RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **IDY-RO2**

Defending Against New Phishing Attacks that Abuse OAuth Authorization Flows

Jenko Hwong

Cloud Security Researcher
Netskope, Inc.
@jenkohwong

June 9, 2022

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Security LLC or its affiliates. All rights reserved. RSA Conference logo, RSA and other trademarks are trademarks of RSA Security LLC or its affiliates.

RSAConference2022

what must change

Defending Against New Phishing Attacks that Abuse OAuth Authorization Flows

RSAConference2022

- Domain/URL filtering ineffective
- MFA controls bypassed
- Broad lateral movement
- Logging information is minimal
- Revoking access is difficult

what must change

Defending Against New Phishing Attacks that Abuse OAuth Authorization Flows

RSAConference2022

credential attack

what must change

protocol-specific

Defending Against New Phishing Attacks that Abuse OAuth Authorization Flows

de facto standard

dynamic user authorization of application access to resources

- Domain/URL filtering ineffective
- MFA controls bypassed
- Broad lateral movement
- Logging information is minimal
- Revoking access is difficult

OAuth 2.0

De facto standard for web app authorization and access to resources (data)

The New Web: redirects user to authenticate…

3rd-Party Website(apps)

Authentication

1 Item

Cart Subtotal

$229.99

CHECKOUT NOW

REP Sabre Olympic Bar - 20 kg

$229.99

Qty: 1

Remove

VIEW AND EDIT CART

PAYMENT METHOD

Credit Card

PayPal

Pay with PayPal

+ Apply Discount Code

+ Apply Gift Card

Log in to your PayPal account

paypal.com/checkoutnow?locale.x=en_US&fundingSource=paypal...

PayPal

Pay with PayPal

Enter your email or mobile number to get started.

Email or mobile number

Forgot email?

Next

or

Checkout as Guest

Cancel and return to REP Fitness

English | Français | Español | 中文

Contact Us Privacy Legal Worldwide

The New Web: user approves/consents...

Authentication

Authentication

Authorization

RSAConference2022

A New Class of Phishing Attacks

Microsoft Device Code Flow[1]

[1] Introducing a new phishing technique for compromising Office 365 accounts, Dr. Nestori Syynimaa

The New Web: Phishing Attack: Device Code Flow (DEMO)

netskope

The New Web: Phishing Attack: Device Code Flow

1 Assumed Application Identity

Authorization

Cloud Data, Compute, Users

Attacker

OAuth Tokens

5 Access

API Calls

lateral movement

Office 365 -> Azure

4 Token

2 Phish

User

Username
Password

3 Authenticate, ~~Authorize~~

https://microsoft.com/...

Azure

The New Web: OAuth Defenses are Lacking

1 Assumed Application Identity

Authorization

Cloud Data, Compute, Users

4 Cannot prevent or detect assumed app identities

Attacker

OAuth Tokens

5 Access

API Calls

5 ~~MFA~~

6 Cannot prevent pivot

lateral movement

Office 365 -> Azure

4 Token

2 Phish

1 ~~URL Inspection~~

Content Inspection

Sender Reputation

User

2 ~~URL Inspection~~

Username

Password

3 Authenticate, ~~Authorize~~

https://microsoft.com/...

3 Cannot force approvals

Azure

7 SecOps

- Bypass of approved app lists
- Pivot is not logged
- Revoke tokens incomplete
- Tokens are permanent

What can we do about it?

- **Security Operations**
- **Proactive Measures**

Protecting your crucial assets took draconian measures.

In 621 B.C., Draco attempted to deter criminal activity by passage of an extremely harsh code that made even minor offenses such as stealing cabbage punishable by death.[1]

[1] J. David Hirschel, William O. Wakefield. Criminal Justice in England and the United States. Ed. Greenwood Publishing Group, 1995. ISBN 9780275941338. p.160.

Protecting your crucial assets takes draconian measures.

DENY ALL
BY DEFAULT
ALL THE TIME
TO EVERYONE
EVERYWHERE

Protecting your crucial assets takes draconian measures.

