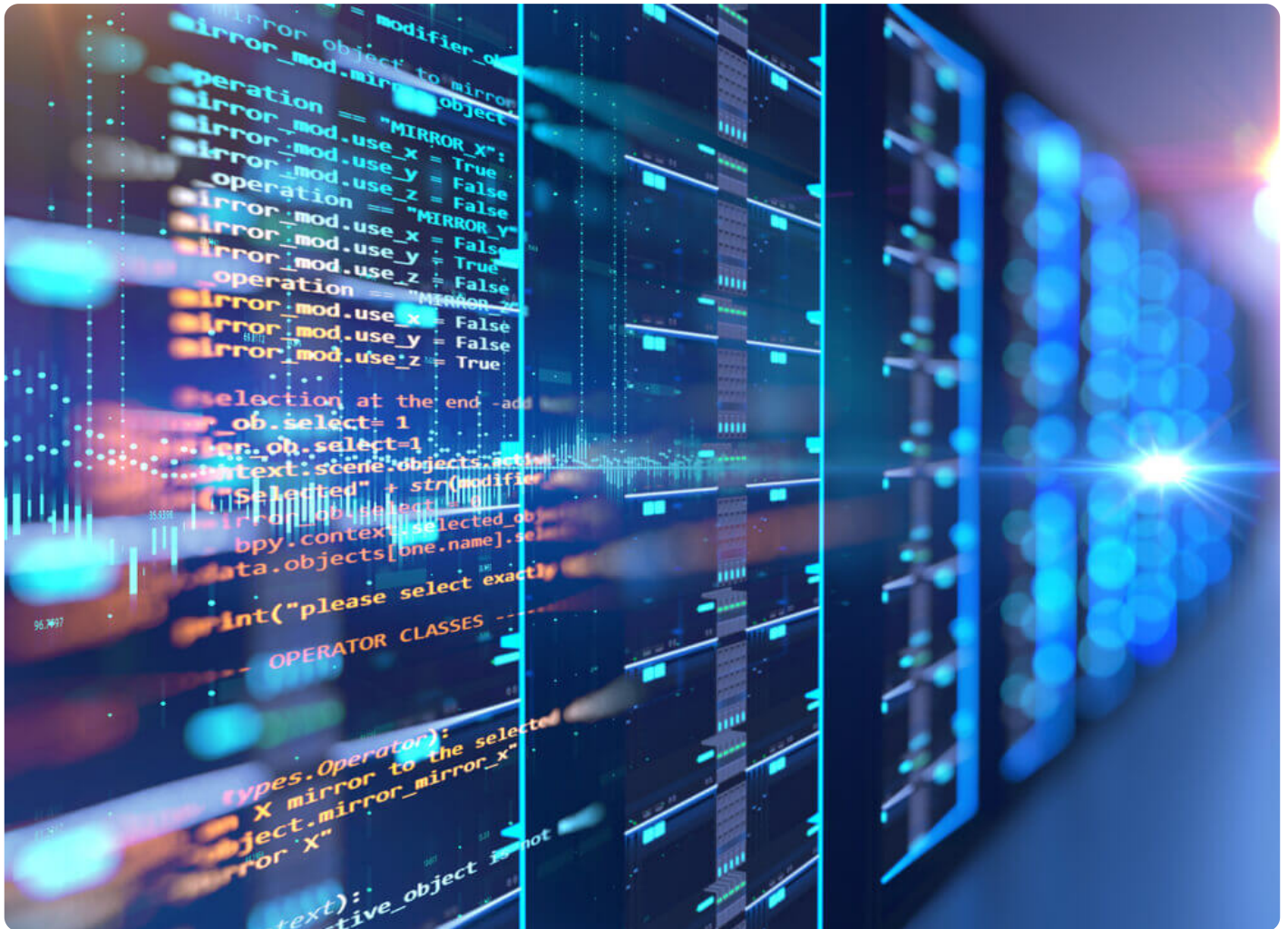


# Reverse WHOIS in action: find all domains or websites of a company, and more

Posted on February 24, 2019



See [Reverse WHOIS Search](#) in action by searching for all the domains a company owns or controls. We will use the [web-based Reverse WHOIS Search tool](#). An alternative would be to use [Reverse WHOIS API](#), a RESTful solution that has the same capabilities.

We picked a popular brand, the Eastman Kodak Company, as an example for our investigation, although the tool works for any company you may be interested in. If you are a domainer, a marketer, a legal investigator, an IT security expert, or anyone interested in or working with Internet domains, you are in the right place. We'll present a Swiss Army knife designed to fit your every need.

## Table of Contents

- [1. Our tool: the Domain Research Suite](#)
- [2. Our example: Eastman Kodak Company's](#)
  - [1.1 Basic search](#)
  - [2.2 Advanced search](#)
- [3. Summary](#)

## 1. Our tool: the Domain Research Suite

WhoisXML API has been collecting and normalizing the ownership details of domains and IP netblocks for years. While this information is publicly available, it is scattered across highly distributed and not always coherent data sources. Hence, trying to get the data in a useful form is challenging. WHOIS data, for instance, comes primarily from servers that still use a protocol dating back to the early days of the Internet, and their operators impose several query limitations.

WhoisXML API has the appropriate infrastructure and expertise to collect the huge data set and normalize it to facilitate more efficient querying. This complete and coherent database of current and historical domain ownership data is the solid basis of advanced domain research and

monitoring tools, now integrated into our [Domain Research Suite \(DRS\)](#).

What we'll demonstrate in this post is just a small part of DRS's functionality. The tool makes it possible not only to find a particular domain's owner but also pivot on its details to find other domains that belong to the same owner. All of this can be done through a webpage or a RESTful API. We'll leave the choice up to you.

