Cyber Hunter Academy Explains How They Use WhoisXML API Tools to Teach OSINT

By Naiara Morales, cyber intelligence instructor at Cyber Hunter Academy.

Following our roadmap of collaborations with prestigious partners, today we want to talk about WhoisXML API. Many will know this name, but for those of you who don't, I would like to tell you who they are. The WhoisXML API team has been collecting, analyzing and correlating domain, IP, and DNS data for years. We're talking billions of pieces of information, which provides an unmatched scope for our research.

WhoisXML API's goal is aligned with Cyber Hunter Academy's "Make the Internet a safer place". We focus on teaching and high-level training to achieve that goal. They provide ready-to-use data as a source of intelligence. As you will see, our collaboration is obvious.

We assume the service provided by the WhoisXML API to have two major audiences. On the one hand, they have proven valuable in augmenting the capabilities of SIEMs, Threat Intelligence Platforms (TIPs), and SOCs around the world. On the other hand, the speed, scope and historical value of the data is a valuable tool for all analysts looking for reliable information.

In addition, WhoisXML API is integrated with Maltego. Here I would like to make an explanation for our Junior students. Maltego is an open-source intelligence tool (OSINT) security investigators use to gather data relevant to their investigations. It extracts data from various sources via transforms. Maltego's Transform Hub allows investigators to collect data from over 30 data partners under diverse categories, such as blockchain, social media, web content, and threat intelligence. As you can see, it is a powerful tool that also allows the information to be presented in the form of graphs. These graphs are very useful in the Analysis phase, but also in the Information Dissemination phase. Personally, I find it a great tool to use during an investigation.

Going back to WhoisXML API, what does this integration bring to us, as Analysts? Well, Maltego transforms provide us with several functionalities:

- **WHOIS Lookup:** Users can identify the current owner of a particular domain name by extracting registration details from the WHOIS Records Transform set. That allows investigators to see who is responsible for a suspicious or malicious domain.

- **Historical WHOIS Lookup:** In most instances, current WHOIS records are redacted or privacy-protected. However, with the To Historical WHOIS Records [WhoisXML] Transform, investigators can trace past ownership records and see website owners' real identities. A domain name or an IP address can serve as a starting point for a historical WHOIS lookup, coming in handy for cybercrime and person of interest investigations. Personally, I would like to point out that since the WhoisXML team has been collecting data for decades, with their tool we will often find information that would be impossible with others.

- **Reverse WHOIS Search:** With a single keyword, investigators can look up domain names that contain the text string in their WHOIS records. Users can thus see domain names that have a particular email address, company name, nameserver, mail server, registrant country, or any other WHOIS data point. Combining Maltego transforms with WhoisXML advanced searches can be a combination that makes all the difference in an investigation.

Now, let's look at a practical case. We are going to perform a search for information about the domain presstv.com, and then compare the results we get with different tools. We encourage you to do the test at the same time as us with your favorite whois tool.
As expected, the result we get is Redacted.

```
Domain Name: presstv.com
Registry Domain ID: 85275201_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.instra.net
Registrar URL: http://www.instra.com
Updated Date: 2020-04-05T08:10:52Z
Creation Date: 2002-04-05T03:55:48Z
Registrar Registration Expiration Date: 2021-04-05T02:55:48Z
Registrar: Instra Corporation Pty Ltd.
Registrar IANA ID: 1376
Registrar Abuse Contact Email: abuse@instra.com
Registrar Abuse Contact Phone: +61.397831800
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Auckland District
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: NZ
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: info@domain-contact.org
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
```

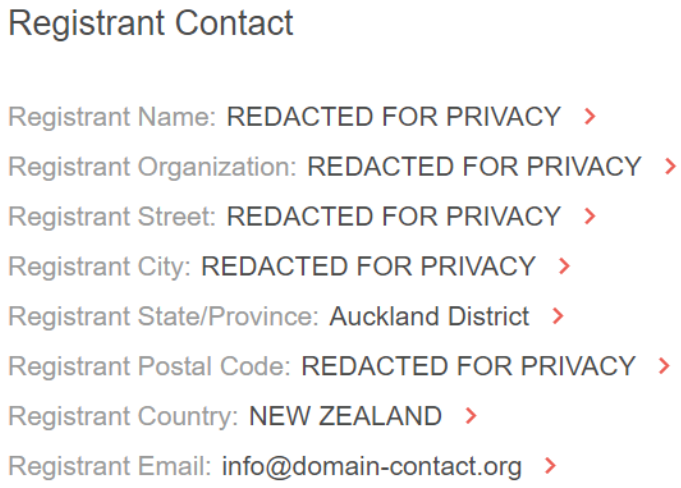
Let's try another one. Again, we get no useful information.

```
Registrant Contact Information:
        Name                                    REDACTED FOR PRIVACY
        Organization                            REDACTED FOR PRIVACY
        Address                                 REDACTED FOR PRIVACY
        Address                                 REDACTED FOR PRIVACY
        City                                    REDACTED FOR PRIVACY
        State / Province                        Auckland District
        Postal Code                             REDACTED FOR PRIVACY
        Country                                 NZ
        Phone                                   REDACTED FOR PRIVACY
        Fax                                     REDACTED FOR PRIVACY
        Email                                   info@domain-contact.org

Administrative Contact Information:
        Name                                    REDACTED FOR PRIVACY
        Organization                            REDACTED FOR PRIVACY
        Address                                 REDACTED FOR PRIVACY
        Address                                 REDACTED FOR PRIVACY
        City                                    REDACTED FOR PRIVACY
        State / Province                        Auckland District
        Postal Code                             REDACTED FOR PRIVACY
        Country                                 NZ
        Phone                                   REDACTED FOR PRIVACY
        Fax                                     REDACTED FOR PRIVACY
        Email                                   info@domain-contact.org

Technical Contact Information:
```

Now, let's use WhoisXML API. The first thing I would like to point out is the number of snapshots of information available:

We have a history of information going as far back as 2011.

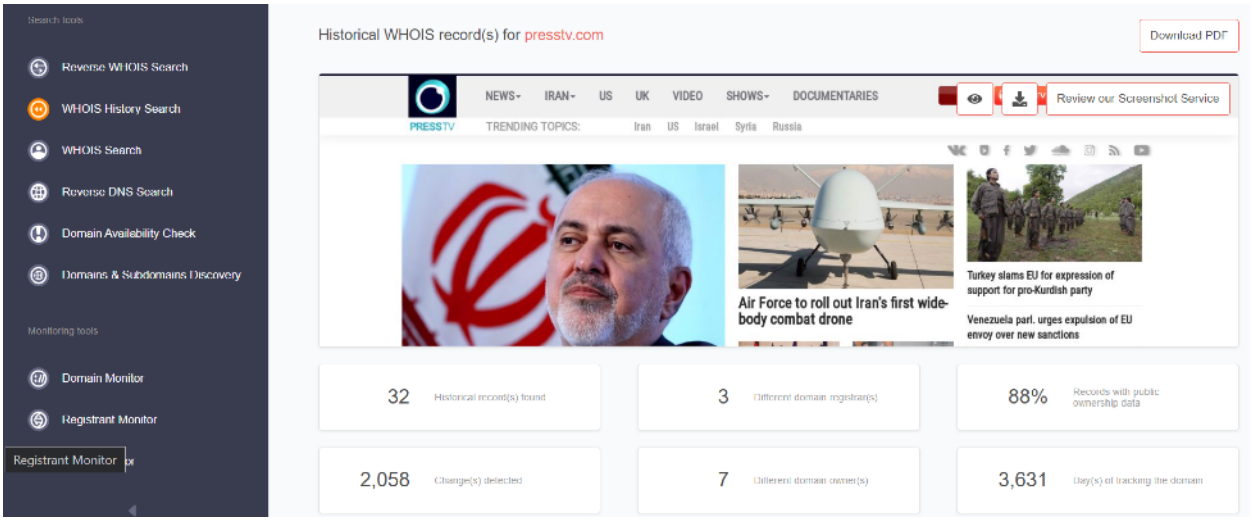
When reviewing the most recent record, which is from 2021, we see that the information is censored. This is expected, because the provider, in compliance with the legislation, has hidden the information, presumably because it was requested to do so by the registrant. [image 5]



But this is where this gets interesting. If we go back to 2016, we will find un-censored domain registration details. And if we go as far back as to 2011 we'll find different domain registration details.

WhoisXML API has provided useful information for our research, and not just one lead to tap into, but several.

In addition, and I love this, WhoisXML API shows us a preview of the domain. This can be of interest when we do not want to access it yet, but we want to see what it looks like without them detecting our presence.



As you can see at the bottom of the image, WhoisXML API also provides us with some statistics about the data it has. Here we can see that, in fact, there are not two, but three log data at our disposal.

With this real example, it is clear that WhoisXML API goes where other tools cannot.

At Cyber Hunter Academy, we are methodical in our training. One of the things we never cease to repeat to our students is that Intelligence has to be actionable and that it has to arrive at the right time and in the right fashion. A perfect report that arrives late loses its value. That's why we encourage our students, especially professionals, to invest in the tools that can make a difference in their investigations. WhoisXML API is one of them, in terms of the quality of the data it provides, its well-organized interface, its coverage and the speed it provides.