~~DENIAL~~

BY DEFAULT
ALL THE TIME
TO EVERYONE
EVERYWHERE

Security Operations

+ Proactive Measures

Proactive Measures: Research

- Educate
  - Ubiquitous authorization protocol
  - Not so obvious uses of OAuth...
    - Azure CLI: device code authorization flow
    - Google CLI with service accounts: OAuth tokens
  - Treat as seriously as data, users, applications
  - User-driven Internet model (shadow IT)

Proactive Measures: Research

- Educate
  - Ubiquitous authorization protocol
  - Not so obvious uses of OAuth...
    - Azure CLI: device code authorization flow
    - Google CLI with service accounts: OAuth tokens
  - Treat as seriously as data, users, applications
  - User-driven Internet model (shadow IT)
  - OAuth token attacks
    - Challenges: MFA bypass, ***not*** temporary, unmanaged, logging limited, prevention/detection difficult, revocation challenging, can leverage existing processes but controls differ
  - Non-phishing attack vectors

Security Operations: Assess

- OAuth audit logs
  - New OAuth applications
  - Permissions requested (scopes)
  - User approvals of resources

Security Operations: Assess

- OAuth audit logs
  - New OAuth applications
  - Permissions requested (scopes)
  - User approvals of resources

Security Operations: Assess

- OAuth audit logs
  - New OAuth applications
  - Permissions requested (scope
  - User approvals of resources
- Baseline normal activity
  - Counts, Top-N, distributions

	Application	Description	# Users	% Total Users
1	Google Chrome	Chrome Browser	463,286	91.0%
2	iOS Account Manager	iOS application	183,730	36.1%
3	Zoom	Video calls	135,361	26.6%
4	Android device	Operating-system level, mobile	117,927	23.2%
5	Slack	Messaging	95,848	18.8%
6	Virtru	End-to-end encryption of email and files	63,217	12.4%
7	iOS	Operating-system level, mobile	53,334	10.5%
8	Atlassian	Jira (ticketing), Confluence (wikis)...	45,473	8.9%
9	Google Drive for desktop	Local sync client	42,585	8.4%
10	macOS	Operating-system level	31,860	6.3%
11	Adobe	Adobe Suite	28,719	5.6%
12	Pinterest	Consumer photo pinning	25,635	5.0%

	Application	Description	# Users	% Total Users
6	Virtru	End-to-end encryption of email and files	63,217	12.4%
12	Pinterest	Consumer photo pinning	25,635	5.0%
17	The New York Times	Consumer news	17,130	3.4%
21	Glassdoor	Jobs, salaries, complaints	15,175	3.0%
24	Postman	Technical tool: REST API calls...	13,125	2.6%

April 18, 2021 dataset from anonymized customers:
- 439 Google Workspace organization
- 509,079 users
- 60,875 unique applications

[1] Who Do You Trust? OAuth Client Application Trends: https://www.netskope.com/blog/who-do-you-trust-oauth-client-application-trends

Security Operations: Assess

- OAuth audit logs
  - New OAuth applications
  - Permissions requested (scopes)
  - User approvals of resources
- Baseline normal activity
  - Counts, Top-N, distributions

Scopes	# Users	# Apps
View and manage the files in your Google Drive	168,369	3,605
Manage your calendars	113,798	1,152
View and manage your mail	107,402	3,145
View and manage Google Drive files and folders that you have opened or created with this app	84,529	755
View and manage your spreadsheets in Google Drive	34,591	11,124
View and manage its own configuration data in your Google Drive	26,949	458
Manage your contacts	14,665	220
Manage mailbox labels	14,300	55
View and manage the provisioning of users on your domain	12,341	146
Manage your tasks	11,996	78

[1] Who Do You Trust? OAuth Client Application Trends: https://www.netskope.com/blog/who-do-you-trust-oauth-client-application-trends

Security Operations: Assess

- OAuth audit logs
  - New OAuth applications
  - Permissions requested (sc
  - User approvals of resourc
- Baseline normal acti
  - Counts, Top-N, distrib

