WHOIS Lookups & Enterprise Cybersecurity Policies: A Secure Way to Search for Domain Names

Posted on July 27, 2020



These days, it's unwise to assume that all websites are safe to access. For this reason, security teams typically advise employees against clicking on any links embedded in an email, especially from an unknown sender. This recommendation may even extend to suspicious search results that appear in search engines.

What's more, for most companies, visiting websites that are not related to an employee's work is a violation of established cybersecurity policies and procedures. Most cybersecurity policies include:

- Standard steps for accessing work data and applications remotely
- Rules for encrypting emails
- Instructions on creating and managing passwords
- Rules on using social media
- Guidelines for accessing nonwork-related websites

While this last policy may sound extreme to some, it has become common practice, especially among companies that want to beef up their cybersecurity posture. Their stance is 'Prevention is better than cure'. And keeping employees from visiting potentially dangerous websites is always safer and more cost-effective than dealing with a ransomware attack or data breach.

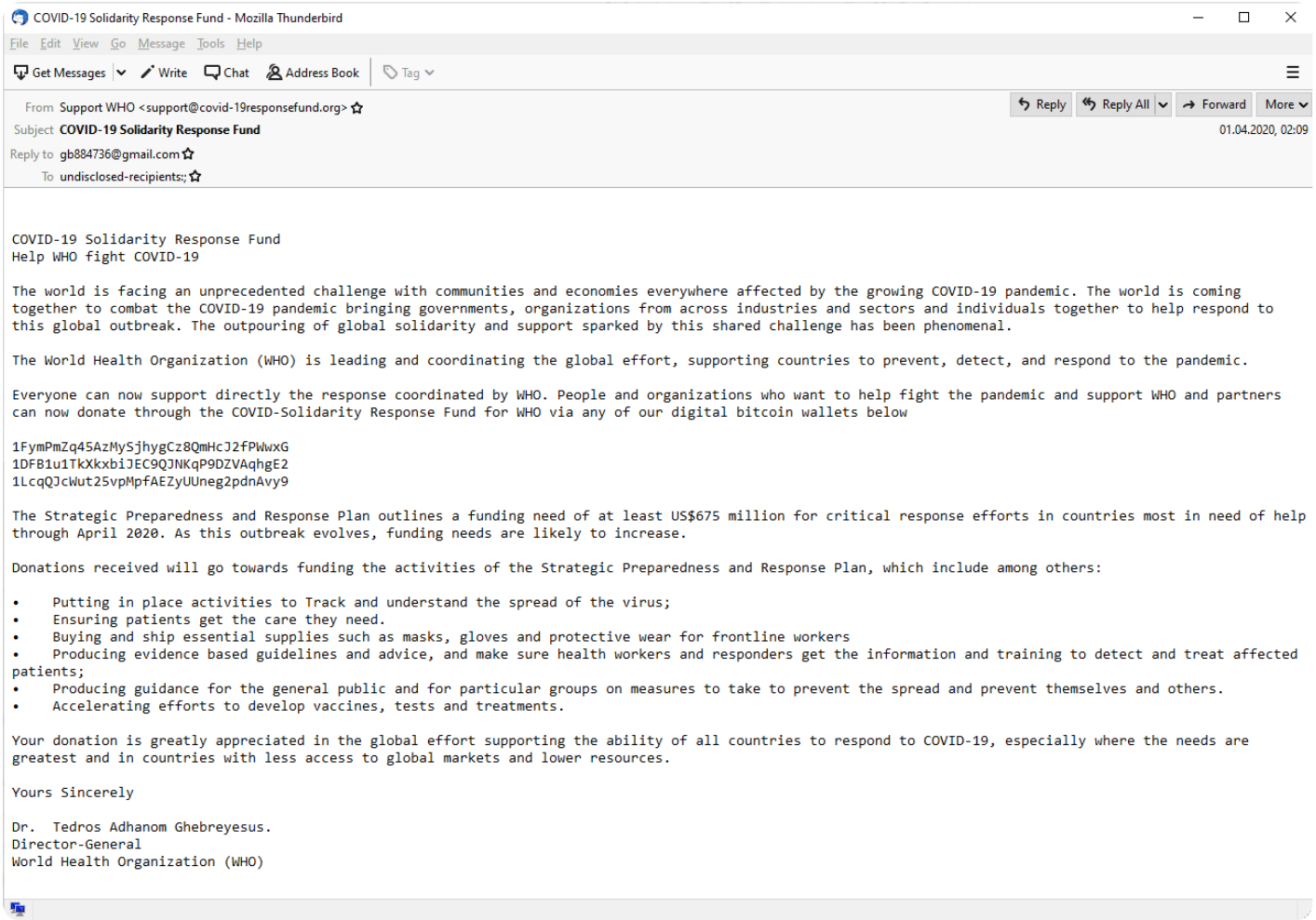
Given this policy, though, how can one search for domain names that might help the business gain more customers? In parallel, how can security operation centers (SOCs) investigate suspicious online activities with domain names possibly involved in an attempt or attack? Thankfully, tools such as WHOIS Lookup enable SOCs and businesses in general to do extensive research without violating the cybersecurity policies mentioned above.

