Integrating a Newly Registered Domains Database into Enterprise Cybersecurity Strategies

Posted on May 18, 2020

It's generally agreed that newly registered domains are potential sources of threats. After all, many of these domain registrations are made opportunistically—sometimes even in bulk, following public announcements and global events. While not all of these domains have to be avoided at all costs, they certainly deserve more scrutiny than others that have been established for years.

The good news is that monitoring newly registered domains is doable with the help of the Newly Registered & Just Expired Domains Database.

Enterprise Cybersecurity Stakeholders: Who Can Benefit From a Newly Registered Domains Database Integration?

In this post, we explore how security platform developers, security operations centers (SOCs), and managed security service providers (MSSPs) can use a newly registered domains list to bolster their cybersecurity strategies.

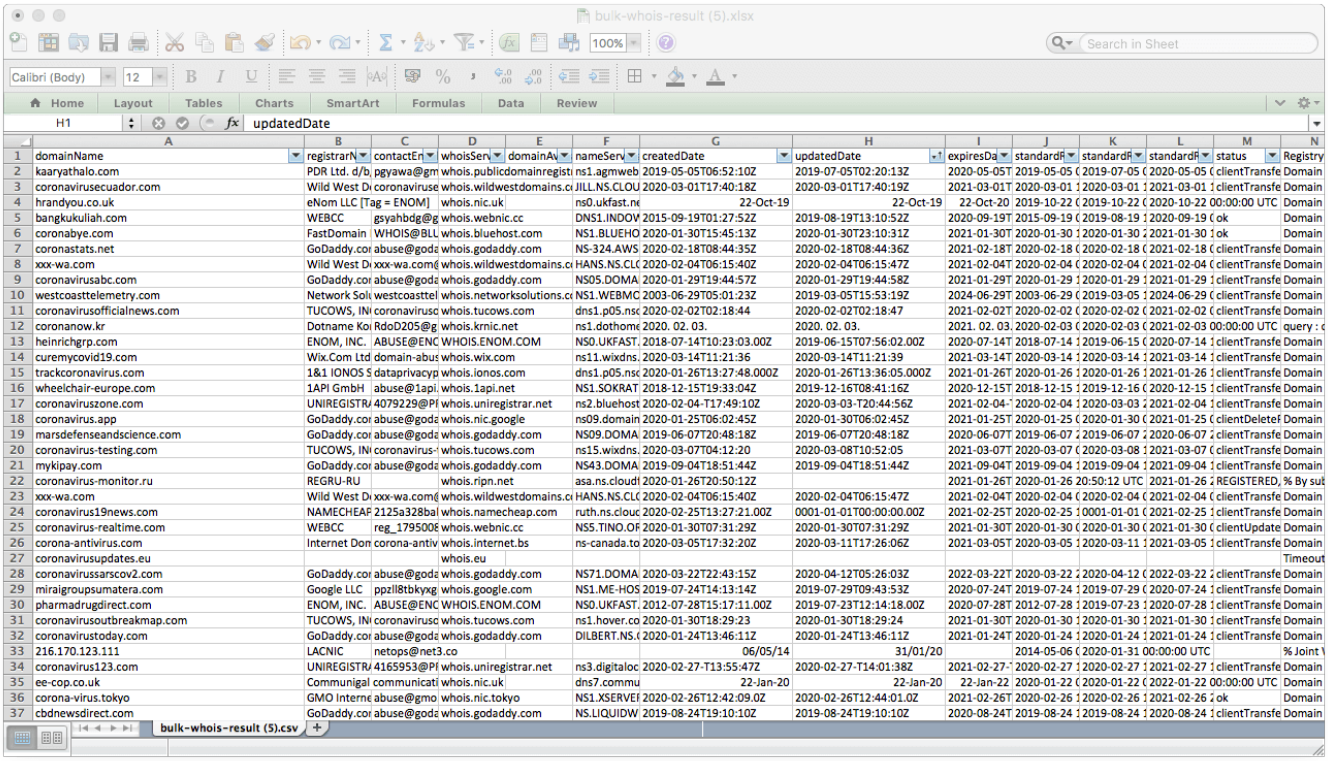
1. Security Platform Developers

With statistics revealing that 70% of newly-registered domains are malicious, developers can deliver a lot of value to users by adding the monitoring of said domain names to their applications. Let's take a look at an example.