Scopes
View and manage the files in your Google Drive
Manage your calendars
View and manage your mail
View and manage Google Drive files and folders that you
View and manage your spreadsheets in Google Drive
View and manage its own configuration data in your Goo
Manage your contacts
Manage mailbox labels
View and manage the provisioning of users on your dom
Manage your tasks

Scopes	# Users	# Apps	Application	# Users
View and manage your mail	107402	3145	Virtru	63217
View and manage your mail	107402	3145	iOS	53334
View and manage your mail	107402	3145	macOS	31860
View and manage your mail	107402	3145	Lever	12991
View and manage your mail	107402	3145	Microsoft apps & services	11055
View and manage your mail	107402	3145	G Suite Sync for Microsoft Outlook¬Æ	8866
View and manage your mail	107402	3145	TemplateEmailService	7759
View and manage your mail	107402	3145	Gmail to PDF	6543
View and manage your mail	107402	3145	Untitled project	4189
View and manage your mail	107402	3145	Adobe Acrobat	3155
View and manage your mail	107402	3145	Boomerang for Gmail	3059
View and manage your mail	107402	3145	Outreach	2991
View and manage your mail	107402	3145	Project Default Service Account	2681
View and manage your mail	107402	3145	Highspot	2081
View and manage your mail	107402	3145	Salesforce.com	2005

Scopes	# Users	# Apps	Application	# Users
View and manage your spreadsheets in Google Drive	34591	11124	Slack	95848
View and manage your spreadsheets in Google Drive	34591	11124	draw.io	16882
View and manage your spreadsheets in Google Drive	34591	11124	LucidChart	12461
View and manage your spreadsheets in Google Drive	34591	11124	Zendesk	8331
View and manage your spreadsheets in Google Drive	34591	11124	Asana	6606
View and manage your spreadsheets in Google Drive	34591	11124	Doordash	5070
View and manage your spreadsheets in Google Drive	34591	11124	Untitled project	4189
View and manage your spreadsheets in Google Drive	34591	11124	Zapier	3245
View and manage your spreadsheets in Google Drive	34591	11124	Project Default Service Account	2681
View and manage your spreadsheets in Google Drive	34591	11124	Titus	2592
View and manage your spreadsheets in Google Drive	34591	11124	JIRA	2424
View and manage your spreadsheets in Google Drive	34591	11124	Awesome Table	2220
View and manage your spreadsheets in Google Drive	34591	11124	SurveyMonkey	2078
View and manage your spreadsheets in Google Drive	34591	11124	MITRA	1931
View and manage your spreadsheets in Google Drive	34591	11124	Yet Another Mail Merge	1774
View and manage your spreadsheets in Google Drive	34591	11124	Google APIs Explorer	1723
View and manage your spreadsheets in Google Drive	34591	11124	Google Marketing Platform	1565
View and manage your spreadsheets in Google Drive	34591	11124	Quickstart	1487
View and manage your spreadsheets in Google Drive	34591	11124	Remove Duplicates	1421
View and manage your spreadsheets in Google Drive	34591	11124	HubSpot	1408

[1] Who Do You Trust? OAuth Client Application Trends: https://www.netskope.com/blog/who-do-you-trust-oauth-client-application-trends

Security Operations: Prevent

- Block

  Unnecessary OAuth authorization flows e.g., device code
  - https://www.microsoft.com/devicelogin
  - https://login.microsoftonline.com/common/oauth2/deviceauth
  - **NOTE**: exceptions such as Azure CLI

Security Operations: Prevent

- Block

  Unnecessary OAuth authorization flows e.g., device code
  - https://www.microsoft.com/devicelogin
  - https://login.microsoftonline.com/common/oauth2/deviceauth
  - **NOTE**: exceptions such as Azure CLI

- Lockdown[1]
  - Centralize the OAuth application approval process
  - Identify and enforce an allowed OAuth applications list

[1] Configure how users consent to applications :https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

Security Operations: Prevent

- Block
  Unnecessary OAuth author
  - https://www.microsoft.
  - https://login.microsofto
  - **NOTE**: exceptions such a
- Lockdown[1]
  - Centralize the approval proce
  - Identify and er applications lis

Configure user consent settings

To configure user consent settings through the Azure portal, do the following:

1. Sign in to the Azure portal as a Global Administrator.
2. Select **Azure Active Directory** > **Enterprise applications** > **Consent and permissions** > **User consent settings**.
3. Under **User consent for applications**, select which consent setting you want to configure for all users.
4. Select **Save** to save your settings.

