID Sample: 13f33779-fe8e-4f64-8252-79e8ec962fb4
- Consent redirect URL Sample: hxxps://www-registros-apps-mx.e18220[.]com/1/autoriza.php
- Scope values observed in consent
  URL: User.Read, User.ReadBasic.All, Contacts.Read, Contacts.Read.Shared, People.Read

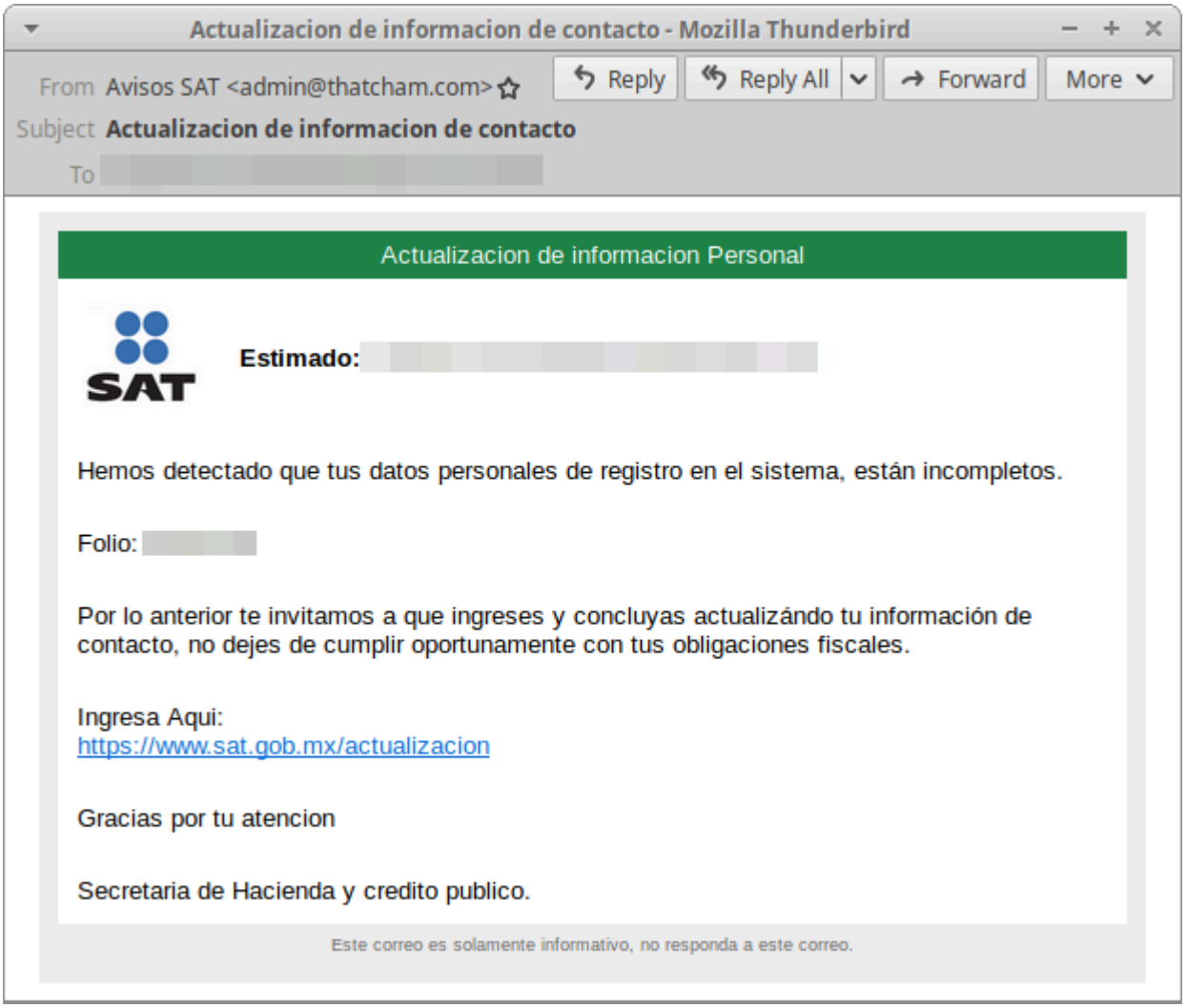

Figure 4: Mexican tax authority lure with accurate branding

- OAuth Access Token Phish Lure Theme: update your information with SAT of Mexico
- OAuth Access Token Phish URL Sample: hxxps://app452-sat-mx.i3720[.]xyz/leap/983.php
- ClientID Sample: 4f641680-a8cd-4f96-8181-08efaf2563b1
- Consent redirect URL Sample: hxxps://www-registros-appsmx-sat.x030720[.]xyz/regs/autoriza.php
- Scope values observed in consent
  URL: User.Read, Contacts.Read, Contacts.Read.Shared, People.Read, Mail.Read

Mexican tax- and government-themed messages are regularly observed with this actor, though they have occasionally deviated from this messaging and impersonated popular consumer brands. In July, we observed this actor's lures impersonating Netflix Mexico (Figure 5) and Amazon Prime Mexico (Figures 6, 7).

