Jonathan Zhang, WhoisXML API: “DNS abuse instances are among the top threats we see when monitoring domain and DNS activity”

Posted on May 16, 2022

While the world is facing major crises of the century, cybercriminals are taking advantage of the situation and are rapidly setting digital traps in numerous creative ways. Cyberattacks affect not only individuals but also organizations and governments, begging for top-notch tools to help combat the threats.

The Cybernews team has invited Jonathan Zhang, the CEO of WhoisXML API, an Internet and security data aggregator, to discuss the importance of data and the current situation in the cybersecurity field.

What has the journey for WhoisXML API been like?

WhoisXML API was founded out of a market need I identified after years of working with organizations like NASA JPL and L-3 Communications. I was a software engineer around 2010 and needed access to structured and unified raw WHOIS data for a network security project.

The challenge was that WHOIS records were highly disaggregated and came from multiple registries and registrars, each with a different format. While it was theoretically possible to consolidate everything, the job would have required hundreds if not thousands of work hours. There were also other limitations like lookup restrictions, and while I could think of a few providers of unified data back then, they were quite expensive. The bottom line—nothing made sense to me at the time.

So the problem remained. I mean, how can one achieve optimal network security without the necessary data?

The solution was to create a company that would help make the Internet a safer place for all organizations. And what better way to work toward that goal than by providing a building block for security systems, which is data.

Can you introduce us to what you do? What methods do you use to collect and analyze such large amounts of data?

At its core, WhoisXML API is an Internet and security data aggregator. We offer complete, real-time, and actionable data using a data-as-a-service model.

Through legal partnerships, we collect WHOIS, IP, and domain data from different aggregators like ISPs, registrars, and registries. We then parse, analyze, and normalize vast amounts of data using advanced data sensing technology and machine learning algorithms.

We enable various use cases, notably to amplify crucial cybersecurity practices and contribute to security platforms designed to mitigate cyber-attacks and protect organizations. For instance, our data can help scope out attack surfaces, giving organizations clearer and broader visibility. At the same time, we have clients who use our data for third-party risk assessment and management.

Threat investigators and law enforcement agencies use our data to look for clues when investigating cybercrime. You may have an IP address, a person's name, an organization's name, a website, an email address, a nameserver, or any related data point. From there, our data can help you map out the actor's digital footprint.

Our domain and IP intelligence also supports phishing prevention and brand protection. We do that by mainly providing real-time information about newly registered and cybersquatting or typosquatting domains.

All these use cases are aligned with the company's initial goal of making the Internet a safer place.

Across all industries that you work with, what types of threats are the most common nowadays?

DNS abuse instances are among the top threats we see when monitoring domain and DNS activity. These threats include phishing, malware attacks, spamming, and botnet attacks.

A contributing factor is the growing number of domains across different TLDs. As they increase, the potential for DNS abuse also grows. In March 2022 alone, the ICANN classified more than 609,000 domains across 360 TLDs as security threats.

With a satellite view of domain and DNS activity, we continue to encounter thousands of typosquatting domains or domains that impersonate legitimate brands. Some domain groups impersonate car manufacturers, airline companies, luxury brands, NFT platforms, CEOs, and many others.

Several of these typosquatting domains are often already flagged as malicious, which means they have already been abused to display phishing or spam content, for example. Others may have been used to distribute malware or as C&C server URLs.

DNS abuse is further amplified by its time-sensitive nature. Attackers work round-the-clock. If a company's defenses go down for even a minute, that could be enough time for the threat actors to infiltrate corporate networks. One undetected phishing domain that manages to go through security filters may be enough to launch a ransomware attack.

READ THE FULL ORIGINAL ARTICLE >>