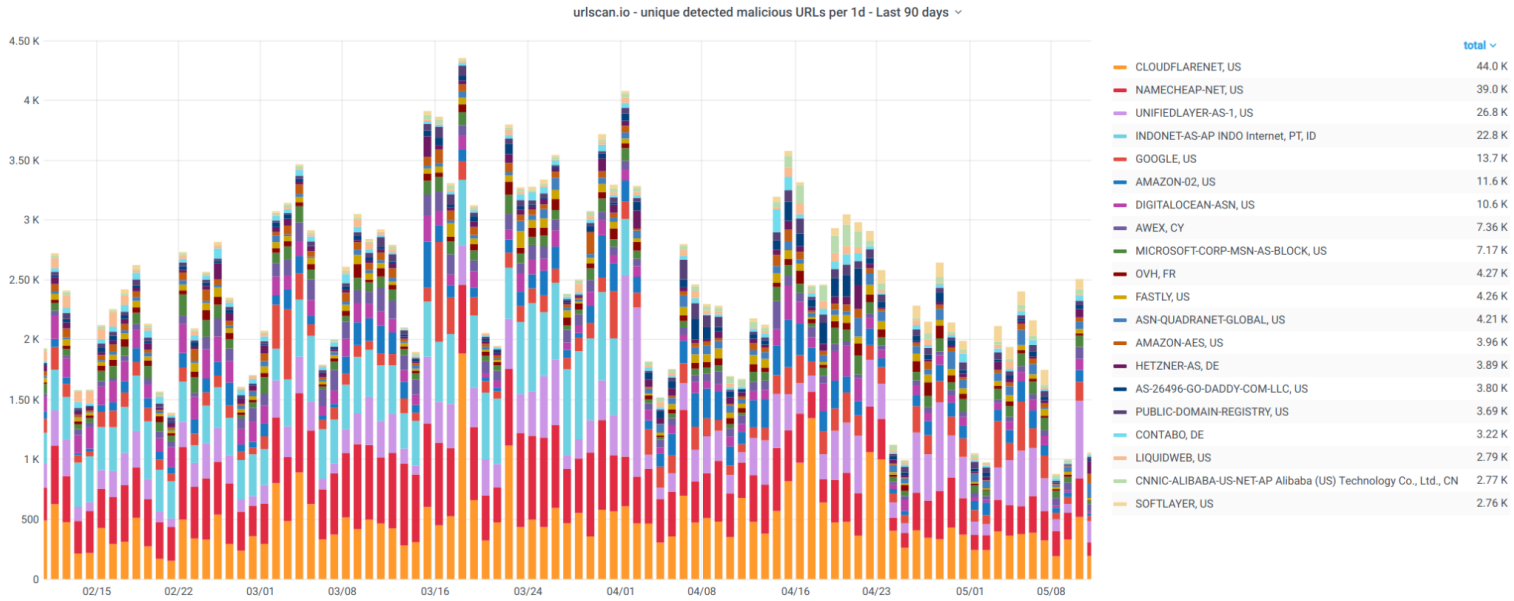
urlscan.io

A sandbox for the web

Over the past four years, **urlscan.io** has become one of the most widely used public services for *scanning* and *analyzing* potentially malicious links and websites. The service is used by tens of thousands of users daily who submit a total of 200,000 URLs for scanning every day. urlscan.io provides users with a quick summary of the key characteristics of the page and the infrastructure it is hosted on. Since its launch, more than 100 million URLs have been submitted to urlscan.io.



