Synapse Bootcamp - Pre-Course Setup

Synapse Bootcamp - Pre-Course Setup **1**
Overview **2**
Setup Instructions **3**
Step 1 - Email account 4
Step 2 - Register for API Keys 4
LevelBlue Labs OTX 4
MalShare 9
MalwareBazaar (Abuse.ch) 10
VirusTotal 17
Optional Keys **22**

Overview

The following steps should be completed **BEFORE** attending Synapse Bootcamp!

Synapse includes **Power-Ups** that provide additional features and functionality. Many Power-Ups that import data from third-party sources, such as VirusTotal or AlienVault, require an API key.

This document walks you through the process of registering for and obtaining several **free** API keys that we will use to configure the Power-Ups used in Synapse Bootcamp.

The pre-course setup process will take approximately 30 - 60 minutes. Completing these steps **before** class allows us to spend time learning about Synapse and performing hands-on analysis instead of setup tasks.

If you have questions or need assistance with the setup process, please contact us at training@vertex.link.

Without the API keys, you will be unable to use the Power-Ups!
This may limit or prevent you from completing some lab exercises.

Setup Instructions

To register for the API keys used in this course you will need an email account.

You can:

- use an **existing** email account (work or personal), or
- create a **new** email account just for Bootcamp (i.e., using a free email service).

Either way, **you must be able to log in to the email account** to receive confirmation emails from the various services. You must use the confirmation messages to activate your service accounts and obtain your API keys.

Note: Abuse.ch (MalwareBazaar) only supports OAuth authentication. You will need one of the following accounts to log in to MalwareBazaar and create your API key:

- Google (e.g., Gmail)
- X (Twitter)
- LinkedIn
- Github

If you do not want to use an existing personal or professional account, you can create one (e.g., a Gmail account) specifically for use in Bootcamp.

As you work through this setup process, **be sure to record the following.** You'll want to have this information readily accessible for Synapse Bootcamp:

- The email account you use, and its associated password.
- The username / password used to set up **each** free account with the third-party vendors / services below.
  - You will need to log in to each service to obtain your API key.
- The API key associated with each service.
  - Some services may require a second piece of data, such as a secret.
- **Protip:** If you have one, a password manager allows you to keep all of your account information in one location for both security and ease of access.

You will need to copy / paste your API keys during class to configure and use the Synapse Power-Ups.

Step 1 - Email account

Have the email account you will use to register for your API keys ready before you begin. You can use an existing account or create a new one to use for this class.

Step 2 - Register for API Keys

Note: If you have existing API keys for any of the following services, you may use those keys instead of registering for new ones. However, API keys may vary as to the API version or specific API endpoints they can access, quota limits, etc. **Pre-existing keys are not guaranteed** to be compatible with the hands-on exercises in Synapse Bootcamp.

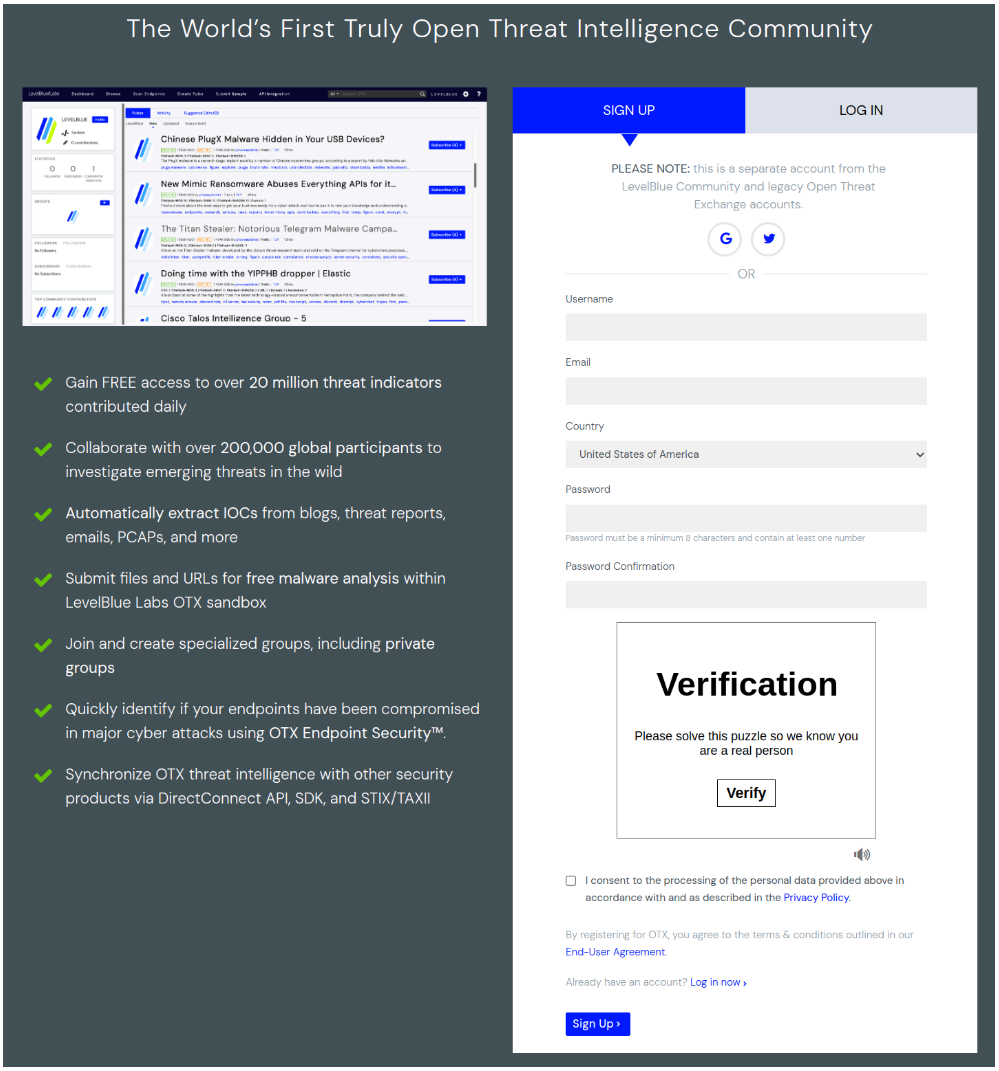
- AlienVault OTX
- MalShare
- MalwareBazaar (Abuse.ch)
- VirusTotal
- Optional Keys

LevelBlue Labs OTX

LevelBlue Labs Open Threat Exchange (OTX) (formerly AlienVault OTX) is a free resource for sharing threat data. OTX "delivers community-generated threat data, enables collaborative research, and automates the process of updating your security infrastructure with threat data from any source". (https://levelblue.com/open-threat-exchange).

Registration Link: https://otx.alienvault.com/

1. Use the **registration link** above to sign up for an LevelBlue/AlienVault account:



The World's First Truly Open Threat Intelligence Community

Chinese PlugX Malware Hidden in Your USB Devices?

New Mimic Ransomware Abuses Everything APIs for it...

The Titan Stealer: Notorious Telegram Malware Campa...

Doing time with the YIPPHB dropper | Elastic

Cisco Talos Intelligence Group – 5

- ✓ Gain FREE access to over **20 million threat indicators** contributed daily
- ✓ Collaborate with over **200,000 global participants** to investigate emerging threats in the wild
- ✓ **Automatically extract IOCs** from blogs, threat reports, emails, PCAPs, and more
- ✓ Submit files and URLs for **free malware analysis** within LevelBlue Labs OTX sandbox
- ✓ Join and create specialized groups, including **private groups**
- ✓ Quickly identify if your endpoints have been compromised in major cyber attacks using **OTX Endpoint Security™**.
- ✓ Synchronize OTX threat intelligence with other security products via DirectConnect API, SDK, and STIX/TAXII

PLEASE NOTE: this is a separate account from the LevelBlue Community and legacy Open Threat Exchange accounts.

