# Hackers are taking over CEO accounts with rogue OAuth apps

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

January 28, 2022 09:29 AM **0**

According to a report from Proofpoint, the campaign is still ongoing, though Microsoft is monitoring the activity and has already blocked most of the apps.



The impact of executive account takeovers ranges from lateral movement on the network and insider phishing to deploying ransomware and business email compromise incidents.



## Employing OAuth apps

OAuth is a standard for token-based authentication and authorization, removing the need to enter account passwords.

Apps that use OAuth require specific permissions such as file read and write permissions, access to calendar and email, and email send authorization.



The purpose of this system is to offer increased usability and convenience while maintaining a high security level within trustworthy environments by reducing credential exposure.

With OAuth tokens, cloud-based third-party applications can access the data points required to provide businesses with productivity features without getting the users' passwords.

The actors behind the OiVaVoii campaign used at least five malicious OAuth applications, four of them currently blocked: 'Upgrade', 'Document', 'Shared', and 'UserInfo'.

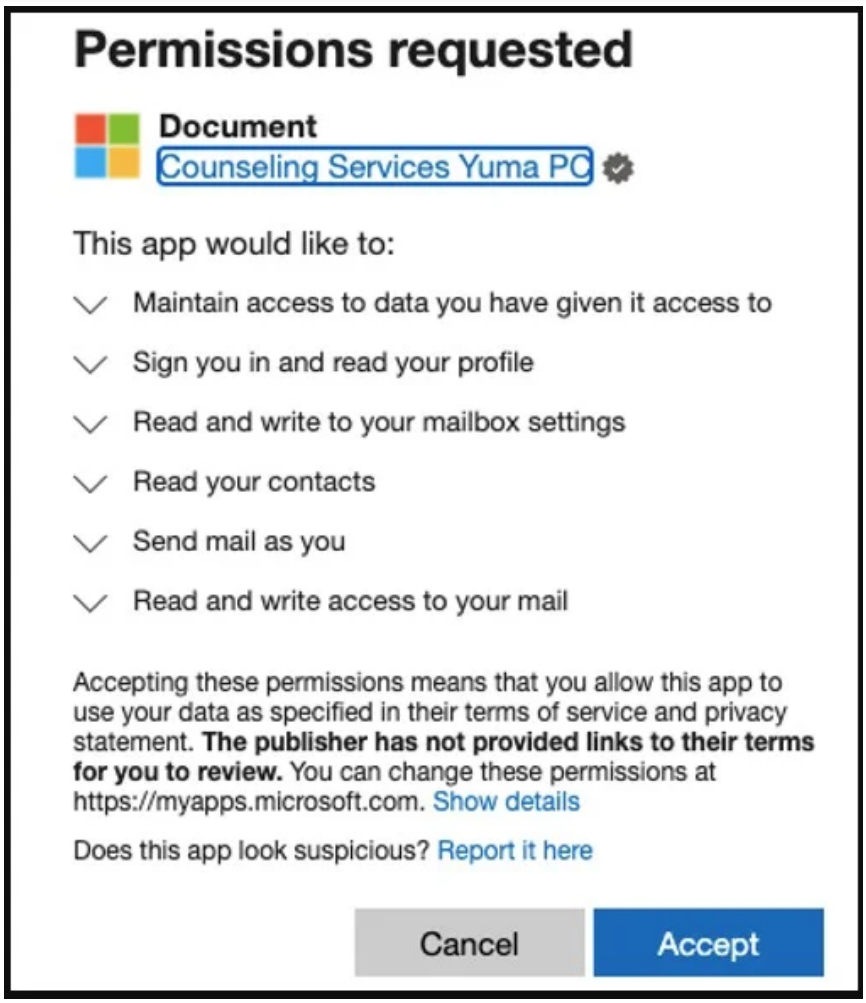
| App name | App id | Published Type | Creation Date | Status |
|---|---|---|---|---|
| *Upgrade* | 01d33e0a-83c1-4e5c-98be-096bc270eabf | Verified | 16/11/21 | Blocked |
| *Upgrade* | f9b75e84-5235-48d3-b745-37c99c056b64 | Verified | 23/1/22 | Blocked |
| *Document* | c517e6b9-a1d5-4f7e-8081-dfb2142c056a | Verified | 26/1/22 | Blocked |
| *Shared* | b2710450-6cec-4e4f-989f-c16f3041620a | Unverified | 27/1/22 | Available |
| *UserInfo* | 32fc064d-d4ea-43f9-ae7f-e90da936053f | Unknown | 27/1/22 | Blocked |

**Malicious OAuth apps employed in the campaign**

*Source: Proofpoint*

Three of these apps were created by verified publishers, which indicates that the threat actors compromised the account of a legitimate Office tenant.

The threat actors then used the apps to send out authorization requests to high-ranking executives in the targeted organizations. In many cases, the recipients accepted the requests, seeing nothing suspicious in them.




**OAuth app using Microsoft logo and a verified publisher**

*Source: Proofpoint*

If they click on Cancel, a manipulation in the Reply URL redirects them back to the consent screen, locking them on the same page until they accept the permission request.

Proofpoint also mentions (https://www.proofpoint.com/us/blog/cloud-security/oivavoii-active-malicious-hybrid-cloud-threats-campaign) the likelihood of man-in-the-middle proxy attacks that could also compromise the target's account credentials.

same way.

Also, executives who have already been compromised and given access to their accounts remain high-risk points for impacted organizations.

The potentially compromised firms need to revoke the permissions, delete the apps, remove any malicious mailbox rules added by the actors, and scan for any dropped files.

Finally, all employees should be trained to suspect internal communications, especially messages from high-ranking executives that don't align with their standard business practices.

## Related Articles:

Microsoft warns of multi-stage phishing campaign leveraging Azure AD (https://www.bleepingcomputer.com/news/security/microsoft-warns-of-multi-stage-phishing-campaign-leveraging-azure-ad/)

Convincing Microsoft phishing uses fake Office 365 spam alerts (https://www.bleepingcomputer.com/news/security/convincing-microsoft-phishing-uses-fake-office-365-spam-alerts/)

US universities targeted by Office 365 phishing attacks (https://www.bleepingcomputer.com/news/security/us-universities-targeted-by-office-365-phishing-attacks/)

Finland warns of Facebook accounts hijacked via Messenger phishing (https://www.bleepingcomputer.com/news/security/finland-warns-of-facebook-accounts-hijacked-via-messenger-phishing/)

Lazarus hackers use Windows Update to deploy malware (https://www.bleepingcomputer.com/news/security/lazarus-hackers-use-windows-update-to-deploy-malware/)