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data.

- ○ Do not allow user consent
  An administrator will be required for all apps.
- ◉ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
  7 permissions classified as low impact
- ○ Allow user consent for apps
  All users can consent for any app to access the organization's data.

[1] Configure how users consent to applications :https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

Security Operations: Prevent

- Block
  Unnecessary OAuth author
  - https://www.microsoft.
  - https://login.microsofto
  - **NOTE**: exceptions such a
- Lockdown[1]
  - Centralize the approval proce
  - Identify and er applications lis

Configure user consent settings

To configure user consent settings through the Azure portal, do the following:

1. Sign in to the Azure portal as a Global Administrator.

s.

User consent settings probably won't work against a phishing attack which impersonates a common, approved application like Outlook.

organization.

7 permissions classified as low impact

Allow user consent for apps
All users can consent for any app to access the organization's data.

[1] Configure how users consent to applications :https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent

Security Operations: Prevent

- Block

  <u>Unnecessary OAuth authorization flows e.g., device code</u>
  - https://www.microsoft.com/devicelogin
  - https://login.microsoftonline.com/common/oauth2/deviceauth
  - **NOTE**: exceptions such as Azure CLI

- Lockdown
  - Centralize the OAuth application approval process
  - Identify and enforce an allowed OAuth applications list

- Mitigate compromised credentials
  - IP allow lists with proxies, VPNs, etc.
  - Device policies (managed endpoint)

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Security Operations: Prevent

- Block
  Unnecessary OAuth authorizatio
  - https://www.microsoft.com/d
  - https://login.microsoftonline.c
  - **NOTE**: exceptions such as Azu
- Lockdown
  - Centralize the OA approval process
  - Identify and enfor applications list
- Mitigate compro
  - IP allow lists with
  - Device policies (managed endpoint)

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Security Operations: Prevent

- Block

  <u>Unnecessary OAuth authorization flows e.g., device code</u>
  - https://www.microsoft.com/devicelogin
  - https://login.microsoftonline.com/common/oauth2/deviceauth
  - **NOTE**: exceptions such as Azure CLI

- Lockdown
  - Centralize the OAuth application approval process
  - Identify and enforce an allowed OAuth applications list

- Mitigate compromised credentials
  - IP allow lists with proxies, VPNs, etc.
  - Device policies (managed endpoint)

    https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
  - Session or token timeouts

Security Operations: Detect

- Detect failed access (IP/device conditional policies)

Security Operations: Detect

- Detect failed access (IP/device conditional policies)
- Behavioral detection
  - Compromised account activity
  - Abnormal or unexpected application activity
  - Track risky users (phishing targets, URL clicks, suspect app approvals)

Security Operations: Mitigate

- Update ops runbooks to address protocol-specific challenges
- Revocation of tokens is limited, confusing, and incomplete
  - Microsoft: you can revoke refresh tokens easily[1] but not access tokens.[2]

[1] Revoke-AzureADUserAllRefreshToken: https://docs.microsoft.com/en-us/powershell/module/azuread/revoke-azureaduserallrefreshtoken?view=azureadps-2.0
[2] Revoke user access in Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-revoke-access
[3] Continuous access evaluation: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

Security Operations: Mitigate

Revoke-AzureADUserAllRefreshToken

Reference

Module: AzureAD

Invalidates the refresh tokens issued to applications for a user.

When access is revoked

Once admins have taken the above steps, the user can't gain new tokens for any application tied to Azure Active Directory. The elapsed time between revocation and the user losing their access depends on how the application is granting access:

- For **applications using access tokens**, the user loses access when the access token expires.

