PHISHING DOMAINS PUSHING COVID-19 DRUGS, PREYING ON INNOCENT CONSUMERS

BLACK KITE

As the global death toll rises, unemployment filings reach record highs, and uncertainty skyrockets, everyone is searching for the same thing - relief. While no treatment exists for COVID-19 at the time, hackers are now capitalizing on false treatments, or treatments mentioned in the news to have cured other illnesses, to turn a crisis into an opportunity.

Following President Donald Trump's discussion of potential pharmaceutical treatments, including hydroxychloroquine in a March 19th briefing at the White House, Black Kite researchers began combing through data finding radical increases in phishing domains containing these drug names. While several of the phishing domains are not yet active or working links, these researchers found staggering examples of a problematic emerging market in its infancy stages.

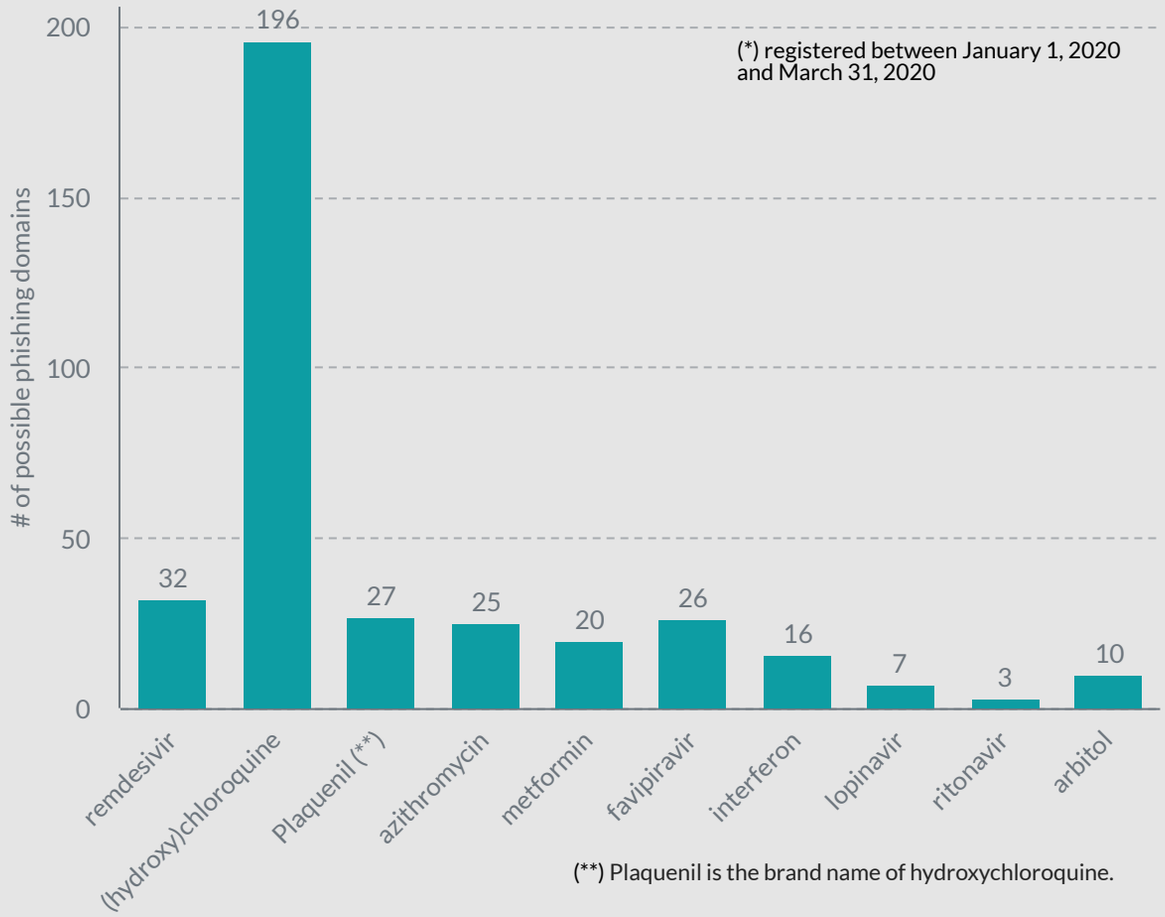
Fraudulent Domains 2

Cyber attackers have used e-commerce websites to exploit unsuspecting users for decades. As COVID-19 infiltrates communities at an unimaginable rate worldwide, these cybercriminals appear to have wasted no time in capitalizing on this health crisis.

Black Kite researchers began with the names of ten medicines, either mentioned by world leaders and/or having a high frequency on search engines. Most of these medicines are already known by scientists and have been used in the treatment of Malaria, Parkinson's disease, and some forms of cancer. Using these names, Black Kite researchers conducted a search for possible phishing domains. The researchers found that over the last two months alone, dozens of domain names, including medicines such as (hydroxy)chloroquine or azithromycin, have been purchased or sought after. The findings for the specific mentions of both hydroxychloroquine and chloroquine are merged for the research purposes of this report, as domain names using hydroxychloroquine contain chloroquine. [1]

In the first three months of 2020 alone, we detected 362 new possible phishing domains[2] with references to or containing exact names of these ten medicines.

FIG. 1: # of Possible Drug-Related Phishing Domains (*)



(**) Plaquenil is the brand name of hydroxychloroquine.