Username

Email

Country

United States of America

Password

Password must be a minimum 8 characters and contain at least one number

Password Confirmation

Verification

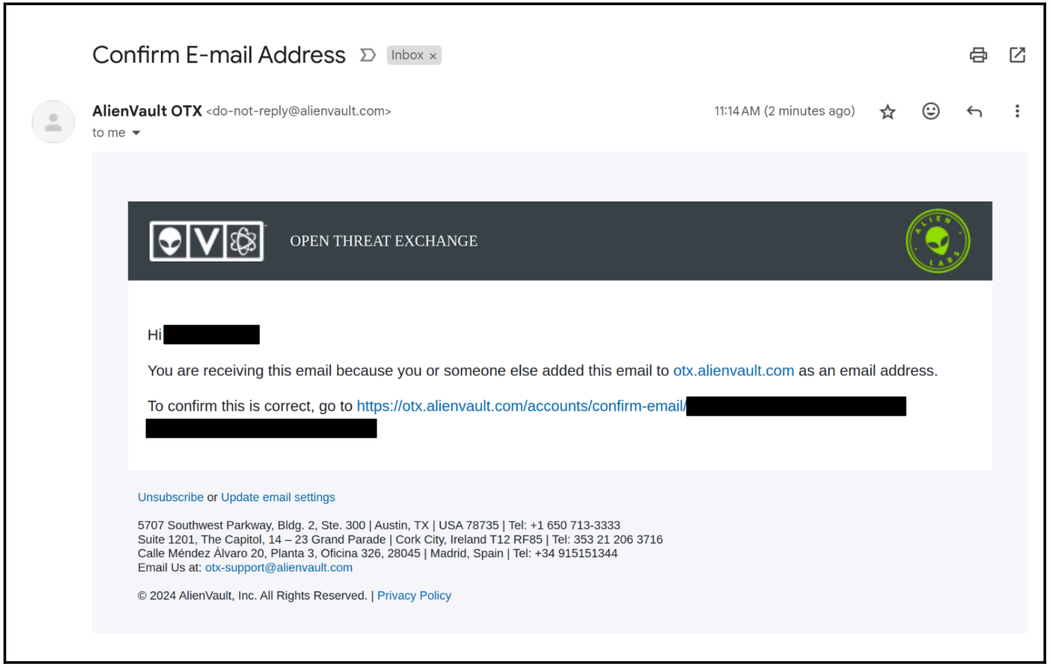
Please solve this puzzle so we know you are a real person

□ I consent to the processing of the personal data provided above in accordance with and as described in the Privacy Policy.

By registering for OTX, you agree to the terms & conditions outlined in our End-User Agreement.

Already have an account? Log in now ›

2. You will receive a **confirmation email**. Click the link in the email to go to the account confirmation page:



Confirm E-mail Address

AlienVault OTX <do-not-reply@alienvault.com>
to me

11:14 AM (2 minutes ago)

Hi [redacted]

You are receiving this email because you or someone else added this email to otx.alienvault.com as an email address.

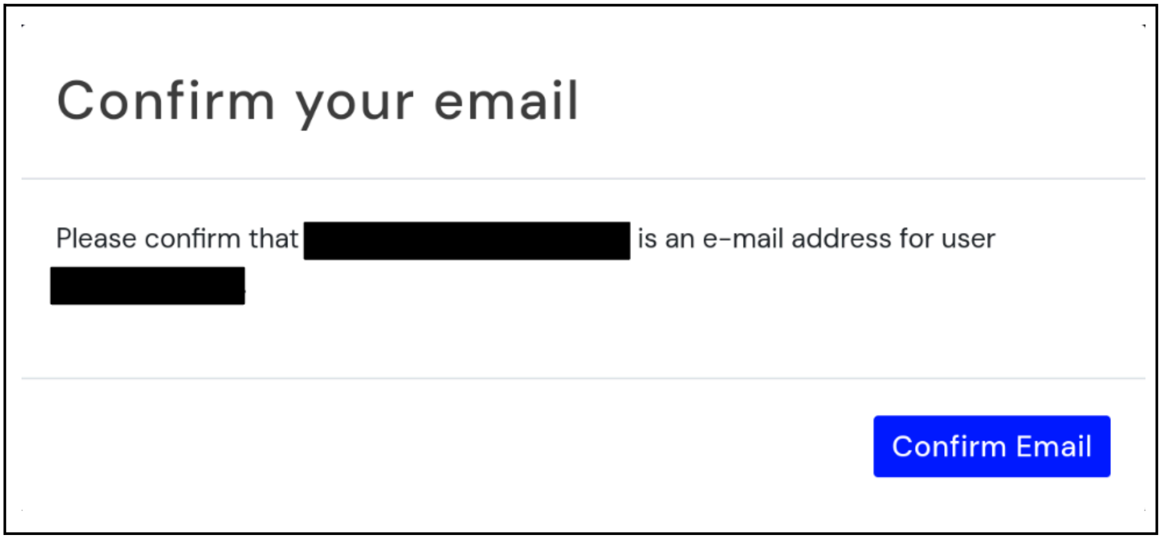
To confirm this is correct, go to https://otx.alienvault.com/accounts/confirm-email/[redacted]

Unsubscribe or Update email settings

5707 Southwest Parkway, Bldg. 2, Ste. 300 | Austin, TX | USA 78735 | Tel: +1 650 713-3333
Suite 1201, The Capitol, 14 – 23 Grand Parade | Cork City, Ireland T12 RF85 | Tel: 353 21 206 3716
Calle Méndez Álvaro 20, Planta 3, Oficina 326, 28045 | Madrid, Spain | Tel: +34 915151344
Email Us at: otx-support@alienvault.com

© 2024 AlienVault, Inc. All Rights Reserved. | Privacy Policy

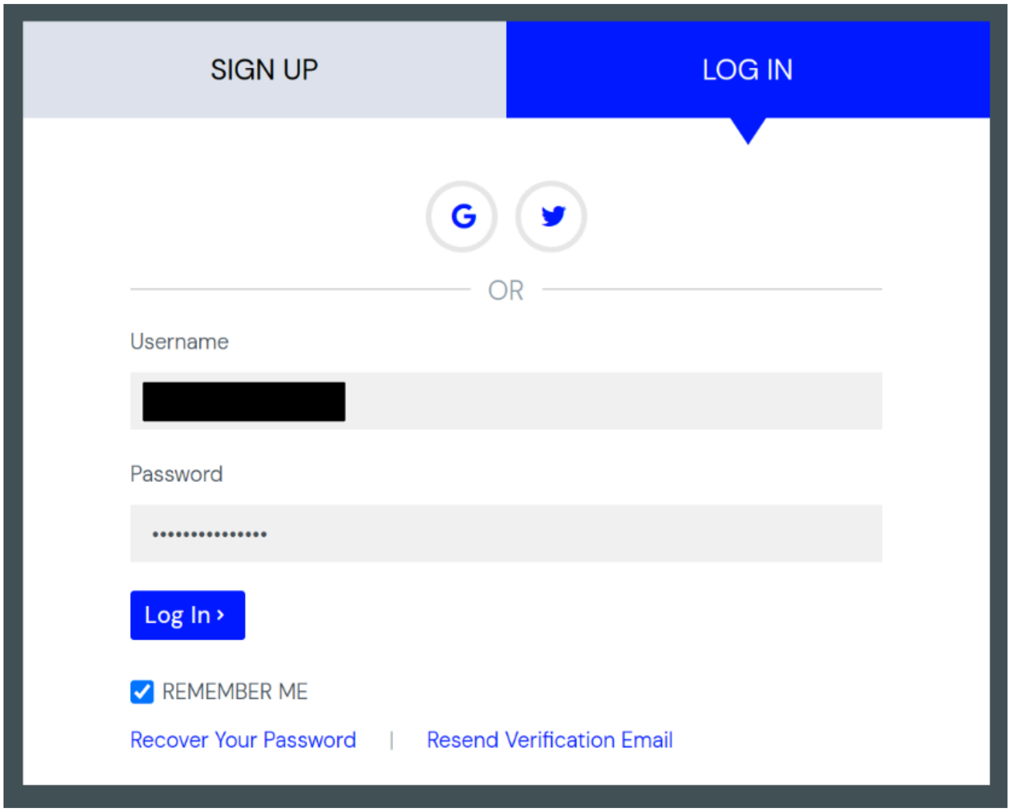
3. Click the **Confirm Email** button to confirm and activate your account:



Confirm your email

Please confirm that [redacted] is an e-mail address for user [redacted]

4. Once you confirm your email, you should be returned to the LevelBlue signup / login page. Click the LOG IN tab to sign in to LevelBlue:



Username

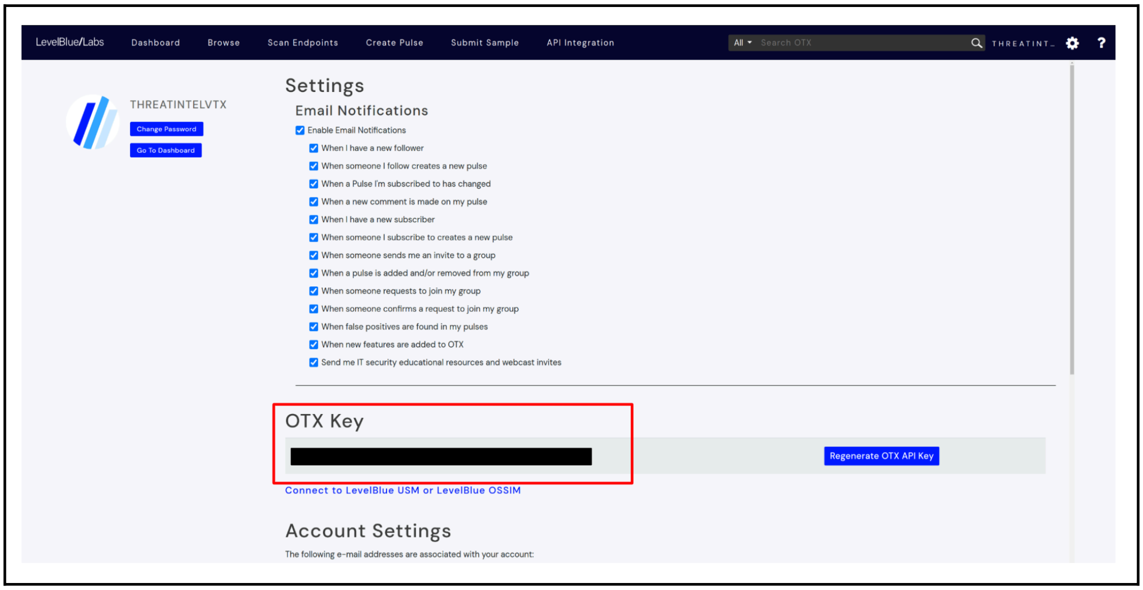
[redacted]