Access tokens can be a security concern if access must be revoked within a time that is shorter than the lifetime of the token, which is usually around an hour. For this reason, Microsoft is actively working to bring continuous access evaluation to Office 365 applications, which helps ensure invalidation of access tokens in near real time.

[1] Revoke-AzureADUserAllRefreshToken: https://docs.microsoft.com/en-us/powershell/module/azuread/revoke-azureaduserallrefreshtoken?view=azureadps-2.0
[2] Revoke user access in Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-revoke-access
[3] Continuous access evaluation: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

Security Operations: Mitigate

- Update ops runbooks to address protocol-specific challenges
- Revocation of tokens is limited, confusing, and incomplete
  - Microsoft: you can revoke refresh tokens easily[1] but not access tokens.[2]
  - “Hope is not a strategy.”
    - disable the user account for 1 hour
    - delete/restore the account
    - don’t forget about registered devices

[1] Revoke-AzureADUserAllRefreshToken: https://docs.microsoft.com/en-us/powershell/module/azuread/revoke-azureaduserallrefreshtoken?view=azureadps-2.0
[2] Revoke user access in Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-revoke-access

Security Operations: Analyze

- High-risk users
  - Phishing targets (URLs)

Security Operations: Analyze

- High-risk users
  - Phishing targets (URLs)
  - Trust of high-risk applications or large number of applications

	Application	Description	# Users	% Total Users
1	Google Chrome	Chrome Browser	463,286	91.0%
2	iOS Account Manager	iOS application	183,730	36.1%
3	Zoom	Video calls	135,361	26.6%
4	Android device	Operating-system level, mobile	117,927	23.2%
5	Slack	Messaging	95,848	18.8%
6	Virtru	End-to-end encryption of email and files	63,217	12.4%
7	iOS	Operating-system level, mobile	53,334	10.5%
8	Atlassian	Jira (ticketing), Confluence (wikis)...	45,473	8.9%
9	Google Drive for desktop	Local sync client	42,585	8.4%
10	macOS	Operating-system level	31,860	6.3%
11	Adobe	Adobe Suite	28,719	5.6%
12	Pinterest	Consumer photo pinning	25,635	5.0%

Who Do You Trust? OAuth Client Application Trends: https://www.netskope.com/blog/who-do-you-trust-oauth-client-application-trends

Security Operations: Analyze

- High-risk users
  - Phishing targets (URLs)
  - Trust of high-risk applications or large number of applications
  - Highly-privileged users (admins)

	Application	Description	# Users	% Total Users
1	Google Chrome	Chrome Browser	463,286	91.0%
2	iOS Account Manager	iOS application	183,730	36.1%
3	Zoom	Video calls	135,361	26.6%
4	Android device	Operating-system level, mobile	117,927	23.2%
5	Slack	Messaging	95,848	18.8%
6	Virtru	End-to-end encryption of email and files	63,217	12.4%
7	iOS	Operating-system level, mobile	53,334	10.5%
8	Atlassian	Jira (ticketing), Confluence (wikis)...	45,473	8.9%
9	Google Drive for desktop	Local sync client	42,585	8.4%
10	macOS	Operating-system level	31,860	6.3%
11	Adobe	Adobe Suite	28,719	5.6%
12	Pinterest	Consumer photo pinning	25,635	5.0%

Who Do You Trust? OAuth Client Application Trends: https://www.netskope.com/blog/who-do-you-trust-oauth-client-application-trends

Security Operations: Analyze

- High-risk users
  - Phishing targets (URLs)
  - Trust of high-risk applications or large number of applications
  - Highly-privileged users (admins)
- High-risk applications
  - Request of broad privileges e.g., read-write all Google Drive