[1] Hydroxychloroquine(Plaquenil) and chloroquine(Aralen) are listed in the same category as a result of appearing in the same domain searches. Hydroxychloroquine and chloroquine are not the same drug. Both drugs are under investigation for treatment of the COVID-19 coronavirus disease.

[2] Black Kite generates possible characters from a domain name with specific algorithms, then uses these generated names in searches among all domain databases. Black Kite's phishing-domain detection algorithm utilizes many features, including checking whether the URL is typo-squatted, the date of registration, and page rank to its contents. Click here for more information.

Rise in drug-related domains

In a press briefing on March 19th, President Donald Trump mentioned the investigation into the use of chloroquine and azithromycin as potential treatments for COVID-19. Two days before President Trump's comments, Elon Musk tweeted that chloroquine is "worth considering" as a treatment for COVID-19, citing his own experience with the drug after contracting Malaria. Shortly following Musk's tweet, a statement released in the news on the 18th announced Bayer was donating this Malaria drug to the U.S. government.

On March 28th, the U.S. Food and Drug Administration (FDA) issued an Emergency Use Authorization (EUA) permitting the use of chloroquine phosphate supplied from the Strategic National Stockpile. The EUA only applies to adults and adolescents who weigh 59kg or more and are hospitalized with the coronavirus for whom a clinical trial is not available, or participation is not feasible.

FIG. 2: # of Possible Drug-Related Phishing Domains

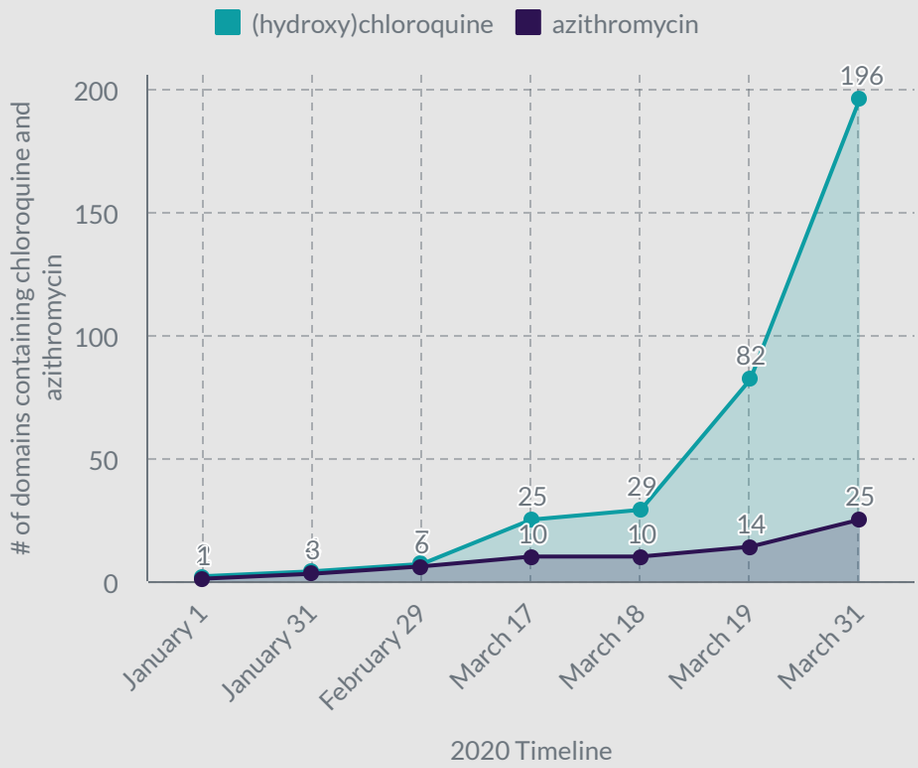
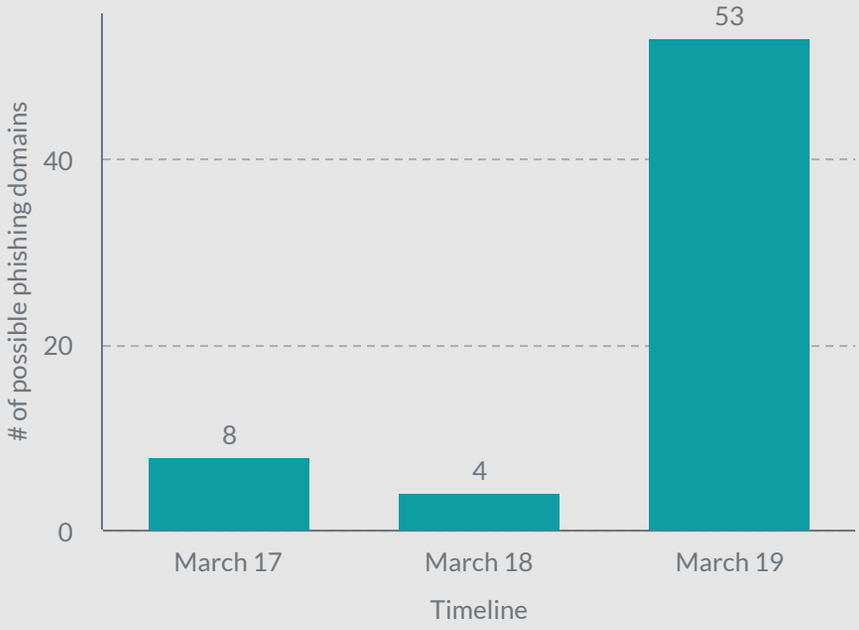


FIG. 3: # of Possible Phishing Domains Containing Chloroquine (or Hydroxychloroquine)



61% (221) of the newly registered 362 domains are possible phishing domains containing the names of these drugs mentioned chloroquine and azithromycin during the span of January 1 - March 31. The number of domains created for chloroquine (including hydroxychloroquine), the drug mentioned most frequently by the media during this period, accounts for more than half of the number of false domains created.

Rise in drug-related domains

While the number of phishing domains catapulted for chloroquine and azithromycin in particular, domain names containing eight other drugs increased as well. As depicted below, only 54 possible phishing domains were registered prior to the media reports in March. Following these media reports and comments from influential world leaders, an additional 254 possible phishing domains were created, with chloroquine remaining the most utilized named drug (see Figures 2 and 3).

FIG. 4: # of Possible Phishing Domains Containing 10 Specified Drugs

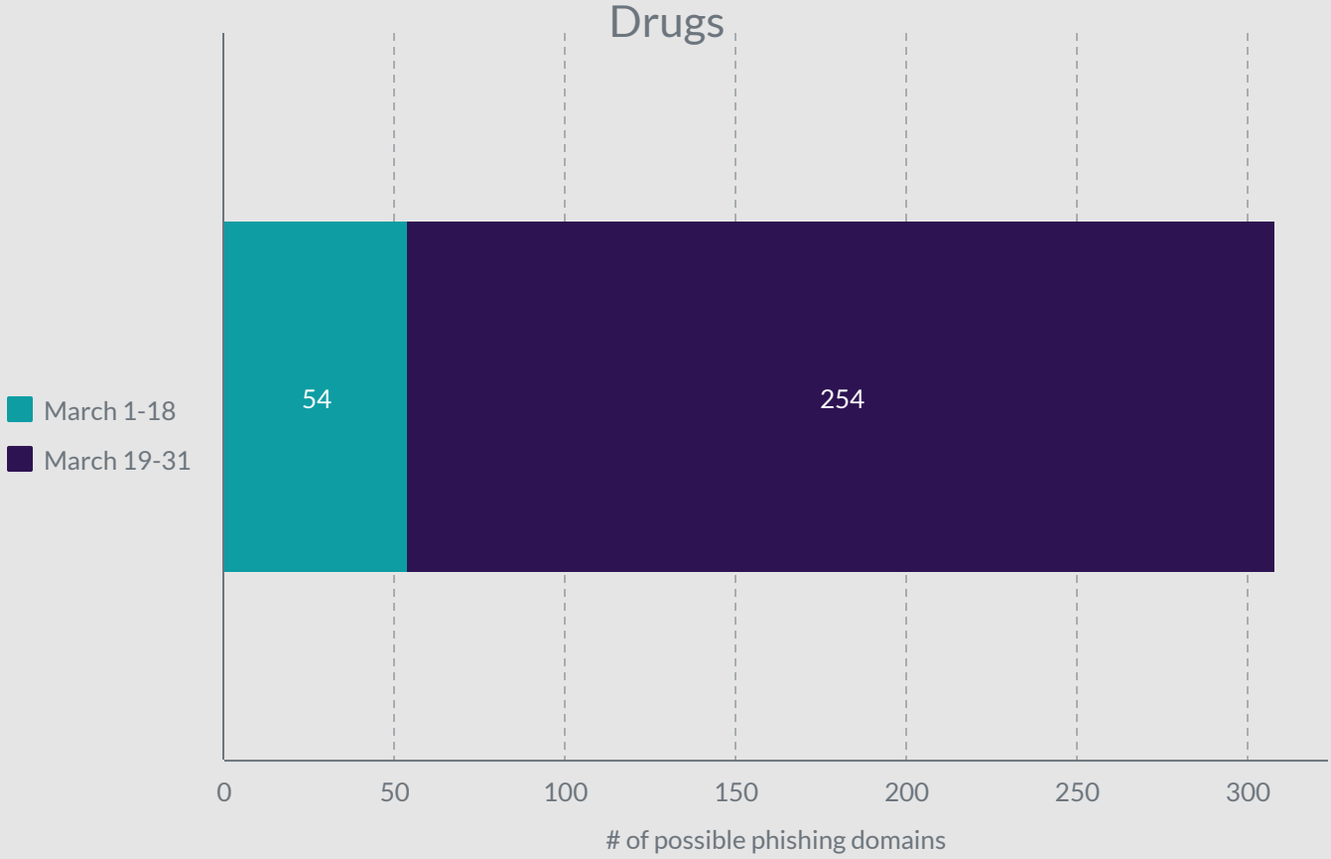
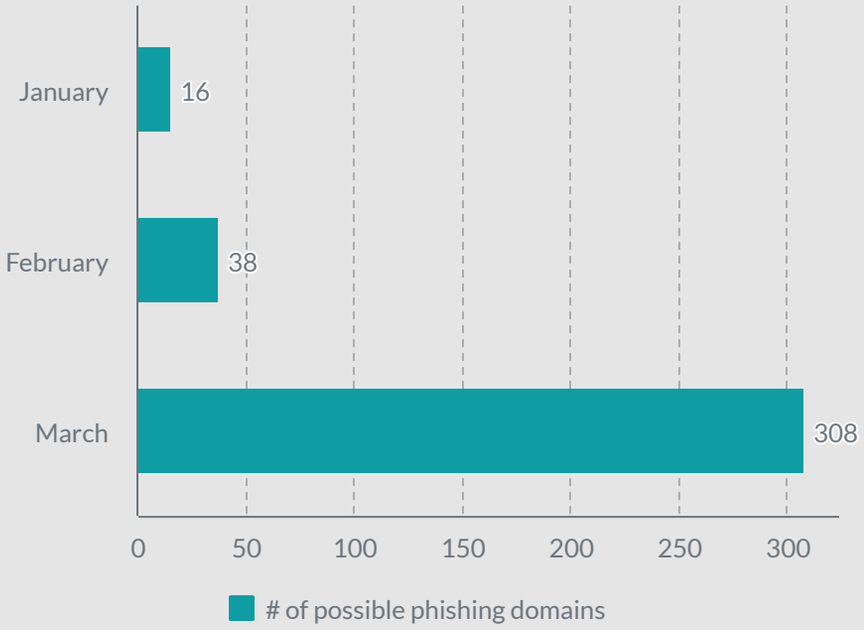


FIG. 5: # of Possible Phishing Domains Containing 10 Specified Drugs



In Figure 5, you can see the evolution of these phishing domains in 2020, and the dramatic spike from February to March alone.

Example of phishing domains 5

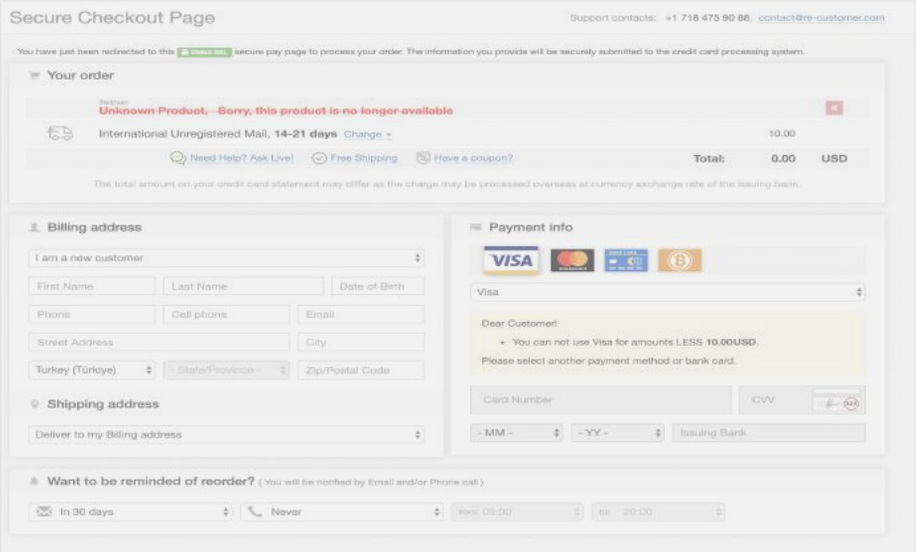
As mentioned in the introduction of this report, several of the example sites provided below are not yet active or working domains. While every domain below has either been purchased or selected in 2020, the motives for each domain vary, which often determines the functionality of the link.

Possible Fraudulent Domains Containing Alleged COVID-19 Drugs

Domain Name	Creation Date
remdesivirchina(.)com	2020-02-05
remdesivirpharmacy(.)com	2020-02-07
remdesivircoronavirus(.)com	2020-02-07
avigantablet(.)com	2020-02-14
fapilavir(.)shop	2020-02-19
fapilavir(.)store	2020-02-19
azithromycin500mg(.)shop	2020-03-17
favipiravircovid19(.)com	2020-03-19
hydroxychloroquinecoronavirus(.)com	2020-03-19
hydroxychloroquinecovid-19(.)com	2020-03-19
chloroquinecoronavirus(.)com	2020-03-19
plaquenilhydroxychloroquine(.)com	2020-03-19
favipiravir-avigan(.)online	2020-03-19
avigancovid(.)com	2020-03-19
remdesivirus(.)com	2020-03-20
aviganfavipiravir(.)com	2020-03-20
hydroxychloroquine-azithromycin(.)com	2020-03-21
remdesivirbuy(.)com	2020-03-21
azithromycinhydroxychloroquine(.)com	2020-03-22
chloroquineforcovid19(.)com	2020-03-22
plaquenil-covid(.)com	2020-03-23
azithromycinstore(.)com	2020-03-23
corona-chloroquine(.)com	2020-03-25
azithromycinshop(.)com	2020-03-25
azithromycincovid19(.)com	2020-03-26
chloroquineforcovid(.)com	2020-03-29
buy-hydroxychloroquine-online(.)com	2020-03-31

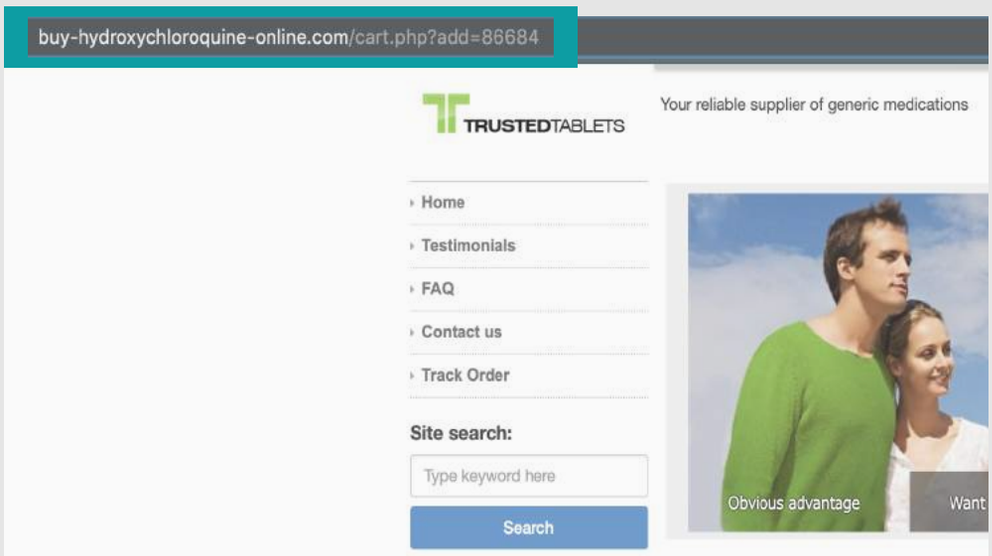
1- Gather Personal Information & Multiply the Problem

Attackers often add a payment option to their website in order to capture credit or debit card information. For example, one of the domains that we examined (www[.]buy-hydroxychloroquine-online[.]com) redirects to an unrelated domain (checkoutpagewithhttps[.]com) if a visitor clicks on “checkout” after adding an item to the cart. The below image shows what information is asked from the visitor when redirected to the unrelated domain.

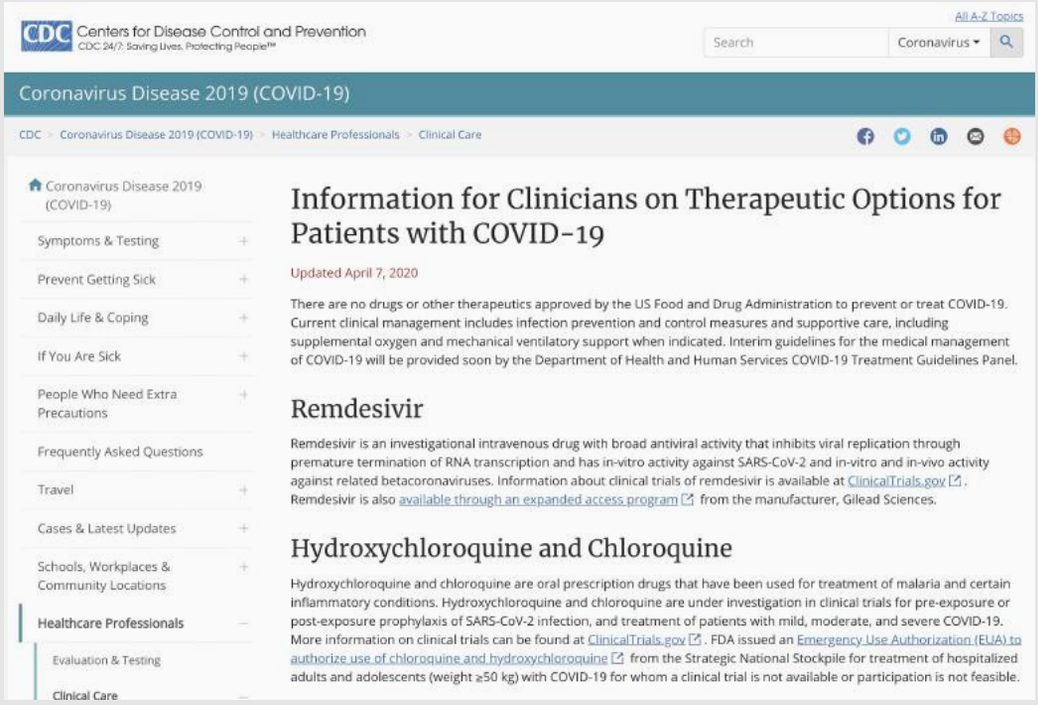


Little do site visitors know, they will often never receive anything for their purchase because hackers add features to the site to make them appear legitimate.

Captured below is an example of a fake COVID-19 drug website created on March 31, 2020, with the domain address www[.]buy-hydroxychloroquine-online[.]com. You can see these attackers have become so crafty they even included a lock sign in the domain bar. This lock sign represents an SSL connection, a visual typically depicting a website is secure.



Some of these domains are even taking it to the extreme of using government website attributes to increase their credibility. One of the possible fraudulent domains (hydroxychloroquinecoronavirus[.]com) redirects visitors to the CDC's official webpage (see below).



We examined the registration records of this domain and found nine additional domains with same domain owner records were also registered on the 19th of March, including:

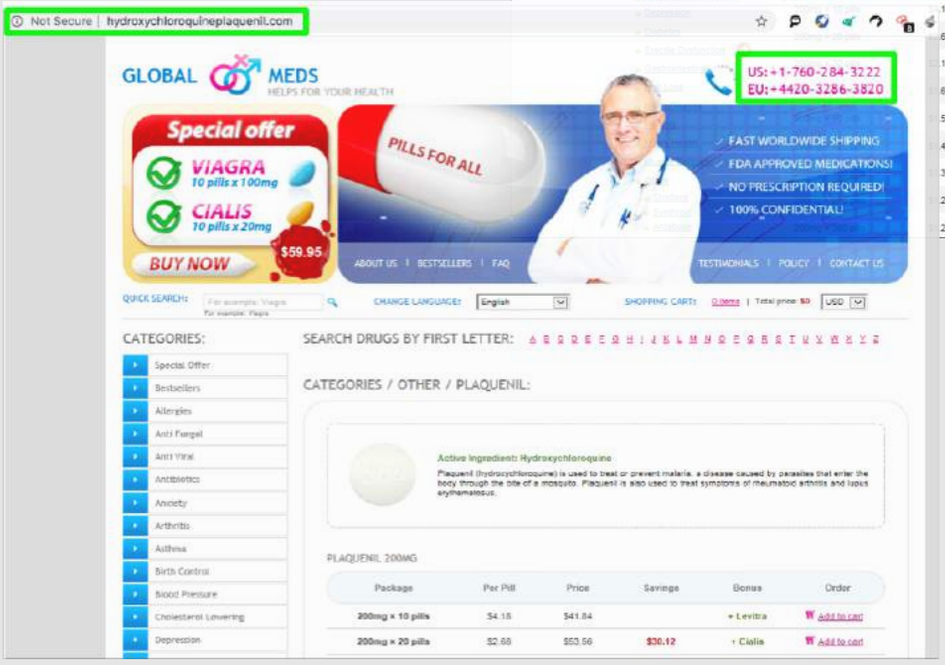
hydroxychloroquinedrug[.]com
hydroxychloroquinebayer[.]com
hydroxychloroquine200mg[.]com
hydroxychloroquineshop[.]com
hydroxychloroquinetablets[.]com
hydroxychloroquinestore[.]com
hydroxychloroquinetablets[.]com
hydroxychloroquinesulfate[.]com
hydroxychloroquinesulfatetablets[.]com

We do not know how these domains will be used, however, it is clear these attackers are trying to gain visitor confidence through false motives.

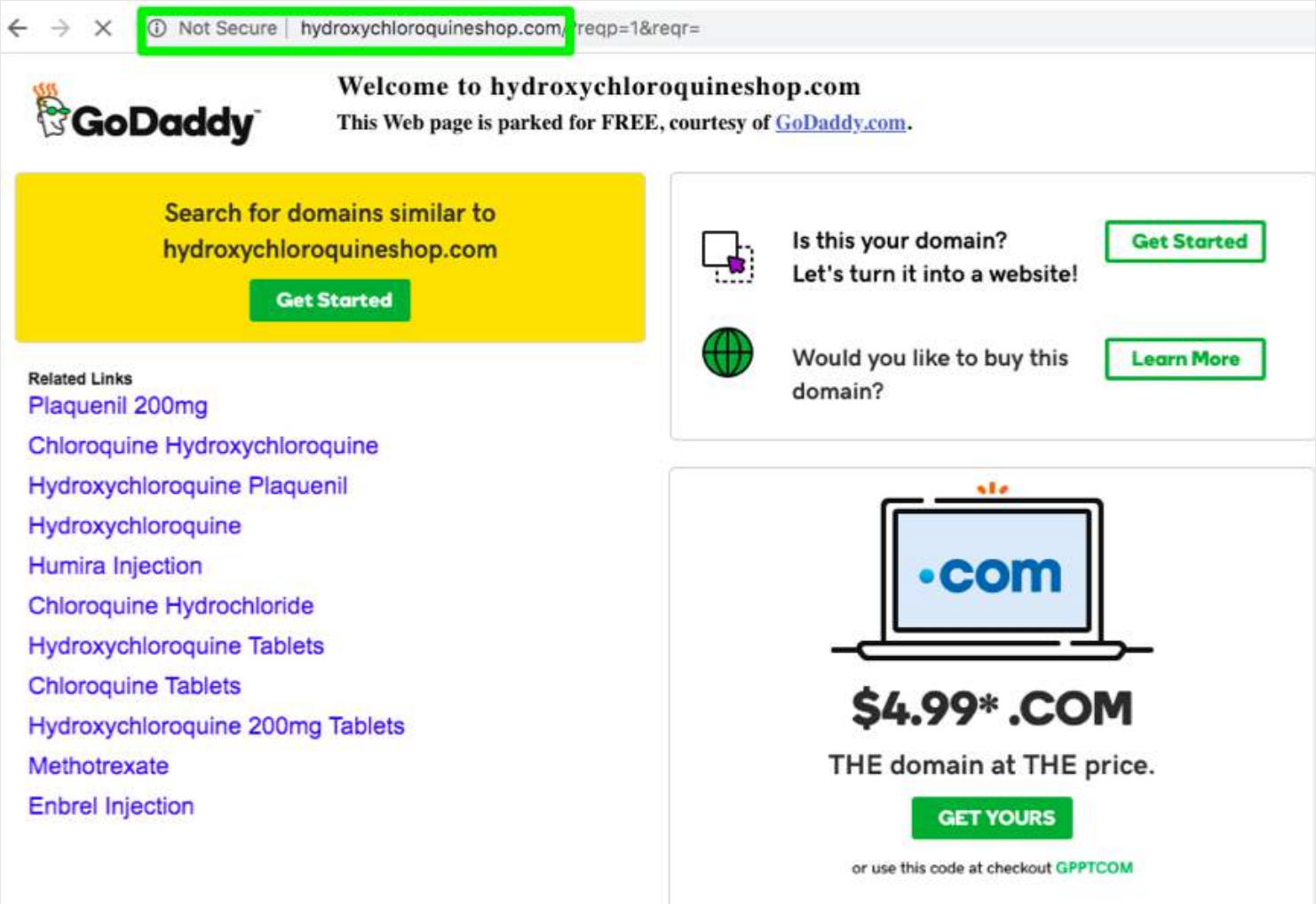
Attackers are also duplicating website content, almost exactly, under similar domain names. Such attacks are usually done very quickly. For example, attackers purchase a domain name, create a website, and work to ensure a certain number of people visit the site to purchase items within a few hours. Shortly after, the hacker will shut down the website immediately.

What do cybercriminals want?

Below images show the screenshots (taken on March 31st) of the domains registered by the same registrant name. All three have similar designs and the same phone numbers.

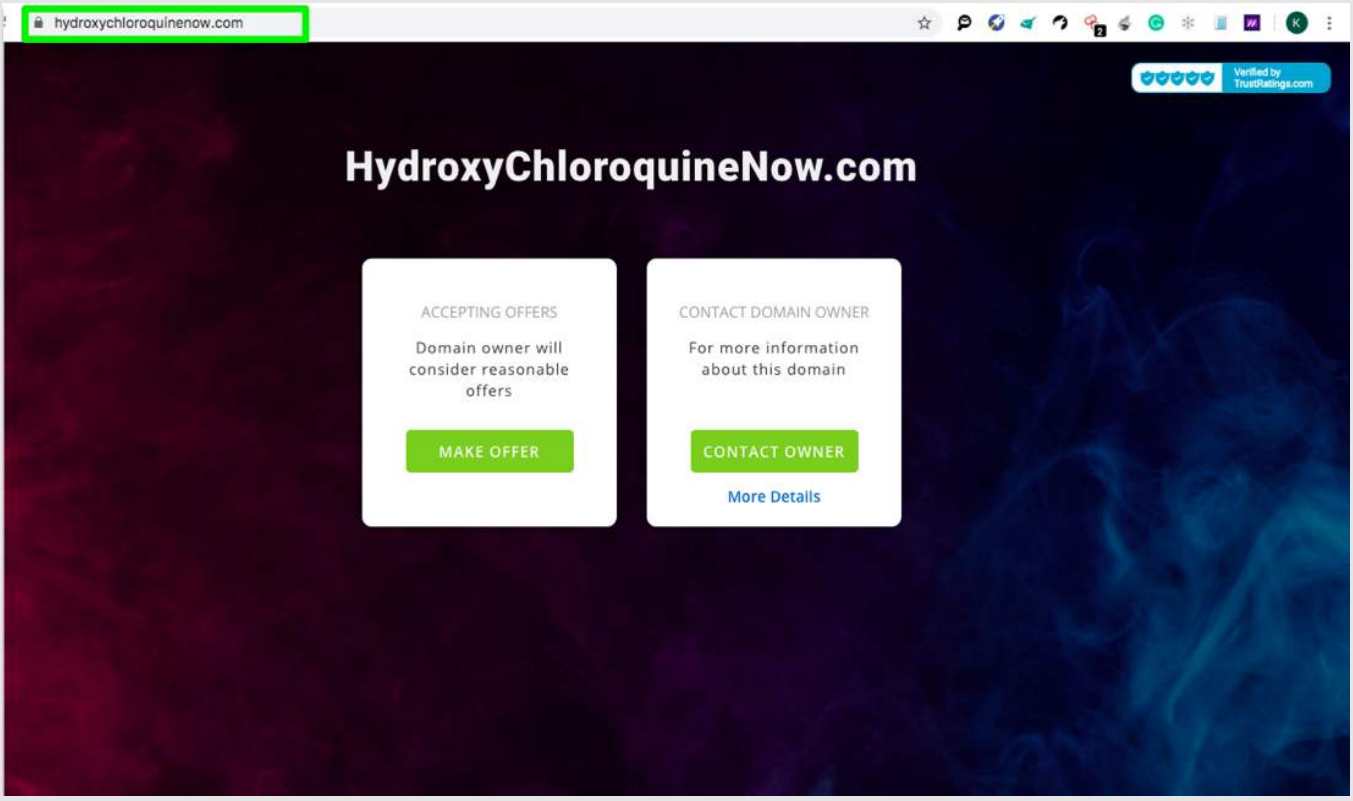


Typically, even though the attacker purchased the domain for a year, they delete the site within the same day to eliminate as much proof as possible and leave no trace behind. In a case like this, it's common to see the reselling of that domain name by the hosting company. When we examine the false COVID-19 drug domains registered on the 19th of March, it's no surprise many of them are now for sale again.



2- Make a Profit Off Those in Need, and Increase Casualties in the Process

While healthcare professionals, pharmaceutical companies, and those on the frontlines have not yet found a cure to COVID-19, they are making groundbreaking discoveries with experimental drugs along the way. Opportunists trying to capitalize on the pandemic have already purchased sought-after domains by medical professionals and are now trying to re-sell the domains at a much higher price. Below, you can see a domain purchased on March 23rd available.



Finally, if unprescribed drugs are in fact distributed, the unknown ingredients can be extremely dangerous and often cause serious consequences.

*****Black Kite researchers added the above findings based on data trends. While our research points to a high likelihood cybercriminals are the origins of the above sites rather than medical professionals, our team of researchers did not perform intrusive tests to track the IP addresses of domain owners.**

1- What can “Public Institutions” do?

In order to protect public health sectors during this crisis and the casualties they may experience, each country's government response team (**CERT**) can close these domains or restrict access. It is also recommended that healthcare providers, professionals, and officials become educated on the increasing prevalence of these fake drug domains.

