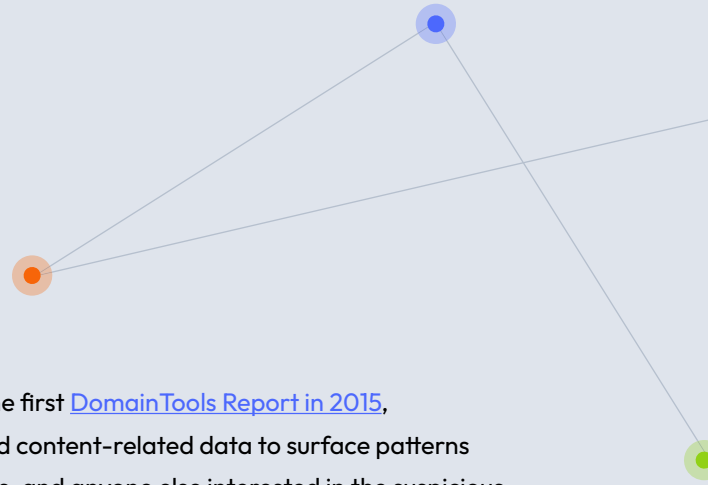**The DomainTools Report**

Patterns of Malicious Infrastructure

domaintools.com

Introduction

Welcome to the Spring 2024 edition of the DomainTools Report. Since the first [DomainTools Report in 2015](#), we have sought to explore our stores of domain registration, hosting, and content-related data to surface patterns and trends that might be of interest to security practitioners, researchers, and anyone else interested in the suspicious or malicious use of online infrastructure. Most of the reports to date have had specific areas of focus, ranging from TLDs (top level domain) and email privacy providers (2015) to [affixes in domain names](#) (2016) to [domain "blooms" and "spikes"](#) (Spring 2021).

In this edition, we again focus on concentrations of malicious activity by the same six categories we studied in the last two editions of the report. We expect that some criteria (such as top level domain, IP autonomous system number, and IP geolocation) will remain relevant over the foreseeable future; that is, as datapoints related to domain names, these are unlikely to become less forensically-valuable unless the Internet's fundamental structure changes. Other datapoints may wax and wane in relevance. For example, email privacy providers as a category that we studied in the first DomainTools Report, are dramatically less relevant in the post-GDPR world of default privacy for most registrations. Similarly, as you will read in the section on SSL Certificate Authorities, there are few strong correlations to malicious activity in the overall data (though of course for individual domains, a given CA might still sound a note of caution to an analyst).

The constant across all of these reports is our interest in providing insights into where malicious activity lurks on the Internet, with the aim of ultimately helping the community continue to improve their practices at staying ahead of those entities wishing to do harm online.

Criteria & Methodology

Domain Characteristics Evaluated

In this report, we examined the following features of a domain:

- ✓ **Top Level Domain (TLD);** for example, .com or .net

- ✓ **IP Autonomous System Number (ASN**); these represent an aspect of the domain's hosting

- ✓ **Name server ASN**; these represent the hosting of the name server associated with a domain

- ✓ **IP Geolocation:** the country code associated with the location of the domain's IP address

- ✓ **Registrar:** the entity through which the domain was registered

- ✓ **SSL Certificate Authority (CA):** the CA for certificate(s) associated with domains

We chose these features because **they are often used by defenders and security researchers as part of a process of building out a better understanding of a domain**. Seasoned practitioners often develop intuitions about the implications of a given feature, based on their experience, expertise, and judgment in the analysis of adversary assets. In many cases, the data seen at scale tend to support those intuitions. Certain TLDs, for example, have reputations among security analysts as being dangerous "neighborhoods" of the Internet, and as this and previous DomainTools Reports show, there are indeed some TLDs that have high concentrations of malicious domains. Other criteria are more ambiguous, such as the aforementioned SSL CAs.

Methodology

Candidate Domains

The DomainTools Iris database includes around 360 million currently-registered domains. How did we determine which of the candidate domains represent threats? There were two components to this. We identified domains that were known-bad by checking the domain names against several well-known industry blocklists which give indications of malware, phishing, or spam activity.

Secondly, we focused on those domains that were active (as of the report data snapshot), and therefore capable of packing a punch. Thus, **we excluded domains that appear to be dormant**. We did this by cross-checking the domains against our passive DNS sources; only those domains that have recently shown up in passive DNS are candidates for signal strength calculations.

We also imposed thresholds for absolute numbers of domains associated with each domain characteristic, so as to eliminate those entities that had extremely small populations of domains associated with them. **To be part of the evaluation, the characteristic had to have at least 1,000 active domains of the threat type in question**. For example, for Top Level Domain, or TLD, when looking at the highest signal strengths for phishing, we eliminated any TLDs that had fewer than 1,000 phishing domains. We then sorted the remaining TLDs by signal strength, and this composed our Top 10 list in that category.

This thresholding implies that **there exist some concentrations of malicious activity that may have higher signal strengths than what is included in the findings below**, but such hotspots are so small that they are unlikely to represent major threat vectors overall (of course, that doesn't mean that any given SOC couldn't have an encounter with a domain from one of those hotspots).

Signal Strength

The tables in this report are populated and sorted based on the strongest signals for phishing, malware, or spam activity associated with the populations of known-bad domains sharing the characteristic (such as TLD, IP ASN, etc). We developed this approach because when we created our Domain Risk Score machine learning algorithms, it was critical to produce scoring that achieved a good balance between a low false positive rate and an effective catch rate. A high signal strength value means that the characteristic in question is over-represented in the population of known bad domains, as compared with neutral ones.

The larger the proportion of malicious domains in a given population (an IP address, a name server, a registrar, etc) the higher our confidence that any unknown domain from that population may be involved in the threat in question. In actual practice, many defenders treat these signals in exactly this way: many characteristics of a domain (such as certain TLDs or certificate authorities) are viewed as caution signs. Signal strengths closer to 1.00 indicate a neutral signal, and if the signal strength is below 1.00, the item in question is actually more associated with neutral/good domains than with malicious ones. **There were some cases in which, for a given threat type, our Top 10 lists had fewer than ten entities with signals above 1.00** - in other words, there were some items in some of these lists that signal more goodness than badness—a phenomenon we first noted in the Fall 2021 edition of the Report.

A high signal strength value means that the concentration of malicious domains associated with that characteristic is high. When we know that a large proportion of the domains in a given population (an IP address, a name server, a registrar, etc) is malicious, this raises our confidence that any unknown domain from that population is relatively likely to be involved in the threat in question.

Snapshot in Time

For our calculations, **we took a snapshot of the domains in existence and active as of mid March, 2024**.

Interpreting the Data

In each of the following six sections, we show "Top Ten" tables, sorted by the signal strength, for each of the three threat types (phishing, malware, spam). Each table also includes the actual counts of domains associated with the item. As an example, consider this row of data from the TLD section:

	Signal Strength	Malware	Phishing	Spam	Neutral
.tk	**28.77**	3,093	3,429	2,159	5,713

The TLD **.tk** has a malware signal strength of **28.77**, and there are 3,093 domains in that TLD whose chief threat type is malware, according to the blocklists we used. For comparison, we also give the numbers of phishing, spam, and neutral domains associated with the TLD. As a reminder, **all domains under consideration had shown recent activity shown in passive DNS records** as of the time the snapshot was taken, so the numbers do not include the inactive domains associated with that TLD.

In each Top Ten list, the individual entities on the list that were repeats from the previous report in Spring of 2023 are shown in **bold**. Entities with **bold*** indicate that they not only repeat, but repeat in the same rank as in the last report. And those with ***bold**** are multiple (3x or more) repeaters that are also in the same position as last time.

It's important to keep in mind what signal strength represents, and what it does not. Most importantly, **a high *signal strength* for maliciousness does not necessarily correspond to a high *absolute number* of malicious domains.** The purpose of the report is not to show where the highest numbers of dangerous domains are, but rather what data points should be considered the strongest indicators that something unsavory might be afoot.

Findings
Top-Level Domains (TLDs)

It's usually a safe bet that the most populous TLDs such as .com, .net, .org, .co.uk, and so forth, will have the most malicious domains associated with them, but there are a number of country code (.tk, .gq), and new generic (.monster, .live) TLDs that have gained notoriety in the cybersecurity community for hosting malicious domains. There are several reasons for this, including extremely inexpensive (or sometimes free) domain registration and lax enforcement policies. But when defenders say that they automatically distrust certain TLDs, they have plenty of reason for doing so, as the following Top Ten lists will show—just as in 2023, gTLDs abound in this year's Top Ten lists.