Digging Deeper into Incidents Using WHOIS Lookups

In the Eyes of Cybersecurity Experts

When a suspicious email or item in a network log turns up, the first course of action for SOCs is to find out more about the email sender or the domain. Let's take as an example the email address support@covid-19responsefund[.]org, which attackers have been using to ask recipients for donations on behalf of the World Health Organization (WHO).

The sample email below asks explicitly for donations in the form of digital currencies. It also supposedly comes from the Director-General of WHO.



While the world deals with the difficulties brought about by these unprecedented times, threat actors are taking advantage of the ensuing pandemic. Employees with good intentions may want to donate to such a good cause, so SOCs need to step in. Thus, let's dig deeper into the domain

name used in the email address cited above.

A quick run on WHOIS Lookup reveals the following details:

- The domain name was only registered on March 13, 2020.
- The domain registrant is a certain Wang Ping from Guang Dong in China.
- The registrar is Alibaba Cloud Computing Co.

Parsed domain name: covid-19responsefund.org

Domain name extension: .org

Estimated domain age: 30 day(s)

Contact email: DomainAbuse@service.aliyun.com

Registrar name: Alibaba Cloud Computing (Beijing) Co., Ltd.

Registar Internet Assigned Numbers Authority ID: 420

Record update dates

Created date: Mon, 13 Apr 2020 06:43:29 GMT

Updated date: Mon, 13 Apr 2020 06:43:29 GMT

Registry data

Created date: Fri, 13 Mar 2020 17:04:15 GMT

Expires date: Sat, 13 Mar 2021 17:04:15 GMT

Domain's registrant

Organization: wang ping

State: guang dong

Country: CHINA

Country code: CN

In contrast, the official domain name of WHO, that is who[.]int, has entirely different details on its WHOIS record.

- The domain name was registered on June 5, 1998.
- The domain registrant reflects the address of the WHO headquarters in Geneva, Switzerland.
- The technical and administrative contact name is WHO-IMT-ESS, the IT department of the organization.

Parsed domain name: who.int

Domain name extension: .int

Estimated domain age: 7987 day(s)

Contact email: hostmaster@who.int

Record update dates

Created date: Sun, 12 Apr 2020 11:50:17 GMT

Updated date: Sun, 12 Apr 2020 11:50:17 GMT

Registry data

Created date: Fri, 05 Jun 1998 00:00:00 GMT

Updated date: Wed, 14 Jun 2017 00:00:00 GMT

Domain's registrant

Name: address: 20, Avenue Appia

Street: 20, Avenue Appia Geneva 27 Geneva Geneva CH-1211 Switzerland

Country: SWITZERLAND

Country code: CH

One could argue that covid-19responsefund[.]org is new because it was specifically created by WHO in light of the pandemic. But the registrant details don't match, and that's quite suspicious. If WHO indeed created the domain, why use a different name and address?

In line with cybersecurity policies, SOCs should block the domain name and the email address to

prevent employees from falling victim to this heartless scam. Also, they would do well to educate staff about possible scams and cyberattacks that take advantage of COVID-19 in general.

In fact, the above domain is not the only one of its kind. A quick look at the Typosquatting Data Feed's file on the day when covid-19responsefund[.]org appeared in the DNS reveals the following list of resembling domain names:

- covid19responsefund[.]nu
- covid19responsefund[.]mobi
- covid19responsefunds[.]com
- covid19responsefund[.]com
- covid-19responsefund[.]com
- covid19responsefunds[.]org
- covid19responsefund[.]top
- covid19responsefund[.]xyz
- covid-19responsefund[.]org
- covid19responsefund[.]biz
- covid19responsefund[.]se
- covid19responsefund[.]info

Before Going into Business Ventures

Cybersecurity policies and procedures should not exempt C-suites. Studies show that 34% of executives and business owners have succumbed to phishing emails. IT staff members follow at

25%. Everyone needs to follow the rules.

If executives and employees are interested in a business venture but can't seem to establish the legitimacy of a potential partner or even suspect phishing activities, they may not want to visit the site immediately. Instead, they can use WHOIS Lookup. If they need more information after learning the domain registrant's details, they can use Screenshot API to preview what the website looks like. Good design and coherent text could help in dispelling doubts.

Executives and employees can also coordinate with SOCs to ascertain the security of a website they wish to access. They could ask for assistance in running the domain name through the company's threat intelligence platform and other security systems.

WHOIS Lookup provides a way for SOCs and employees to search for domain names without violating cybersecurity policies. After all, these policies and procedures are in place to protect the company and everyone in it. Exempting a few people could lead to disaster, especially since threat actors are adept at weaponizing domain names.

No one, not even cybersecurity experts, would know for sure if a domain name is a malware host without using the right domain intelligence. As such, it's always better to err on the side of caution and run domain names you're interested in through WHOIS Lookup as a first step.