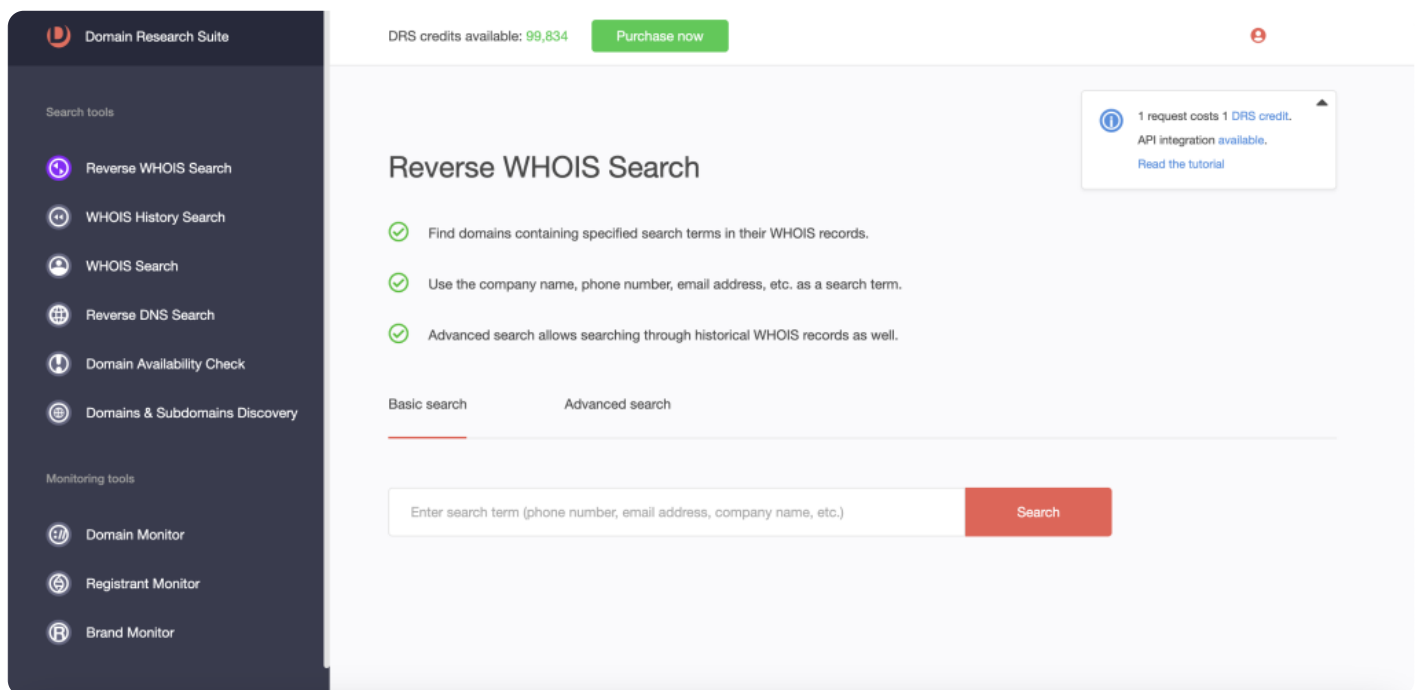
You may be asking yourself what practical uses a reverse WHOIS search tool has. Here's a list of some things that [Reverse WHOIS Search](#) or [Reverse WHOIS API](#) can do for you.

- **Cybersecurity:** Cybersecurity analysts and researchers can use reverse WHOIS search reports to get more information regarding a spam or malware attack or any other kind of online intrusion or crime.
- **Law enforcement:** Law enforcement agencies, meanwhile, can use the same data to track and possibly block access to all domains, websites, and IP addresses related to malicious activities.
- **Brand protection:** Businesses can also use reverse WHOIS information to protect their intellectual property and check potential trademark infringements by scoping for domain name similarities, duplicates, or copycats.
- **Cyber fraud detection:** Payment processors and banks, on the other hand, can use the same data to detect and collect intelligence on transaction fraud.
- **Marketing research:** Finally, marketing researchers, analysts, and other professionals, along with business owners, can use reverse WHOIS information to identify new business and partnership opportunities and locate potential buyers.

Now, we will act as an analyst and use the interactive approach. To do so, we'll visit the [DRS web page](#).

First, you need to register for a free account in case you don't have one for this or any other WhoisXML API tool. The free account, which comes with 50 credits, is perfectly sufficient if you want to give it a try or only occasionally need to analyze web pages. If you need more, you can purchase additional credits at reasonable prices. We have a flexible pricing structure tailor-made for various needs. For more information, visit our [pricing page](#).

After logging in, you will see a page like this.



The available search and monitoring tools are shown on the left panel.

- Search tools:
  - Reverse WHOIS Search
  - WHOIS History Search
  - WHOIS Search

- Domain Availability Check
- Monitoring tools:
  - Domain Monitor
  - Registrant Monitor
  - Brand Monitor

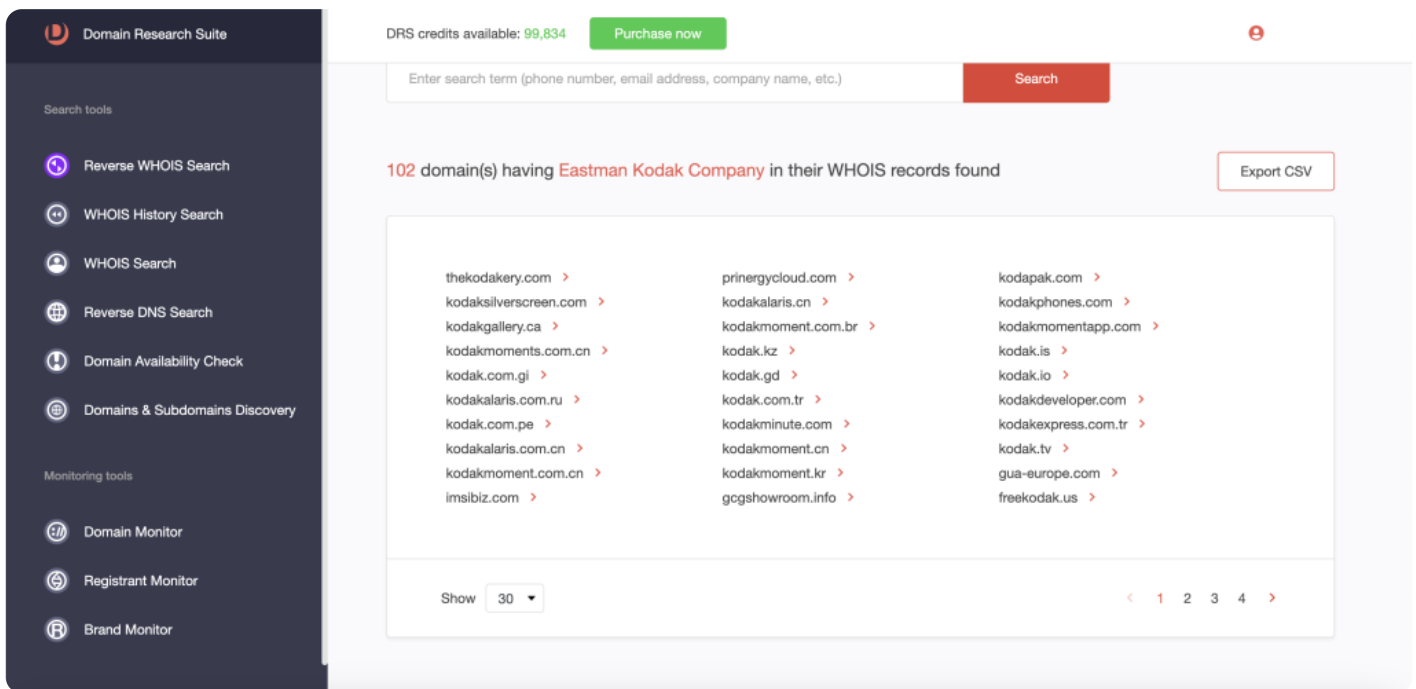
By default, we'll see Reverse WHOIS Search, one of the nine tools that make up DRS. Let's get started.