That said, a notable feature of all three threat types for TLDs is that **the signal strengths are substantially milder**, particularly in the spam category. What this means for defenders is that seeing one of the TLDs represented in our Top Ten lists as an indicator on their network is not as clear a sign of maliciousness as it was last year. Most analysts will still pay attention to such domains, which is appropriate; but certain activities, such as wholesale blocking of entire TLDs, could result in higher false positive rates than it might have in the past.

But the big story in TLDs, which dropped shortly after we published the March 2023 report, was Freenom's exit from registration of domains in several of the TLDs that have frequented our lists, including .tk, .ga, .gq, .ml, and .cf. Freenom returned control of these country-code TLDs to the countries to which they were actually assigned by ICANN. And as you will see in the three top ten lists in this category, several of these TLDs remain on the lists with high signal strengths, but the numbers of domains associated with them are dramatically lower. The .gq TLD, for example, topped our phishing Top Ten list but had a total (for the table row) of 4,160 domains, vs. 80,128 a year ago—more than an order of magnitude fewer domains, albeit with a distribution that still gives .gq high signal strength in phishing.

When doing some extreme "low flying" over the data, we found that there were a few domains that existed before Freenom's exit, and still existed at the time of our 2024 snapshot, that were on our blocklists. Examples are `instagram-copyright-team[.]gq`, `instagramclient[.]gq`, `freenomisratelimitingme[.]gq`, `blackhatseoservices[.]tk`, `yahootk[.]tk`, `qnap[.]tk`, `instagram-badge-verify[.]cf`, `chronopostt[.]cf`, `1and1[.]cf`, and `freenomisratelimitingme[.]cf` (the shade against Freenom comes through clearly!).

Phishing

We saw some turnover in the top ten, as we did last year, although it was slightly lower this year. The signal strengths were also milder, topping out at 50.59 for .gq this year, vs. 102.49 for .cyou last time around. Speaking of .gq, it moved up from eighth spot last year, while two other TLDs made the Top Ten lists in multiple threat types—.tk was in all three threat categories' top ten lists, and .live was in two.

March 2024	Signal Strength	Phishing	Malware	Spam	Neutral
.gq	50.59	1626	537	471	1526
.cf	28.68	1420	704	428	2351
.tk	28.50	3429	3093	2159	5713
.lol	19.30	19743	4624	575	48557
.party	13.84	1039	46	20	3564
.autos	12.11	4296	660	188	16838
.live	10.98	28353	13254	5241	122584
.support	8.89	1267	254	200	6769
.monster	8.64	3254	2040	317	17892
.top	7.19	143892	72499	31712	950381

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
.cyou	102.49	35659	21,683	409	18,834
.cfd	85.98	3944	2,100	504	2,483
.top	51.69	105949	27,326	13,543	110,951
.buzz	51.33	16335	4,774	610	17,227
.rest	49.17	1694	456	800	1,865
.ga	36.17	36469	10,294	6,799	54,575
.quest	34.55	1629	915	541	2,552
.gq	32.16	23985	9,364	6,407	40,372
.monster	31.39	2530	1,327	2,303	4,363
.live	26.87	20446	3,286	12,110	41,183

Malware

The Top Ten list for malware had more turnover than the phishing list, with only two repeaters. Again, this may be attributable to the Freenom exit; but we also saw lower signal strength overall in this category, with .tk showing 28.77 in first spot this time, vs. .cyou's 135.09 signal strength in 2023. Notable in this list is gTLD .online, with more domains than any other top ten TLD, by a factor of over three times. Two of the TLDs in the Malware list—.live and .monster—also appeared in the phishing list above.

March 2024	Signal Strength	Malware	Phishing	Spam	Neutral
.tk	28.77	3093	3429	2159	5713
.pics	7.76	3596	1673	677	24641
.today	7.24	12834	2235	386	94210
.life	6.83	12290	14175	2562	95565
.online	6.66	103945	43251	9435	830008
.space	6.27	11767	5966	3334	99758
.monster	6.06	2040	3254	317	17892
.live	5.75	13254	28353	5241	122584
.link	5.68	5668	3027	929	53032
.buzz	5.30	11010	8514	1312	110397

March 2023	Signal Strength	Malware	Phishing	Spam	Neutral
.cyou	135.09	21,683	18,834	409	18,834
.cfd	99.24	2,100	2,483	504	2,483
.monster	35.69	1,327	4,363	2,303	4,363
.buzz	32.52	4,774	17,227	610	17,227
.top	28.90	27,326	110,951	13,543	110,951
.gq	27.22	9,364	40,372	6,407	40,372
.click	24.76	4,178	8,831	11,403	19,799
.ga	22.13	10,294	54,575	6,799	54,575
.icu	21.76	2,070	4,779	606	11,163
.xyz	15.06	32,687	85,505	7,215	254,684

Findings Top-Level Domains (TLDs)

Spam

Of the three threat types, spam had the biggest drop in signal strength vs. 2023, from 692.36 to 44.80. Other features of this Top Ten list are somewhat similar to last year's, in that the counts were relatively comparable and there was a fairly high level of turnover, with only three repeaters (though this is a change from last year, when all ten TLDs were new to the list). As noted earlier, .tk, which tops the spam list, featured in all three threat types this year.

March 2024	Signal Strength	Spam	Phishing	Malware	Neutral
.tk	**44.80**	2159	3429	3093	5713
.tokyo	**26.61**	4172	268	103	18586
.ws	**13.91**	1310	450	161	11169
.best	**13.35**	2485	2439	1968	22071
.wiki	**9.90**	1337	641	243	16004
.cn	**8.49**	37455	58125	11868	522885
.media	**8.08**	1312	818	312	19248
.click	**5.24**	7078	18074	11804	160165
.ng	**5.10**	1915	1298	1530	44494
.cc	**5.07**	8680	14866	12619	203020

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
.beauty	**692.36**	3,461	972	249	1,341
.click	**154.50**	11,403	8,831	4,178	19,799
.monster	**141.60**	2,303	2,530	1,327	4,363
.live	**78.88**	12,110	20,446	3,286	41,183
.gq	**42.57**	6,407	23,985	9,364	40,372
.ga	**33.42**	6,799	36,469	10,294	54,575
.top	**32.75**	13,543	105,949	27,326	110,951
.tokyo	**27.57**	1,531	603	379	14,899
.tk	**26.95**	7,093	28,151	8,690	70,612
.cf	**24.15**	6,844	28,265	8,451	76,030

IP ASNs

For this category, we provide both the Autonomous System number itself and the organization name to which the ASN is delegated. As you read the ASN tables, note that, as in the last two editions, **the signal strengths at the top are dramatically higher than what we recorded in the TLD lists**. Note, too, the extraordinary ratios between the numbers of malicious domains vs neutral domains in some of these ASNs, or between one threat type and another (for example, ASN 198953 has 1695 phishing domains and not a single neutral one). With each AS in this and the following section, we provide its country code of registration in parentheses.

Phishing

We saw a DomainTools Report first this year, with a hosting AS (ASN 198953, Proton 66 OOO of Russia) **having exactly <u>zero</u> neutral domains**. This gives this AS a signal strength of infinity. **Please, dear reader, do not allow any traffic at all to this ASN!** Likewise the next two, which are almost entirely devoted to malicious activity, with 1 and 11 neutral domains, respectively, vs. hundreds to thousands of phishing domains. (Your report's authors speculate that the presence of those twelve neutral domains in these ASNs may simply reflect that the threat intelligence feeds we use for categorizing threats may simply not have gotten around to classifying those domains as of our data snapshot date. And you'll see a "bonus" table below the March 2024 snapshot, prompted by that infinite score—read on!)

Only two of the ASNs on this list were on last year's list—41564, Orion Network Limited and 58065, Packet Exchange Limited (both of Great Britain)—repeated from last year. Those two ASNs also feature in the malware Top Ten list, as you will see.