Password

•••••••••••••••

☑ REMEMBER ME

5. The first time you log in, you should be taken to the "Settings" page. Your OTX key is available here:



Settings

Email Notifications

☑ Enable Email Notifications

- ☑ When I have a new follower
- ☑ When someone I follow creates a new pulse
- ☑ When a Pulse I'm subscribed to has changed
- ☑ When a new comment is made on my pulse
- ☑ When I have a new subscriber
- ☑ When someone I subscribe to creates a new pulse
- ☑ When someone sends me an invite to a group
- ☑ When a pulse is added and/or removed from my group
- ☑ When someone requests to join my group
- ☑ When someone confirms a request to join my group
- ☑ When false positives are found in my pulses
- ☑ When new features are added to OTX
- ☑ Send me IT security educational resources and webcast invites

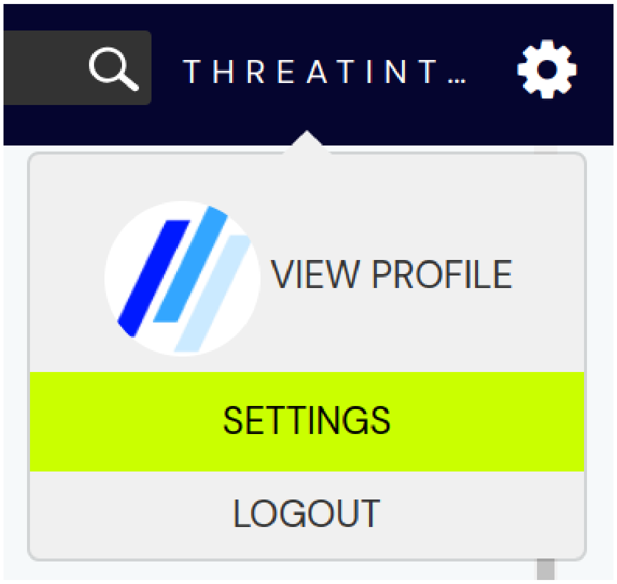
OTX Key

[redacted]

Account Settings

The following e-mail addresses are associated with your account:

6. You can access your settings / key at any time using the menu in the upper right of the screen:

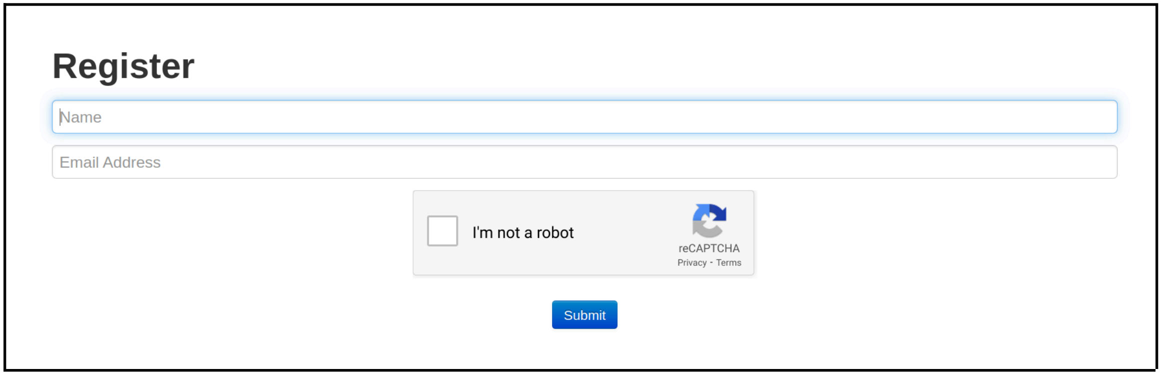


MalShare

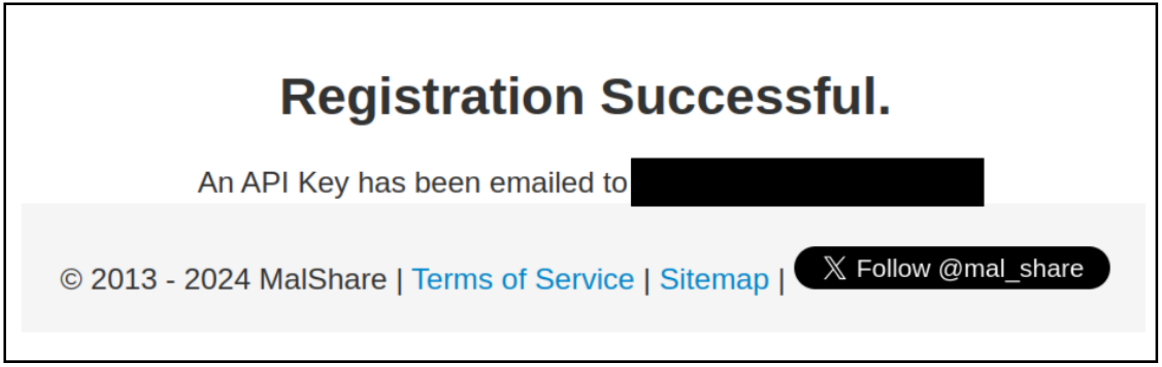
MalShare is "...a collaborative effort to create a community driven public malware repository that works to build additional tools to benefit the security community at large." (https://malshare.com/about.php). MalShare allows you to download metadata about samples as well as actual files.

Registration link: https://malshare.com/register.php

1. Use the **registration link** above to sign up for a MalShare account:



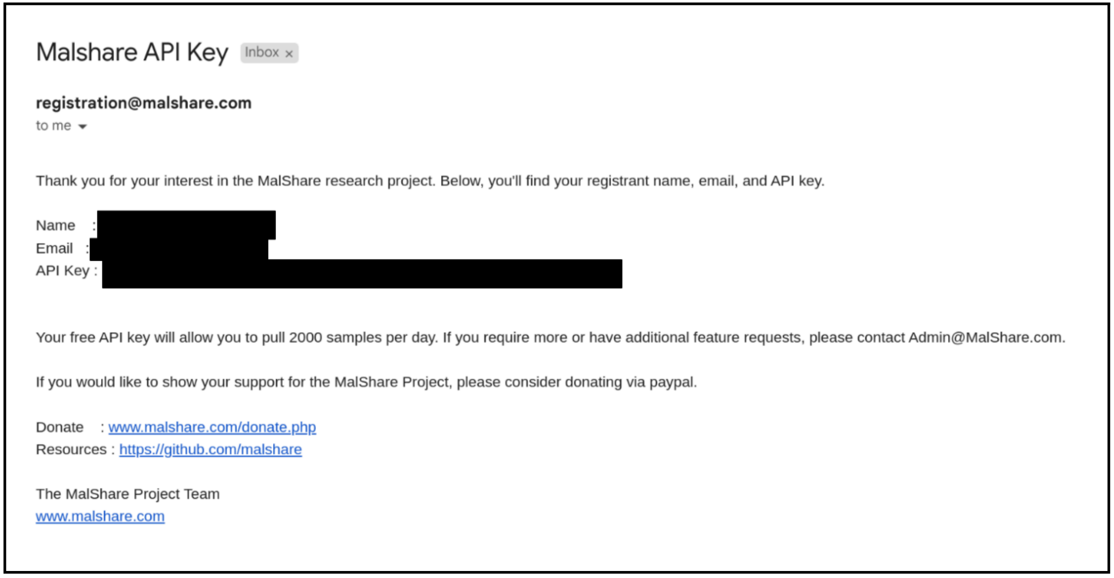
2. You should see a confirmation message after you register:



Registration Successful.

An API Key has been emailed to [redacted]

3. MalShare will **email** you an API key:



Malshare API Key

registration@malshare.com
to me

Thank you for your interest in the MalShare research project. Below, you'll find your registrant name, email, and API key.

Name : [redacted]
Email : [redacted]
API Key : [redacted]

Your free API key will allow you to pull 2000 samples per day. If you require more or have additional feature requests, please contact Admin@MalShare.com.

If you would like to show your support for the MalShare Project, please consider donating via paypal.