## 2. Our example: Eastman Kodak Company

Since the author of this blog post is also interested in photography, we opted to search for details for the Eastman Kodak Company or Kodak for short, which has always played a significant role in both the production and innovation of photographic technology. Let's find all the domains owned by the company.

### Basic search

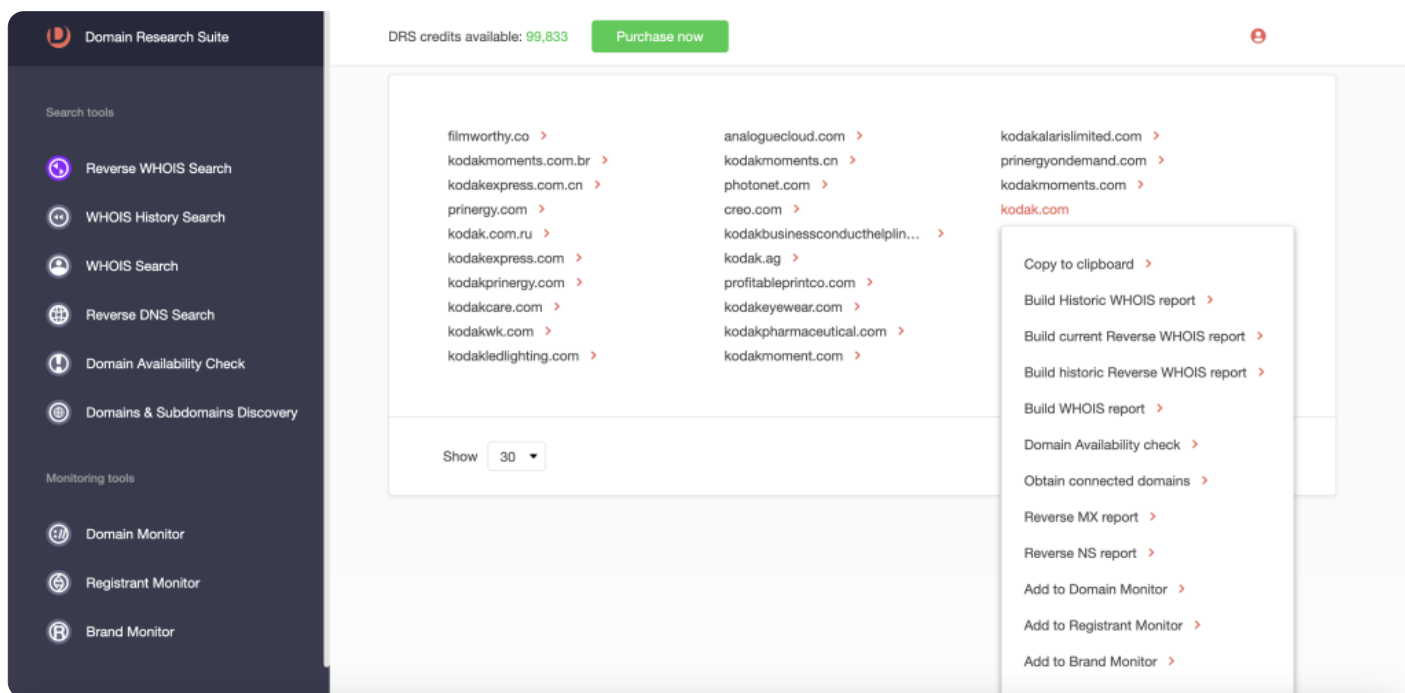
First, we'll do a basic search to find all websites Kodak owns. After entering **Eastman Kodak Company** into the basic search input field and pressing the **Search** button, we'll see the following:



The screenshot displays the 'Domain Research Suite' interface. On the left is a dark sidebar with navigation links: 'Reverse WHOIS Search', 'WHOIS History Search', 'WHOIS Search', 'Reverse DNS Search', 'Domain Availability Check', 'Domains & Subdomains Discovery', 'Domain Monitor', 'Registrant Monitor', and 'Brand Monitor'. The main area shows a search bar with the text 'Enter search term (phone number, email address, company name, etc.)' and a red 'Search' button. Above the search bar, it says 'DRS credits available: 99,834' and a green 'Purchase now' button. Below the search bar, a message states '102 domain(s) having Eastman Kodak Company in their WHOIS records found'. To the right of this message is a red 'Export CSV' button. Below the message is a list of 102 domains arranged in three columns, each with a red arrow pointing to the right. The domains include: thekodakery.com, kodaksilverscreen.com, kodakgallery.ca, kodakmoments.com.cn, kodak.com.gi, kodakalaris.com.ru, kodak.com.pe, kodakalaris.com.cn, kodakmoment.com.cn, imsibiz.com, prinerigycloud.com, kodakalaris.cn, kodakmoment.com.br, kodak.kz, kodak.gd, kodak.com.tr, kodakminute.com, kodakmoment.cn, kodakmoment.kr, gogshowroom.info, kodapak.com, kodakphones.com, kodakmomentapp.com, kodak.is, kodak.io, kodakdeveloper.com, kodakexpress.com.tr, kodak.tv, gua-europe.com, and freekodak.us. At the bottom of the list, there is a 'Show 30' dropdown menu and a pagination bar with the numbers 1, 2, 3, 4.