Scopes	# Users	# Apps	Application	# Users
View and manage your spreadsheets in Google Drive	34591	11124	Slack	95848
View and manage your spreadsheets in Google Drive	34591	11124	draw.io	16882
View and manage your spreadsheets in Google Drive	34591	11124	LucidChart	12461
View and manage your spreadsheets in Google Drive	34591	11124	Zendesk	8331
View and manage your spreadsheets in Google Drive	34591	11124	Asana	6606
View and manage your spreadsheets in Google Drive	34591	11124	Doordash	5070
View and manage your spreadsheets in Google Drive	34591	11124	Untitled project	4189
View and manage your spreadsheets in Google Drive	34591	11124	Zapier	3245
View and manage your spreadsheets in Google Drive	34591	11124	Project Default Service Account	2681
View and manage your spreadsheets in Google Drive	34591	11124	Titus	2592
View and manage your spreadsheets in Google Drive	34591	11124	JIRA	2424
View and manage your spreadsheets in Google Drive	34591	11124	Awesome Table	2220

Security Operations: Analyze

- High-risk user
  - Phishing targe
  - Trust of high-r number of app
  - Highly-privileg
- High-risk appl
  - Request of bro ve

Scopes
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets
View and manage your spreadsheets

```
Manage data access permissions for users on your domain
Manage delegated admin roles for your domain
Manage messages in groups on your domain
Manage the list of sites and domains you control
Manage your Google Classroom class rosters
Manage your Google Classroom classes
Manage your calendars
Manage your contacts
View and manage Google Apps licenses for your domain
View and manage customer related information
View and manage data transfers between users in your organization
View and manage organization units on your domain
View and manage the provisioning of calendar resources on your domain
View and manage the provisioning of domains for your customers
View and manage the provisioning of groups on your domain
View and manage the provisioning of user schemas on your domain
View and manage the provisioning of users on your domain
View and manage the settings of a Google Apps Group
View and manage your Chrome OS devices' metadata
View and manage your mobile devices' metadata
View audit reports of Google Apps for your domain
View the email addresses of people in your classes
View the profile photos of people in your classes
View usage reports of Google Apps for your domain
View your basic profile info
View your data in Google Cloud Storage
View your email address
```

Security Operations: Analyze

- High-risk users
  - Phishing targets (URLs)
  - Trust of high-risk applications or large number of applications
  - Highly-privileged users (admins)
- High-risk applications
  - Request of broad privileges e.g., read-write all Google Drive
  - Used by large number of users (large impact)

	Application	Description	# Users	% Total Users
1	Google Chrome	Chrome Browser	463,286	91.0%
2	iOS Account Manager	iOS application	183,730	36.1%
3	Zoom	Video calls	135,361	26.6%
4	Android device	Operating-system level, mobile	117,927	23.2%
5	Slack	Messaging	95,848	18.8%
6	Virtru	End-to-end encryption of email and files	63,217	12.4%

Security Operations: Analyze

- High-risk u
  - Phishing t
  - Trust of hi number o
  - Highly-pri
- High-risk a
  - Request o
  - Used by la

Security Operations: Analyze

- High-risk users

As a different example, the CamScanner application is only used by 219 users (.04% of 509.079) and requests "View and manage the files in your Google Drive," one of the broadest data scopes for regular users. CamScanner was found by Kaspersky in August 2019 to contain malware and was banned by the Indian government over security concerns in June 2020. This reinforces the need to manage application trust and usage, and that risky behavior for a small number of users should also be analyzed, not just applications affecting the largest number of users.

  - Highly-privileged users (admins)

from
Users

- High-risk applications
  - Request of broad privileges e.g., read-write all Google Drive
  - Used by large number of users (large impact)
  - Obscure applications (suspect developer/reputation)

Who Do You Trust? OAuth Client Application Trends: https://www.netskope.com/blog/who-do-you-trust-oauth-client-application-trends

Security Operations: Analyze

- High-risk users
  - Phishing targets (URLs)
  - Trust of high-risk applications or large number of applications
  - Highly-privileged users (admins)
- High-risk applications
  - Request of broad privileges e.g., read-write all Google Drive
  - Used by large number of users (large impact)
  - Obscure applications (suspect developer/reputation)
- Changes and anomalies
  - New applications, new scopes, top-N apps, top-N users