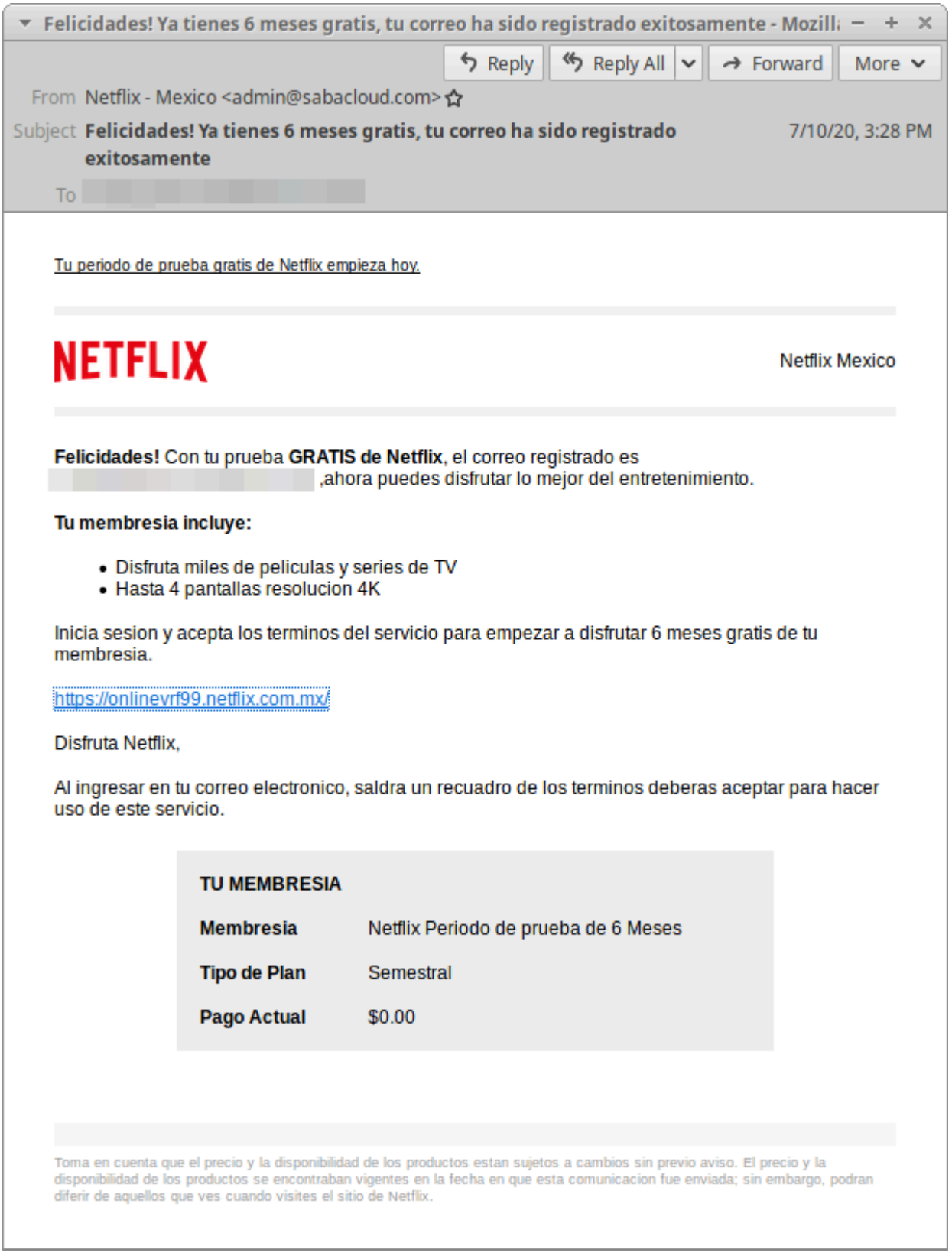

Figure 5: Netflix Mexico lure offering 6 free months of service

- OAuth Access Token Phish Lure Theme: Netflix Mexico free trial
- OAuth Access Token Phish URL Sample: hxxps://485online.rs10720[.]xyz/xPsY
- ClientID Sample: d76c652c-7ba7-4205-8666-059985a0ec54

- Consent redirect URL Sample: hxxps://www-netfflix-registros.i10720[.]xyz/regs/autoriza.php
- Domain reused in Amazon Prime free trial phish below
- Scope values observed in consent
  URL: User.Read, Contacts.Read, Contacts.Read.Shared, People.Read, Mail.Read