You can see a list of 102 domains that have **Eastman Kodak Company** in their WHOIS records. That means all these domains have ties to your search term. Since we gave a rather specific company name, the simple search found a reasonable number of records. That is what we were primarily looking for—a complete list of domains owned by the Kodak Eastman Company. But we can take a few more steps in the investigation.

We can look at the details of any of the domains. Let's take a look at **kodak.com**. Clicking the domain name will give you the following choices:



**Build WHOIS report** will display the domain's current WHOIS record and reveal its owner's contact information, relevant dates (i.e., creation, last updated, and expiration), and other data. What may be even more interesting, however, is **Build Historic WHOIS report**, which provides all the previous statuses of the domain from 2011 to the current year.

Each WHOIS report shows the following information:

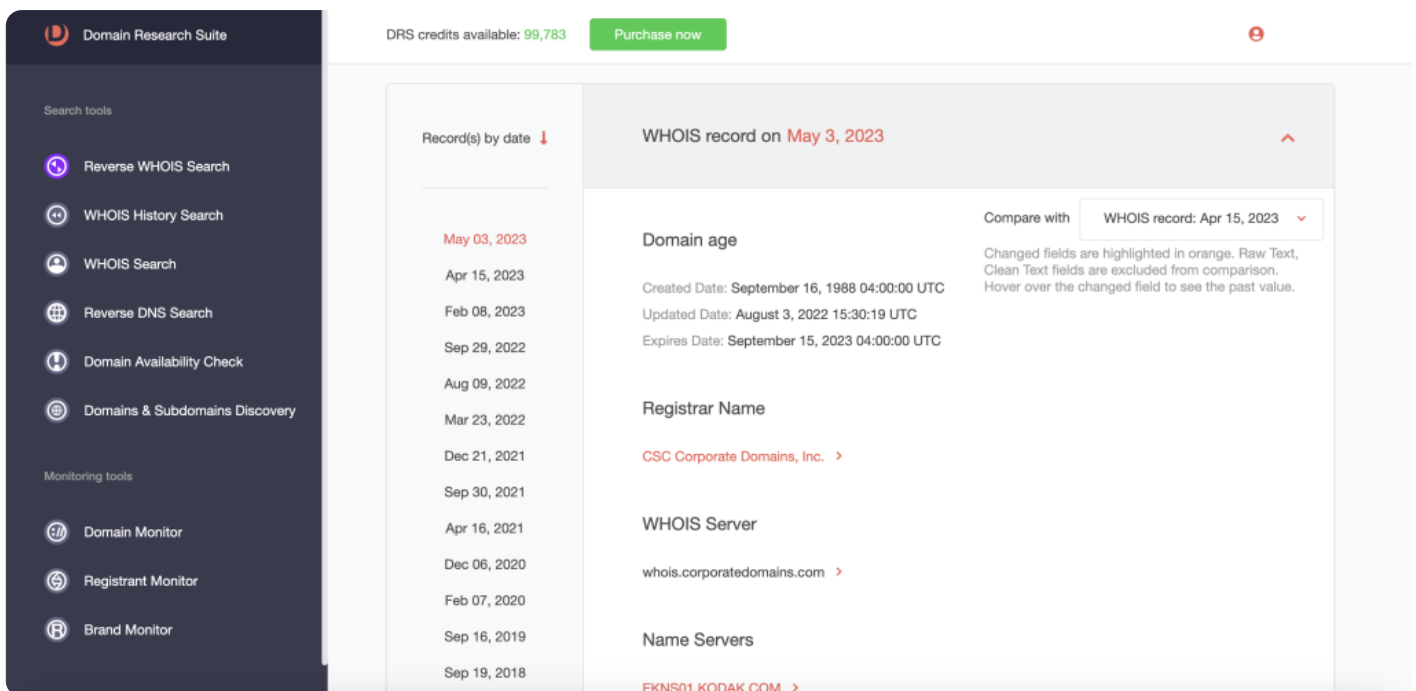
- **Domain age:** How long the domain has been in existence, specifically, when it was created, last updated, and will expire.
- **Registrar name:** The name of the domain name's seller.
- **Registrar's server name:** The name of the server where the domain is hosted.
- **Related name servers:** Names of the registrar's backup servers should there be any problems with the domain's main server.
- **Domain status:** Whether the domain is active or not. It may also indicate restrictions



imposed on the name's use, if any.

- **Registrant contact details:** What the owner's phone number, email address, and street address are.

Note that the registrant, administrative, billing, and technical contact details may vary. In most cases, though, they refer to the same person, typically, the company's web administrator. In cases where the domain registrant opted for anonymous registration, which is an accepted practice by those who want to restrict access to their personal information, the contact details would belong to a representative of the web hosting provider. None of the information on a WHOIS report may be falsified as that could result in the revocation of a website's license to operate.



The screenshot displays the 'Domain Research Suite' interface. On the left is a dark sidebar with 'Search tools' (Reverse WHOIS Search, WHOIS History Search, WHOIS Search, Reverse DNS Search, Domain Availability Check, Domains & Subdomains Discovery) and 'Monitoring tools' (Domain Monitor, Registrant Monitor, Brand Monitor). The main area shows 'DRS credits available: 99,783' and a 'Purchase now' button. Below this is a 'Record(s) by date' list with dates from May 03, 2023 down to Sep 19, 2018. The selected record for 'May 03, 2023' is expanded, showing a 'WHOIS record on May 3, 2023'. The record details include: Domain age (Created: Sep 16, 1988, Updated: Aug 3, 2022, Expires: Sep 15, 2023), Registrar Name (CSC Corporate Domains, Inc.), WHOIS Server (whois.corporatedomains.com), and Name Servers (EKNS01.KODAK.COM). A 'Compare with' dropdown shows 'WHOIS record: Apr 15, 2023'.