Proactive Measures: Innovate

Anticipate

- Track latest threat research
- Skate to where the puck is: OAuth 2.x
- Inventory OAuth use
  - Identity systems, SaaS apps
  - Hidden dependencies[1]
- Assume non-phishing attack vectors
- Vendor research and roadmap

Initiate

- Early warning indicators
  - Failures against IP allow lists (compromised creds)
  - Suspicious HTTP/URL traffic (phish targeting)
- Threat intel specific to protocol-based attacks
  - Fingerprint approved applications
  - Detect suspicious OAuth applications
  - Attribution for OAuth threats

[1] Hacking G Suite: The Power of Dark Apps Script Magic, Matthew Bryant, DEF CON 29

RSA Conference2022

Applying This Presentation

Applying This Presentation

- Next week you should:
  - Ownership: identify appropriate security personnel
  - Educate your team on OAuth
    - https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authorization-flows-part-1
    - Dr. Nestori Syynimaa: https://o365blog.com/post/phishing
    - See References slide at end for more links
  - Assess risk
    - Review critical cloud apps & data => tighten existing controls

Applying This Presentation

- Checklist: review current and future apps (internally or with vendors)
- Customize: update checklist by reviewing every app's admin controls

Identity Design		Auditing	
Oauth Use Is OAuth used? Is it the only option or 1 of many? Which flows? Documentation Scopes clearly documented? Vendor app ids documented? Approvals Are the approval screens clear? Is what is being asked clear to users? Application Identity Is the application's identity clearly described? Are vendor application ids clearly documented? Integration Is there a 3rd-party app ecosystem? With publicly documented APIs? Is there vendor verification? Are verified applications clearly shown in approval dialogs? Is there a directory of approved applications? Vendor websites? App ids?		Activities Authentication: failed logins? Authorization: are detailed OAuth protocol steps logged? e.g., token refreshes? Application: which application activities (events) are logged? Fields App ids? Scopes? Users? Location/IPs? OAuth URLs and parameters? Reporting Content: Which apps have been approved? By user? # Users? Timestamps? Sort/filters? Which scopes approved/granted? By user? # Users? Which resources granted access to? Aggregations: counts, top-N, grouping, distribution/breakdowns? Generation: Saved reports? Scheduled reports? Pushed? Notifications: Alerts? Criteria?	

Applying This Presentation

- Checklist: review current and future apps (internally or with vendors)
- Customize: update checklist by reviewing every app's admin controls

Prevention		Mitigation	
Timeouts What are the default timeouts for: GUI sessions, access tokens, refresh tokens? Can you change the timeouts for: GUI sessions, access tokens, refresh tokens? Access controls Can you restrict to admin only? allow users? admin approvals required? Application allow lists? deny lists? IP allow lists? Device endpoint requirements?		Revocation Can you revoke access tokens? Can you revoke refresh tokens? Can you revoke GUI sessions? Do you revoke using the Admin Console and/or API ?	
Detection			
Can you alert or take action on failed logins? Can you alert or take action on failed approvals? Any support for detecting compromised credentials?			

Applying This Presentation

- In the first 3 months following this presentation:
  - Inventory: create/update list of approved OAuth applications
  - Baseline OAuth activity
    - Collect OAuth audit logs
    - Baseline normal activity
    - Identify Top-N applications, permissions granted, users
  - Policies: review/refine/plan
    - Restrict device code authorization grants
    - Lockdown OAuth application approval policy

Applying This Presentation

- In the first 3 months following this presentation (cont.):
  - Prevent
    - Block device code URLs
    - Exceptions should be restricted with IP allow policies
    - Restrict OAuth application approval process
  - Detect
    - Update detections for failures with respect to IP allow lists
    - Create a behavioral detection plan to detect compromised credentials, suspicious application activity, and risk users based on their OAuth activities

Applying This Presentation

- In the first 3 months following this presentation (cont.):
  - Mitigate
    - Focus on temporary token behavior with all IAM vendors
    - Update playbooks for compromised OAuth credentials
    - Focus on and test revocation
    - Use any available controls that govern OAuth protocol behavior e.g., timeouts

