ProPrivacy Open Data Project: Mapping Malicious Coronavirus Domains Using WHOIS Data

Posted on July 13, 2020

The COVID-19 pandemic has driven many people to do almost everything within the confines of their homes. Nearly exclusive reliance on digital means to work, study, shop, and communicate amid uncertainty opened many avenues for cybercrime to take place—notably through the use of coronavirus-related domain names.

To demonstrate this trend, ProPrivacy has partnered with WhoisXML API and VirusTotal to investigate the extent to which cybercriminals are weaponizing the Domain Name System (DNS) in an open data project called “COVID-19 Malicious Domain Research Hub.”

The Open Data Project: Objectives

Domain names, especially newly registered ones, have long been used by cybercriminals in

phishing campaigns, malware attacks, financial scams, and other nefarious activities. Even before the coronavirus pandemic, many newly registered domains (NRDs) were found to be malicious or suspicious, at the very least.

To gain a perspective on how many coronavirus-related domain names are being used maliciously, ProPrivacy started the open data project. The project has simple, interrelated objectives, enumerated below:

- To obtain a continuously updated list of domain names related to the COVID-19 pandemic;
- To determine whether or not these domains are used maliciously;
- To share this information with the general public.

Partnering with WhoisXML API

By providing access to its extensive Whois Database via API calls, WhoisXML API has helped ProPrivacy monitor coronavirus-themed registrations among the hundreds of thousands of new registrations occurring daily.

Once a domain name has been tagged “malicious” by VirusTotal, ProPrivacy runs this domain via WhoisXML API’s domain intelligence to retrieve its complete WHOIS records. Such records include registration and expiration dates, registrant names, and email addresses. To ensure the robustness and accuracy of the dataset, ProPrivacy also used WhoisXML API’s historical WHOIS record-retrieving API.

The open data project further highlighted the fact that domain name registration behaviors are often closely related to news events. In particular, the team detected a 648% increase in coronavirus-inspired malicious domain names the same day the World Health Organization (WHO) named the disease COVID-19.

The Open Data Project: Findings

The ProPrivacy open project is ongoing and revealed the following findings so far:

- ProPrivacy analyzed over 600,000 coronavirus-related domain names to date.
- More than 125,000 of the domains analyzed were deemed malicious after cross-referencing data from WhoisXML API's database and VirusTotal.

Check out the ProPrivacy COVID-19 Malicious Domain Research Hub here. The data can be accessed on their Github repository as well.

You can also learn more about WhoisXML API's database offerings by visiting the following pages:

- Newly Registered & Just Expired Domains Database
- WHOIS Database Download
- DNS Database Download