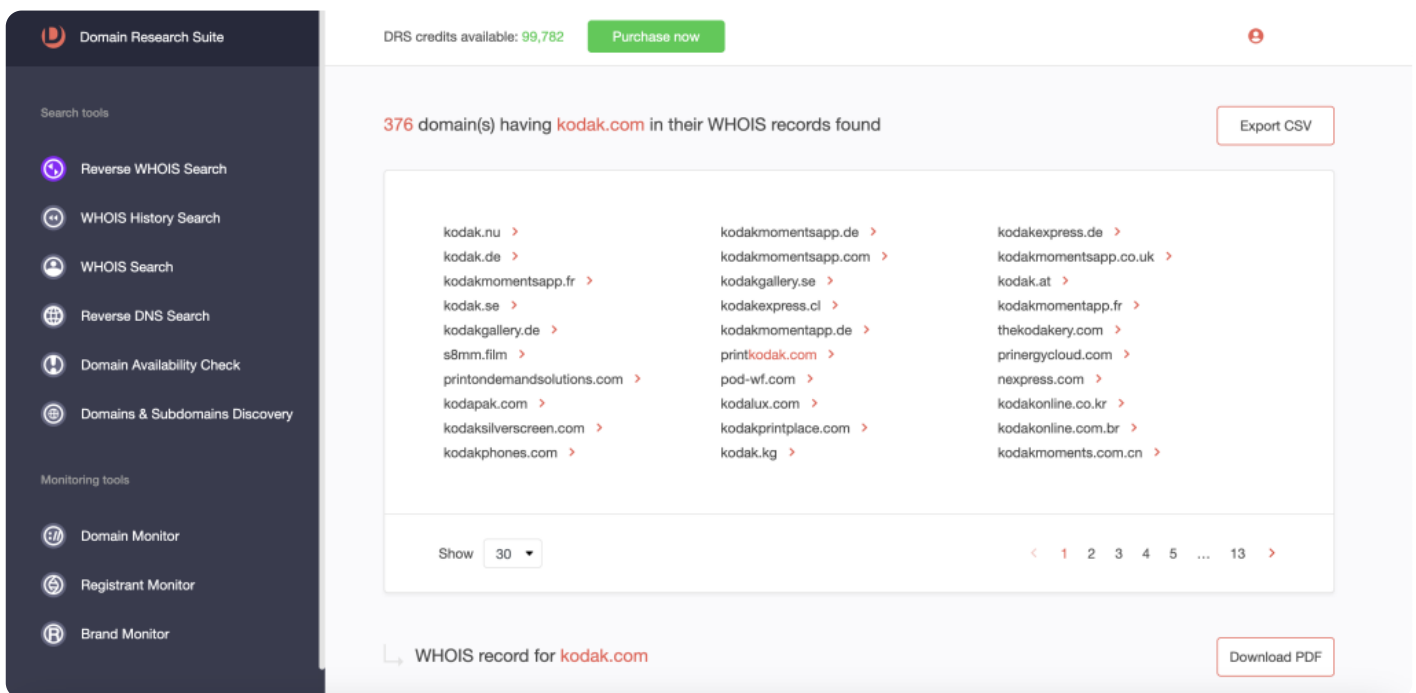
We omitted the details from the record in this screenshot, except for the relevant dates, but they are all there. And we have all the 29 versions of the WHOIS records the domain has had since 2011 in full detail. The cumulative numbers in the top blocks are also quite interesting as they can reveal company name changes and more.

**Records with public ownership data** is of particular interest, as the whole WHOIS ecosystem is



currently undergoing significant changes due to new data protection regulations (notably the new GDPR of the European Union). As no better source of ownership information appears, we still have WHOIS as the only method to find out who owns a domain.

Let's build a reverse WHOIS report for **kodak.com**.



The screenshot shows the Domain Research Suite interface. On the left is a dark sidebar with navigation options: Search tools (Reverse WHOIS Search, WHOIS History Search, WHOIS Search, Reverse DNS Search, Domain Availability Check, Domains & Subdomains Discovery) and Monitoring tools (Domain Monitor, Registrant Monitor, Brand Monitor). The main area has a header with 'DRS credits available: 99,782' and a 'Purchase now' button. Below the header, it states '376 domain(s) having kodak.com in their WHOIS records found' with an 'Export CSV' button. A list of domains is displayed in three columns, each with a right-pointing arrow. The domains include: kodak.nu, kodak.de, kodakmomentsapp.fr, kodak.se, kodakgallery.de, s8mm.film, printondemandsolutions.com, kodapak.com, kodaksilverscreen.com, kodakphones.com, kodakmomentsapp.de, kodakmomentsapp.com, kodakgallery.se, kodakexpress.cl, kodakmomentapp.de, printkodak.com, pod-wf.com, kodalux.com, kodakprintplace.com, kodak.kg, kodakexpress.de, kodakmomentsapp.co.uk, kodak.at, kodakmomentapp.fr, thekodakery.com, prinerycloud.com, nexpress.com, kodakonline.co.kr, kodakonline.com.br, and kodakmoments.com.cn. At the bottom, there is a 'Show 30' dropdown, pagination links (1, 2, 3, 4, 5, ..., 13), and a 'Download PDF' button.

As you can see, **kodak.com** was searched for in all WHOIS record fields, so the resulting page contains those that were registered under the company's alternative name. For instance, the WHOIS record of **kodakmomentsapp.com** reveals that it was registered by **Eastman Kodak** (without **Company**). Another possibility is that the domain may be owned by a different company that has to do something with it (e.g., affiliates, third parties selling Kodak goods, etc.).

An example would be **islander.nf**, which is run by **Norfolk Island Data Services Ltd. Pty.** but its administrative contact appears to coincide with that of the Eastman Kodak Company. The domain may have been bought by Kodak or its affiliate. A quick Google search, however, reveals that it is currently inactive. It is, after all, a common practice for big brands to buy all domains that may be very similar to the ones they actively use for brand protection.

