Domain Registration Data Aids in Understanding the State of Online Scams

Posted on November 7, 2022

For over a decade now, ScamAdviser has been helping consumers make safe and informed online shopping decisions by allowing them to check a website's trust scores, report scams, and learn about the different types of online scams.

As part of this initiative, ScamAdviser has been investigating how countries worldwide are fighting online scams through their annual "The Global State of Scams Report." Their mission is aligned with WhoisXML API's aim to realize a safer and more transparent Internet.

In line with this, we collaborated with ScamAdviser in The Global State of Scams Report for 2022 by providing domain registration data that allowed them to see online scams through the DNS lens. WhoisXML API CEO Jonathan Zhang also participated in an interview published in the same report.

The 2022 Global State of Scams Report: An Overview

If there's anything we have learned in the last couple of years, it's that scammers take advantage of everything—from global events, such as the Coronavirus vaccination, pandemic-related financial stimulus packages, and the war between Ukraine and Russia to personal struggles in romance and finances.

Moreover, online scams are no longer concentrated in certain countries. They have gone global, with more countries stating that scams comprise the most reported type of crime.

ScamAdviser found that online scams remained among the most underreported crimes. Some of

the most common online scams are:

- Investment scams
- Romance scams
- Online shopping scams
- False billing scams
- Remote access scams

In 2021, around 293 million scams were reported, and approximately US$55.3 billion was lost worldwide. The largest amount scammers took in a single case was US$6.4 million.

As scammers continue to abuse digital properties, social media, and technologies to lure victims in, these figures may continue to rise.

The Fight against Scammers

ScamAdviser reported that while more countries are centralizing their anti-cybercrime efforts, scams are still not a priority. This could be because of the number of countries involved and the bureaucracy it entails. For instance, scam cases in a given country may originate from somewhere else.

How, then, can we effectively fight against scammers?

Raising awareness can't be the be-all and end-all strategy. "Prevention could take the form of a global sharing system of scam data (be it domains, email addresses, cryptocurrency addresses, or bank accounts). The data cannot only be used to help consumers check if they run the risk of getting scammed, but also proactively block or take down malicious assets," says ScamAdviser.

Data sharing and Internet transparency are part of WhoisXML API's mission, and we contribute by providing the cybersecurity community with domain, DNS, and IP intelligence.

For instance, in a recent study on business impersonation in the DNS, we found more than 49,000

cybersquatting domains targeting some of the largest companies worldwide. The data from these types of research can help organizations and consumers assess their risk of getting scammed. It can help the cybersecurity community proactively block and take down malicious web properties.

Reiterating Jonathan Zhang's statement in his interview with ScamAdviser, "We help our clients fight fraud by aiding security teams and cybersecurity companies in real-time DNS-based threat contextualization. Law enforcement agents, threat hunters, and private investigators also work with us to find DNS cues, add context to indicators of compromise (IoCs), and find new artifacts with hidden connections."

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