March 2024	Signal Strength	Phishing	Malware	Spam	Neutral
198953 Proton66 OOO, RU	∞	1695	18	85	0
49943 ITRESHENIYA-AS IT Resheniya LLC, RU	149833.21	2094	10	22	1
140803 HQDATA-AS-VN 8, Vietnam	12625.96	1941	54	0	11
59692 IQWEB IQWeb FZ-LLC, AE	1511.18	38670	360	6616	1831
216234 yy-as Komkov Vadim Aleksandrovich, RU	1494.56	1483	56	21	71
41564 Orion Network Limited (GB)	862.36	6496	1962	20	539
48950 GLOBALCOLOCATION GLOBAL COLOCATION LIMITED, GB	732.60	2232	508	4	218
58065 PacketExchange Packet Exchange Limited (GB)	688.03	9731	2874	117	1012
46805 AS-46805 Angelnet Limited, SC	366.05	1105	159	1	216
9002 RETN-AS RETN Limited, GB	320.83	1103	942	12	246

● IP ASNs

We were as surprised as you to see that score of infinity, so we decided to do an extra step for IP ASNs for phishing: we ran a longitudinal analysis looking back at a 110-day period from December of 2023 to March of 2024. This changed the Top Ten list mildly, though as you can see, most of the same entities appear in both tables, and we still see some extreme signal strengths. Shaded AS names are those appearing in both the snapshot and the 110-day study. *NOTE: because this is a longitudinal data set, the domain counts are averages rounded to the nearest whole number.*

There are a couple of things that we find noteworthy:

● **Higher overall signal strengths** across the 110-day table than the snapshot (discounting the infinity oddity in the snapshot). Intuitively, one might expect signal strengths to be milder in a larger data sample, but that's not the case here. These ASNs truly are ones for defenders to watch out for.

● We see a lot of **consistency in the countries represented**. For example, Flynet and PROSPERO-AS, which didn't appear in the snapshot but do appear in the longitudinal, are both Russian. That said, there is one country in the longitudinal data that don't appear in the snapshot: Singapore (GREYWOLFNETWORKS).

110-Day Average Dec '23 - Mar '24	Signal Strength	Phishing	Malware	Spam	Neutral
49943 ITRESHENIYA-AS IT Resheniya LLC, RU	144987.44	2490	23	71	2
140803 HQDATA-AS-VN 8, Vietnam	32219.16	3030	39	0	8
151609 GREYWOLFNETWORKS-AS-AP GREYWOLF NETWORKS PTE. LTD., SG	22483.64	1274	0	39	4
198953 Proton66 OOO, RU	13584.80	1662	13	87	3
51724 FLYNET-AS Flynet Ltd, RU	6590.75	1027	34	203	11
200593 PROSPERO-AS PROSPERO OOO, RU	3512.70	2046	74	311	345
216234 yy-as Komkov Vadim Aleksandrovich, RU	1439.56	1403	60	21	72
59692 IQWEB IQWeb FZ-LLC, AE	1080.25	25909	454	10991	1846
48950 GLOBALCOLOCATION GLOBAL COLOCATION LIMITED, GB	744.53	2172	694	3	264
41564 Orion Network Limited (GB)	741.91	6006	2519	13	651

As a side note, we will consider whether it might be helpful to run an entire DomainTools Report in the future on longitudinal data sets such as this one—watch this space! But now, back to the snapshots.

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
133955 WLINCL-AS World-Link International (HK)	33,632.73	1,404	599	0	3
64270 PACIFICRACK (US)	3,535.41	12,348	497	3904	251
3214 XTOM xTom GmbH (DE)	3,408.99	17,077	36	4,270	360
58065 PacketExchange Packet Exchange Limited (GB)	2,484.73	4,149	3,596	192	120
41564 Orion Network Limited (GB)	2,277.18	3,644	3,597	84	115
211252 AS_DELIS Delis LLC (US)	884.86	2,598	770	2846	211
59447 Istanbuldc Veri Merkezi Ltd Sti (TR)	302.67	2,388	485	6	567
35913 DEDIPATH-LLC (US)	116.32	17,683	307	4674	10,925
46573 LAYER-HOST (US)	115.10	17,216	417	5991	10,749
31624 VFMNL-AS Yoursafe Holding B.V. (NL)	111.81	105,458	29,704	2405	67,785

Malware

As noted above, ASNs 41564 and 58065 also appear on the phishing Top Ten list, but the other notable thing about these two is that they appear in the same rankings as last year—#1 and #2 respectively. Having said that, it's worth noting that the signal strengths are considerably lower this time around. This list had substantial turnover, with four ASNs repeating from March 2023. The overall counts of domains were also a bit lower this time around.

ASNs 7979, 51852, and 33387 were in this malware list and the name server ASN malware Top Ten list, a bit later in the report.

IP ASNs

March 2024

March 2024	Signal Strength	Malware	Phishing	Spam	Neutral
41564* Orion Network Limited, GB	**230.56**	1962	6496	20	539
58065* PacketExchange Packet Exchange Limited, GB	**179.88**	2874	9731	117	1012
7979 SERVERS-COM, US	**133.53**	7539	4439	13	3576
39572 ADVANCEDHOSTERS-AS DataWeb Global Group B.V., NL	**54.75**	7048	837	1	8153
205056 DHNETWORK DIAHOSTING LIMITED, GB	**45.72**	1170	394	0	1621
35908 VPLSNET, US	**13.45**	4039	596	61	19024
29873 BIZLAND-SD, US	**6.65**	30056	1984	97	286163
51852 PLI-AS Private Layer INC, PA	**6.63**	1521	742	103	14531
147008 DIANJIANG-AS-AP Shenzhen Dianjiang Technology Co Ltd, CN	**4.91**	1355	614	43	17493
33387 NOCIX, US	**4.86**	5705	1326	521	74414

March 2023

| March 2023	Signal Strength	Malware	Phishing	Spam	Neutral
41564 Orion Network Limited, GB	**3,769.73**	3,597	3,644	84	115
58065 PacketExchange Packet Exchange Limited, GB	**3,611.66**	3,596	4,149	192	120
61969 TEAMINTERNET-AS Team Internet AG, DE	**198.08**	29,821	1459	84	18,145
7979 SERVERS-COM, US	**176.86**	3,601	467	96	2,454
207713 GIR-AS GLOBAL INTERNET SOLUTIONS LLC, RU	**160.60**	2,901	807	87	2,177
31624 VFMNL-AS Yoursafe Holding B.V., NL	**52.81**	29,704	105,458	2405	67,785
39572 ADVANCEDHOSTERS-AS DataWeb Global Group B.V., NL	**46.32**	3,166	325	14	8,237
60592 GRANSY Gransy s.r.o., CZ	**29.74**	2,639	2036	46	10,695
58061 SCALAXY-AS Scalaxy B.V., NL	**23.44**	3,167	1455	277	16,283
206834 TEAMINTERNET-CA-AS Team Internet AG, DE	**19.86**	42,021	2541	149	255,014

● **IP ASNs**

Spam

While the signal strengths among the first two rows of the spam Top Ten list are not as astronomical as those in the phishing list, they are nothing to sneeze at, coming in at 65,535.49 for 56291, ACE-AS-AP Ace Inc.; and 31,159.78 for 24295, AS-PNAPOSK Unitas Global Co., Ltd., both of Japan. Below these two the signal strengths are substantially milder, but still high relative to some of the other Top Ten lists in this report. If we discount the first two ASNs as outliers, the signal strengths of this list are in roughly the same ballpark as in 2023. There were some ASNs that appear in other Top Ten lists; 59692, IQWEB IQWeb FZ-LLC of the United Arab Emirates, is in the phishing list, and 59796, STORMWALL-AS StormWall s.r.o. of Slovakia, and 137951, ASLINE-AS-AP ASLINE LIMITED of Hong Kong, are in the name server ASN spam list. Turnover was high in this list, with just 4686, BEKKOAME BEKKOAME INTERNET INC. of Japan repeating from March of 2023.