Over the past few months, companies have been battling COVID-19-related phishing attacks, some of which rely on fake emails sent by impersonators of known healthcare organizations. When falling for the usual traps, victims either get redirected to a phishing website and lose their credentials to attackers or install malware that steals data from their computers.

What victims may not know is that most of the domains figuring in these phishing attacks are newly registered. To illustrate this point and how risky it can be to let them into corporate networks, we obtained a list of indicators of compromise (IoCs) related to COVID-19 attacks from the U.S. Department of Homeland Security.

The said IoC list contained close to 2,300 domains, which we subjected to a bulk WHOIS lookup.



domainName	registrarN	contactEn	whoisServ	domainAv	nameServ	createdDate	updatedDate	expiresDa	standardR	standardR	standardR	status	Registry
kaaryathalo.com	PDR Ltd. d/b	pgyawa@gm	whois.publicdomainregisti		ns1.agmweb	2019-05-05T06:52:10Z	2019-07-05T02:20:13Z	2020-05-05T	2019-05-05 (	2019-07-05 (	2020-05-05 (	clientTransfe	Domain
coronavirusecuador.com	Wild West D	coronavirusе	whois.wildwestdomains.c		JILL.NS.CLOU	2020-03-01T17:40:18Z	2020-03-01T17:40:19Z	2021-03-01T	2020-03-01 (	2020-03-01 (	2021-03-01 (	clientTransfe	Domain
hrandyou.co.uk	eNom LLC [Tag = ENOM]		whois.nic.uk		ns0.ukfast.ne	22-Oct-19	22-Oct-19	22-Oct-20	2019-10-22 (	2019-10-22 (	2020-10-22	00:00:00 UTC	Domain
bangkukuliah.com	WEBCC	gsyahbdg@g	whois.webnic.cc		DNS1.INDOV	2015-09-19T01:27:52Z	2019-08-19T13:10:52Z	2020-09-19T	2015-09-19 (	2019-08-19 (	2020-09-19 (	ok	Domain
coronabye.com	FastDomain	WHOIS@BLU	whois.bluehost.com		NS1.BLUEHO	2020-01-30T15:45:13Z	2020-01-30T23:10:31Z	2021-01-30T	2020-01-30 (	2020-01-30 (	2021-01-30 (	ok	Domain
coronastats.net	GoDaddy.cor	abuse@godz	whois.godaddy.com		NS-324.AWS	2020-02-18T08:44:35Z	2020-02-18T08:44:36Z	2021-02-18T	2020-02-18 (	2020-02-18 (	2021-02-18 (	clientTransfe	Domain
xxx-wa.com	Wild West D	xxx-wa.com@	whois.wildwestdomains.c		HANS.NS.CL	2020-02-04T06:15:40Z	2020-02-04T06:15:47Z	2021-02-04T	2020-02-04 (	2020-02-04 (	2021-02-04 (	clientTransfe	Domain
coronavirusabc.com	GoDaddy.cor	abuse@godz	whois.godaddy.com		NS05.DOMA	2020-01-29T19:44:57Z	2020-01-29T19:44:58Z	2021-01-29T	2020-01-29 (	2020-01-29 (	2021-01-29 (	clientTransfe	Domain