Donate : www.malshare.com/donate.php
Resources : https://github.com/malshare

The MalShare Project Team
www.malshare.com

4. Your API key serves as your login credential to access your MalShare account via their website.

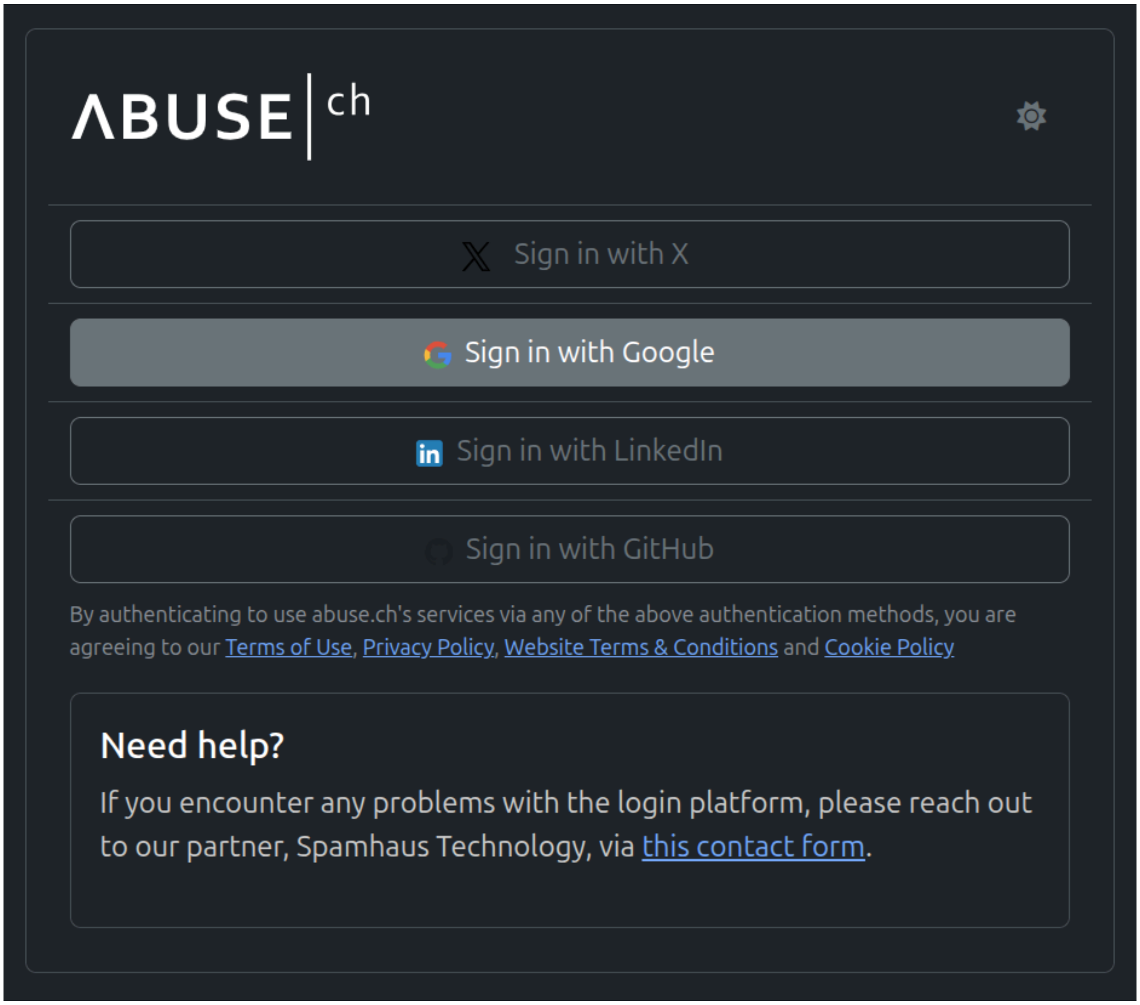
MalwareBazaar (Abuse.ch)

Abuse.ch partners with Spamhaus to "provide the largest, independently crowdsourced intelligence of tracked malware and botnets to the industry". Their offerings include MalwareBazaar, a platform "dedicated to sharing malware samples with the infosec community, antivirus vendors, and threat intelligence providers" (https://bazaar.abuse.ch/).

Note: MalwareBazaar / Abuse.ch uses OAuth authentication. You need an existing Google, X, LinkedIn, or Github account to log in to MalwareBazaar.

Registration link: https://auth.abuse.ch/

1. Use the **registration link** above to select the account to use for OAuth authentication to MalwareBazaar:



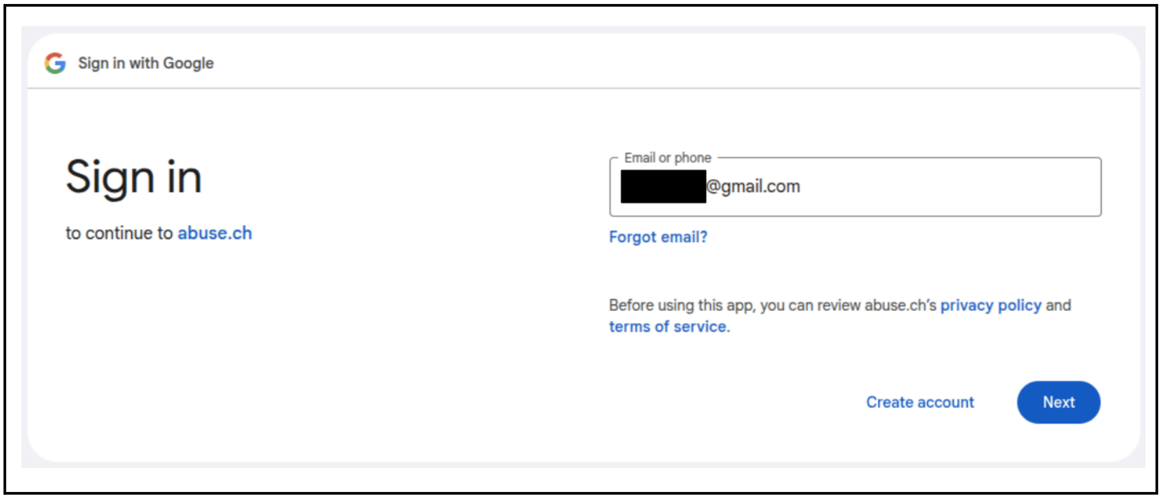
By authenticating to use abuse.ch's services via any of the above authentication methods, you are agreeing to our Terms of Use, Privacy Policy, Website Terms & Conditions and Cookie Policy

Need help?

If you encounter any problems with the login platform, please reach out to our partner, Spamhaus Technology, via this contact form.

(We will use **Google** as our example.)

2. Enter the Gmail address to use and click **Next:**



Sign in with Google

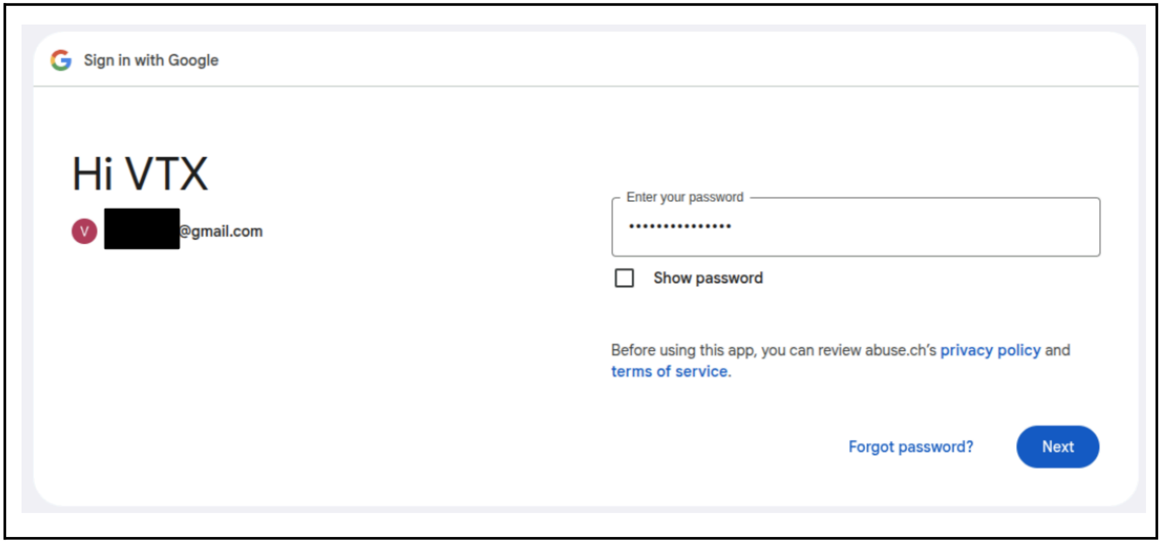
Sign in

to continue to abuse.ch

Email or phone: [redacted]@gmail.com

Before using this app, you can review abuse.ch's privacy policy and terms of service.