Unique URLs detected as malicious per day on urlscan.io - Last 90 days

To learn about our platform and products,

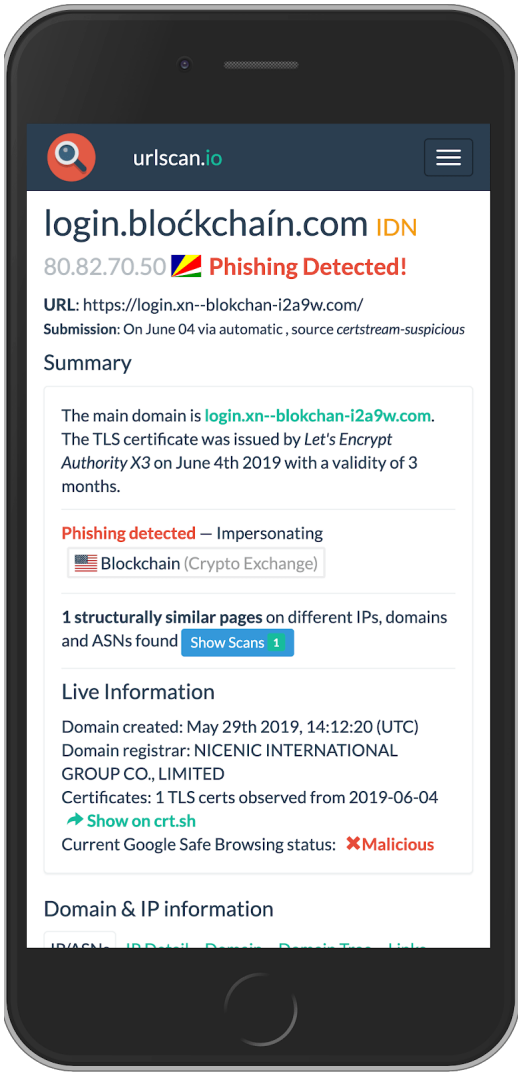
reach out to us at **info@urlscan.io**

Maliciousness

urlscan.io has a number of features to indicate whether a page contains malicious content. Our proprietary set of patterns to detect phishing will identify phishing attacks against 550+ popular brands such as banks, consumer services and public institutions. Additionally, urlscan.io records a variety of additional attributes about each URL, enabling professionals to make a quick determination about whether a given website is legitimate.

Search

urlscan.io offers a powerful, high-performance search API which will find related scans by a number of criteria. Scans can be searched by the domains and IPs that were contacted during page load, Autonomous Systems (AS), the resources that were requested and the geographical locations of the servers.



Similarity Search

To find pages which are similar to a given scan, users can use the *Similarity Search* feature. This allows to find pages which use the same resources and has been proven to work reliably for finding new installations of well-known phishing kits as well as unknown impersonation attempts.

Retrievable website information

When urlscan.io analyses a website, it stores a number of artifacts which can be retrieved later. For each scan, urlscan.io records a screenshot. It will also get a snapshot of the Document Object Model (DOM) when the page has finished loading. Lastly, urlscan.io will save any JavaScript and HTML resources requested during navigation of the page. These can then be retrieved and analysed for malicious behavior later.

Product – urlscan.io API Plans

urlscan.io is an API-first platform, which means you can perform any action on our platform via an API call. This includes submitting a URL to be scanned as well as searching for and retrieving scans. urlscan.io is integrated into a number of commercial and Open-Source security solutions, among them many of the most popular Security Automation and Orchestration (SOAR) platforms. This way urlscan.io can fit into your custom workflow for identifying, scanning, and searching for potentially malicious pages.

Some of our third-party SOAR integration partners

Our API plans allow you to fully utilise our APIs, either with your existing SOAR or security tool or via a custom API integration. Submit URLs to be scanned, search for historical results by IP, domain or URL, retrieve results and pivot to further leads. You can search all Public scans as well as your own Private scans on our platform. You can subscribe to our API plans as a Team and share your available quota amongst multiple users on the urlscan.io platform. You can also manage team-wide preferences like the default classification of scans.

On the Free plan you will be able to make a limited amount of API requests and submit a certain number of websites to be scanned every day which covers many basic use-cases and allows you to evaluate our platform. Anonymous users without a user account and API key can use our API for searching and retrieving results, but not for submitting scans.

Product – urlscan Pro - Threat Hunting

urlscan Pro is the Threat Intelligence platform based on urlscan.io. It provides insight into phishing campaigns and malicious websites, leveraging the unique information collected through urlscan.io and additional open and proprietary data-sources.

urlscan Pro supports teams of professional analysts by exposing more powerful query capabilities and pulling in more data to make sense of infrastructure and scanned websites.

urlscan Pro
Threat Hunting

Users will have access to a toolbox that allows investigating potentially malicious websites. All features are available through the UI as well as via a dedicated API. **urlscan Pro** subscriptions contain the **Real-Time Phishing URL Feed** product and the **urlscan.io API Plan "Professional"**.

Brand Detection

The Brand Detection API scans through all public websites scans performed on the urlscan.io instance and identifies phishing and impersonation attacks against an ever-growing list of popular consumer brands, such as banks, insurance companies, crypto exchanges, mail and social networking websites, and government entities. The API can be used to retrieve new hits by brand or industry vertical. A convenient page to explore this dataset is integrated into the user interface.