westcoasttelemetry.com	Network Sol	westcoasttel	whois.networksolutions.c		NS1.WEBMC	2003-06-29T05:01:23Z	2019-03-05T15:53:19Z	2024-06-29T	2003-06-29 (	2019-03-05 (	2024-06-29 (	clientTransfe	Domain
coronavirusofficialnews.com	TUCOWS, IN	coronavirusc	whois.tucows.com		dns1.p05.nsc	2020-02-02T02:18:44	2020-02-02T02:18:47	2021-02-02T	2020-02-02 (	2020-02-02 (	2021-02-02 (	clientTransfe	Domain
coronanow.kr	Dotname Ko	RdoD205@g	whois.krnic.net		ns1.dothome	2020. 02. 03.	2020. 02. 03.	2021. 02. 03.	2020-02-03 (	2020-02-03 (	2021-02-03	00:00:00 UTC	query :
heinrichgrp.com	ENOM, INC.	ABUSE@ENC	WHOIS.ENOM.COM		NS0.UKFAST.	2018-07-14T10:23:03.00Z	2019-06-15T07:56:02.00Z	2020-07-14T	2018-07-14 (	2019-06-15 (	2020-07-14 (	clientTransfe	Domain
curemycovid19.com	Wix.Com Ltd	domain-abus	whois.wix.com		ns11.wixdns.	2020-03-14T11:21:36	2020-03-14T11:21:39	2021-03-14T	2020-03-14 (	2020-03-14 (	2021-03-14 (	clientTransfe	Domain
trackcoronavirus.com	1&1 IONOS S	dataprivacyp	whois.ionos.com		dns1.p05.nsc	2020-01-26T13:27:48.000Z	2020-01-26T13:36:05.000Z	2021-01-26T	2020-01-26 (	2020-01-26 (	2021-01-26 (	clientTransfe	Domain
wheelchair-europe.com	1API GmbH	abuse@1api.	whois.1api.net		NS1.SOKRAT	2018-12-15T19:33:04Z	2019-12-16T08:41:16Z	2020-12-15T	2018-12-15 (	2019-12-16 (	2020-12-15 (	clientTransfe	Domain
coronaviruszone.com	UNIREGISTR/	4079229@PI	whois.uniregistrar.net		ns2.bluehost	2020-02-04-T17:49:10Z	2020-03-03-T20:44:56Z	2021-02-04-'	2020-02-04 (	2020-03-03 (	2021-02-04 (	clientTransfe	Domain
coronavirus.app	GoDaddy.cor	abuse@godz	whois.nic.google		ns09.domain	2020-01-25T06:02:45Z	2020-01-30T06:02:45Z	2021-01-25T	2020-01-25 (	2020-01-30 (	2021-01-25 (	clientDeletef	Domain
marsdefenseandscience.com	GoDaddy.cor	abuse@godz	whois.godaddy.com		NS09.DOMA	2019-06-07T20:48:18Z	2019-06-07T20:48:18Z	2020-06-07T	2019-06-07 (	2019-06-07 (	2020-06-07 (	clientTransfe	Domain
coronavirus-testing.com	TUCOWS, IN	coronavirus-'	whois.tucows.com		ns15.wixdns.	2020-03-07T04:12:20	2020-03-08T10:52:05	2021-03-07T	2020-03-07 (	2020-03-08 (	2021-03-07 (	clientTransfe	Domain
mykipay.com	GoDaddy.cor	abuse@godz	whois.godaddy.com		NS43.DOMA	2019-09-04T18:51:44Z	2019-09-04T18:51:44Z	2021-09-04T	2019-09-04 (	2019-09-04 (	2021-09-04 (	clientTransfe	Domain
coronavirus-monitor.ru	REGRU-RU		whois.ripn.net		asa.ns.cloud	2020-01-26T20:50:12Z		2021-01-26T	2020-01-26 20:50:12 UTC		2021-01-26 (	REGISTERED,	% By sut
xxx-wa.com	Wild West D	xxx-wa.com@	whois.wildwestdomains.c		HANS.NS.CL	2020-02-04T06:15:40Z	2020-02-04T06:15:47Z	2021-02-04T	2020-02-04 (	2020-02-04 (	2021-02-04 (	clientTransfe	Domain