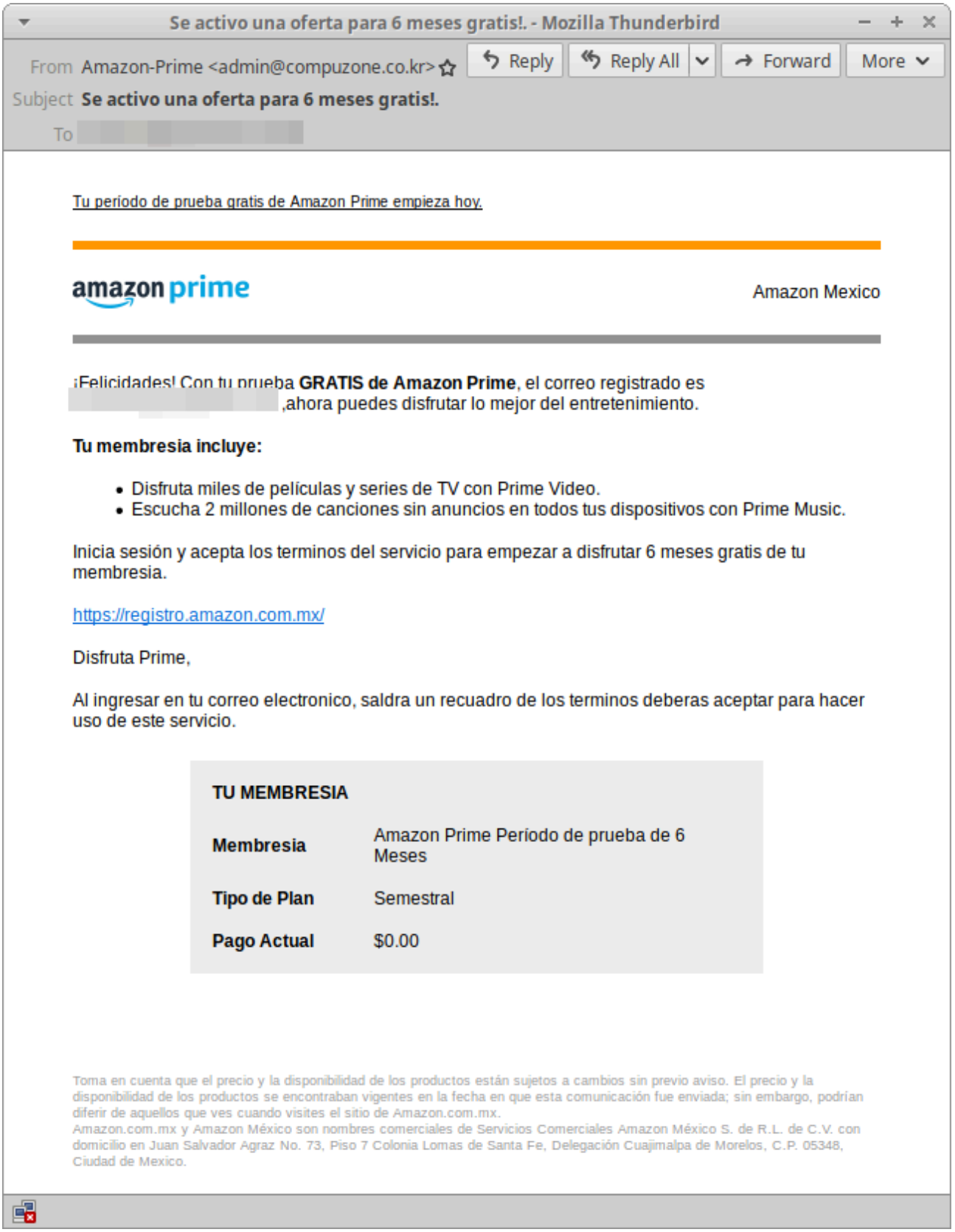

Figure 6: Amazon Prime Mexico lure offering 6 months of free service

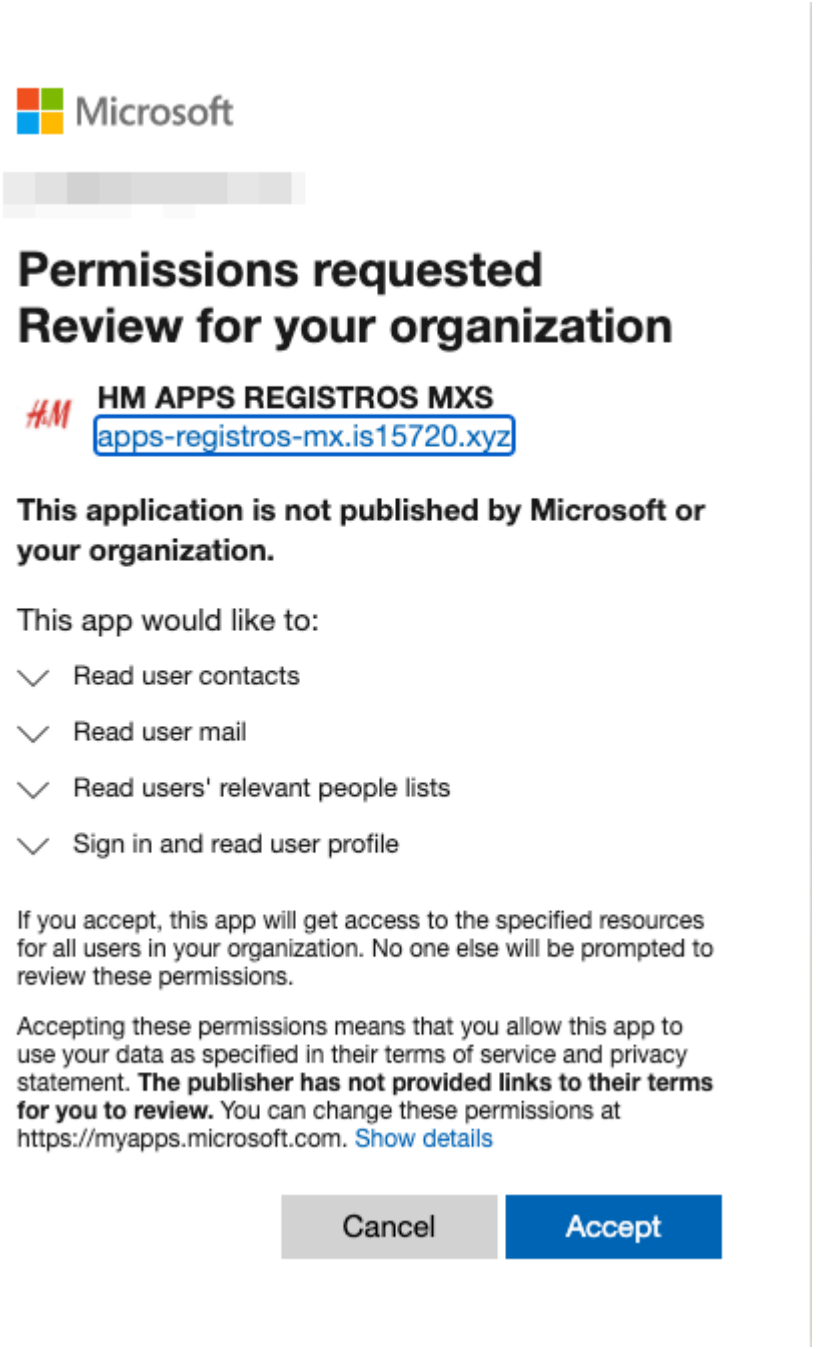

Figure 7: 3PA consent request, featuring H&M branding incongruent with the Amazon Prime lure

- Phish Lure Theme: Amazon Prime Mexico free trial
- OAuth Access Token Phishing URL Sample: hxxps://printstockphoto[.]com/img/01/redirect.html
- ClientID Sample: f6b5e94d-f5d8-4f4e-9a68-4c06aa2e4cba
- Consent redirect URL Sample: hxxps://apps-registros-mx.is15720[.]xyz/1/auth.php
- Notable brand mismatch between the email lure (Amazon Prime) and the consent page (H&M)

Third-Party Applications and Permission Risks

It's important to understand the scope and risk of permissions requested by the third-party apps linked in these messages. The official consent page presents a list of permissions requested by the third-party application (Figure 8 is an example).

Figure 8: Itemized permission list for a third-party application

All permissions we've observed requested thus far have been read-only. While that might seem relatively benign, even allowing an actor read access to a user's inbox and contacts can have significant regulatory and privacy consequences. The minimal permissions requested by these apps also likely help them appear inconspicuous if an organization's O365 administrator audits connected apps for their users' accounts. The apps don't request many permissions, and those they do might not appear particularly far-reaching, allowing them to blend in with other benign apps.

