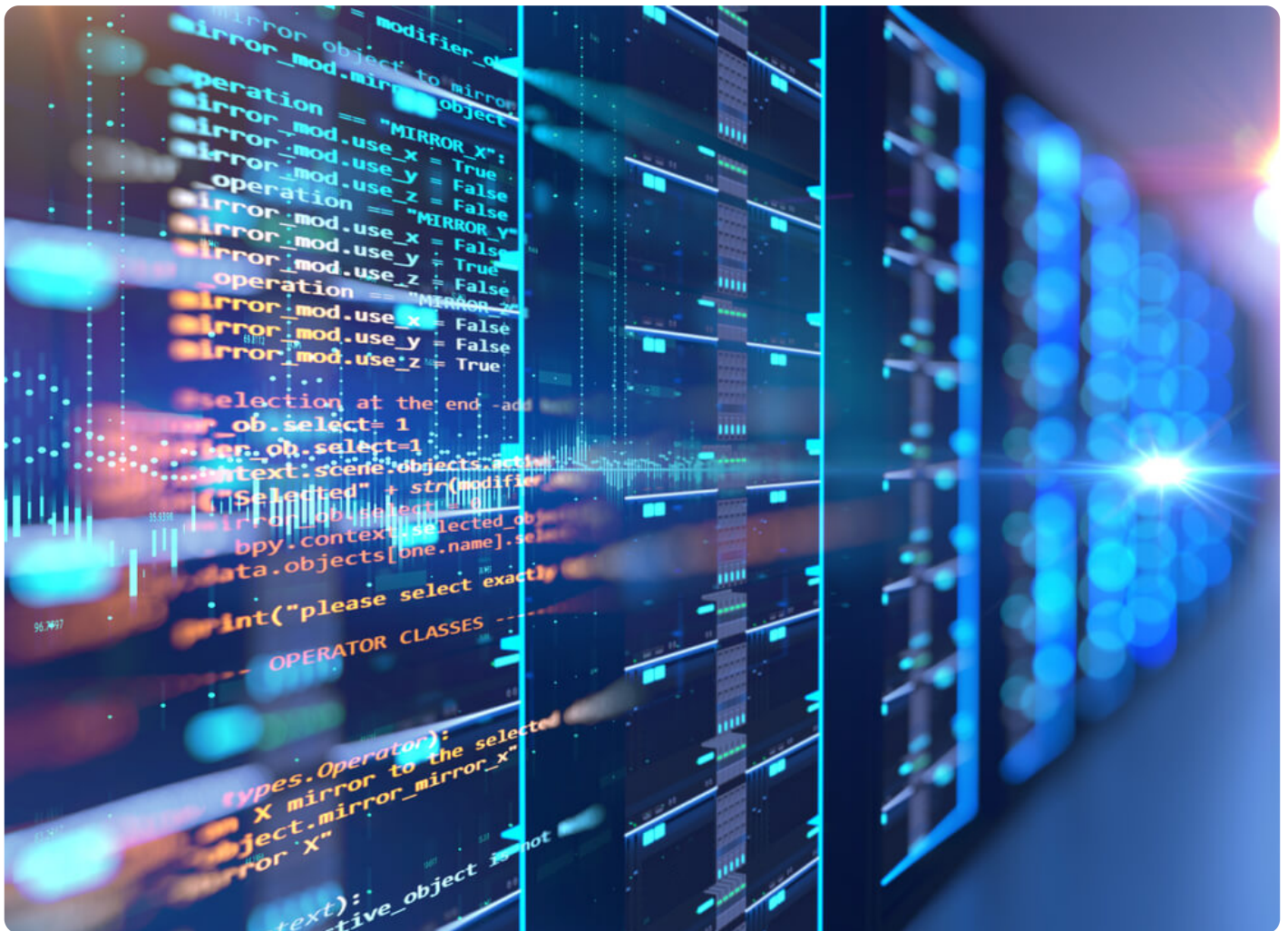


Reverse WHOIS in action: find all domains or websites of a company, and more

Posted on February 24, 2019



See [Reverse WHOIS service](#) in action by searching for all Internet domains a company owns or is related to. We shall use the [web-based reverse WHOIS service](#). An alternative would be to use the [reverse WHOIS API](#), a RESTful solution which is also available with the same capabilities. We shall pick a popular brand, the Eastman Kodak Company, as an example for our investigation, although it works for any other one you might 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 present the Swiss Army knife designed to fit in your very pocket.

Table of Contents

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

1. Our tool: the Domain Research Suite

WhoisXML API, Inc. has been collecting and normalizing ownership data of domains and IP netblocks for several years. While this information is publicly available on the Internet, it is scattered into highly distributed and not always coherent data sources. Hence, trying to get these data in a useful form is really a challenge. WHOIS data, for instance, come primarily from servers still using a protocol dating back to the early days of Internet, and the operators of these servers

impose several limitations on queries.

WhoisXML API has the appropriate infrastructure and expertise to collect the huge set of all these data and put it into a normalized form facilitating efficient queries. This complete and coherent database of current and historic ownership (domain WHOIS) data is the solid basis of advanced domain research and monitoring tools, now integrated into a [Domain Research Suite](#). What we demonstrate here is just a small part of its functionality. Namely, it makes it possible not only to find the owner of a particular domain, but also to pivot on its details, for instance, find the other domains belonging to the same owner. All of this can be used either interactively on a webpage or through RESTful APIs. We leave the choice up to you.

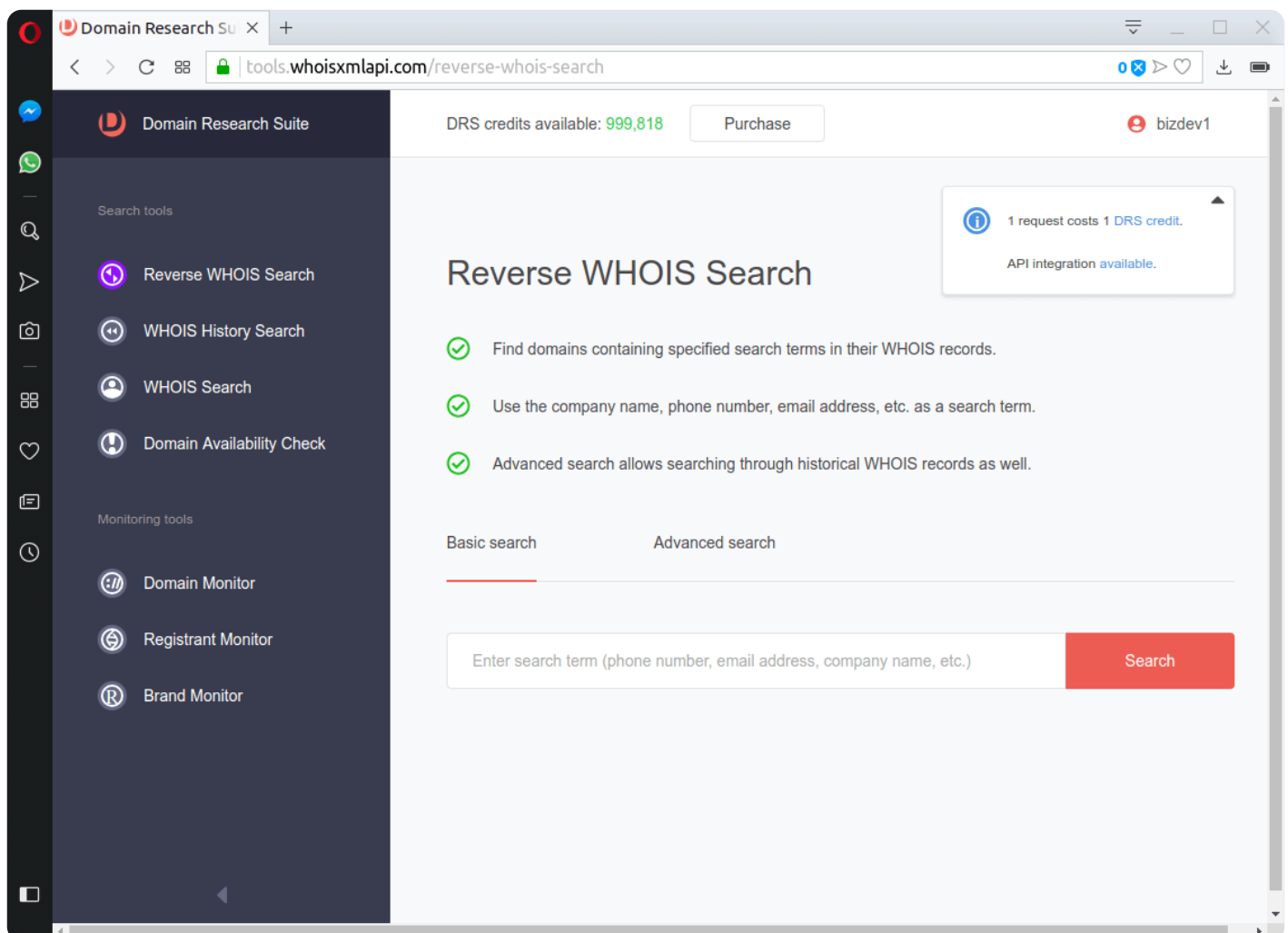
You may be asking yourself what practical uses a reverse WHOIS search has. Here is a list of some things that the [Reverse WHOIS Search](#) service or the [Reverse WHOIS API](#) can do for you:

- **Cybersecurity:** Cybersecurity analysts and researchers use reverse WHOIS 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, 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, 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, use reverse WHOIS information to identify new business and partnership opportunities and locate potential buyers.

Now we shall act as an analyst and use interactive approach. To do so we visit the webpage of [Domain Research Suite](#).

First, you need to register your free account (in case you do not yet have an account for this or any other API service here). The free account, which comes with 50 credits, is perfectly sufficient if you want to give it a try, or you are in the occasional need of analyzing some pages. If you need more, you can purchase additional access at a reasonable price. We have a flexible pricing structure tailor-made for varying 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 all close at hand, on the panel on the left:

- The Search tools:
 - Reverse WHOIS search;
 - WHOIS History search;
 - WHOIS Search;
 - Domain Availability check;
- and the Monitoring tools:
 - Domain Monitor;
 - Registrant Monitor;
 - Brand Monitor.

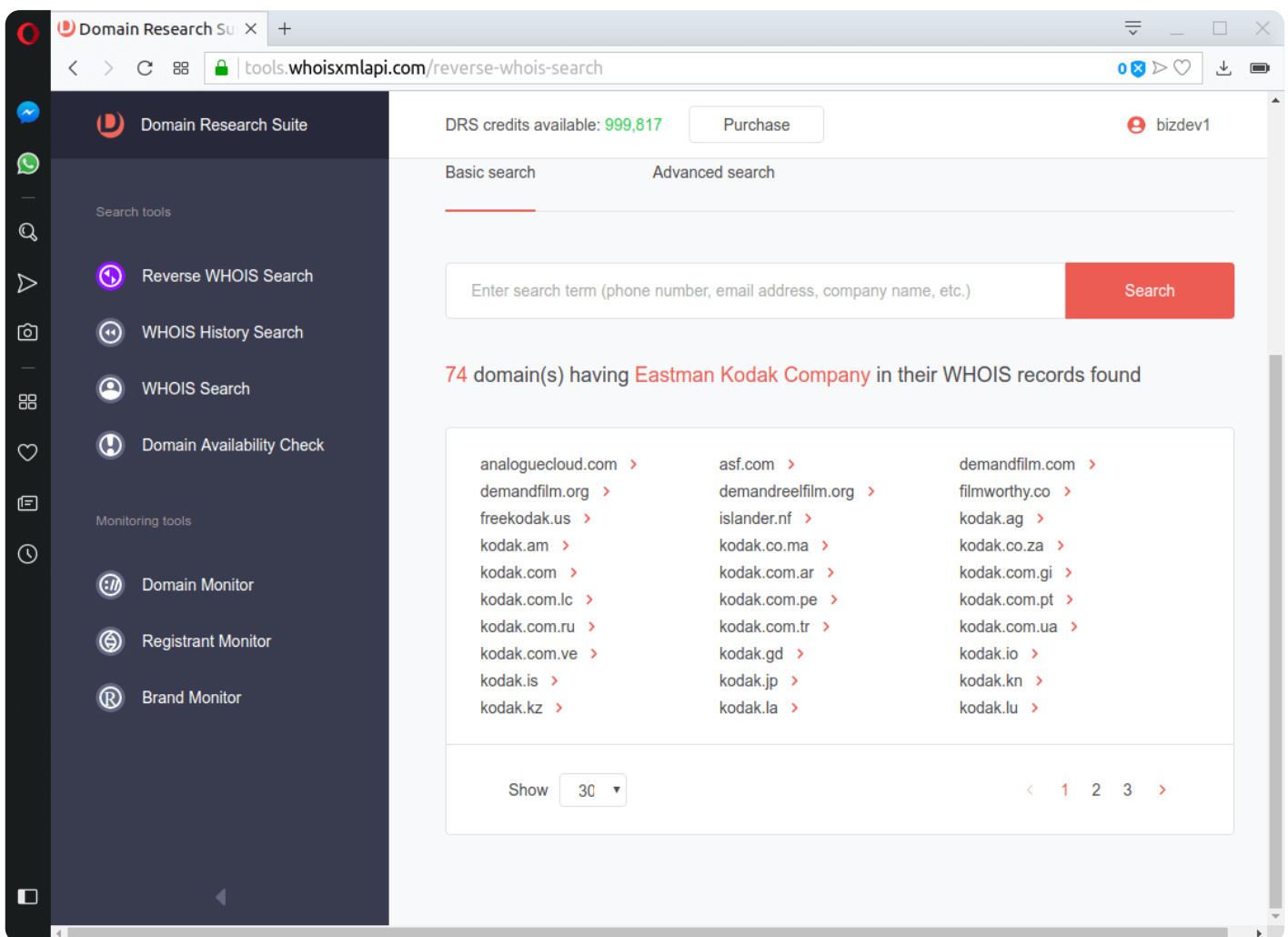
By default, we see the Reverse WHOIS search, the very tool we are about to take a good look at. Let us now get started.

2. Our example: Eastman Kodak Company

As the author of this blog is also interested in photography, we opt for the Eastman Kodak Company, or Kodak in short, which has always played a significant role in both production and innovation for photographic technology. Let's find out what they have on the web.

2.1 Basic search

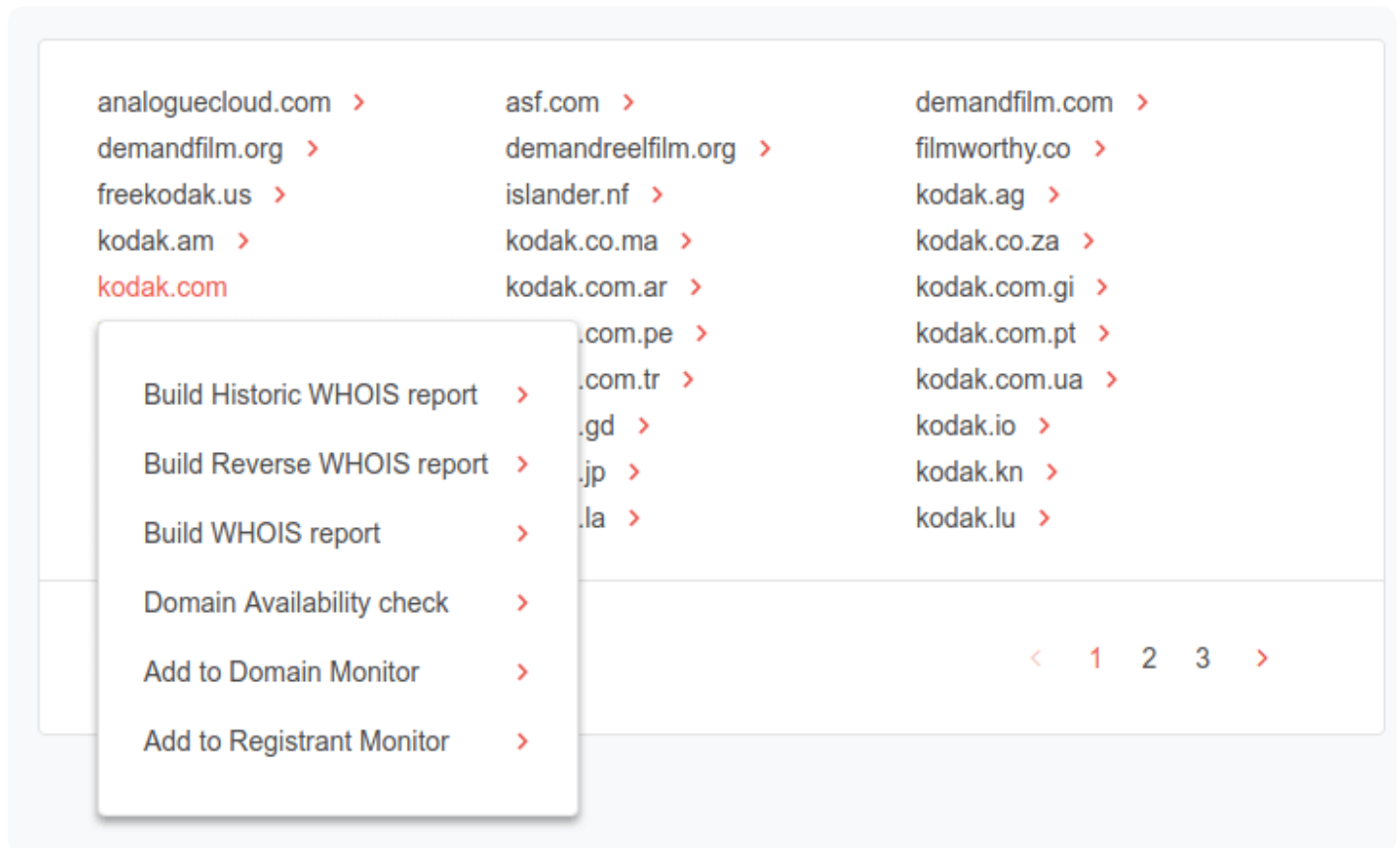
First we do a basic search. After entering "Eastman Kodak Company" in the input field of basic search and pressing the "Search" button, we find the following:



You can see a list of 74 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. This is what we were primarily looking for: a complete list of domains actually 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 see "kodak.com". Clicking on the given line we have the following choices:



The WHOIS report will display the current WHOIS record and reveal contact information, relevant dates (i.e., creation, last updated, and expiration), and other information. What may be even more interesting is the Historic WHOIS report, which provides all the previous statuses of the WHOIS record of the domain, from the year 2012 on 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 its registration 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 may also indicate restrictions imposed on the name's use, if any.
- **Registrant contact details.**

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 would like 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 this could result in the revocation of a website's license to operate.



Historical WHOIS record(s) for **kodak.com**

12

Historical record(s) found

2

Different domain registrar(s)

92%

Records with public ownership data

240

Change(s) detected

2

Different domain owner(s)

2,399

Day(s) of tracking the domain

Record(s) by date ↓

Feb 08, 2019

Jan 08, 2018

Jul 13, 2017

Mar 31, 2017

WHOIS record on **February 8, 2019**

Domain age

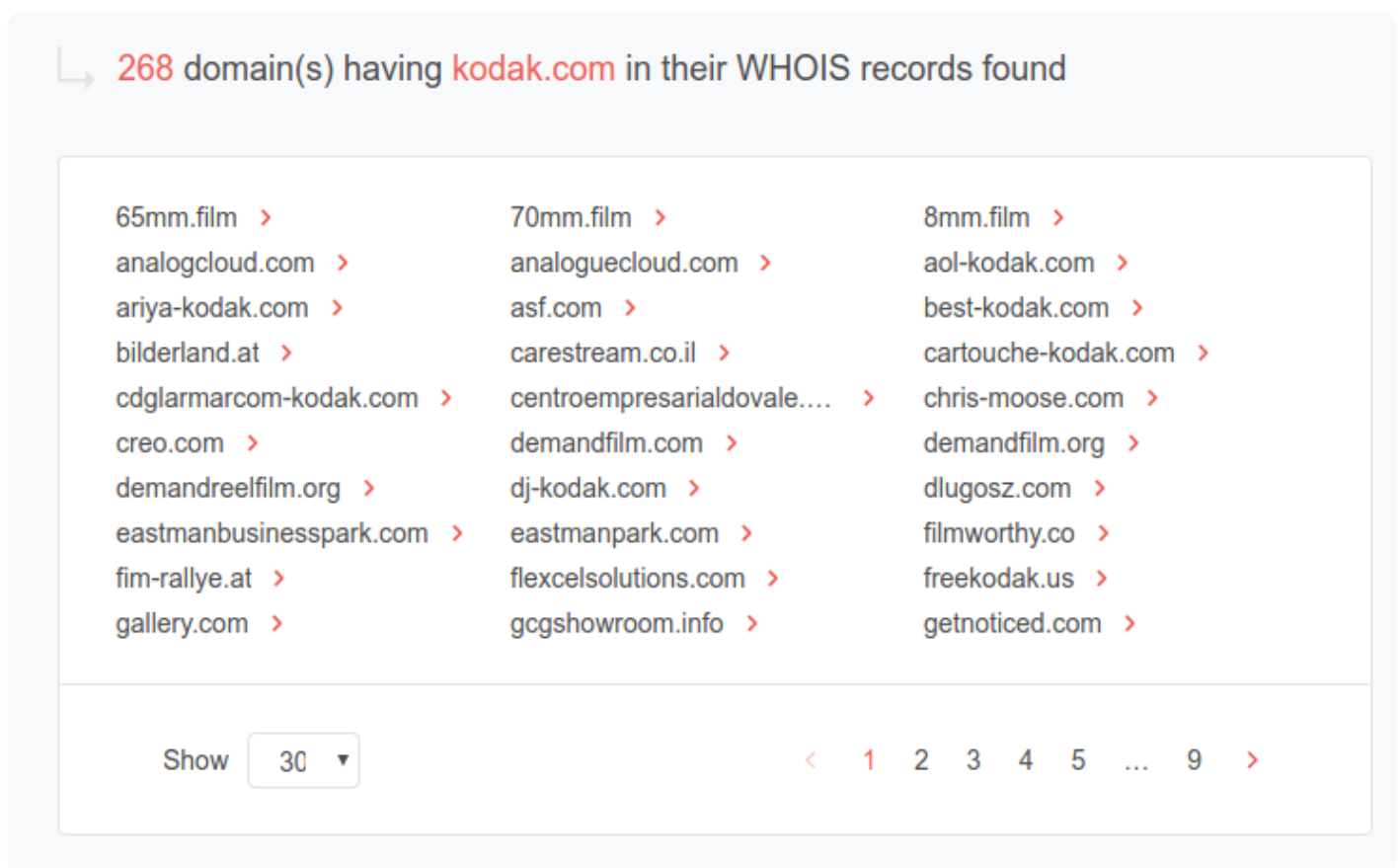
Created Date: September 16, 1988 04:00:00 UTC

Updated Date: September 11, 2018 05:53:42 UTC

Expires Date: September 15, 2019 04:00:00 UTC

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 12 versions of the WHOIS records the domain has had since 2012 in full detail. The cumulative numbers in the top blocks are also quite interesting as they can reveal company name changes, etc. "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 on the way, we still have WHOIS as the only method to find out who owns a domain.

Let us build a "Reverse WHOIS report" of "kodak.com":



↳ 268 domain(s) having **kodak.com** in their WHOIS records found

65mm.film >	70mm.film >	8mm.film >
analogcloud.com >	analoguecloud.com >	aol-kodak.com >
ariya-kodak.com >	asf.com >	best-kodak.com >
bilderland.at >	carestream.co.il >	cartouche-kodak.com >
cdglarmarcom-kodak.com >	centroempresarialdovale.... >	chris-moose.com >
creo.com >	demandfilm.com >	demandfilm.org >
demandreelfilm.org >	dj-kodak.com >	dlugosz.com >
eastmanbusinesspark.com >	eastmanpark.com >	filmworthy.co >
fim-rallye.at >	flexcelsolutions.com >	freekodak.us >
gallery.com >	gcgshowroom.info >	getnoticed.com >

Show 30 ▾

< 1 2 3 4 5 ... 9 >

As you can see now, "kodak.com" has been searched for in all fields of WHOIS records, so the resulting page contains records which were registered under an alternative name of the company. For instance, the WHOIS record of "analogcloud.com" reveals that it was registered by "Eastman

Kodak" (without "Company"). Another possibility is that the domain may be owned by a different company which has to do something with it (Affiliates, third party companies selling Kodak goods, etc.).

To give an example from the present query, "islander.nf" is run by "Norfolk Island Data Services Ltd. Pty.", but their administrative contact appears to coincide with that of the Eastman Kodak Company. The domain may have been bought by Kodak or its affiliate though a quick Google search 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 is done by tricking a company's customers into giving away their personal information (name, address, phone number, email address, 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.

2.2 Advanced search

Let us now explore the "Advanced search" tab and more possibilities to pivot on. You may ask what possible reasons you could have to use this feature. Say, you have been receiving bills from a supposed Kodak company or 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 made-up hypothetical scenario which was just provided for context). Where do you start?

Within "Advanced search" we are also offered 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 shall go for "Specific WHOIS fields", which enables us to give conditions specific to fields of the WHOIS record, e.g. the Registrant's country.

In particular, we shall look for actual domains

- having a name starting with "kodak" and
- having a registrant in Australia:



Basic search

Advanced search

Search where

☐ Anywhere ?

☒ In specific WHOIS fields ?

Search term(s)



Starts with



kodak

Domain Name



Includes



AUSTRALIA

Registrant Contact: Country



Add term

Search through domains

☒ Actual ?

☐ Historic ?

☐ Recently updated ?

Search

10 domain(s) having your specific search terms in their WHOIS records found

[kodak.ai](#) >

[kodakheritagecollections.org](#) >

[kodakonojavan.com](#) >

[kodakview.com](#) >

[kodakam.com](#) >

[kodakminingrigs.com](#) >

[kodakpicturenetwork.com](#) >

[kodakgalery.com](#) >

[kodakoart.com](#) >

[kodakpixpro.com.au](#) >

Let's take a closer look at "kodakpixpro.com.au". A WHOIS report reveals the following:



↳ WHOIS record for kodakpixpro.com.au

Registrar Name

TPP Wholesale Pty Ltd >

WHOIS Server

whois.auda.org.au >

Name Servers

[NS1.PARTNERCONSOLE.NET](https://ns1.partnerconsole.net) >

[NS2.PARTNERCONSOLE.NET](https://ns2.partnerconsole.net) >

[NS3.PARTNERCONSOLE.NET](https://ns3.partnerconsole.net) >

Status

serverRenewProhibited

<https://afiliass.com.au/get-au/whois-status-codes#serverRenewProhibited>

Registrant Contact

Registrant Name: [Directed Electronics Australia Pty Ltd](#) >

So it is owned by "Directed Electronics Australia Pty Ltd". Notice the little red arrow (>) after this Registrant Name: when clicking on, we are offered two options:

- Build Reverse WHOIS report
- Add to Registrant 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 about earlier when doing a Basic search. Note that all [Domain Research Suite](#) reports are downloadable in either CSV or PDF formats.

If we want to monitor the activity 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 by the means of a mere click and choosing to do so.

Apart from monitoring registrant changes, you can also check for domain and brand changes via the Domain Monitor and Brand Monitor, respectively, to stop a variety of threats like, for example, 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 (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 Monitoring to keep track of domains that look very similar to yours in real time

The same can be done with domains with Domain Monitoring. 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 Monitoring. All it takes you is a few extra mouse clicks on the Advanced search tab of the Reverse WHOIS Search tool.

So if we want to monitor the activity of this registrant, we can do that easily from here as well. But right now we go for the reverse WHOIS report. Indeed, we can pivot on the Registrant Name, resulting in the following:

↳ 112 domain(s) having **Directed Electronics Australia Pty Ltd** in their WHOIS records found

3sixtycam.com >	3sixtycamera.com.au >	alliancefleetonline.com.au >
ankeranz.com >	archium.com.au >	audiosavings.com.au >
avital.com.au >	cartech4you.com.au >	cat12volt.com.au >
dashkam.com.au >	dashmate.co.nz >	dashmate.com.au >
dashmate.net >	directed.com.au >	directeddevelopment.com.... >
directedintelligence.com >	directedintelligence.com.au >	directedtelematics.com >
directedtelematics.com.au >	directedtesting.com.au >	dronenation.com.au >
fusotelematics.com >	fusotelematics.com.au >	fyndr.com.au >
g-traq.com >	gear4.com.au >	isuzucustomsound.com >
isuzudrivesafe.com >	isuzudrivesafe.com.au >	isuzufleet.com.au >

Show 30 ▾

< 1 2 3 4 >

They appear to be running 112 domains – a remarkable player of the market indeed. And we can continue our search on each domain by finding current or historic WHOIS records and then possibly pivoting on any fields in the resulting data.

3. Summary

We have demonstrated the [Reverse WHOIS Search](#) tool of [WhoisXML API's Domain Research Suite](#) in action. It is an easy-to-use, flexible, and pivotable tool, orchestrated with various other Search and Monitoring facilities. All of those 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 5.2 billion historic WHOIS records, over 582 million domains tracked, more than 2,864 TLDs tracked, and over 10 years of data crawling experience, [WhoisXML API](#) through its [Domain Research Suite](#) 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](#).