AL2025_19 Malicious Adobe, DocuSign OAuth apps target Microsoft 365 accounts (21st March 2025)

Description

Cybercriminals are exploiting malicious Microsoft OAuth applications disguised as Adobe and DocuSign apps to compromise Microsoft 365 accounts. These apps are designed to gain access to user profiles and email information, which attackers then leverage for further malicious activity, such as phishing campaigns and malware distribution. Researchers from Proofpoint uncovered these highly targeted campaigns, which have primarily affected government, healthcare, supply chain, and retail industries across the U.S. and Europe.

Attack Details

The malicious OAuth apps impersonate legitimate applications like:

- Adobe Drive
- Adobe Drive X
- Adobe Acrobat
- DocuSign

These applications request access to seemingly low-risk permissions, such as:

- Profile - Provides attackers with full names, user IDs, profile pictures, and usernames.
- Email - Grants access to users' primary email addresses.
- OpenID - Allows attackers to confirm a user’s identity and retrieve Microsoft account details.

Attackers distribute phishing emails from compromised email accounts belonging to charities and small businesses, often using Office 365 accounts. The phishing emails typically use lures such as Requests for Proposals (RFPs) and contract-related documents to convince users to grant OAuth permissions.

Once permission is granted, victims are redirected through multiple stages before reaching a phishing page that attempts to steal Microsoft 365 credentials or deploy malware. In some cases, users are redirected to a fake Office 365 login page hosted on a malicious domain. Proofpoint researchers detected suspicious login attempts to victims’ accounts within a minute of authorization.

This attack leverages the ClickFix social engineering technique, a well-known method that deceives users into believing they are resolving an issue by clicking on seemingly harmless links.

Remediation

By implementing these security measures, organizations can mitigate the risk of unauthorized OAuth app permissions and safeguard their Microsoft 365 accounts from compromise.

For Individual Users:

- **Review OAuth App Permissions:**
  - Visit myapplications.microsoft.com → 'Manage your apps' → Revoke any unrecognized applications.
- **Verify OAuth App Requests:**
  - Always verify the source of permission requests before approving them.
  - Be cautious of unsolicited emails requesting app authorization.
- **Enable Multi-Factor Authentication (MFA):**
  - Enforce MFA for all users to add an additional security layer.
- **Monitor Account Activity:**
  - Regularly review login activity for any unauthorized access.

For Microsoft 365 Administrators:

- **Restrict OAuth Permissions:**
  - Navigate to **Enterprise Applications → Consent and Permissions**→ Set **Users can consent to apps** to **No** to prevent users from approving third-party OAuth apps.
- **Implement Conditional Access Policies:**
  - Limit OAuth access based on location, device compliance, or risk level.
- **Deploy Advanced Threat Protection (ATP):**
  - Use ATP policies to detect and block phishing attempts before they reach users.
- **Educate Employees on Phishing Risks:**
  - Conduct security awareness training on identifying and avoiding phishing scams.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Staff, S. (2025, March 17). Microsoft 365 credentials subjected to malicious OAuth app attack. SC Media. https://www.scworld.com/brief/microsoft-365-credentials-subjected-to-malicious-oauth-app-attack
- Toulas, B. (2025, March 16). Malicious Adobe, DocuSign OAuth apps target Microsoft 365 accounts. BleepingComputer. https://www.bleepingcomputer.com/news/security/malicious-adobe-docusign-oauth-apps-target-microsoft-365-accounts/