Microsoft warns of increasing OAuth Office 365 phishing attacks

bleepingcomputer.com/news/security/microsoft-warns-of-increasing-oauth-office-365-phishing-attacks/

Sergiu Gatlan

By
Sergiu Gatlan

- February 5, 2021
- 12:07 PM
- 0

Microsoft has warned of an increasing number of consent phishing (aka OAuth phishing) attacks targeting remote workers during recent months, BleepingComputer has learned.

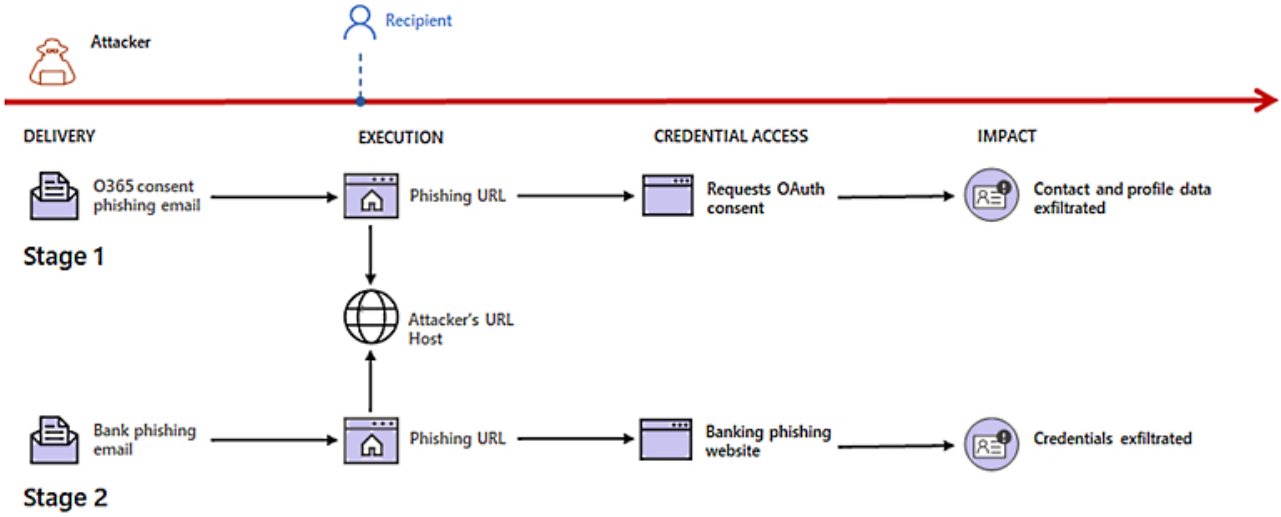
These attacks were part of two campaigns that ran between September and December 2020, targeting victims in multiple recurring waves.

One of the two attack campaigns specifically targeted Spanish speaking victims with OAuth links and lures impersonating Mexico's tax administration service — Servicio de Administración Tributaria (SAT) — on two occasions, in September and October.

The phishing activity of the second spiked multiple times between October and December, spewing financial lures targeting organizations' "investment teams."

Threat actors behind these attacks abused cloud service providers or used previously compromised domains to deliver their phishing emails. The OAuth URLs redirected the potential victims to attacker-owned domains for displaying the authentication request.

Microsoft issued this warning in a private security advisory shared with Microsoft Defender ATP subscribers in late-January.



OAuth phishing attack flow (*Microsoft*)

What is consent phishing?

Consent phishing (also known as OAuth phishing) is an application-based attack variant where the attackers attempt to trick targets into providing malicious Office 365 OAuth apps (web apps registered by the attackers with an OAuth 2.0 provider) with access to their Office 365 accounts.

Once victims grant the malicious apps permissions to their account's data, the threat actors pounce on their access and refresh tokens.

