

Synapse Bootcamp - Pre-Course Setup

Synapse Bootcamp - Pre-Course Setup	1
Overview	2
Setup Instructions	3
Step 1 - Email account	3
Step 2 - Register for API Keys	4
LevelBlue Labs OTX	4
MalShare	9
VirusTotal	10
Optional Keys	15

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.

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](#)
- [VirusTotal](#)
- [Optional Keys](#)

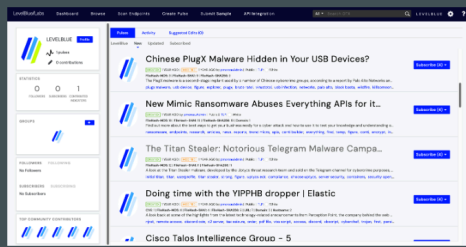
LevelBlue Labs OTX

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://cybersecurity.att.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



- ✔ 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

SIGN UP
LOG IN

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

OR

Username

Email

Country

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

Verify

🔊

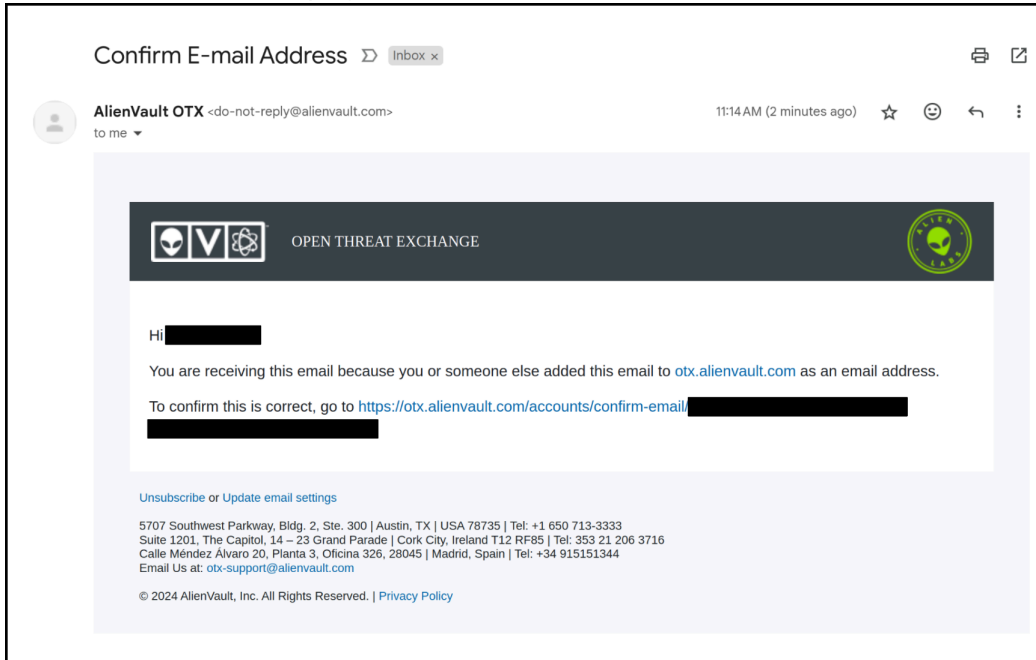
I consent to the processing of the personal data provided above in accordance with and as described in the [Privacy Policy](#).