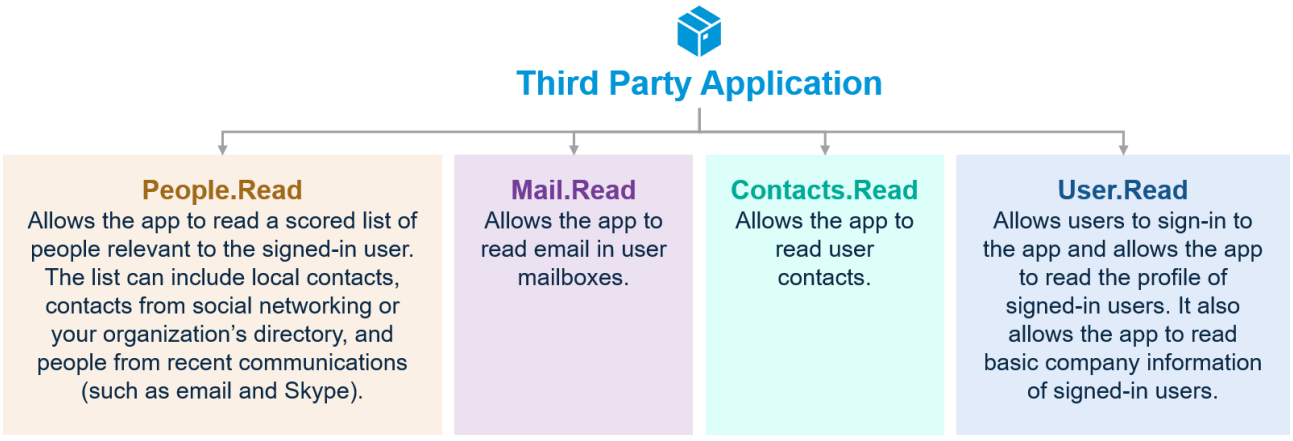

Figure 9: Commonly observed requested permissions

- Contacts.Read and People.Read could be used for email address harvesting. Obtaining email addresses in this way can help ensure addresses are valid and active.
- User.Read can help an actor determine potential value of an account, or the value of compromising the user's other accounts.
- Mail.Read allows an actor to read a user's mail, potentially offering a more subtle manner of collecting credentials. If an actor completes the 'forgot password' flow on a site connected to the email address and a

password reset link is sent via email, they could effectively steal the account. This also assumes that the user's account does not have multifactor authentication measures independent of the readable account's inbox enabled.

Infrastructure and Hosting

The phish URL in the lure is usually a compromised site that takes the recipient to the official O365 login page if they're not authenticated. Once signed into their O365 account, the user is redirected to the official O365 consent process that prompts them to grant permissions to the actor's application. The domains that catch the OAuth tokens are often registered via Namecheap and hosted on Cloudflare.

Conclusion

Threat actors often find creative ways to harvest information. In these attacks, TA2552 doesn't rely on techniques like more traditional credential phishing or dropping malware on a system. Instead, they gain permissions to view the content and activity of resources available through a user's O365 