The footprint of coronavirus disease in domain name registrations

Posted on March 18, 2020

Cybercriminals use all possibilities which can serve their evil aims. They follow the headlines and react quickly – and they do not have ethical considerations. Even the drama of the coronavirus terrorizing the entire world and causing the deaths of thousands of people is seen as a good 'business' opportunity to spread out some malware.

IBM X-force recently reported that the coronavirus went cyber via the Emotet trojan. Rather disgustingly, the miscreants send e-mails to people on behalf of respected health organizations, containing attachments claiming to inform about infection prevention measures. As the victim opens the attachment, it silently installs the trojan on the computer.

Traditional phishers are also on board, a typical case is described by Kaspersky: a coronavirus-related message containing a link to an Outlook-looking page to collect login credentials. All this has attracted a lot of media attention, of course.

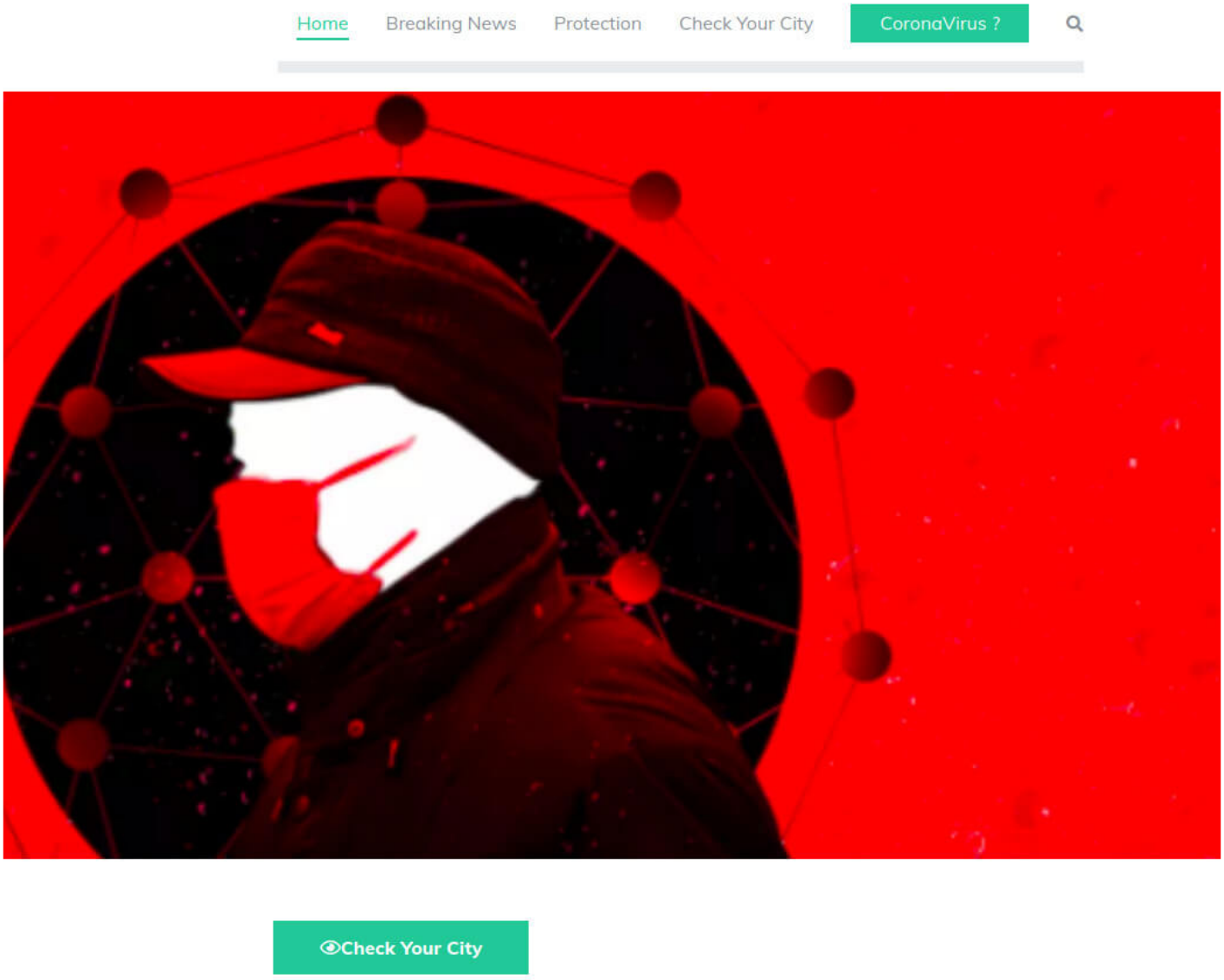
There are other footprints of the coronavirus disease in the cyberspace, too. WhoisXML API's "Typosquatting Data Feed" detects groups of domains which were registered on the same day, and whose names within each group are similar to each other. Looking at the feed data, it appears that as of 21 January, 2020, a burst of bulk domain registrations related to the coronavirus had started. It already resulted in the registration of more than 750 domains till 17 February.

A closer analysis of these domains shows that the majority of them are parked and are for sale. This is not at all unexpected: domainers, who make money from adding and selling domains, apparently expect to profit from these. And, as usual, the parked domains hold pay-per-click ad money collecting pages do so as well. While all this is of course legal, it does not help in finding reliable information sources about the coronavirus.

It is a matter of detailed investigation of individual domains to find those who are potentially related to phishing or malware. Checking data phishing and malware databases like PhishTank or Urlhaus , these domains were not found to be related to malicious activities. This is probably because, as was said before, miscreants prefer domain names looking similar to those of respected organizations for their purposes, and these were registered earlier and possibly in bulk, many similarly sounding domains a day. The Brand Alert API can be useful for finding those, but it is a problem that many of the acronyms, like CDC or WHO are very short, making it hard to find the

actually related pages.

So WhoisXML API tools can provide at least a set of suspicious pages which then can serve as a clue for further manual investigation. As an example, we have found a page which is a very good example of one which has to be treated with caution. A portion of the webpage on that domain looks like this:



The page look-and-feel apparently builds its effect on the fear of coronavirus. Looking at the details of the page, it is hard to decide if it is actually malicious or it is just a page under development. If it is the latter case, and it is benevolent, then it is nevertheless a perfect example of how not to develop a page that is meant to be trusted later.

First of all, why is a page under development publicly visible? And there is not even a sign there that it is not yet a functional page. Secondly, there is no reference to the entity running the page at all. Under "Breaking news" we find a few 3rd party blogs, whereas the "Protection" and "Coronavirus?" options take us to another page which is an apparently in-development web shop to sell masks. The main page shows numbers of "dead" and "infected" people without mentioning any source or scope for their data. Even more suspiciously, there is a "Phone" and "email" entry with a "Submit" button on the main page. Looking at the page source, it looks like an unfinished code not sending the data anywhere yet, but still: it is on a publicly visible page.

The Domain Reputation API points out further shortcomings. Apart from not following the recommendations of timings in the DNS, and having numerous issues with the mail server configuration, the SSL settings are also ill-configured. In addition, their SSL certificate was obtained on 26 January, and is only valid till April 25. Why would a serious company use such a short-lived certificate?

We can conclude that this page is either a seriously amateurish in-development one, visible publicly in a premature phase, illustrating how not to set up a business. Alternatively, it might be a misleading one on purpose. Altogether it is important to draw attention to society that especially in the case of such a serious disaster as the coronavirus, online resources should be used watchfully, and the use of tools (and common sense, of course) to verify their validity is a must-do.