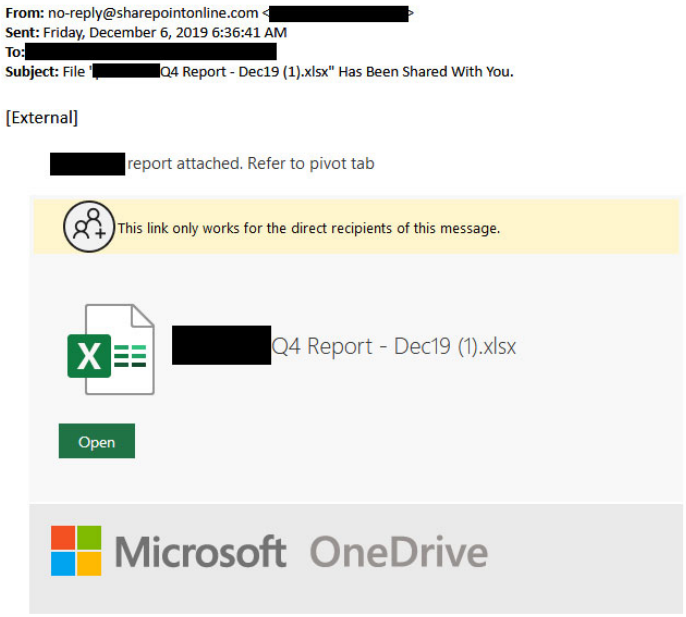
They enable them to take over the targets' Microsoft accounts and make API calls through the attacker-controlled malicious Office 365 OAuth app.

The compromised Office 365 accounts provide the attackers with access to victims' emails, files, contacts, as well as sensitive information and resources stored on corporate SharePoint document management/storage systems and/or OneDrive for Business cloud storage spaces.

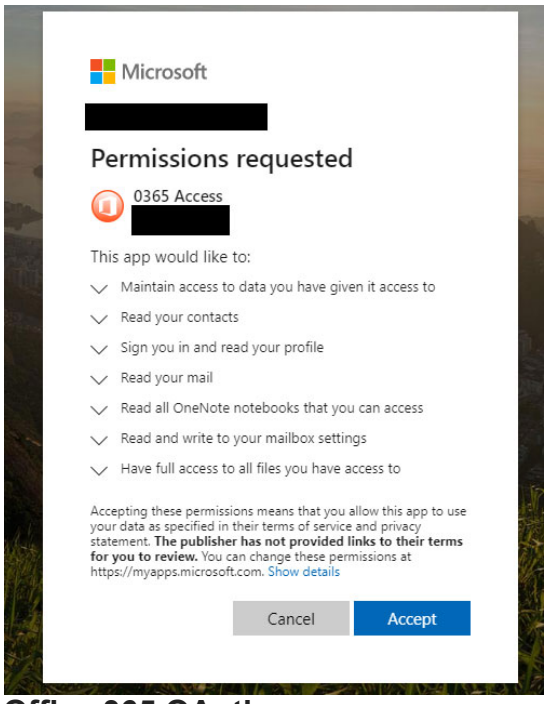
"Once victims clicked on the deceptive links, they were ultimately prompted to grant access permissions to a malicious web application (web app)," Microsoft Corporate Vice President for Customer Security & Trust Tom Burt explained.

"Unknown to the victim, these malicious web apps were controlled by the criminals, who, with fraudulently obtained permission, could access the victim's Microsoft Office 365 account."

BleepingComputer reported on the inner-workings of a consent phishing attack in December 2019, showing how it makes it possible for attackers to hijack Office 365 accounts.



Phishing email sample



Office 365 OAuth app

Consent phishing warnings

Microsoft warned of phishers' shift to new types of phishing tactics such as consent phishing in July 2020, adding to other, more conventional phishing vectors such as email phishing and credential theft attacks.

At the time, multiple phishing campaigns were launching consent phishing attacks against Microsoft customers trying to take control of their accounts, stealing sensitive data, and later using them to defraud organizations in Business Email Compromise (BEC) fraud schemes.