March 2024	Signal Strength	Spam	Phishing	Malware	Neutral
56291 ACE-AS-AP Ace, Inc., JP	65535.49	1993	75	18	4
24295 AS-PNAPOSK Unitas Global Co., Ltd., JP	31159.78	2369	13	208	10
132827 GATEWAY-AS-AP GATEWAY INC, JP	1104.32	1209	5	15	144
4686 BEKKOAME BEKKOAME INTERNET INC., JP	945.12	7746	17	296	1078
18068 ACROSS Dream Wave Shizuoka Co. Ltd., JP	934.69	1606	8	91	226
59796 STORMWALL-AS StormWall s.r.o., SK	892.07	1526	1	7	225
59692 IQWEB IQWeb FZ-LLC, AE	475.27	6616	38670	360	1831
137951 ASLINE-AS-AP ASLINE LIMITED, HK	415.07	104333	9486	2348	33062
52284 Panamaserver.com, PA	288.22	1558	137	73	711
400506 BAIAS, US	203.73	1473	103	542	951

IP ASNs

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
64270 PACIFICRACK, US	4,095.00	3,904	12,348	497	251
211252 AS_DELIS Delis LLC, US	3,551.16	2,846	2,598	770	211
3214 XTOM xTom GmbH (DE)	3,122.80	4,270	17,077	36	360
399471 AS-SERVERION, US	1,095.74	1,594	259	130	383
213035 AS-SERVERION Des Capital B.V., NL	890.44	3,328	203	156	984
4686 BEKKOAME BEKKOAME INTERNET INC., JP	728.30	3,574	82	13	1,292
399629 BLNWX, US	508.52	1,099	526	236	569
46573 LAYER-HOST, US	146.74	5,991	17,216	417	10,749
17941 BIT-ISLE Equinix Japan Enterprise K.K., JP	120.75	2,294	2	6	5,002
35913 DEDIPATH-LLC, US	112.64	4,674	17,683	307	10,925

IP ASNs
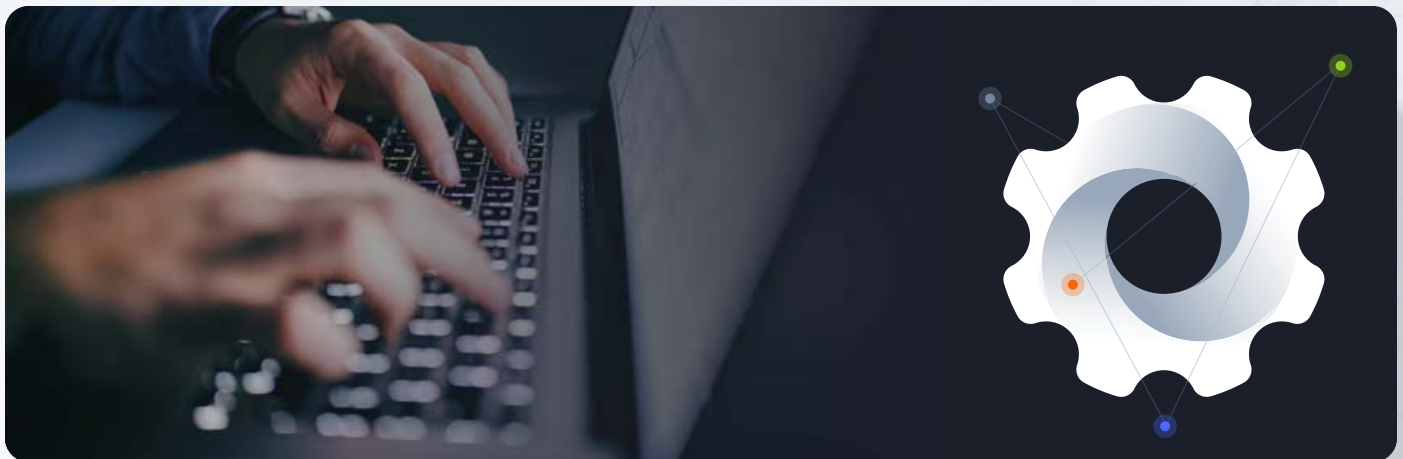
Name Server ASNs

At a glance, these will look similar to the previous category, but in this case, we're looking at the Autonomous System associated with the **name server IPs** for the domains, rather than the hosting IPs. Sometimes registrants use name servers from the same providers they use for hosting, but there's not a direct correspondence. Any domain registrant, legitimate or evil, may have their own preferences for name servers.

As an interesting note, the eagle-eyed reader may observe that in some of the data rows, the counts of domains in different ASNs are identical. These may look like data errors, but in fact, the explanation is that there are some domains for which two or more name servers are assigned, and these name servers have different ASNs. Some analysts may have observed this pattern in individual domains in Iris Investigate or other investigation tools.

Phishing

This Top Ten list features 100% turnover—none of the top ten name server ASNs is seen in the March 2023 list. Here again, we also see some entities that take their malicious infrastructure seriously, with a total of only 42 neutral domains in the first two rows (vs around 9,500 phishing domains).

March 2024	Signal Strength	Phishing	Malware	Spam	Neutral
39845 LV-2CLOUD-ASN16 2 Cloud Ltd., LV	13991.89	8301	6	8	32
216246 RU-AEZA-AS Aeza Group Ltd., RU	6882.51	1276	34	11	10
57043 HOSTKEY-AS HOSTKEY B.V., NL	1645.91	8300	2	2	272
210644 AEZA-AS AEZA INTERNATIONAL LTD, GB	683.22	1292	40	13	102
55967 BAIDU Beijing Baidu Netcom Science and Technology Co., Ltd., CN	208.53	3553	242	41	919
40824 WZ-US-40824, US	189.98	9221	148	47	2618
200019 AlexHost ALEXHOST SRL, MD	173.37	1305	35	94	406
50867 HOSTKEY-RU-AS HOSTKEY B.V., NL	144.23	8471	24	3	3168
7979 SERVERS-COM, US	134.07	10000	6510	45	4023
50613 ThorDC-AS Advania Island ehf, IS	75.43	2053	61	22	1468

Name Server ASNs

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
54990 AS-1337 (KN)	32.32	1,916	944	119	5,135
39287 Abstract ab stract [sic] (FI)	31.06	1,916	944	119	5,343
45102 ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (CN)	20.55	12,274	7,415	1795	51,734
60592 GRANSY Gransy s.r.o. (CZ)	16.92	2,132	2,651	2132	10,916
51167 CONTABO Contabo GmbH (DE)	9.68	18,553	760	4416	166,062
19318 IS-AS-1 (US)	6.84	18,101	467	4345	229,141
131392 RUNSYSTEM-AS-VN GMO-Z.com Runsystem Joint Stock Company (VN)	5.52	3,390	551	46	53,212
22612 NAMECHEAP-NET (US)	5.19	3,035	1069	500	50,630
48357 K4X K4X OU (EE)	5.15	1,765	556	345	29,707
397213 SECURITYSERVICES (US)	4.38	53,175	24860	21622	1,050,967

Malware

While the malware Top Ten list has milder signal strengths than several of the other lists in this report, there is also a significant range, from 108.97 on the top row to 3.63 on the bottom. This means some of these name server ASNs are not particularly strong indicators that a given domain is malicious. As we are of course fond of saying, context is everything; other aspects of a given domain may make it quite suspicious in the eyes of the analyst.

Other things to note:

- This list had 4 repeaters, and ASNs 58519 and 55990 are next to each other again - but further down the list than last year.

- Relative to the last few Top Ten lists in the report, this one features higher numbers of neutral domains

- "Domain names registrar REG.RU", Ltd, RU has two separate ASNs in this list

March 2024	Signal Strength	Malware	Phishing	Spam	Neutral
7979 SERVERS-COM (US)	**108.97**	6510	10000	45	4023
51852 PLI-AS Private Layer INC, PA	**5.69**	6446	1507	13	76328
33387 NOCIX, US	**5.55**	6505	1406	50	78950
30633 LEASEWEB-USA-WDC, US	**4.43**	8013	2642	164	121823
58519 CHINATELECOM-CTCLOUD Cloud Computing Corporation (CN)	**4.19**	2935	4386	77	47193
55990 HWCSNET Huawei Cloud Service data center (CN)	**4.15**	2935	4387	77	47587
136907 HWCLOUDS-AS-AP HUAWEI CLOUDS (HK)	**3.97**	2987	4424	164	50672
198610 BEGET-AS Beget LLC, RU	**3.81**	10548	3708	38	186274
39561 AS-REGRU "Domain names registrar REG.RU", Ltd, RU	**3.78**	22542	4787	395	401161
197695 AS-REGRU "Domain names registrar REG.RU", Ltd, RU	**3.63**	22727	4877	405	421552

Name Server ASNs

March 2023	Signal Strength	Malware	Phishing	Spam	Neutral
60592 GRANSY Gransy s.r.o. (CZ)	34.68	2,651	2132	66	10,916
58519 CHINATELECOM-CTCLOUD Cloud Computing Corporation (CN)	29.96	2,328	304	15	11,098
55990 HWCSNET Huawei Cloud Service data center (CN)	28.91	2,329	304	15	11,507
7979 SERVERS-COM (US)	28.71	2,804	325	31	13,948
136907 HWCLOUDS-AS-AP HUAWEI CLOUDS (HK)	26.85	2,355	338	15	12,525
45102 ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (CN)	20.47	7,415	12274	1795	51,734
207021 RCODEZERO-ANYCAST-SEC2 ipcom GmbH (AT)	11.04	29,831	2297	305	385,794
133618 TRELLIAN-AS-AP Trellian Pty. Limited (AU)	10.78	12,621	3380	164	167,274
1921 NICAT ipcom GmbH (AT)	8.87	29,885	2338	305	480,957
46475 LIMESTONENETWORKS (US)	7.99	5,392	1807	167	96,343

Spam

The spam Top Ten list had high turnover, with only one ASN, 4686 (BEKKOAME BEKKOAME INTERNET INC of Japan) repeating (and in the same rank as last year). This list also sees a return to incredibly high signal strengths, showing once again that certain providers are truly dedicated to supporting malicious infrastructure. Even if we discount the first few rows, the signal strengths are higher than in last year's list. Finally, this is the list in which the assignment of name servers in separate ASNs really stands out, with rows 3, 4, and 5 having nearly identical counts of domains.

Name Server ASNs

March 2024

March 2024	Signal Strength	Spam	Phishing	Malware	Neutral
212913 TIMEHOST-AS FOP Hornostay Mykhaylo Ivanovych, UA	222820.58	4836	156	16	2
209375 Euroweb-DE SC ITNS.NET SRL, MD	214711.31	4660	4	7	2
140224 SGPL-AS-AP STARCLOUD GLOBAL PTE., LTD., SG	13996.68	1367	14	33	9
132585 SIA-HK-AS SkyExchange Internet Access, HK	12597.01	1367	14	32	10
137951 ASLINE-AS-AP ASLINE LIMITED, HK	4665.56	1367	14	32	27
59796 STORMWALL-AS StormWall s.r.o., SK	702.37	1593	4	14	209
4686 BEKKOAME BEKKOAME INTERNET INC. (JP)	355.50	6215	3	22	1611
56655 TERRAHOST TerraHost AS, NO	259.45	4105	24	15	1458
140227 HKCICL-AS-AP Hong Kong Communications International Co., Limited, HK	68.53	3234	797	214	4349
209242 CLOUDFLARESPECTRUM Cloudflare London, LLC, US	58.08	1401	26	49	2223

March 2023

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
4686 BEKKOAME BEKKOAME INTERNET INC. (JP)	1473.11	4,207	69	15	1003
7684 SAKURA-A SAKURA Internet Inc. (JP)	107.28	5,935	10	393	19430
45102 ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (CN)	12.19	1,795	12274	7415	51734
9370 SAKURA-B SAKURA Internet Inc. (JP)	11.40	5,280	141	181	162714
51167 CONTABO Contabo GmbH (DE)	9.34	4,416	18553	760	166062
38283 CHINANET-SCIDC-AS-AP CHINANET SiChuan Telecom Internet Data Center (CN)	7.55	2,093	3572	2043	97395
397213 SECURITYSERVICES (US)	7.23	21,622	53175	24860	1050967
19318 IS-AS-1 (US)	6.66	4,345	18101	467	229141
397220 SECURITYSERVICES (US)	6.34	21,625	53452	24959	1198951
134543 UNICOM-DONGGUAN-IDC China Unicom Guangdong IP network (CN)	6.25	5,628	11868	7860	316436

IP Geolocation

This category examines hotspots of malicious activity by the country code of the IP address hosting the domains in question. As we have noted in previous editions, the IP hosting region is not generally a strong indicator of maliciousness, as illustrated by the presence of mild malicious signal strengths and even in a couple of cases, slightly better-than-average (less malicious) entries.

Phishing

The phishing Top Ten list features 4 repeaters, 2 of which are double-repeaters (they appeared in the last two reports). Belize came on strong this year, with both signal strength and domain counts substantially higher than the second-place country (Moldova). Belize, Russia, and Ukraine also figure on this year's spam list, while Taiwan is on this and the malware list. Hong Kong and Singapore, meanwhile, are on all three Top Ten lists.

March 2024	Signal Strength	Phishing	Malware	Spam	Neutral
BZ (Belize)	495.92	38299	276	6177	5367
MD (Moldova)	23.89	1751	429	350	5093
IS (Iceland)	13.74	1249	55	49	6318
TW (Taiwan)	3.35	3354	1175	2211	69517
VN (Vietnam)	3.34	2532	810	458	52627
HK (Hong Kong)	3.29	16049	11594	13960	338625
SG (Singapore)	2.53	8453	8937	2286	232503
RU (Russia)	2.39	22384	26120	5214	651721
SE (Sweden)	2.28	5226	1391	412	159206
UA (Ukraine)	1.62	2005	661	1218	85846

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
LU (Luxembourg)	10.74	6852	2507	3719	45919
HK (Hong Kong)	5.08	10210	4722	5059	144766
TW (Taiwan)	2.48	1728	746	400	50079
RU (Russia)	2.18	13862	5014	3886	457399
CN (China)	2.09	3930	1643	456	135266
LT (Lithuania)	1.58	1099	844	491	50105
VN (Vietnam)	1.54	1921	475	202	89824
BR (Brazil)	1.54	7775	3870	1064	364573
NL (Netherlands)	1.43	27907	12215	6808	1408415
US (United States)	1.23	205543	109958	42041	12036790

Malware

The malware Top Ten has less turnover than some of the other lists, with half of the top ten repeating from last year; two of the entries, Hong Kong and China, are double-repeaters. Signal strengths are fairly similar to last time around (and are quite low, reminiscent of what we observed in TLDs).

But perhaps the most notable thing about this list is that we only had 9 countries that positively correlated with spam; Taiwan, in tenth spot, actually has a below-1 signal strength, which means that it correlates more with neutral domains than with spam domains. The domain counts illustrate this.

March 2024	Signal Strength	Malware	Phishing	Spam	Neutral
BR (Brazil)	2.37	17301	9342	1948	413050
LT (Lithuania)	2.30	9803	4837	713	240268
RU (Russia)	2.26	26120	22384	5214	651721
SG (Singapore)	2.17	8937	8453	2286	232503
HK (Hong Kong)	1.93	11594	16049	13960	338625
IN (India)	1.53	5239	2116	2312	193809
CH (Switzerland)	1.50	5849	1924	1682	220274
US (United States)	1.30	372108	255738	71200	16142004
CN (China)	1.28	3325	1933	576	146546
TW (Taiwan)	0.95	1175	3354	2211	69517

March 2023	Signal Strength	Malware	Phishing	Spam	Neutral
CA (Canada)	7.41	40315	5056	610	655830
LU (Luxembourg)	6.58	2507	6852	3719	45919
HK (Hong Kong)	3.93	4722	10210	5059	144766
AU (Australia)	3.18	13045	4397	281	494694
CN (China)	1.46	1643	3930	456	135266
CZ (Czech Republic)	1.39	4021	2365	188	348230
RU (Russia)	1.32	5014	13862	3886	457399
BR (Brazil)	1.25	3780	7775	1064	364573
US (United States)	1.10	109958	205543	42041	12036790
NL (Netherlands)	1.05	12215	27907	6808	1408415

Spam

The story on this list is actually quite similar to the malware list. There are four countries that repeated from March 2023, and Hong Kong is a double-repeater. Unlike 2023, however, none of the top ten entries has a "green" (more neutral than malicious) signal strength.

Meanwhile, Belize, which had its Top Ten debut in phishing, also tops this list in 2024. What is going on in Belize? (Your authors may need to go there on a fact-finding mission.)

March 2024	Signal Strength	Spam	Phishing	Malware	Neutral
BZ (Belize)	162.08	6177	38299	276	5367
JP (Japan)	9.10	15565	5103	2046	240913
HK (Hong Kong)	5.81	13960	16049	11594	338625
TW (Taiwan)	4.48	2211	3354	1175	69517
UA (Ukraine)	2.00	1218	2005	661	85846
IN (India)	1.68	2312	2116	5239	193809
BG (Bulgaria)	1.66	1320	2366	588	112038
TR (Turkey)	1.55	3119	2334	2474	283982
SG (Singapore)	1.38	2286	8453	8937	232503
DE (Germany)	1.36	35373	31395	32379	3659302

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
LU (Luxembourg)	23.22	3719	6852	2507	45919
HK (Hong Kong)	10.02	5059	10210	4722	144766
JP (Japan)	8.82	6677	993	739	217153
BG (Bulgaria)	2.60	1128	1446	377	124490
RU (Russia)	2.44	3886	13862	5014	457399
NL (Netherlands)	1.39	6808	27907	12215	1408415
TR (Turkey)	1.14	1454	2096	1000	365450
US (United States)	1.00	42041	205543	109958	12036790
BR (Brazil)	0.84	1064	7775	3780	364573
GB (United Kingdom)	0.75	3422	12286	5140	1316678

Domain Registrars

While the GDPR veiled a considerable amount of the registrant information that can help researchers or defenders cluster domains, those domains still have to be registered somewhere, and the domain registrar is always shown in a Whois record. Therefore, we judge that registrar remains a useful category for searching for signals of malicious activity across the Internet's active domains.