3. Enter the password for your Gmail account and click **Next:**



Sign in with Google

Hi VTX

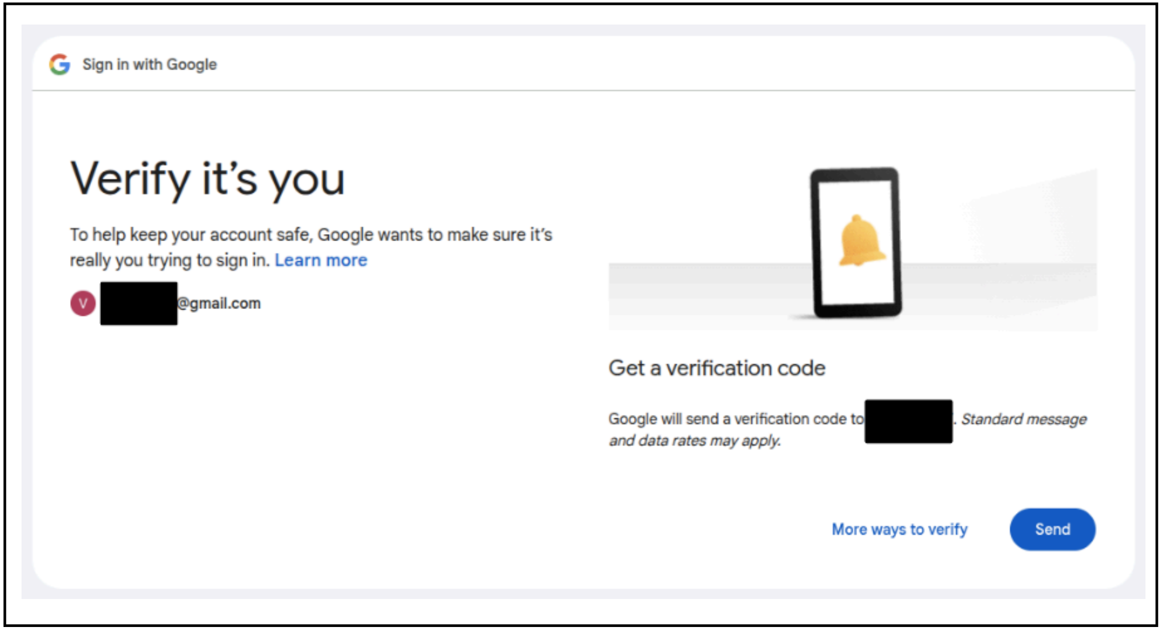
V [redacted]@gmail.com

Enter your password: •••••••••••••••

□ Show password

Before using this app, you can review abuse.ch's privacy policy and terms of service.

4. If you are prompted to verify your identity, click **Send** to have a one-time code sent to the mobile device associated with your Google account:



Sign in with Google

Verify it’s you

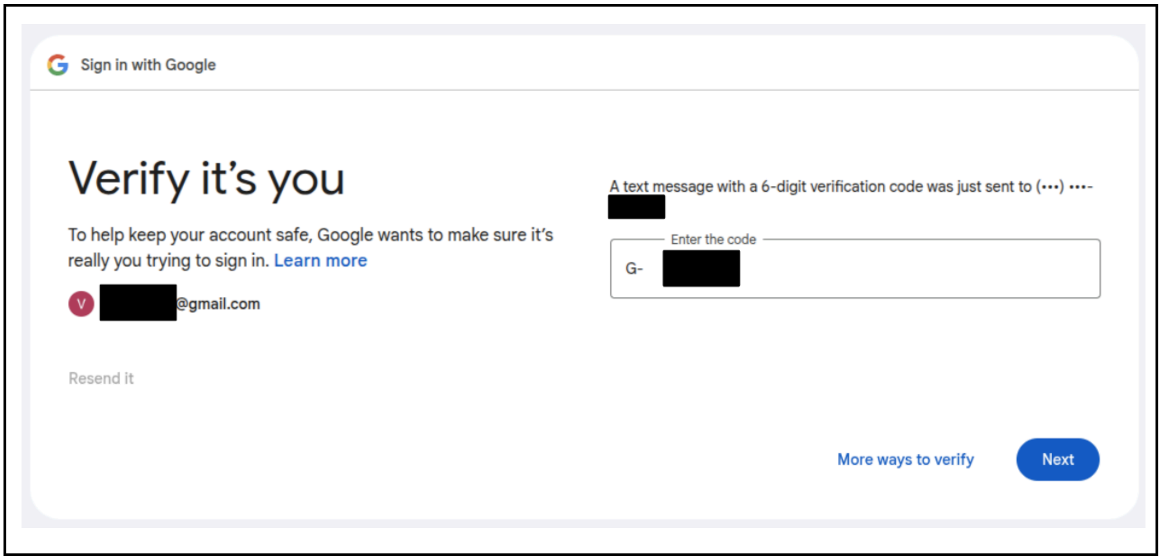
To help keep your account safe, Google wants to make sure it’s really you trying to sign in. Learn more

V [redacted]@gmail.com

Get a verification code

Google will send a verification code to [redacted]. *Standard message and data rates may apply.*

5. Enter your verification code and click **Next:**



Sign in with Google

Verify it’s you

To help keep your account safe, Google wants to make sure it’s really you trying to sign in. Learn more

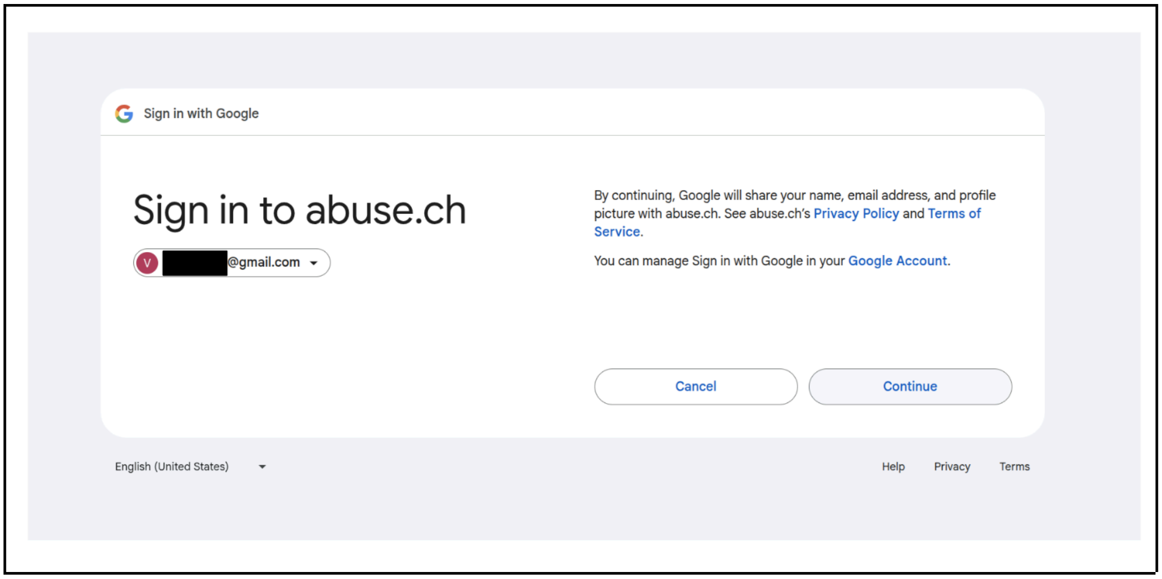
V [redacted]@gmail.com

A text message with a 6-digit verification code was just sent to (•••) •••-[redacted]

Enter the code: G-[redacted]

Resend it

6. Review the information that will be shared with Abuse.ch and click **Continue:**



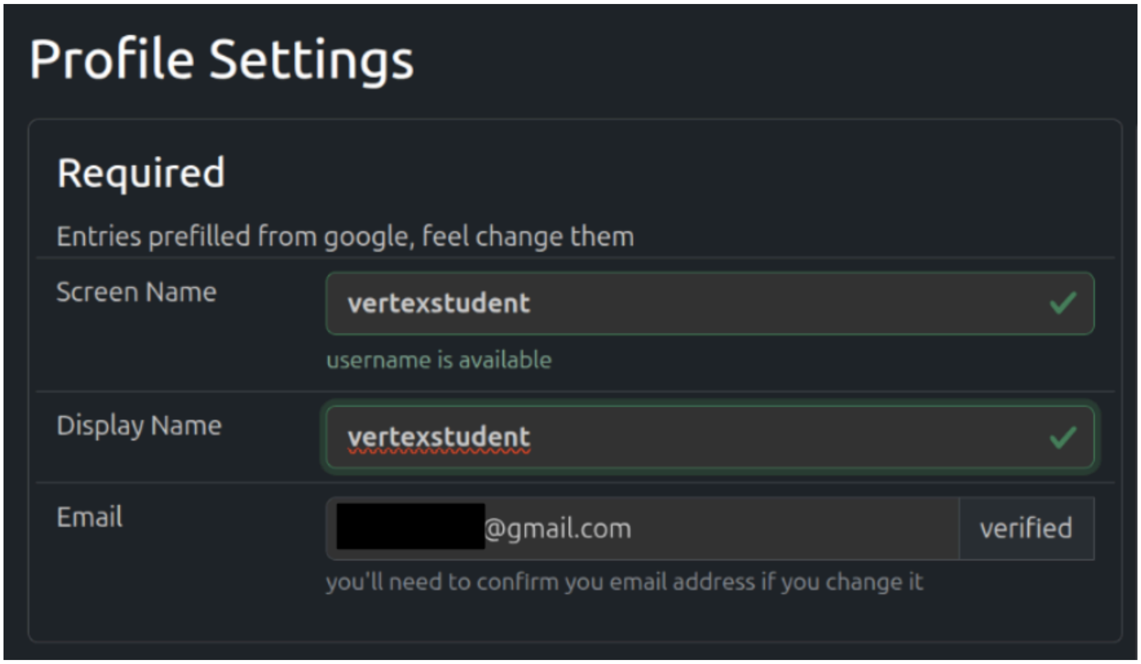
Sign in to abuse.ch

[redacted]@gmail.com

By continuing, Google will share your name, email address, and profile picture with abuse.ch. See abuse.ch's Privacy Policy and Terms of Service.

You can manage Sign in with Google in your Google Account.

7. You will be redirected to the Abuse.ch profile page. Under **Profile Settings > Required,** specify a Screen Name and Display Name:



Profile Settings

Required

Entries prefilled from google, feel change them

Screen Name: vertexstudent ✓

username is available

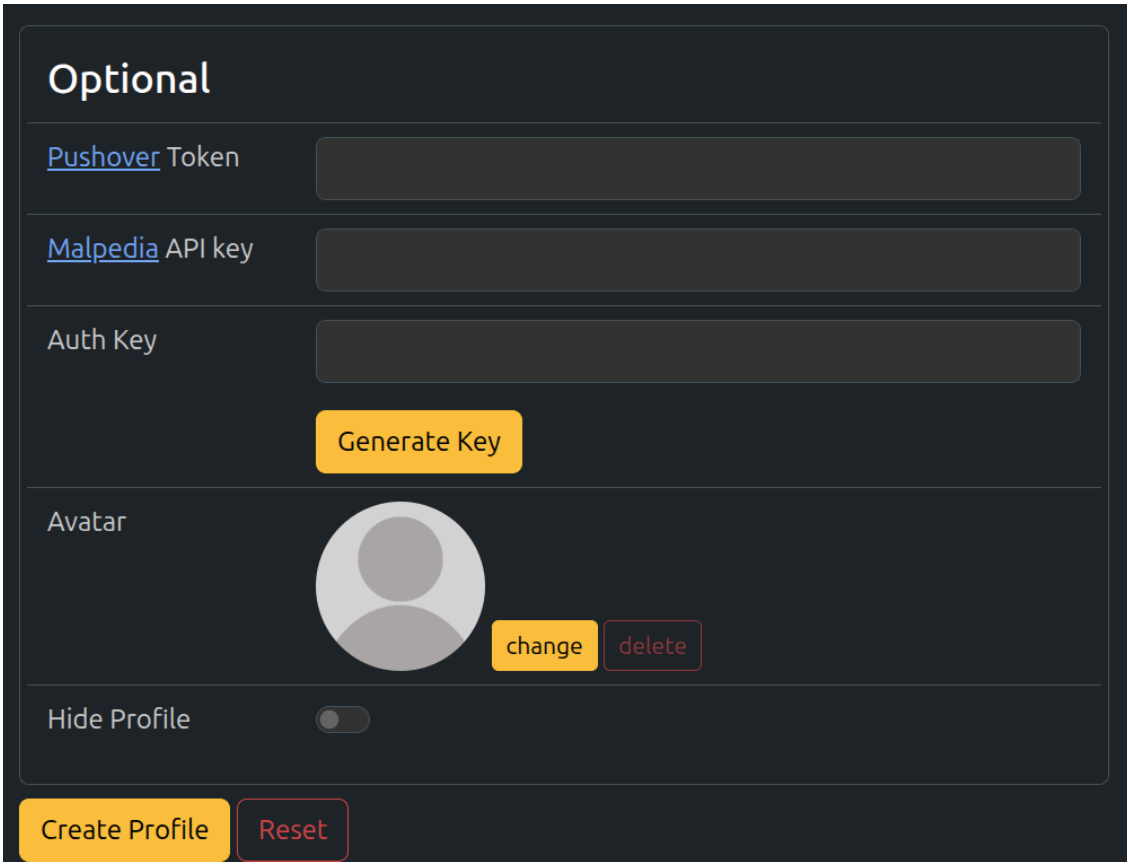
Display Name: vertexstudent ✓

Email: [redacted]@gmail.com verified

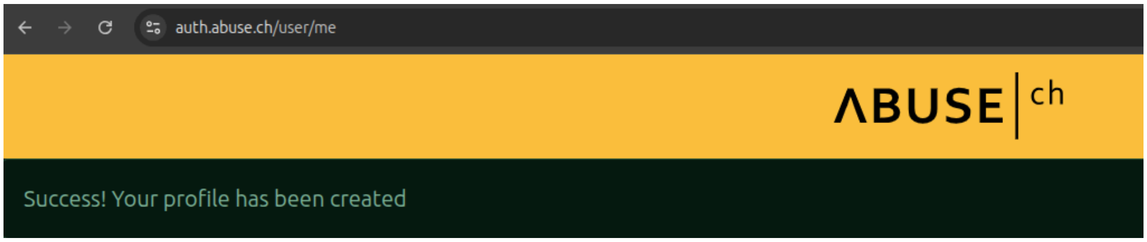
you'll need to confirm you email address if you change it

Note: make up your own name, we already used "vertexstudent"!

8. Under **Profile Settings > Optional**, review the settings and make any changes, if needed. (**Note:** you cannot generate an Auth Key until after your account is created, so ignore the "Generate Key" option.) Click **Create Profile** to create your account:

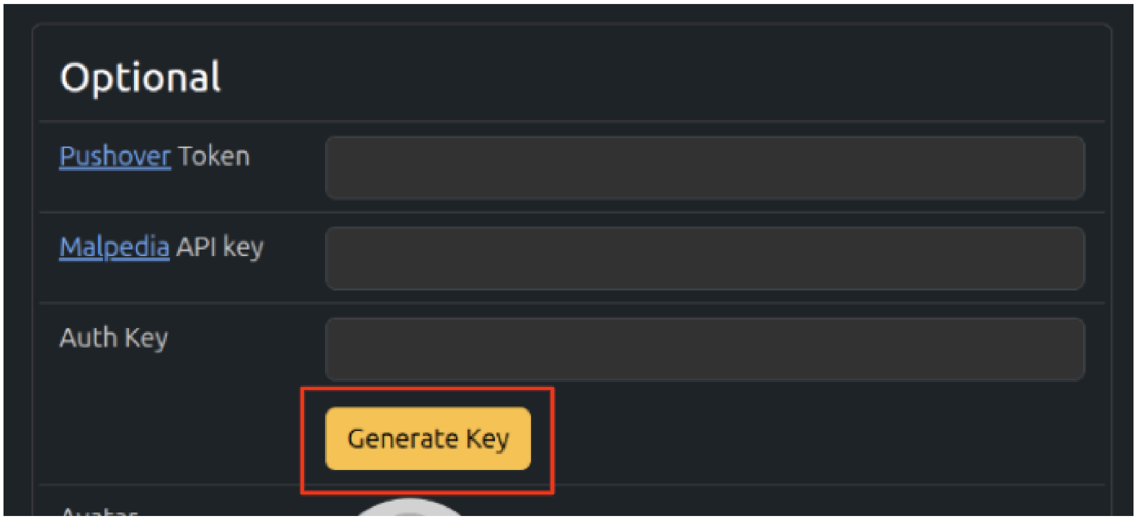


9. You should see a "Success" message at the top of the webpage indicating your profile has been created:

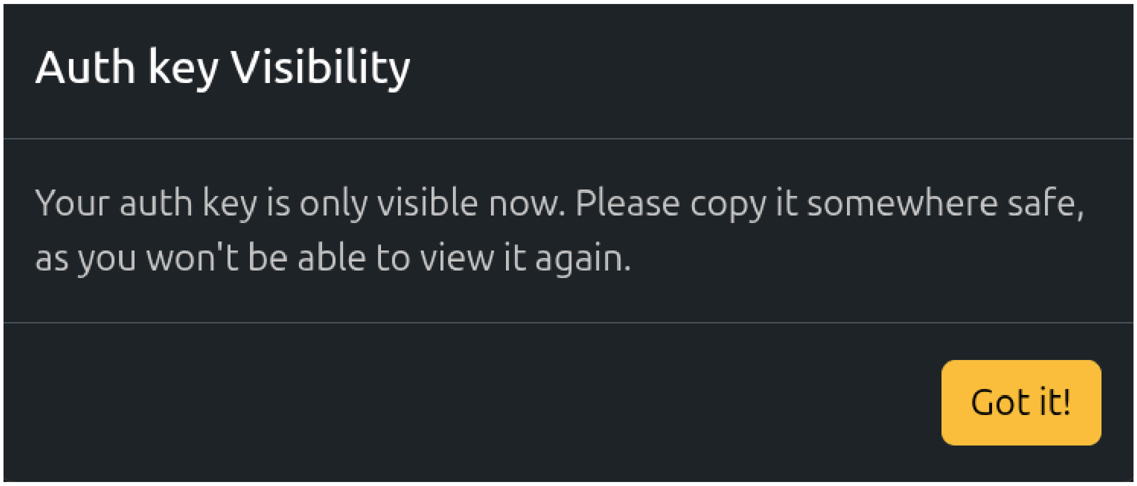


Success! Your profile has been created

10. After your account has been created, click the **Generate Key** button under the **Optional** settings:



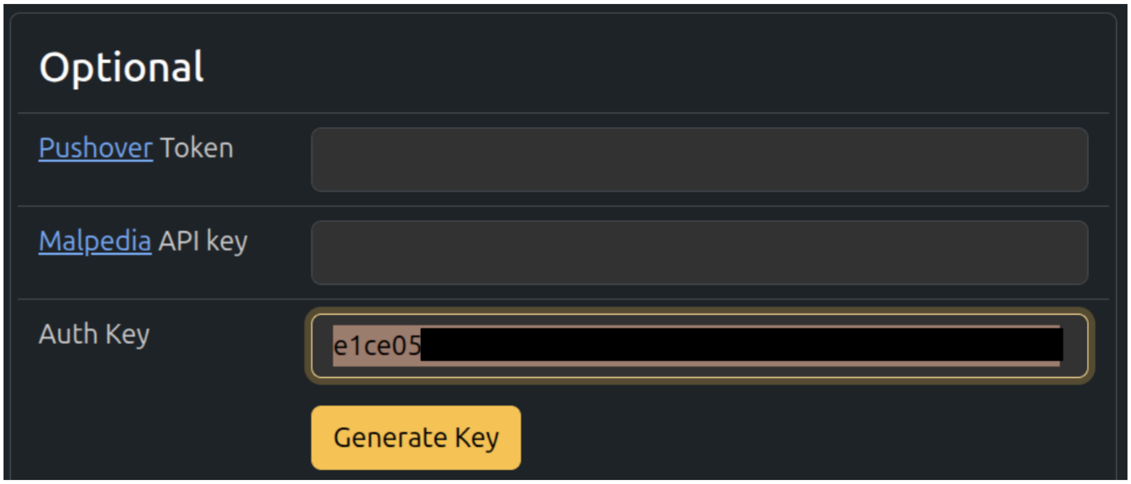
11. You will see a pop–up warning that your auth key is only visible now. Click **Got it!** to acknowledge the message:



Auth key Visibility

Your auth key is only visible now. Please copy it somewhere safe, as you won't be able to view it again.

12. **Highlight** and **copy** your key. Store it in a safe location for use in Synapse Bootcamp:



Optional

Pushover Token

Malpedia API key

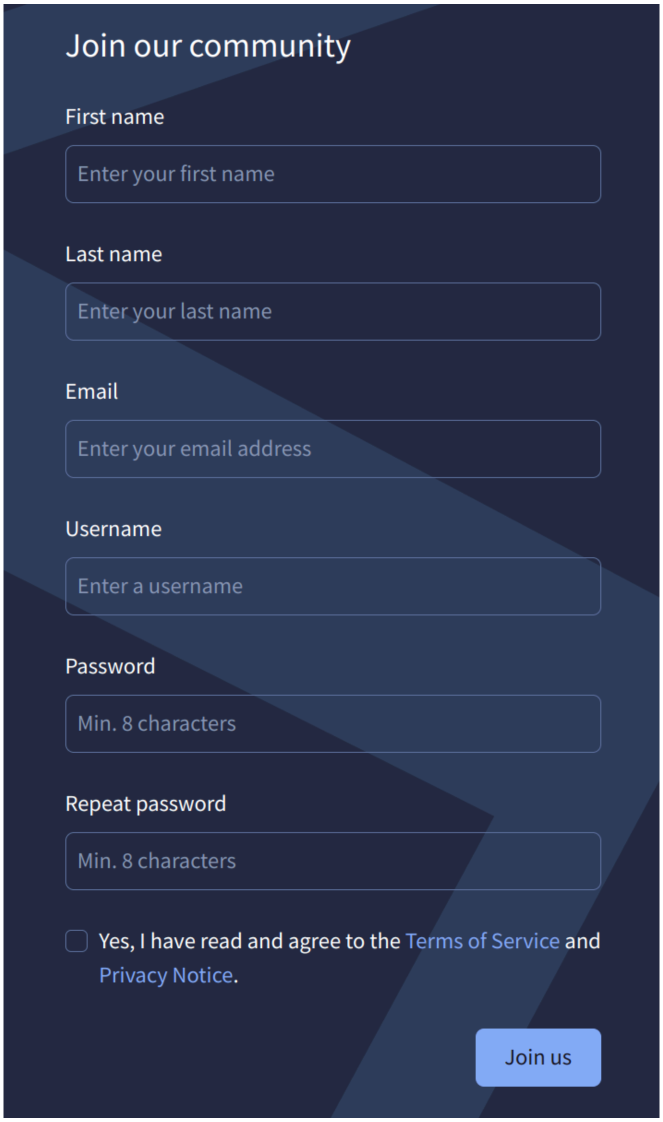
Auth Key: e1ce05[redacted]

VirusTotal

VirusTotal "inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content" (https://docs.virustotal.com/docs/how-it-works). VirusTotal offers a number of ways to query potentially malicious files, domains, IP addresses, and URLs.

Registration link: https://www.virustotal.com/gui/join-us

1. Use the **registration link** above to sign up for a VirusTotal Community account:



Join our community

First name

Enter your first name

Last name

Enter your last name

Email

Enter your email address

Username

Enter a username

Password

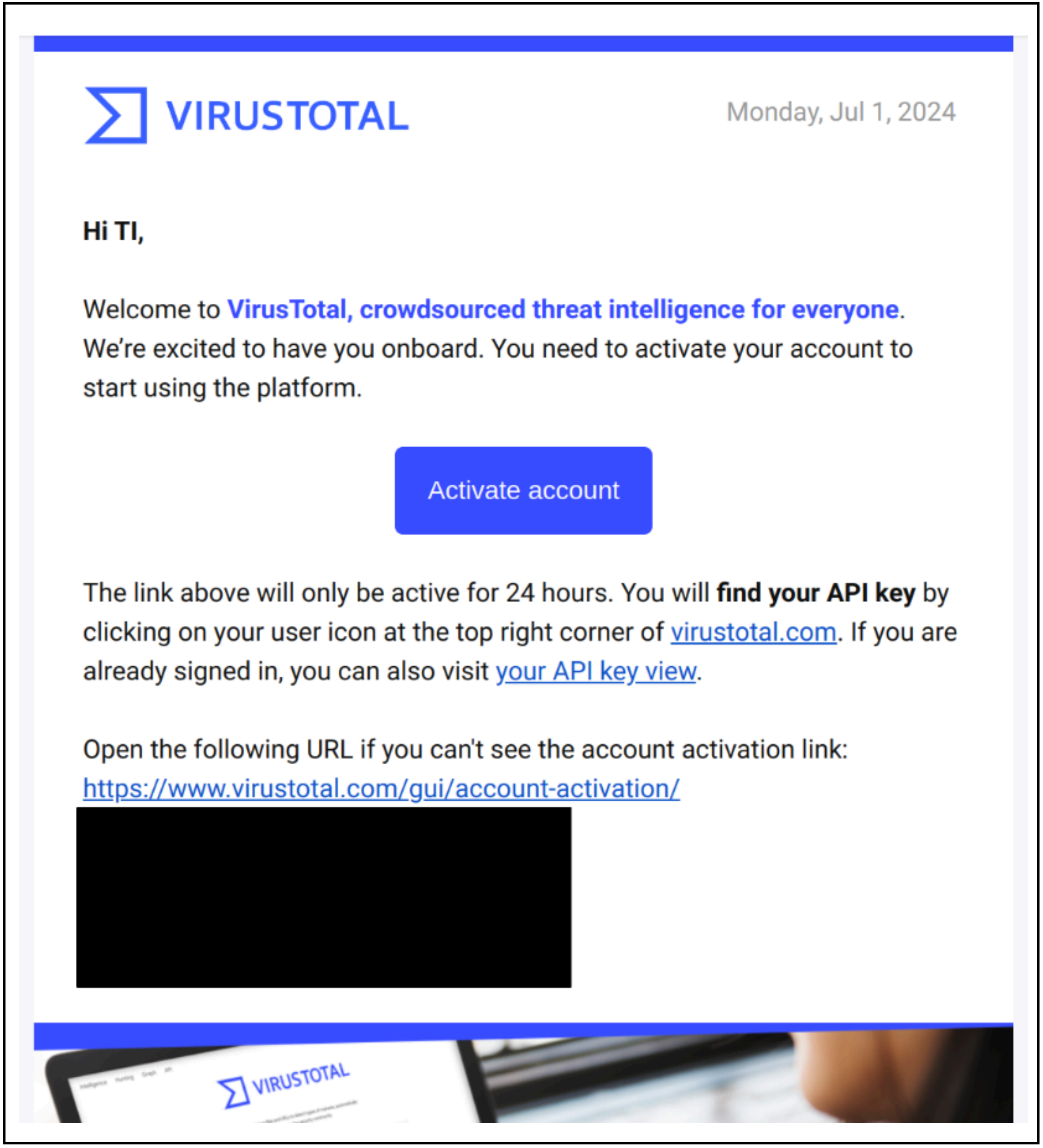
Min. 8 characters

Repeat password

Min. 8 characters

□ Yes, I have read and agree to the Terms of Service and Privacy Notice.