One of the reasons for that is protecting customers from phishing, which occurs when a company's

customers are tricked into giving away their personal information (e.g., name, address, phone number, email address, and even their passwords) via various social engineering tactics so they can use these for other fraudulent deeds.

They could, for instance, use an inactive domain (something really similar to the company they are spoofing) that nobody likely monitors and build their own forms laced with a keylogger — a malicious program employed to log the computer keystrokes of a target victim to obtain usernames and passwords.

Little would the customers know that they are handing out their online credentials to unknown malicious actors who can then use these to access their real online accounts with the company and get their credit card details. That could even go unnoticed when credit card bills are paid without scrutinizing every little detail on it.

## Advanced search

Let us now explore the **Advanced Search** tab and more possibilities to pivot on. You may be wondering what possible reasons you could have to use this feature.

Say, you have been receiving bills from a supposed Kodak company or its affiliate in Australia while you have never even been to the country and you want to find out if you are being victimized by a cybercriminal. (Note that this is a hypothetical scenario we just provided for context.) Where do you start?

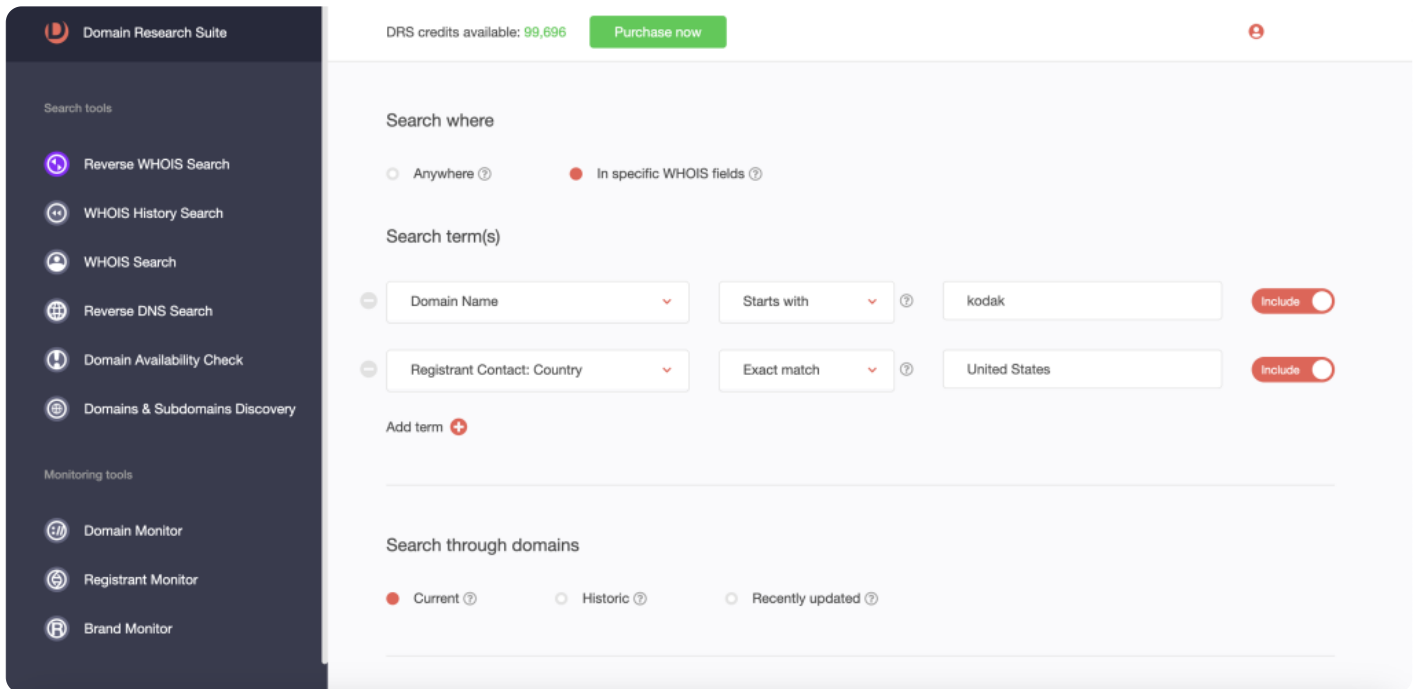
Within **Advanced Search** are two options. **Anywhere** enables us to give multiple search terms to include or exclude as well as the choice of searching **Actual**, **Historic**, or **Recently updated** records.

Now, we'll go for **Specific WHOIS fields**, which enables us to give conditions specific to particular WHOIS record fields, such as the registrant's country.

In particular, we'll look for:

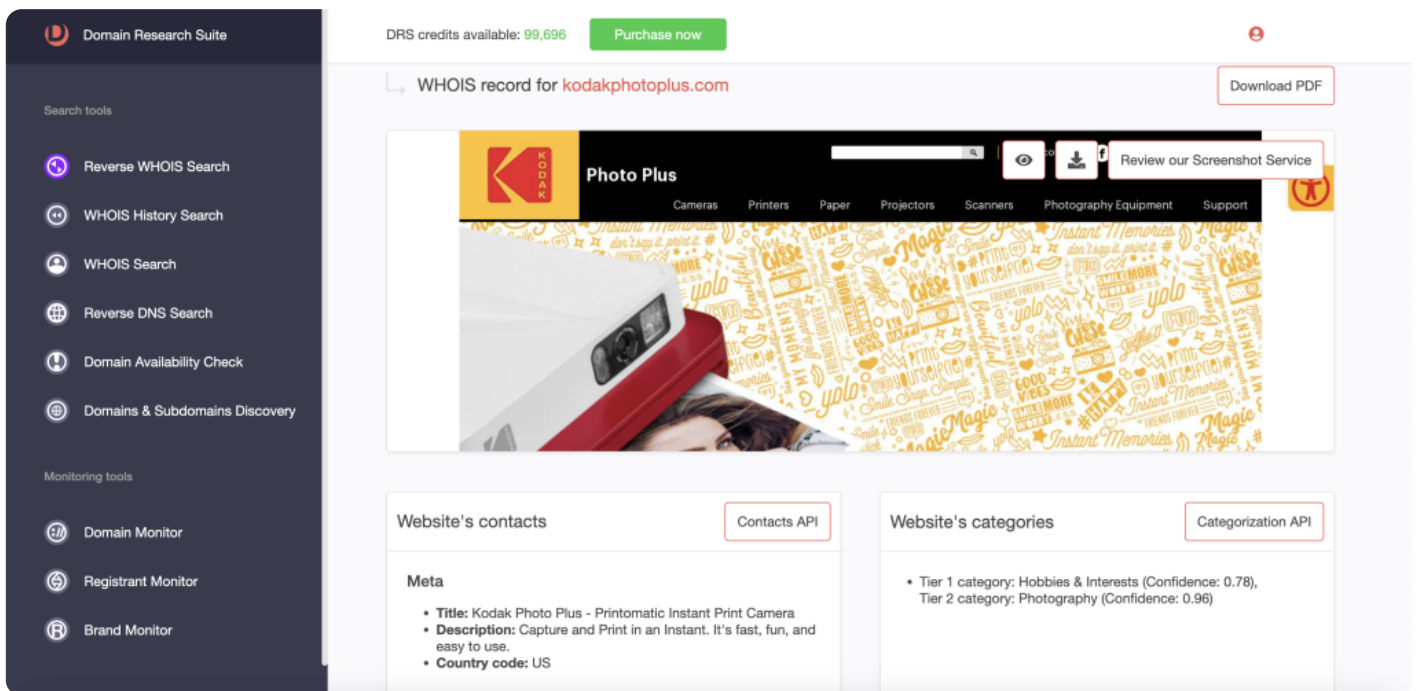
- Domain names that start with **kodak**