Phishing

This list features 4 repeaters, with NiceNIC repeating as the top - but check out the signal strength—they seem to have registered only 8 neutral domains! NiceNIC is also a double-feature on this and the Malware lists. Other notable features:

- Alibaba, Sav.com, URL Solutions, and OwnRegistrar are on all 3 Top Ten lists

- URL Solutions, moving from 9th to 2nd place, also seemed to rid itself of neutral domains over the last year

- Alibaba, on the other hand, picked up a lot of neutral domains as well as phishing domains, with a mildly lower signal this year

- Paknic and CNOBIN INFORMATION TECHNOLOGY LIMITED is on this and the malware lists, while Hongkong Kouming International Limited is on this and the Spam lists

March 2024	Signal Strength	Phishing	Malware	Spam	Neutral
3765 NICENIC INTERNATIONAL GROUP CO., LIMITED*	125050.20	26315	5608	353	8
1449 URL Solutions, Inc.	90903.30	59779	10254	7252	25
1367 Paknic (Private) Limited	99.01	2560	1193	4	983
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	21.15	53318	14408	5535	95824
609 Sav.com, LLC	9.46	45907	31141	39464	184475
3972 Hongkong Kouming International Limited	9.10	4591	1794	1175	19175
817 MAFF Inc.	8.55	1087	384	86	4835
3858 Aceville Pte. Ltd.	6.81	15304	2721	473	85431
1250 OwnRegistrar, Inc.	6.70	12693	8714	4506	72026
3254 CNOBIN INFORMATION TECHNOLOGY LIMITED	6.56	1402	1776	517	8128

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
3765 NICENIC INTERNATIONAL GROUP CO., LIMITED	**53.41**	6769	3017	544	5412
1915 West263 International Limited	**32.84**	33850	4130	261	44014
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	**30.78**	24015	8645	1502	33314
1868 Eranet International Limited	**21.24**	7538	1361	185	15153
1556 Chengdu West Dimension Digital Technology Co., Ltd.	**15.74**	40205	20642	529	109094
3806 Beget LLC	**13.05**	2425	515	28	7933
609 Sav.com, LLC	**10.82**	37967	23273	17467	149890
1479 NameSilo, LLC	**9.64**	140781	29130	17196	623435
1449 URL Solutions, Inc.	**9.40**	8287	5110	186	37637
1606 Registrar of Domain Names REG.RU LLC	**9.33**	17315	4778	843	79285

Malware

NiceNIC has gotten busy - it takes top position in both phishing and malware, and look at those signal strengths—similar to what we've seen in a few of the other lists this year. Like NiceNIC, URL Solutions also seems to have shed neutral domains since last year. Having said this, if we discount the outliers, the bulk of the list actually shows overall lower signal strengths than in March 2023.

There was less turnover in malware, with 6 registrars repeating from last year. Finally, we note that Cloud Yuqu also appears on this year's spam list.

Domain Registrars

March 2024	Signal Strength	Malware	Phishing	Spam	Neutral
3765 NICENIC INTERNATIONAL GROUP CO., LIMITED*	**29335.34**	5608	26315	353	8
1449 URL Solutions, Inc.	**17164.31**	10254	59779	7252	25
1367 Paknic (Private) Limited	**50.79**	1193	2560	4	983
3254 CNOBIN INFORMATION TECHNOLOGY LIMITED	**9.14**	1776	1402	517	8128
3806 Beget LLC	**7.65**	7019	3028	69	38421
609 Sav.com, LLC	**7.06**	31141	45907	39464	184475
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	**6.29**	14408	53318	5535	95824
1606 Registrar of Domain Names REG.RU LLC	**5.83**	26351	15929	799	189192
1250 OwnRegistrar, Inc.	**5.06**	8714	12693	4506	72026
3824 Cloud Yuqu LLC	**4.35**	4480	2791	4504	43104

| March 2023	Signal Strength	Malware	Phishing	Spam	Neutral
3765 NICENIC INTERNATIONAL GROUP CO., LIMITED	**48.21**	3017	6769	544	5412
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	**22.44**	8645	24015	1502	33314
3824 Cloud Yuqu LLC	**20.93**	3297	1161	28	13620
1556 Chengdu West Dimension Digital Technology Co., Ltd.	**16.36**	20642	40205	529	109094
609 Sav.com, LLC	**13.43**	23273	37967	17467	149890
1449 URL Solutions, Inc.	**11.74**	5110	8287	186	37637
1555 22net, Inc.	**9.57**	2781	1710	47	25140
1250 OwnRegistrar, Inc.	**9.10**	9192	9218	1043	87355
1915 West263 International Limited	**8.12**	4130	33850	261	44014
1868 Eranet International Limited	**7.77**	1361	7538	185	15153

Spam

URL Solutions "overachieved" (dubious achievement) vs. the other registrars, with a signal strength more than three orders of magnitude higher than the next-place registrar. It and four other registrars were repeaters this year, but none was a double-repeater.

March 2024	Signal Strength	Spam	Phishing	Malware	Neutral
1449 URL Solutions Inc	**17164.31**	10254	59779	7252	25
609 Sav.com, LLC	**7.06**	31141	45907	39464	184475
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	**6.29**	14408	53318	5535	95824
1250 OwnRegistrar, Inc.	**5.06**	8714	12693	4506	72026
3824 Cloud Yuqu LLC	**4.35**	4480	2791	4504	43104
1923 Gname.com Pte. Ltd.	**4.05**	55114	74585	35074	569645
3972 Hongkong Kouming International Limited	**3.92**	1794	4591	1175	19175
460 Web Commerce Communications Limited dba WebNic.cc	**3.76**	13328	15219	4226	148524
1509 Cosmotown, Inc.	**2.95**	5572	5992	1085	78913
1601 Atak Domain Bilgi Teknolojileri A.S.	**2.71**	3992	6022	1200	61657