coronavirus19news.com	NAMECHEAF	2125a328ba	whois.namecheap.com		ruth.ns.cloud	2020-02-25T13:27:21.00Z	0001-01-01T00:00:00.00Z	2021-02-25T	2020-02-25 (	0001-01-01 (	2021-02-25 (	clientTransfe	Domain
coronavirus-realtime.com	WEBCC	reg_179500E	whois.webnic.cc		NS5.TINO.OF	2020-01-30T07:31:29Z	2020-01-30T07:31:29Z	2021-01-30T	2020-01-30 (	2020-01-30 (	2021-01-30 (	clientUpdate	Domain
corona-antivirus.com	Internet Don	corona-antiv	whois.internet.bs		ns-canada.to	2020-03-05T17:32:20Z	2020-03-11T17:26:06Z	2021-03-05T	2020-03-05 (	2020-03-11 (	2021-03-05 (	clientTransfe	Domain
coronavirusupdates.eu			whois.eu										Timeout
coronavirussarscov2.com	GoDaddy.cor	abuse@godz	whois.godaddy.com		NS71.DOMA	2020-03-22T22:43:15Z	2020-04-12T05:26:03Z	2022-03-22T	2020-03-22 (	2020-04-12 (	2022-03-22 (	clientTransfe	Domain
miraigroupsumatera.com	Google LLC	ppzll8tbkyxg	whois.google.com		NS1.ME-HOS	2019-07-24T14:13:14Z	2019-07-29T09:43:53Z	2020-07-24T	2019-07-24 (	2019-07-29 (	2020-07-24 (	clientTransfe	Domain
pharmadrugdirect.com	ENOM, INC.	ABUSE@ENC	WHOIS.ENOM.COM		NS0.UKFAST.	2012-07-28T15:17:11.00Z	2019-07-23T12:14:18.00Z	2020-07-28T	2012-07-28 (	2019-07-23 (	2020-07-28 (	clientTransfe	Domain
coronavirusoutbreakmap.com	TUCOWS, IN	coronavirusc	whois.tucows.com		ns1.hover.co	2020-01-30T18:29:23	2020-01-30T18:29:24	2021-01-30T	2020-01-30 (	2020-01-30 (	2021-01-30 (	clientTransfe	Domain
coronavirustoday.com	GoDaddy.cor	abuse@godz	whois.godaddy.com		DILBERT.NS.(	2020-01-24T13:46:11Z	2020-01-24T13:46:11Z	2021-01-24T	2020-01-24 (	2020-01-24 (	2021-01-24 (	clientTransfe	Domain
216.170.123.111	LACNIC	netops@net3.co				06/05/14	31/01/20		2014-05-06 (	2020-01-31	00:00:00 UTC		% Joint
coronavirus123.com	UNIREGISTR/	4165953@PI	whois.uniregistrar.net		ns3.digitaloc	2020-02-27-T13:55:47Z	2020-02-27-T14:01:38Z	2021-02-27-'	2020-02-27 (	2020-02-27 (	2021-02-27 (	clientTransfe	Domain
ee-cop.co.uk	Communigal	communicati	whois.nic.uk		dns7.commu	22-Jan-20	22-Jan-20	22-Jan-22	2020-01-22 (	2020-01-22 (	2022-01-22	00:00:00 UTC	Domain
corona-virus.tokyo	GMO Interne	abuse@gmo	whois.nic.tokyo		NS1.XSERVE	2020-02-26T12:42:09.0Z	2020-02-26T12:44:01.0Z	2021-02-26T	2020-02-26 (	2020-02-26 (	2021-02-26 (	ok	Domain
cbdnewsdirect.com	GoDaddy.cor	abuse@godz	whois.godaddy.com		NS.LIQUIDW	2019-08-24T19:10:10Z	2019-08-24T19:10:10Z	2020-08-24T	2019-08-24 (	2019-08-24 (	2020-08-24 (	clientTransfe	Domain

We found that around 98% of them were recently registered and therefore could have been detected by a security solution that incorporates a newly registered domains database. Some of the remaining 2% (54 out of 2,264) of the domains could have been freshly registered when they were possibly used in attacks.

What's more, while the rise in new COVID-19 domain registrations may be utterly understandable as talks about the disease only surfaced late last year, the domains in the list claiming connections to institutions like the World Health Organization (WHO), for instance, are certainly deceitful. Established entities like WHO are more likely to house a COVID-19 page on their domain who[.]int rather than obtain a new one for it.

2. SOCs

One of the primary tasks of SOC staff is to dig deeper into ongoing attempts and attacks. It is their sworn duty to protect their organizations from all kinds of cyber threats.

Much like the phishing attacks we've seen a lot of these past few months, business email compromise (BEC) gangs are also ramping up their COVID-19-themed schemes. There has been an increase in the number of BEC scams targeting municipalities hoping to purchase personal protective equipment (PPE) and other related supplies to ward off the spread of the coronavirus.

One such group, dubbed "Ancient Tortoise," became known for exploiting aging reports that finance teams use to track unpaid customer invoices. Researchers discovered that the actors behind Ancient Tortoise jumped onto the coronavirus-themed attacks bandwagon as well.

The Ancient Tortoise gang isn't the only one hoping to lure companies and their customers or employees currently working from home into their traps, though. Another guise that BEC scammers employ is that of a legitimate co-worker providing a victim with the latest COVID-19 information. And much like phishers, BEC scammers are also fond of using newly registered domains that are copycats of popular suppliers' legitimate domains.

At the time of writing, all 25 IoCs related to this particular attack are newly registered domains and known malware hosts. Take a look at the Threat Intelligence Platform analysis results for coronavirusmedicalkit[.]com, beatingcoronavirus[.]com, and corona-crisis[.]com as examples.

All in all, SOC staff can get alerted and quickly block access to these by integrating a newly registered domains list into their security information and event management (SIEM) or security orchestration, automation, and response (SOAR) platforms.

Parsed domain name: coronavirusmedicalkit.com

Domain name extension: .com

Estimated domain age: 43 day(s)

Contact email: 44ef50ba64694dbcb3aac7c6c8a91b16.protect@whoisguard.com

Created date: Thu, 05 Mar 2020 03:58:05 GMT

Updated date: Mon, 01 Jan 0001 00:00:00 GMT

Registrar name: NAMECHEAP INC

Registar Internet Assigned Numbers Authority ID: 1068

WHOIS server: whois.namecheap.com

Domain EEP status codes by ICANN list: clientHold clientTransferProhibited

Custom field name 1: RegistrarContactEmail

Custom field value 1: abuse@namecheap.com

Custom field name 2: RegistrarContactPhone

Custom field value 2: +1.6613102107

Custom field name 3: RegistrarURL

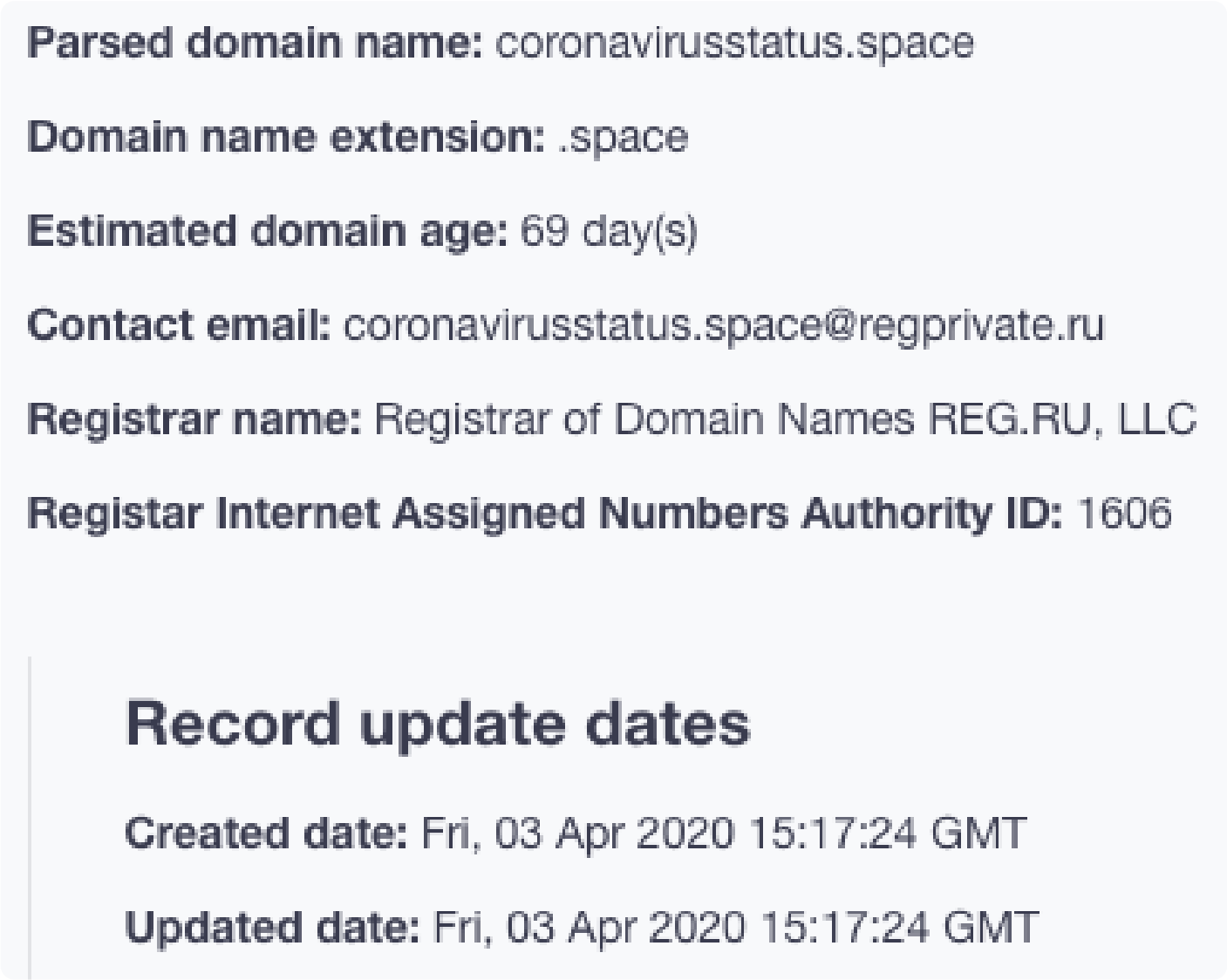
Custom field value 3: http://www.namecheap.com

3. MSSPs

Client protection should not only cover blocking known attack vectors but extend to preventing access to unknown threat sources, too. And these, of course, are likely to be newly registered domains that security solutions have yet to analyze and consequently block.

Take, for instance, a malicious domain connected to another COVID-19 related threat. Attackers preyed on user fear and anxiety to spread an information stealer via a fake coronavirus infection map. Apart from getting updates on the ensuing pandemic, however, users (who could be part of the organization an MSSP serves) also installed a malware application.

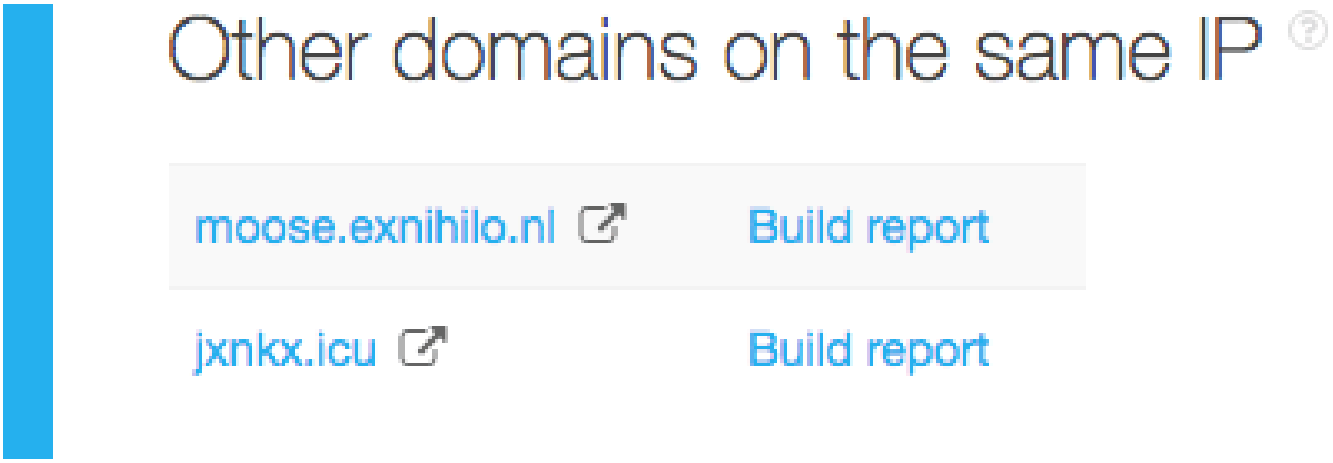
Much like in the other COVID-19-themed cases, the malware host's domain—coronavirusstatus[.]space—is a recently registered domain.



Such a threat is, therefore, avoidable with the help of a newly registered domains database. But as was said, the buck doesn't stop there for MSSPs. They should also be able to protect clients from the unknown. Apart from screening newly registered domains, they can use other domain and IP intelligence solutions.

MSSPs can, for instance, identify IP addresses and other domains connected to the known threat source via solutions like the Threat Intelligence Platform. They can then monitor and subsequently block access to related IP addresses and domains should the need arise. An example would be domains related to known malware host corona-explained[.]com. MSSPs can subject the domains

on the same IP address to further scrutiny, too.



Threats That Organizations Can Avoid by Constantly Monitoring Their Newly Registered Domains List

Phishing, BEC, and malware attacks aren't the only threats that Newly Registered & Just Expired Domains Database can help protect against. Others include:

- Spammers who are ramping up their campaigns with fake emails supposedly coming from institutions at the forefront of fighting the ensuing pandemic such as WHO and the Centers for Disease Control and Prevention (CDC).

From: **Steve Garcia** <steve.garcia@ucdavis-edu.group>
Date: Thu, Apr 9, 2020 at 6:50 AM
Subject: QUOTE ?
To:

Hello,

I'm writing on behalf of UCDavis. for inquiries on below products.

Our request needed in setting up a new location we are working on.

we are certainly in position to use several of these products to meet up our requirement.

Quote,

*) Ventilator LTV1150
*) Philips HeartStart AEDs Defibrillator (M5066A-CO2/753182615684)

I will like to know the range of discount you offer.Get back on availability price and stock.

Regards.

Steve Garcia
Purchasing Agent/Saftey Coordinator
University of Califonia,Davis
Davis,CA 95616-8504
510 279 4927

- Typosquatters who are also bringing their A-game as evidenced by the proliferation of bulk coronavirus-themed domain registrations in the past few months alone.