Applying This Presentation

- Within 6 months, you should:
  - Analysis: implement a process to analyze OAuth risk
    - Start tracking high-risk users and applications, using top-N filters
    - Focus on abnormal changes / anomalies
  - Vendor roadmaps: discuss OAuth threats, vendor controls and solutions
  - Detection: advanced measures
    - IP allow list failures
    - Start tracking risky users based on their OAuth activities
    - Honey tokens
  - OAuth Threat Intel: catalog approved OAuth applications (client ids, expected URLs and HTTP traffic)

References

1.0 OAuth Attacks and Defense Measures

1.1 Introducing a new phishing technique for compromising Office 365 accounts: https://o365blog.com/post/phishing/#oauth-consent
1.2 New Phishing Attacks Exploiting OAuth Authorization Flows (Part 1): https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authorization-flows-part-1
1.3 New Phishing Attacks Exploiting OAuth Authorization Flows (Part 2): https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authentication-flows-part-2
1.4 New Phishing Attacks Exploiting OAuth Authorization Flows (Part 3): https://www.netskope.com/blog/new-phishing-attacks-exploiting-oauth-authentication-flows-part-3
1.5 GCP OAuth Token Hijacking in Google Cloud – Part 1: https://www.netskope.com/blog/gcp-oauth-token-hijacking-in-google-cloud-part-1
1.6 GCP OAuth Token Hijacking in Google Cloud—Part 2: https://www.netskope.com/blog/gcp-oauth-token-hijacking-in-google-cloud-part-2

2.0 Evolving Phishing Attacks

2.1 A Big Catch: Cloud Phishing from Google App Engine and Azure App Service: https://www.netskope.com/blog/a-big-catch-cloud-phishing-from-google-app-engine-and-azure-app-service
2.2 Microsoft Seizes Malicious Domains Used in Mass Office 365 Attacks: https://threatpost.com/microsoft-seizes-domains-office-365-phishing-scam/157261/
2.3 Phishing Attack Hijacks Office 365 Accounts Using OAuth Apps: https://www.bleepingcomputer.com/news/security/phishing-attack-hijacks-office-365-accounts-using-oauth-apps/
2.4 Office 365 Phishing Attack Leverages Real-Time Active Directory Validation: https://threatpost.com/office-365-phishing-attack-leverages-real-time-active-directory-validation/159188/
2.5 Demonstration - Illicit Consent Grant Attack in Azure AD: https://www.nixu.com/blog/demonstration-illicit-consent-grant-attack-azure-ad-office-365
https://securecloud.blog/2018/10/02/demonstration-illicit-consent-grant-attack-in-azure-ad-office-365/
2.6 Detection and Mitigation of Illicit Consent Grant Attacks in Azure AD: https://www.cloud-architekt.net/detection-and-mitigation-consent-grant-attacks-azuread/
2.7 HelSec Azure AD write-up: Phishing on Steroids with Azure AD Consent Extractor: https://securecloud.blog/2019/12/17/helsec-azure-ad-write-up-phishing-on-steroids-with-azure-ad-consent-extractor/
2.8 Pawn Storm Abuses OAuth In Social Engineering Attack: https://www.trendmicro.com/en_us/research/17/d/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks.html

3.0 OAuth Device Code Flow

3.1 OAuth 2.0 RFC: https://tools.ietf.org/html/rfc6749
3.2 OAuth 2.0 Device Authorization Grant RFC: https://datatracker.ietf.org/doc/html/rfc8628
3.3 OAuth 2.0 for TV and Limited-Input Device Applications: https://developers.google.com/identity/protocols/oauth2/limited-input-device
3.4 OAuth 2.0 Scopes for Google APIs: https://developers.google.com/identity/protocols/oauth2/scopes
3.5. Office Device Code Phishing: https://gist.github.com/Mr-Un1k0d3r/afef5a80cb72dfeaa78d14465fb0d333

RSAConference2022

Thank you

Jenko Hwong

Cloud Security Researcher
Netskope, Inc.
@jenkohwong