Domain Registrars

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
Sav.com, LLC	24.34	17467	37967	23273	149890
GMO IntGMO Internet, Inc. d/b/a Onamae.com	17.25	54529	13501	6244	660360
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	9.42	1502	24015	8645	33314
3855 Hong Kong Juming Network Technology Co., Ltd	6.60	1740	2995	1373	55097
1479 NameSilo, LLC	5.76	17196	140781	29130	62,435
1599 Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	5.43	4192	16838	5873	161257
Namecheap, Inc.	4.52	52490	124890	56528	2426272
1250 OwnRegistrar, Inc.	2.49	1043	9218	9192	87355
Dynadot, LLC	2.40	4601	23326	24704	401274
1923 Gname.com Pte. Ltd.	2.27	1604	14414	6190	147642
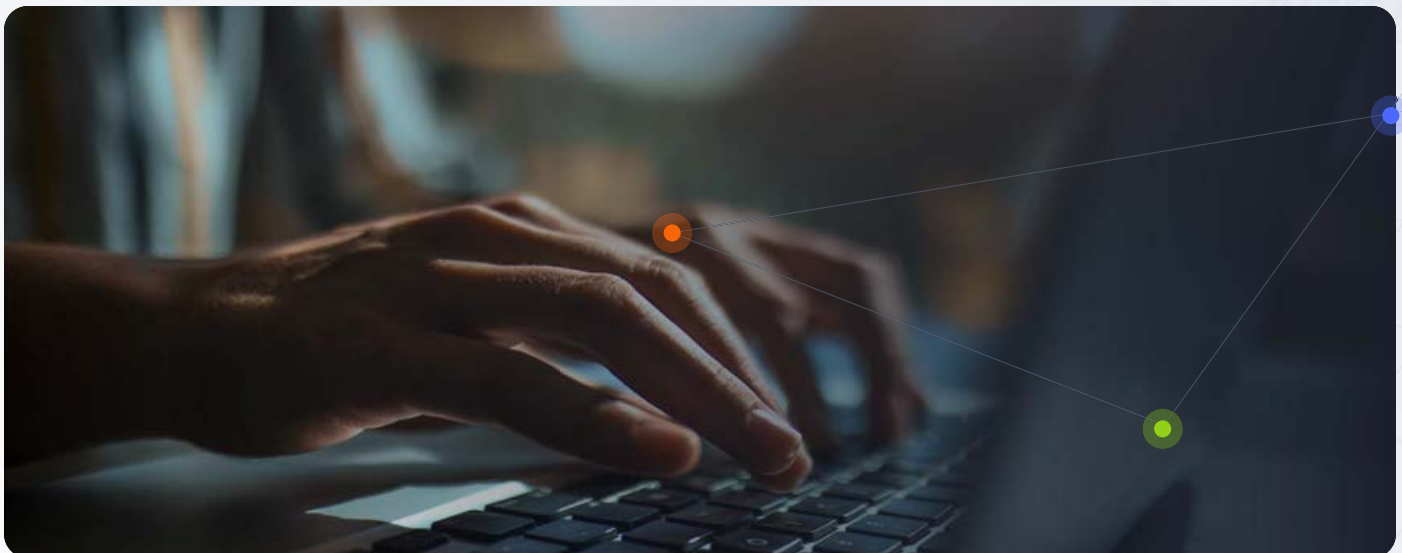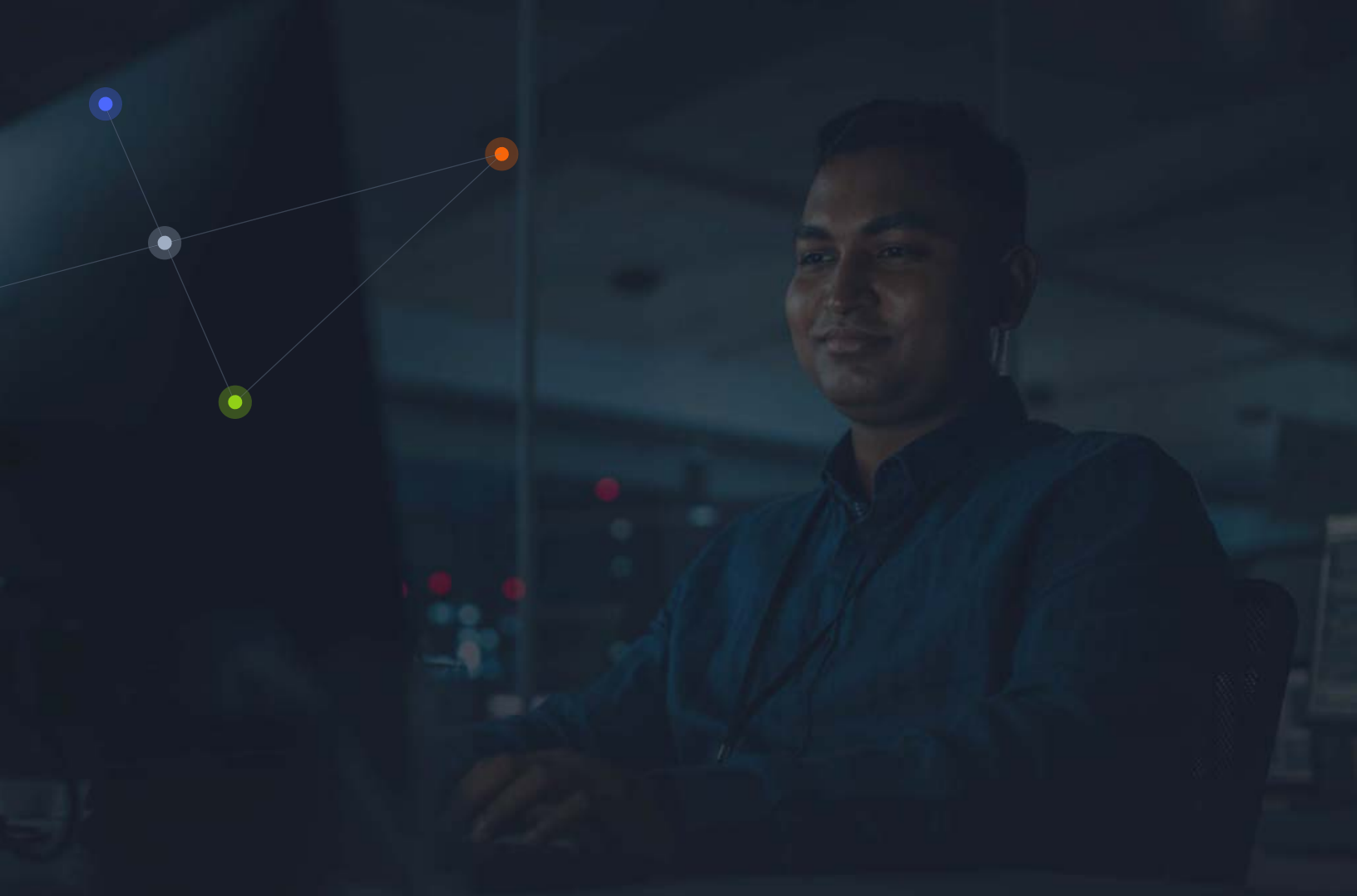
SSL Certificate Authorities

As has been the case previously, with SSL Certificate Authorities (CAs), we have seen threat categories in which **the data did not turn up ten entities that all had signals of maliciousness** in each of the threat types. As a consequence, the tables below include some green cells, as first seen in the Fall 2021 edition. As a reminder, a signal strength of 1.00 is entirely neutral. Almost every data point in the other categories of this report has a signal strength greater than 1.00, indicating that domains sharing that data point have a higher concentration of malicious domains than their lower-signal peers. For the CAs associated with domains, however, fewer than ten had a positive correlation with maliciousness for any of the threat types.

SSL Certificate Authorities

One of the CAs most often pilloried for associations with malicious domains—**Let's Encrypt**—actually had positive signals in every threat type, except in the spam list, where both "flavors" of Let's Encrypt certificates were correlated (albeit very slightly) with malicious domains. What "flavors" do we mean? Each of the Top 10 tables in this section has two entries for Let's Encrypt—one with the CN E1, and one with the CN R3. E1 refers to a certificate type that uses a different cryptographic algorithm. There are not as many of these certificates in circulation as the previously existing R3 type, though it has gained ground in the year-plus that it has been around; but they are associated with enough malicious activity that the **Let's Encrypt E1 certificates took second place in our lists for each threat type, exactly as they did last year**. (It is important to note that this correlation with malicious activity has nothing to do with the certificates themselves. Rather, for reasons unknown, actors who create malicious domains seem to be fans of the newer certificate type, relative to creators of neutral domains.) The more common R3 certificates correlated slightly with more neutral domains, as shown in the previous report.

Some readers may wonder why s**elf-signed certificates make no appearance** in our Top Ten lists. There is a two-part explanation: first, our thresholding eliminates any issuer with fewer than 1,000 domains of the threat type under examination. Second, some of the tunings we did to the inputs to the report (well-regarded domain blocklists) resulted in changes to malicious domain counts. This tuning meant that for this edition of the report (as well as the last report), self-signed certificates were not tied to more than 1000 domains in the phishing or spam categories, though they do appear on the malware list this year.

The spam list also has fewer than ten rows altogether—it's a "Top Seven" list. The reason has to do, again, with our thresholding. There are only seven CAs that have more than 1,000 active spam domains tied to them.

The final point to emphasize for certificate issuers is that we saw more repeaters in these three lists (look for the bold entity names) than in the other categories of both this and the last edition of the report.
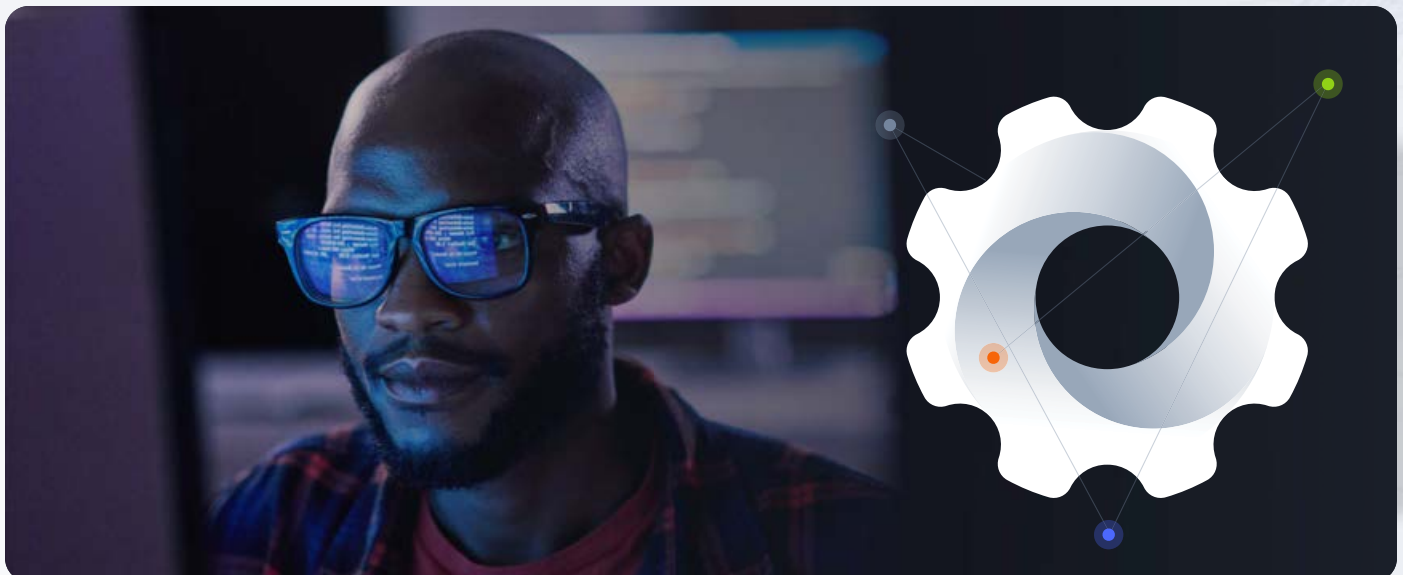
Phishing