Microsoft took legal action and dismantled part of the attack infrastructure by taking down six of the domains used to host malicious 365 OAuth apps used to hijack customers' Office 365 accounts.

Additionally, the company identified and disabled malicious Office 365 OAuth apps to block users from accessing them and getting their accounts hijacked.

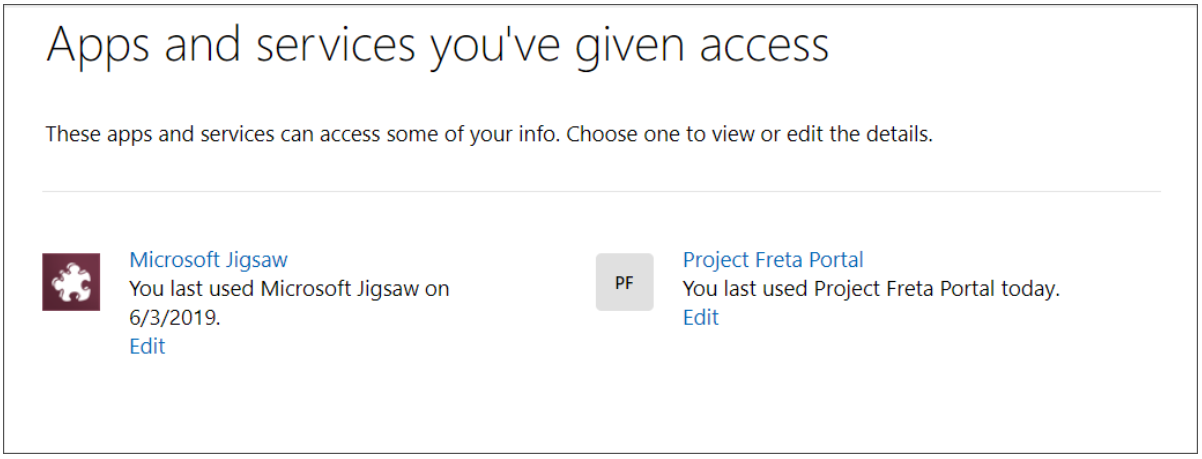
Starting with October 2020, Microsoft announced that Office 365 consent phishing protections are generally available, including app consent policies and OAuth app publisher verification.

Last year, the FBI also warned of BEC scammers abusing cloud email services such as Microsoft Office 365 and Google G Suite in Private Industry Notifications published in March and in April.

Defense measures

Microsoft customers can check if they have any user consent apps or services tied to their accounts by going to their account's consent manager dashboard.

To remove any of the listed consents, you have to click on its entry and, on the page that opens, click on the 'Remove these permissions' button to remove it.



Organizations can also take measures to protect their remote workforce from OAuth phishing by requiring the use of publisher verified apps, educating employees on how to spot consent phishing tactics, and only allow access to OAuth apps trusted by the organization or provided by verified publishers.

Employers can also educate workers on how Microsoft permissions and the consent framework work:

• Understand the data and permissions an application is asking for and understand how permissions and consent work within our platform.
• Ensure administrators know how to manage and evaluate consent requests.
• Audit apps and consented permissions in your organization to ensure applications being used are accessing only the data they need and adhering to the principles of least privilege.

More details on how to defend against security threats can be found in Microsoft's Detect and Remediate Illicit Consent Grants in Office 365 and Five steps to securing your identity infrastructure support docs.

Related Articles:

Intuit warns of QuickBooks phishing threatening to suspend accounts

GitHub: Attacker breached dozens of orgs using stolen OAuth tokens

Google: Russian phishing attacks target NATO, European military

FBI warns election officials of credential phishing attacks

Tails 5.0 Linux users warned against using it "for sensitive information"

- OAuth
- Office 365
- Phishing
- Warning

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

You may also like: