WHOIS Data Aids Lighthouse Reports Shed Light on Years-Long Surveillance Operations

Posted on October 10, 2022

Lighthouse Reports is a nonprofit investigative news organization that undertakes extensive investigations to create an impact and facilitate real-world changes. They employ modern investigative tools and methods, including open source intelligence (OSINT), algorithmic auditing, social media listening, and data mining.

Media partners, such as The Guardian, Le Monde, Der Spiegel, SRF, and Republik, publish Lighthouse Reports investigations in several European Union (EU) countries.

WhoisXML API's data was a part of a massive investigation by Lighthouse Reports entitled “ Revealing Europe’s NSO.” This investigative project brought to light the proliferation of cyber surveillance technology in Europe.

Revealing Europe’s NSO: An Overview

Lighthouse Reports recently performed a comprehensive investigation exposing a massive cyber surveillance outfit operating in Europe. The threat actors hid behind an Italy-based company called “RCS Lab” and rode on phone networks to send thousands of tracking packets worldwide. As a result, the threat actors were able to access users’ locations, messages, contacts, photos, and other information. They also intercepted and recorded calls.

This alarming cyber surveillance tactic prompted confidential sources to track suspicious traffic, providing Lighthouse Reports with enough data to initiate an investigation. During the course of their inquiry, cybersecurity experts provided Lighthouse Reports with a list of fake domain names confirmed to have been used by the threat actors in luring victims to download malicious software.

Lighthouse Reports enriched the domains with WHOIS data provided by WhoisXML API, enabling them to determine the span of the malicious operations. While some domains were registered as early as 2015, others were added more recently, specifically in March 2022.

“We analyzed this list using the domain database of WhoisXML API and found that RCS Lab purchased some of these fake domains as early as 2015, while others were bought in March this year, indicating years of potential hacking operations by the company,” the researchers disclosed.

It Takes a Village to Build Internet Security

As an active and long-standing advocate of Internet transparency and security, WhoisXML API continues to work with the security community to unmask malicious digital infrastructure by providing WHOIS, DNS, and IP contextualization to cyber incidents and resources.

Our vision and goal align with the efforts made by Lighthouse Reports in exposing the massive cyber surveillance operation in Europe. Investigations like this can unearth weaknesses and lapses that may have contributed to the success of featured malicious campaigns.

“Revealing Europe’s NSO,” for instance, found that some global phone providers have not patched an eight-year-old vulnerability that the threat actors exploited. Industry practices and government policies were also cited as contributing factors to the cyber surveillance operation’s alarming reach and success.

In the words of CEO Jonathan Zhang, “Cybersecurity requires collaboration between all stakeholders. WhoisXML API’s part is to provide contextual information in the form of WHOIS, IP, and DNS intelligence. Security teams use our data to enrich processes and, thus, help contribute to a more transparent and safer Internet.”

We are constantly on the lookout for joint research projects and investigations. Please feel free to contact us for inquiries.