account. The departure from such traditional techniques gives this actor an advantage, as users likely aren't trained to spot or inspect suspicious applications. Even read-only access comes with considerable risk. The ability to perform reconnaissance on an O365 account supplies an actor with valuable information that can later be weaponized in business email compromise (BEC) attacks or account takeovers.

IOCs

Phish URL Domains:

The actor has used a blend of what appear to be compromised sites and custom domains.

- casperinfosystem[.]com
- ultimatetravel[.]in
- nivedafoundation[.]org
- calyss[.]in
- mucla[.]in
- akglass[.]in
- i3720[.]xyz
- rs10720[.]xyz
- photobalkan[.]com
- printstockphoto[.]com
- ccgdm[.]org
- al-thawiya[.]com
- dev.tvs[.]st

ClientIDs:

- 13f33779-fe8e-4f64-8252-79e8ec962fb4
- 4f641680-a8cd-4f96-8181-08efaf2563b1

- d76c652c-7ba7-4205-8666-059985a0ec54
- 2c8cd500-52d3-4b88-8d0b-1f8ad8a3b714
- 1ed6cd93-7682-4584-9e1e-f9251f056cbd
- 2385bb0e-b757-4b1c-830b-c5076d1c8ca2
- 41b33fb0-7a42-4f9a-a649-62fa456e85ea
- 6337785c-1c50-4b4f-befa-9b70b9fd78ad
- 81f521a0-8db3-42cc-a3ff-9756474c7d14
- a04f33b3-efee-4d74-93ce-59b157381c0b
- a972fde8-6e7a-41bb-9c63-d3cc6c0603fe
- ab6df806-cd0e-462d-af11-3c51bccc6ba3
- b8d51b1a-f464-4ab4-ac0d-9d8dc190cb9e
- f6b5e94d-f5d8-4f4e-9a68-4c06aa2e4cba

Redirect URL Domains:

- x030720[.]xyz
- e10220[.]com
- xs1920[.]xyz
- i10720[.]xyz
- e1920[.]xyz
- is15720[.]xyz
- e29120[.]com
- rr020920[.]xyz
- e180320[.]xyz
- e18220[.]com
- i5320[.]xyz
- r25820[.]xyz
- ex171019[.]com
- 16720s[.]xyz
- e18220[.]com
