EINPRESSWIRE

WhoisXML API Seeks Media Partnerships to Raise Public Awareness of COVID-19 Security Threats and Typosquatting

Newly registered pandemic-themed domain names containing words like “covid,” “coronavirus,” “lawsuit,” “mask,” “vaccine,” etc. can be phishing traps.

LOS ANGELES, CALIFORNIA, U.S., June 8, 2020 /EINPresswire.com/ -- Cyber threat intelligence provider WhoisXML API launches a Media Partnership Program open to any journalist, public relations specialist, security blogger, and other media professional. The partnership covers free access to WhoisXML API’s domain, IP geolocation, and DNS data and the company’s set of research and monitoring tools. WhoisXML API’s researchers and data scientists are also available upon request to provide support with complex data extraction, analysis, and representation.

The WhoisXML API Media Partnership Program was initiated following a successful collaboration with a Bloomberg columnist, whose story demonstrated an exponential increase in the number of newly registered COVID-19-themed domains. WhoisXML API’s data reveals that at least 56,000 COVID-19-related websites have been put up since the beginning of the year—from about 1,100 in January to 4,900 in February to over 50,000 in March 2020.

Spikes were also noticeable as new events occurred, such as Mike Pence being put in charge of the U.S. COVID-19 response and President Donald Trump’s televised address on March 11. Among the top-level domain (TLD) extensions most used for registration were .com (62.5% of sites), .org (8.7%), .net (4.5%), and .uk (4.3%). WHOIS ownership data showed that the top registrant countries were the U.S., Canada, Panama, the U.K., and Spain.

Large-scale bulk domain registrations can be indicative of cyberattacks in the planning stage or already in execution. In the words of WhoisXML API Founder and CEO Jonathan Zhang:

“The COVID-19 pandemic has affected the world in ways we couldn’t have imagined a few months ago. Cybercriminals are trying to take advantage of the chaos, and people need to watch out for online threats. With this media partnership program, we want to help raise public awareness by providing free access to domain intelligence and other cyber threat intelligence sources to the media.”

Zhang added:

“Typosquatting or URL hijacking, the act of registering confusing domain names, is not a new concern within the cybersecurity community. We saw this squatting practice taking place in many of our investigations. In our experience, typosquatting can lead to full-blown cyberattacks with vectors that include phishing emails and copycat websites.”

ProPrivacy, in partnership with VirusTotal and WhoisXML API, found that almost a third of coronavirus-themed domain names are harmful. The open data project, the largest of its kind, showed that some 98,000 of the 300,000 domains analyzed were malicious. It highlighted as well that registrations frequently spike following world events and news coverage. For instance, a 648% increase in malicious domain registrations was recorded on the day the World Health Organization (WHO) named the disease “COVID-19.” An increase in the number of daily domain registration was also noticed, from 1,306 to 2,672, after the outbreak had been declared a pandemic.

The WhoisXML API research team has also been studying coronavirus-themed domains and found that registrations can be highly specific. They cited the following cases as examples:

The shortage of medical and personal protective equipment (PPE) with domain names such as coronavirusn95mask[.]com, buyn95coronavirusmask[.]com, kn95salecoronavirus[.]com.

The Coronavirus Aid, Relief, and Economic Security (CARES) Act and the release of monetary stimulus checks. Related domain names included covid19stimulusloanassistance[.]com, donateyourstimuluscheck[.]org and coronavirusstimuluspackage[.]org.

Legal actions as a result of layoffs, cancellations, and mishandling due to the pandemic with domain names such as cruisecoronaviruslawsuit[.]com, covidhospitallawsuit[.]com, and covidworkerlawsuit[.]com.

According to a WhoisXML API researcher:

“We see a lot of niche registrations in our typosquatting data feed files. Registrants seem to target vulnerable groups. We suspect that these domains could serve as social engineering baits and trigger emotional responses.”

For more information about the WhoisXML API Media Partnership Program and how our data can help media professionals, please contact us.

WhoisXML API works with cybersecurity enterprises, including security platform vendors, SOCs, MSSPs, Fortune 1000 organizations, government agencies, and small businesses seeking to obtain in-depth information on online threats and their sources. The company has been collecting, processing, and delivering complete domain, IP, and DNS intelligence for more than a decade. WhoisXML API’s products are the result of advanced machine learning and data science processes used to build better security processes, tools, and platforms.

Media Team
WhoisXML API
email us here
+1 800-207-0885