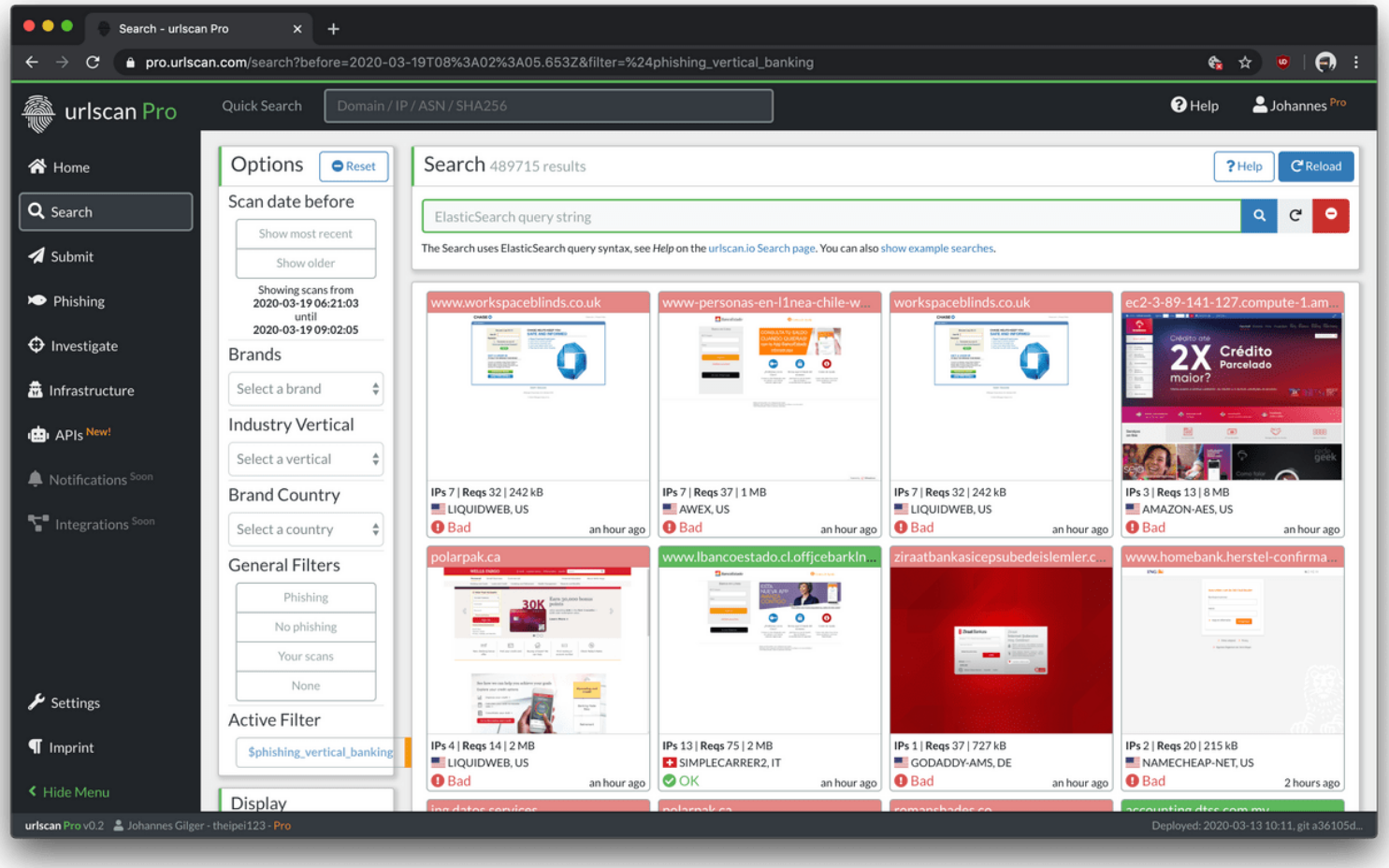
Some of the 550+ brands tracked by urlscan Pro

Similarity Search

We expose the “Similar Sites” features of urlscan.io via a dedicated API with parameters to control the necessary overlap so you can experiment searching with different similarity thresholds. This feature allows quick and painless identification of pages with similar content without any manual queries.

Investigate & Visual Search

Investigative tools included in the user interface enable quick pivoting on infrastructure, finding related websites and manually querying live information about infrastructure. *Visual Search* brings



the power of the urlscan.io search API to a visual, annotated list of results. It allows users to quickly search through many scanned websites and identify interesting candidates.

Real-time Phishing URL Feed

urlscan.io detects thousands of unique malicious and suspicious URLs targeting 550+ popular brands every day, including many phishing attempts. We are making the daily, weekly, and monthly feed of detected URLs available for commercial customers. Each suspicious URL in the feed includes the following pieces of information:

- Unique ID of the scan
- Phishing URL
- Page title
- Targeted Brand, Industry Vertical, Country of Origin
- Domain & TLD of phishing URL
- IP address hosting the phishing URL
- GeoIP information hosting the phishing URL
- ASN and ASN Name hosting the phishing URL
- First-Seen Date of phishing URL
- Country of submission
- Aggregate information - Prevalence of brand, domain, IP, ASN

The feeds are available as CSV, TSV, and JSON and can be queried every minute. Commercial use of the data is allowed.