2. VirusTotal will send you a **confirmation email**. Click the **Activate account** button (or the link) in the email to confirm and activate your account:



VIRUSTOTAL

Monday, Jul 1, 2024

Hi TI,

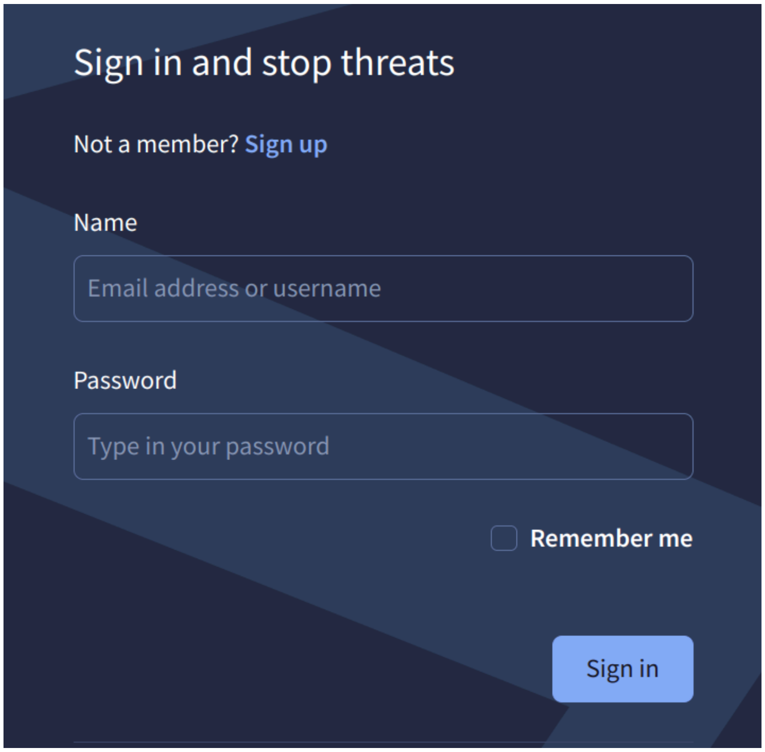
Welcome to **VirusTotal, crowdsourced threat intelligence for everyone**. We're excited to have you onboard. You need to activate your account to start using the platform.

The link above will only be active for 24 hours. You will **find your API key** by clicking on your user icon at the top right corner of virustotal.com. If you are already signed in, you can also visit your API key view.

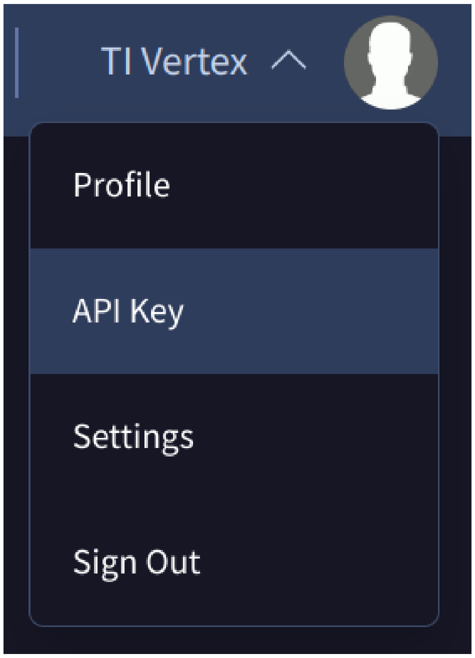
Open the following URL if you can't see the account activation link:
https://www.virustotal.com/gui/account-activation/

[redacted]

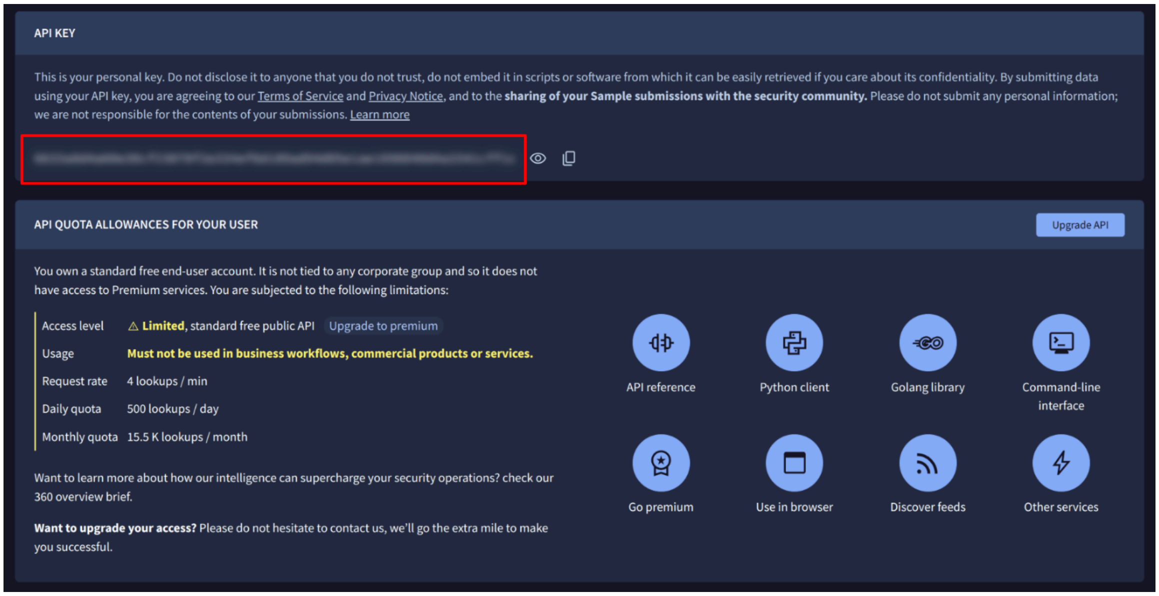
3. Once you have activated your account, use the **Sign in** link to log in to VirusTotal:



4. After you log in, access your **API Key** information from your account settings in the upper right corner of your browser:



5. Your API key and quota information can be found at that link:



API KEY

This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submissions with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submissions. Learn more

[redacted]

API QUOTA ALLOWANCES FOR YOUR USER

You own a standard free end-user account. It is not tied to any corporate group and so it does not have access to Premium services. You are subjected to the following limitations:

Access level	⚠ **Limited**, standard free public API Upgrade to premium
Usage	**Must not be used in business workflows, commercial products or services.**
Request rate	4 lookups / min
Daily quota	500 lookups / day
Monthly quota	15.5 K lookups / month

Want to learn more about how our intelligence can supercharge your security operations? check our 360 overview brief.

Want to upgrade your access? Please do not hesitate to contact us, we'll go the extra mile to make you successful.

Optional Keys

You can **optionally** register for free API keys from the following additional services in order to leverage these Synapse Power-Ups during (or after!) the course.

If you have **existing** keys for any of these services, you may use them.

These API keys are **not required** for Synapse Bootcamp, and we will **not** cover registering for, configuring, or using these services in class. However, the Power-Ups are available to you through the demo instance of Synapse you will receive for the course. If you want to test them out, you can!

Company / Service	Account Registration Site
Apollo (business and contact data)	https://www.apollo.io/signup/
Github (Personal access token) (retrieve and model information related to Github repositories and issues)	https://github.com/signup (Once registered, log into your account and select **settings > Developer settings,** and create a **Personal access token** using **Tokens (classic)**)
GreyNoise (Community API) (distinguish irrelevant or benign network activity from potentially malicious activity)	https://viz.greynoise.io/auth-required
HybridAnalysis (static and dynamic malware data)	https://hybrid-analysis.com/signup
SSLMate CertSpotter (SSL transparency data)	https://sslmate.com/signup?for=ct_search_api
URLScan (scan / obtain scans of URLs, associated files, etc.)	https://urlscan.io/user/signup