- Domains whose registrant resides in the U.S.
- Currently active domains only



The screenshot shows the 'Domain Research Suite' interface. On the left is a dark sidebar with a 'Domain Research Suite' header and two sections: 'Search tools' and 'Monitoring tools'. The 'Search tools' section includes 'Reverse WHOIS Search', 'WHOIS History Search', 'WHOIS Search', 'Reverse DNS Search', 'Domain Availability Check', and 'Domains & Subdomains Discovery'. The 'Monitoring tools' section includes 'Domain Monitor', 'Registrant Monitor', and 'Brand Monitor'. The main content area has a top bar showing 'DRS credits available: 99,696' and a 'Purchase now' button. Below this is the 'Search where' section with two radio buttons: 'Anywhere' (selected) and 'In specific WHOIS fields'. The 'Search term(s)' section contains two rows of search criteria. The first row has a dropdown for 'Domain Name', a dropdown for 'Starts with', a text input with 'kodak', and an 'Include' toggle. The second row has a dropdown for 'Registrant Contact: Country', a dropdown for 'Exact match', a text input with 'United States', and an 'Include' toggle. Below this is an 'Add term' button. The 'Search through domains' section has three radio buttons: 'Current' (selected), 'Historic', and 'Recently updated'.

Let's take a closer look at **kodakphotoplus.com**. Its WHOIS report reveals the following:



The screenshot displays the 'Domain Research Suite' interface. On the left is a dark sidebar with search tools (Reverse WHOIS Search, WHOIS History Search, WHOIS Search, Reverse DNS Search, Domain Availability Check, Domains & Subdomains Discovery) and monitoring tools (Domain Monitor, Registrant Monitor, Brand Monitor). The main area shows the 'WHOIS record for kodakphotoplus.com' with a 'Download PDF' button. Below the domain name is a screenshot of the 'Photo Plus' website. At the bottom, there are sections for 'Website's contacts' (with a 'Contacts API' button) and 'Website's categories' (with a 'Categorization API' button). The 'Meta' section lists: Title: Kodak Photo Plus - Printomatic Instant Print Camera, Description: Capture and Print in an Instant. It's fast, fun, and easy to use., and Country code: US. The 'Categories' section lists: Tier 1 category: Hobbies & Interests (Confidence: 0.78), Tier 2 category: Photography (Confidence: 0.96).

So, it is owned by **C&A IP Holdings, LLC**. Notice the little red arrow (>) after **Registrant Name**: when it's clicked. We'll see five options, namely:

- Copy to clipboard
- Build current Reverse WHOIS report
- Build historic Reverse WHOIS report
- Add to Registrant Monitor
- Add to Brand Monitor

If you want to find out more about the company, build a reverse WHOIS report for it by following the same steps you learned earlier when doing a basic search. Note that all **DRS** reports are downloadable in either CSV or PDF format.

If we want to monitor the activities of this registrant, we can do that easily from here as well. Just click **Add to Registrant Monitor** and you are done. You can monitor any of the items in the WHOIS record with a red arrow (>) beside them with a mere click.