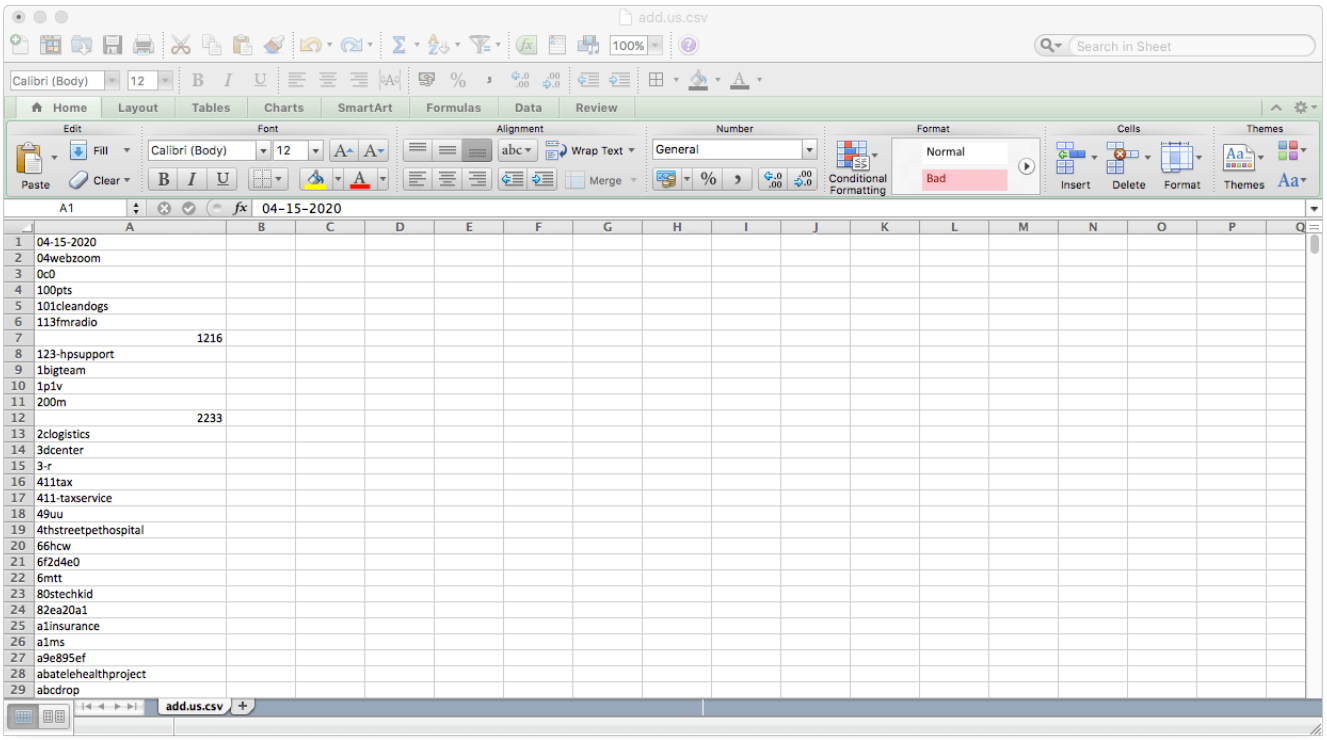
As we demonstrated earlier, however, companies are not helpless. They can ensure their own or clients' protection amid the ever-increasing volume of threats by adding newly-registered domain monitoring to their cybersecurity strategies.

How to Integrate a Newly Registered Domains Database into Existing Systems and Solutions

Security platform manufacturers, SOCs, and MSSPs can reap the benefits that the Newly Registered & Just Expired Domains Database provides by integrating it into existing solutions and systems. Just follow these steps:

- Log in to the Newly Registered & Just Expired Domains Database page with your WhoisXML API account credentials.

- Download the database by following the steps in this post. It comes in the form of a comma-separated values (CSV) file that can work with practically any solution or system. Here's a sample file containing the additions to .us domains on 17 April.



	A
1	04-15-2020
2	04webzoom
3	0c0
4	100pts
5	101cleandogs
6	113fmradio
7	1216
8	123-hpsupport
9	1bigteam
10	1p1v
11	200m
12	2233
13	2clogistics
14	3dcenter
15	3-r
16	411tax
17	411-taxservice
18	49uu
19	4thstreetpethospital
20	66hcw
21	6f2d4e0
22	6mtt
23	80stechkid
24	82ea20a1
25	a1insurance
26	a1ms
27	a9e895ef
28	abatelehealthproject
29	abcdrop

- Hook the database up to your security solutions and processes as an information source.

Newly Registered & Just Expired Domains Database is a comprehensive source of information for organizations looking to avoid dangerous new entities circulating on the Internet. Integrating it into existing solutions and systems will allow security platform manufacturers, SOCs, and MSSPs to offer best-of-breed products and services to clients, whether internal (co-workers in the same organization) or external (third-party customers).