2- What can the “Private Sector” do?

Companies that produce and sell these drugs can track these domains with cyber threat intelligence services and, subsequently, have many of the sites confiscated. For more information please contact us at:

www.blackkitetech.com/contact-us/

3- What can YOU do?

As a reminder, currently there is no cure for COVID-19. It’s also important to know any non-over-the-counter drug requires a prescription. Buying your medicine online can be easy, just make sure you do it safely. To learn more about how to buy your prescribed medicine online, visit *www.fda.gov/cder* and click on “Consumer Education.”

Timeline for Chloroquine mentions

FEB. 6
Chinese scientists state both chloroquine and the antiviral remdesivir are, individually, "highly effective" as Covid-19 treatment

FEB. 16
Korean physicians treat patients infected with COVID-19 with hydroxycholoroquine

FEB. 17
Based on clinical trial results, Chinese experts confirm chloroquine phosphate has a certain curative effect on COVID-19

FEB. 26
Press in France begin covering stories around chloroquine followed by other European countries

MAR. 13
The AIFA Scientific Technical Commission in Italy discusses possibility of using chloroquine

MAR. 16
Australian researchers announce some Covid-19 patients have responded 'very well' to drugs used to treat HIV and malaria

MAR. 17
Elon Musk tweets about choloroquine

MAR. 18
WHO announces chloroquine and the related hydroxychloroquine will be among the four drugs studied as part of the Solidarity clinical trial

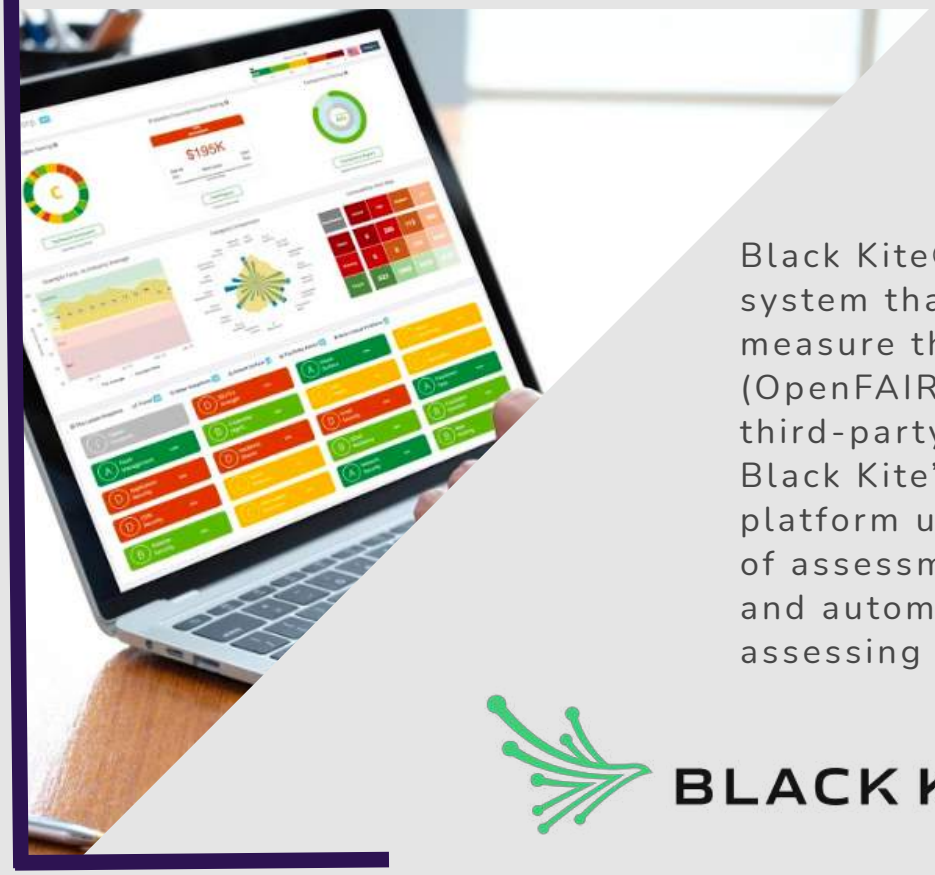
MAR. 19
President Trump comments on chloroquine.

MAR. 24
New York governor Andrew Cuomo announces New York State trials of chloroquine and hydroxychloroquine will begin

MAR. 28
FDA issues an Emergency Use Authorization (EUA) to allow hydroxychloroquine sulfate and chloroquine to be used for certain hospitalized patients with COVID-19

APR. 1
The European Medicines Agency (EMA) issues guidance saying chloroquine and hydroxychloroquine are only to be used in clinical trials or emergency use programs

For a high-resolution image with references **click here**.



Black Kite® is the only cyber risk rating system that enables enterprises to measure the probable financial loss (OpenFAIR) from a cyber attack on a third-party, supplier or business partner. Black Kite's 3D Vendor Risk @ Scale platform uniquely combines three types of assessments to provide more fidelity and automation to the process of assessing third-party risk.

BLACK KITE

By combining these three dimensions; cybersecurity ratings, compliance controls, and the OpenFAIR Analysis, it simplifies the arduous process of assessing hundreds to thousands of third-parties. The Black Kite (formerly known as NormShield) platform provides accurate, quantitative (MITRE), and continuously updated data to assess and monitor the cyber risk posture of any organization.