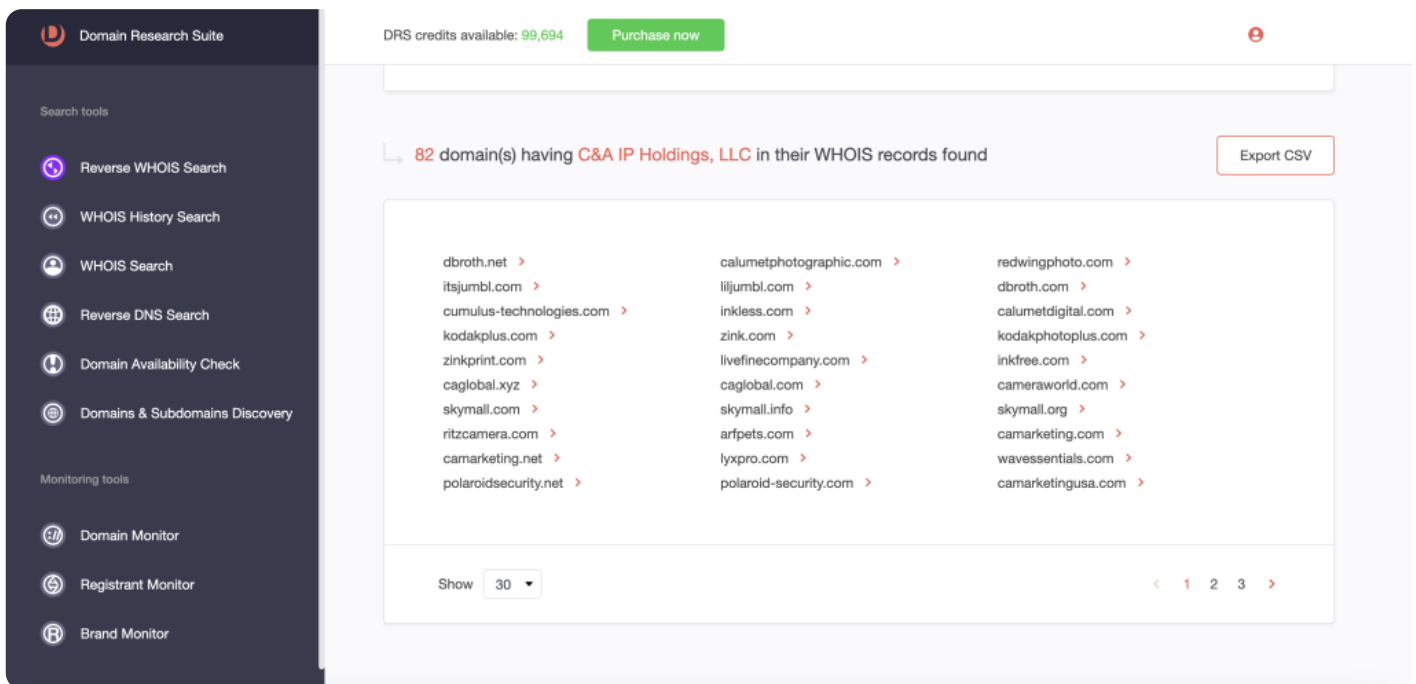
Apart from monitoring registrant changes, you can also check for domain and brand changes via Domain Monitor and Brand Monitor, respectively, to stop a variety of threats like typosquatting (also known as “URL hijacking”) — where a cybercriminal relies on misspelling to get your customers to their malicious sites or pages.

Visitors who land on, say, **kadok.com** instead of **kodak.com** can end up giving the bad guys access to their legitimate kodak.com online accounts and, in essence, their personally identifiable information (e.g., name, address, phone number, email address, credit card details, and more) without realizing it.

If you’re concerned about your brand being abused or misused for phishing attacks and would like to avoid that, you can rely on Brand Monitor to keep track of domains that look very similar to yours in real-time.

The same can be done for domains with Domain Monitor. And should you already have a handy list of registrants who have ties to phishing attacks and other cybercriminal activities in the past, you can monitor them as well with Registrant Monitor. All it takes you is a few extra mouse clicks on the advanced search tab of Reverse WHOIS Search.

But right now, we’ll build a reverse WHOIS report. We can pivot on the **Registrant Name**, resulting in the following:



The screenshot displays the 'Domain Research Suite' interface. On the left is a dark sidebar with navigation links: 'Reverse WHOIS Search', 'WHOIS History Search', 'WHOIS Search', 'Reverse DNS Search', 'Domain Availability Check', 'Domains & Subdomains Discovery', 'Domain Monitor', 'Registrant Monitor', and 'Brand Monitor'. The main content area shows a search result for 'C&A IP Holdings, LLC', indicating 82 domains found. A table lists 24 domains in three columns, each with a right-pointing arrow. At the top right, it says 'DRS credits available: 99,694' and has a 'Purchase now' button. An 'Export CSV' button is also present. At the bottom, there is a 'Show 30' dropdown and pagination controls showing pages 1, 2, 3.

dbroth.net >	calumetphotographic.com >	redwingphoto.com >
itsjumbl.com >	liljumbl.com >	dbroth.com >
cumulus-technologies.com >	inkless.com >	calumetdigital.com >
kodakplus.com >	zink.com >	kodakphotoplus.com >
zinkprint.com >	livefinecompany.com >	inkfree.com >
caglobal.xyz >	caglobal.com >	cameraworld.com >
skymall.com >	skymall.info >	skymall.org >
ritzcamera.com >	arfpets.com >	camarketing.com >
camarketing.net >	lyxpro.com >	wavessentials.com >
polaroidsecurity.net >	polaroid-security.com >	camarketingusa.com >

The registrant appears to own 82 domains. And we can continue our search on each domain by building current or historic WHOIS records and possibly pivoting on any field in the resulting data.

### 3. Summary

We demonstrated how to use DRS's [Reverse WHOIS Search](#). It is an easy-to-use, flexible, and pivotable tool, orchestrated with various other search and monitoring facilities. All of these are based on an accurate and coherent database of domain ownership data. If, however, you feel more comfortable working with JSON or CSV files or want to connect the data to your existing platform, try out [Reverse WHOIS API](#), also part of [WhoisXML API's Domain Research Suite](#), instead.

Big brands are prime cybercriminal targets for simple fraud administered via email. Anyone with malicious intent can pick an unmonitored domain to compromise and abuse it for billing fraud. If you are running a small business and have yet to obtain more advanced security tools and staff, a simple and flexible tool such as [Reverse WHOIS Search](#) or [Reverse WHOIS API](#) may prove

extremely useful for you.

These not only give you information on who may be adversely targeting your business, but also more detailed insights into where your customers are coming from. With that, you can unlock previously untapped opportunities.

Just make sure your WHOIS service provider is reliable. Fortunately, [WhoisXML API](#) is a seasoned provider that gathers domain WHOIS records for all gTLDs and ccTLDs. As such, it provides real-time APIs, database downloads, and domain research and monitoring and threat intelligence tools to meet the demand of a diverse and huge customer base with specific business needs.

We currently serve Fortune 500 companies, threat intelligence and infosec companies, anti-malware and security vendors, cybercrime units, government agencies, brand protection agencies, domain registries and registrars, domain investors and brokers, banks, payment processors, telcos, marketing researchers, big data warehouses, web analytics firms, investment funds, web developers, and many more.

With more than 13.7 billion historical WHOIS records, over 774 million domains tracked, more than 7,298 TLDs tracked, and over 10 years of data crawling experience, [WhoisXML API](#) through [DRS](#) or its components, [Reverse WHOIS Search](#) or [Reverse WHOIS API](#), gives you customizable access to regularly updated WHOIS information worldwide. Interested? Go and get your [free account](#) now.