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

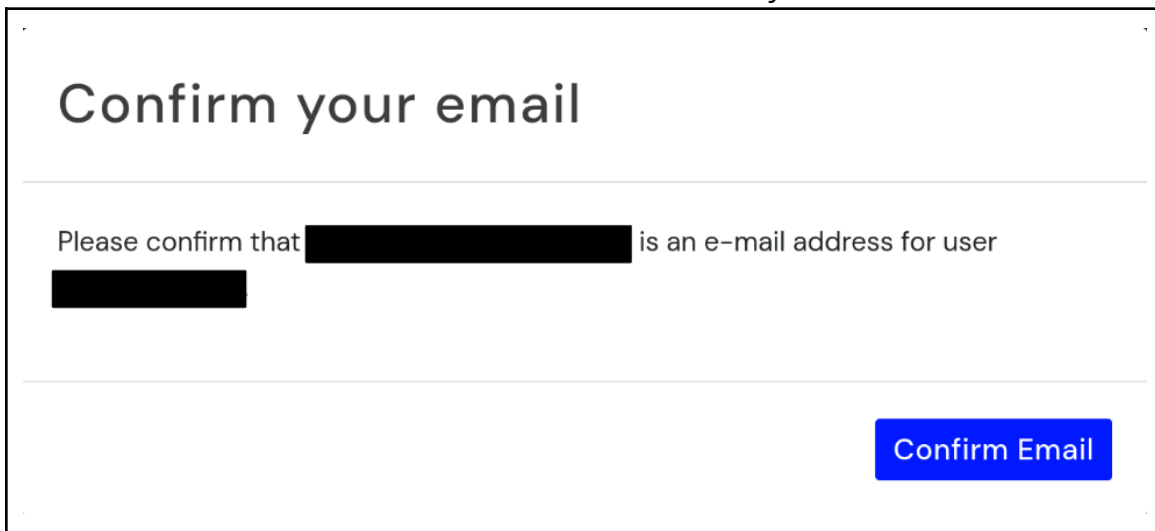
Already have an account? [Log in now](#)

Sign Up

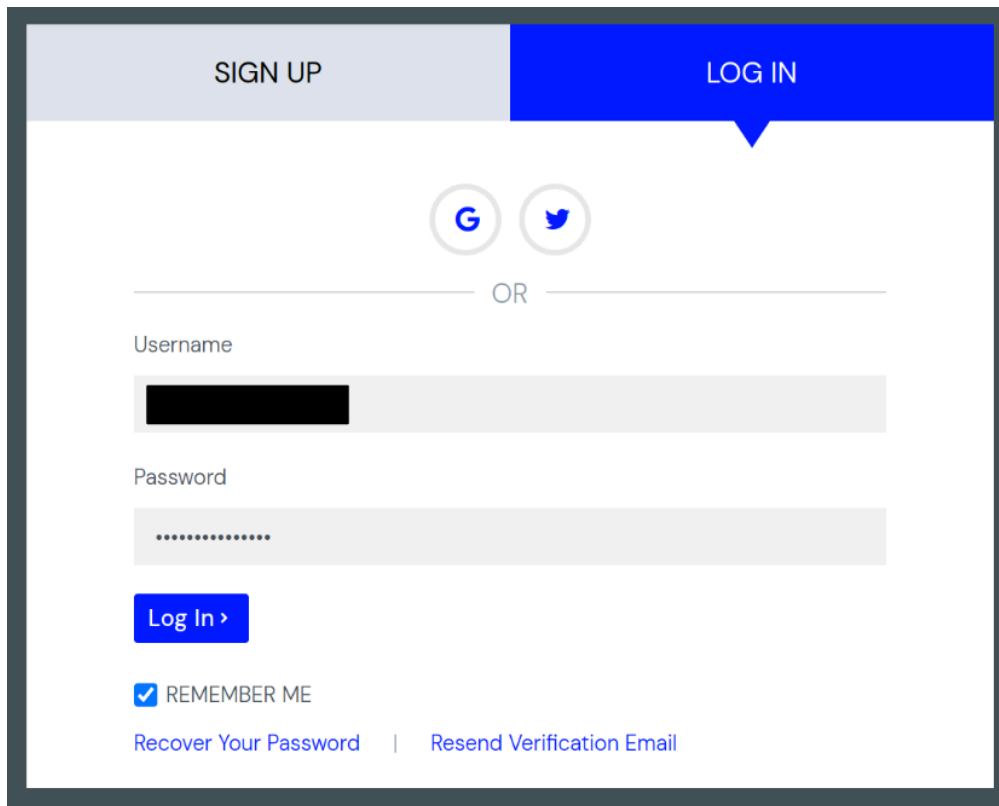
2. You will receive a **confirmation email**. Click the link in the email to go to the account confirmation page:



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

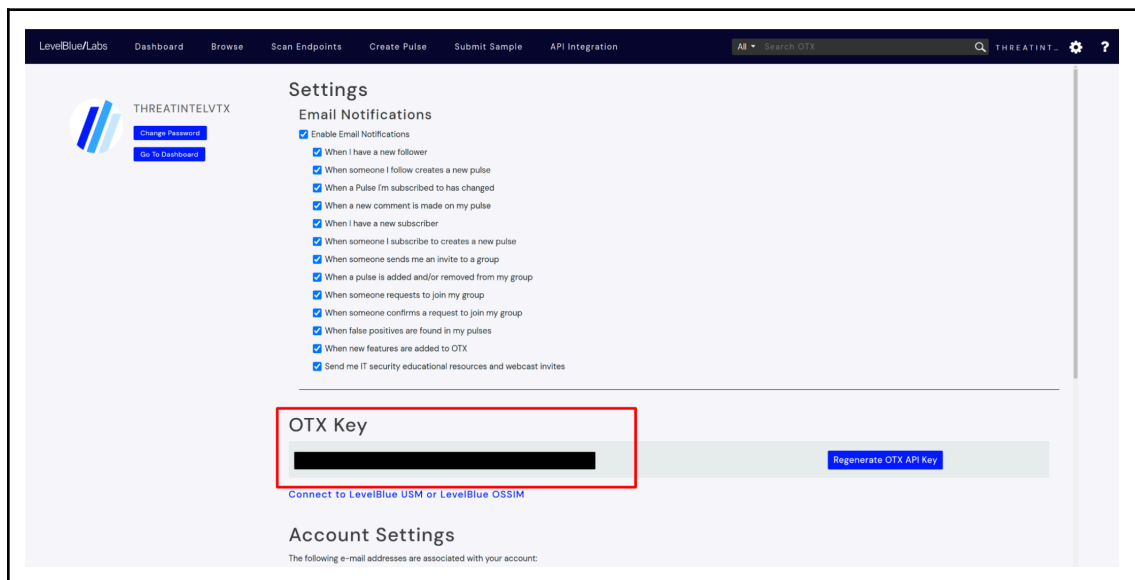


- Once you confirm your email, you should be returned to the LevelBlue signup / login page. Click the LOG IN tab to sign in to LevelBlue:



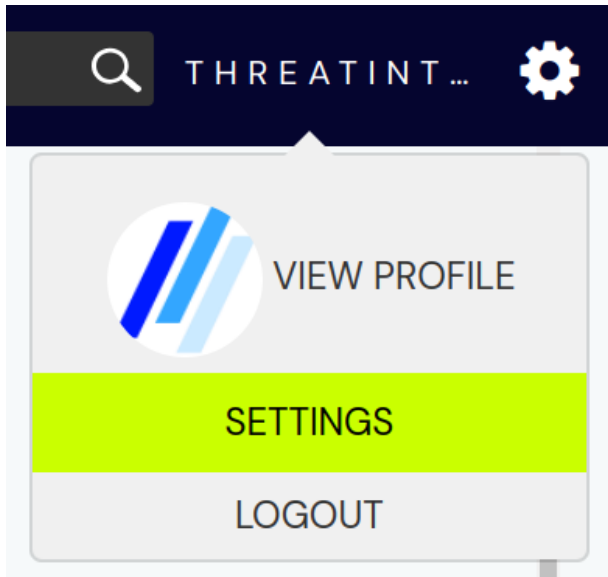
The screenshot shows the LevelBlue login page. At the top, there are two tabs: "SIGN UP" (grey) and "LOG IN" (blue). Below the tabs are social media login options for Google and Twitter. A horizontal line with "OR" in the center separates these from the main login form. The form includes a "Username" field with a blacked-out input, a "Password" field with masked characters, and a blue "Log In >" button. Below the button is a checked checkbox for "REMEMBER ME" and two links: "Recover Your Password" and "Resend Verification Email".

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



The screenshot shows the "Settings" page in the LevelBlue Labs interface. The top navigation bar includes "LevelBlue/Labs", "Dashboard", "Browse", "Scan Endpoints", "Create Pulse", "Submit Sample", and "API Integration". The main content area is titled "Settings" and contains an "Email Notifications" section with a list of 14 checked options. Below this is the "OTX Key" section, where the key is displayed in a blacked-out box and highlighted with a red rectangle. A "Regenerate OTX API Key" button is located to the right of the key. At the bottom, there is an "Account Settings" section with the text "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:

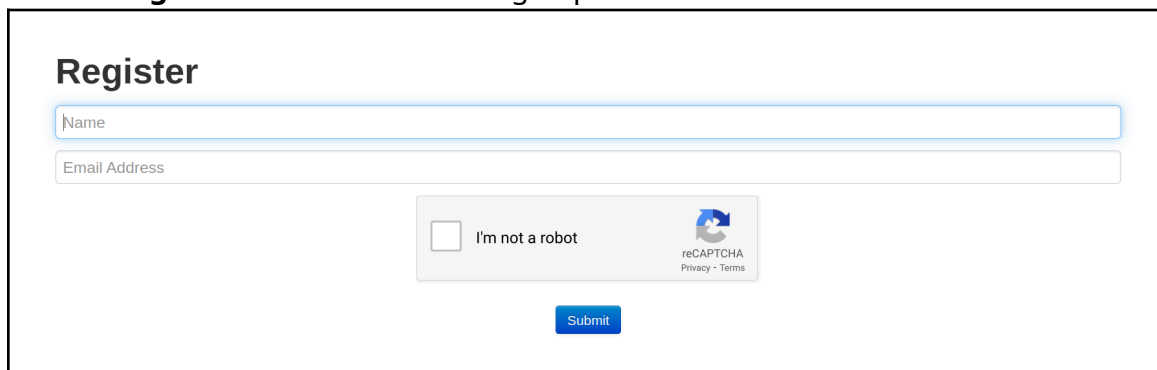


MalShare

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.

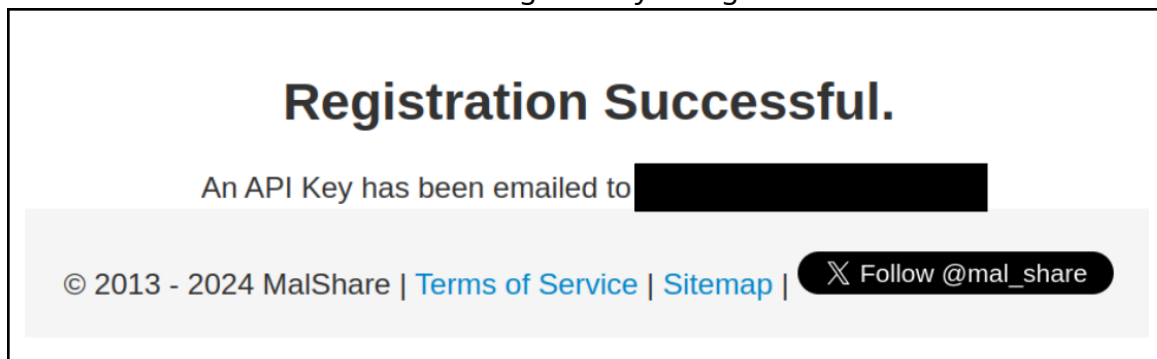
Registration link: <https://malshare.com/register.php>

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



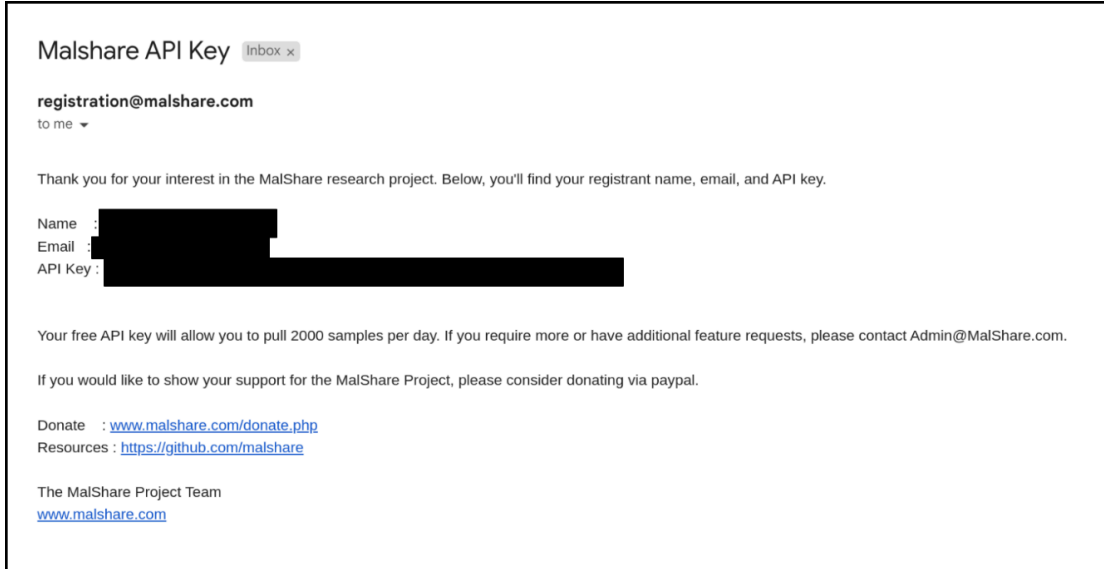
The screenshot shows the MalShare registration page. It features a title "Register" at the top left. Below the title are two input fields: "Name" and "Email Address". To the right of the "Email Address" field is a reCAPTCHA widget with the text "I'm not a robot" and a checkbox. Below the reCAPTCHA widget is a blue "Submit" button.

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



The screenshot shows a confirmation message with the heading "Registration Successful." Below the heading, it says "An API Key has been emailed to" followed by a blacked-out email address. At the bottom, there is a footer with the text "© 2013 - 2024 MalShare | [Terms of Service](#) | [Sitemap](#) | [Follow @mal_share](#)".

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



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

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

Last name

Email

Username

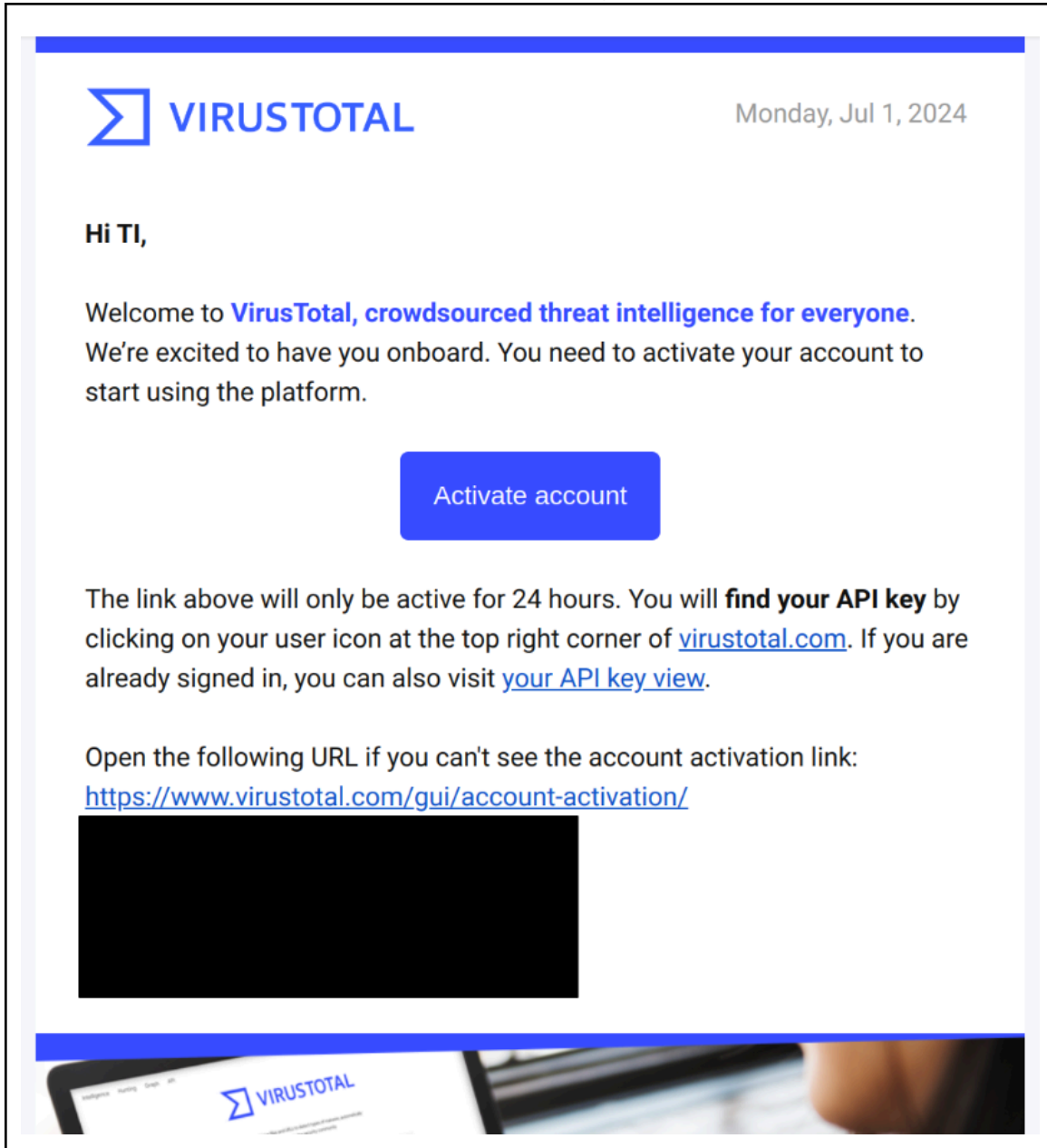
Password

Repeat password

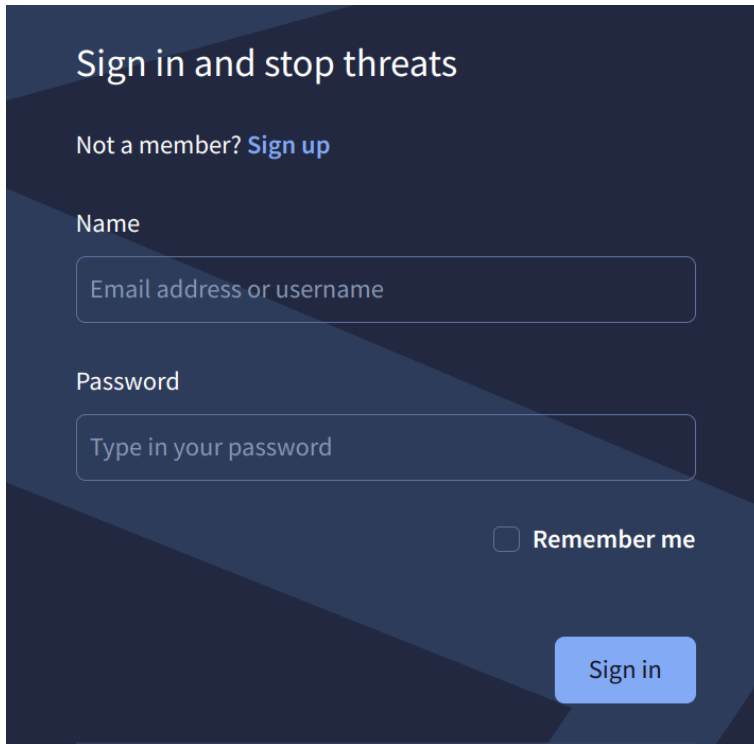
Yes, I have read and agree to the [Terms of Service](#) and [Privacy Notice](#).

Join us

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:



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



Sign in and stop threats

Not a member? [Sign up](#)

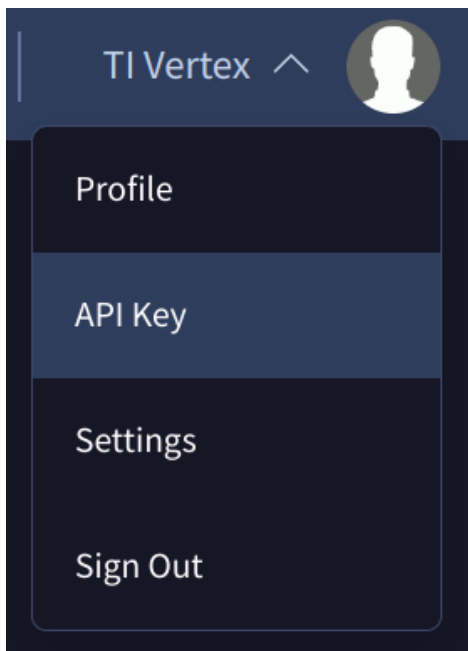
Name

Password

Remember me

Sign in

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



- 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](#)

👁️ 📄


API QUOTA ALLOWANCES FOR YOUR USER Upgrade API


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.



API reference



Python client



Golang library


Command-line interface


Go premium


Use in browser


Discover feeds


Other services

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://www.greynoise.io/viz/signup
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