Certificate issuers showed less correlation with phishing in our 2024 snapshot than in last year's, illustrated by 6 "green" rows in this table, vs. 4 in 2023. The Google Trust Services 1P5 certificate repeated in the same position at the top, though with a milder signal this time. It's also a double-repeater. The same holds true for the aforementioned E1 Let's Encrypt certificates. Finally, CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US moved into the green this time, meaning that these certificates are mildly less correlated with maliciousness than a random sample of domains.

March 2024	Signal Strength	Phishing	Malware	Spam	Neutral
*CN=GTS CA 1P5,O=Google Trust Services LLC,C=US**	3.66	111275	206981	22322	2847881
*CN=E1,O=Let's Encrypt,C=US**	2.81	53540	100941	9043	1780074
CN=ZeroSSL ECC Domain Secure Site CA,O=ZeroSSL,C=AT	2.31	2757	2902	345	111558
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	1.48	4342	6942	1076	274895
CN=Encryption Everywhere DV TLS CA - G2,OU=www.digicert.com,O=DigiCert Inc,C=US	0.75	8147	12143	1223	1018652
CN=R3,O=Let's Encrypt,C=US	0.71	175432	202190	76505	23100405
CN=GTS CA 1D4,O=Google Trust Services LLC,C=US	0.62	2423	2253	323	366536
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	0.57	4243	8307	118	692033
CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=Arizona,C=US	0.54	7719	10221	717	1348476
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.51	7270	5737	1657	1326072

● SSL Certificate Authorities

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
CN=**GTS CA 1P5,O=Google Trust Services LLC,**C=US	10.95	49888	23098	6630	681628
CN=**E1,O=Let's Encrypt,**C=US	5.06	8161	5587	1521	241103
CN=**Cloudflare Inc ECC CA-3,**O=Cloudflare\, Inc.,C=US	2.84	31931	17374	3504	1683623
CN=**Encryption Everywhere DV TLS CA - G2,OU=www.digicert.com,O=DigiCert Inc,**C=US	2.31	1497	443	79	97115
CN=**ZeroSSL RSA Domain Secure Site CA,**O=ZeroSSL,C=AT	1.91	2413	1344	193	189379
CN=**GTS CA 1D4,O=Google Trust Services LLC,**C=US	1.32	2465	1534	112	279858
CN=**cPanel\, Inc. Certification Authority,**O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.65	11758	5763	818	2708969
CN=R3,O=Let's Encrypt,**C=US**	0.63	81563	71733	18516	19520458
CN=**Encryption Everywhere DV TLS CA - G1,**OU=www.digicert.com,O=DigiCert Inc,C=US	0.57	3133	1814	77	821459
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	0.49	6708	4510	235	2038567

Malware

This list may be the most similar to its 2023 counterpart than any other table in this report. The malware category shows the same number of green rows as before (four), comparable signal strengths, and a lot of repeating certificate issuers. Self-signed certificates do make an appearance on this list, just barely registering above a random sample, with a signal strength of 1.03.

● SSL Certificate Authorities

March 2024	Signal Strength	Malware	Spam	Phishing	Neutral
*CN=GTS CA 1P5,O=Google Trust Services LLC,C=US**	**4.45**	206981	111275	22322	2847881
*CN=E1,O=Let's Encrypt,C=US**	**3.47**	100941	53540	9043	1780074
CN=ZeroSSL ECC Domain Secure Site CA,O=ZeroSSL,C=AT	**1.59**	2902	2757	345	111558
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT*	**1.55**	6942	4342	1076	274895
self-signed	**1.03**	4070	715	191	241841
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	**1.02**	27085	7767	1115	1619230
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	**0.74**	8307	4243	118	692033
CN=Encryption Everywhere DV TLS CA - G2,OU=www. digicert.com,O=DigiCert Inc,C=US	**0.73**	12143	8147	1223	1018652
CN=R3,O=Let's Encrypt,C=US	**0.54**	202190	175432	76505	23100405
CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, wInc.,L=Scottsdale,ST=Arizona,C=US	**0.46**	10221	7719	717	1348476

March 2023	Signal Strength	Malware	Spam	Phishing	Neutral
CN=GTS CA 1P5,O=Google Trust Services LLC,C=US	**7.58**	23098	6630	49888	681628
CN=E1,O=Let's Encrypt,C=US	**5.18**	5587	1521	8161	241103
CN=**Cloudflare Inc ECC CA-3**,O=Cloudflare\, Inc.,C=US	**2.31**	17374	3504	31931	1683623
CN=**ZeroSSL RSA Domain Secure Site CA**,O=ZeroSSL,C=AT	**1.59**	1344	193	2413	189379
CN=**GTS CA 1D4,O=Google Trust Services LLC**,C=US	**1.23**	1534	112	2465	279858
CN=**R3,O=Let's Encrypt**,C=US	**0.82**	71733	18516	81563	19520458
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	**0.50**	4510	235	6708	2038567
CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert. com,O=DigiCert Inc,C=US	**0.49**	1814	77	3133	821459
CN=**cPanel\, Inc. Certification Authority**,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	**0.48**	5763	818	11758	2708969

Spam

The spam list showed a bit more change than did the malware list; it consists of 7 rows this time vs 4 last time. This means that there were more issuers associated with at least 1,000 spam domains than there were on the last report. Signal strengths are overall unremarkable, and are very similar to the other threat categories.

March 2024	Signal Strength	Spam	Phishing	Malware	Neutral
*CN=GTS CA 1P5,O=Google Trust Services LLC,C=US**	2.47	22322	111275	206981	2847881
*CN=E1,O=Let's Encrypt,C=US**	1.60	9043	53540	100941	1780074
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	1.23	1076	4342	6942	274895
CN=R3,O=Let's Encrypt,C=US*	1.04	76505	175432	202190	23100405
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.39	1657	7270	5737	1326072
CN=Encryption Everywhere DV TLS CA - G2,OU=www.digicert.com,O=DigiCert Inc,C=US	0.38	1223	8147	12143	1018652
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	0.22	1115	7767	27085	1619230

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
CN=GTS CA 1P5,O=Google Trust Services LLC,C=US	9.25	6,630	49888	23098	681628
CN=E1,O=Let's Encrypt,C=US	6.00	1,521	8161	5587	241103
CN=**Cloudflare Inc ECC CA-3**,O=Cloudflare\, Inc.,C=US	1.98	3,504	31931	17374	1683623
CN=**R3**,O=**Let's Encrypt**,C=US	0.90	18,516	81563	71733	19520458

Conclusion

Perhaps the most interesting takeaway from this year's report is those extreme signal strengths we observed in several tables, including the "infinite" signal strength for the first-place Russian hosting AS. Some entities on the Internet are almost exclusively devoted to malicious activity. Defenders may have seen these appear on their networks (though we hope not), and these entities show that scrutiny of some of these features of domains can help identify dangerous activity.

We identify these "hotspots" of malicious activity in part to point investigators and researchers toward forensic data points that will be useful in helping make sense of Internet infrastructure of unknown quality or nature. We also use the information to help inform our own research and development efforts, as we seek to develop ever-more-accurate algorithms for predicting the nature of a given domain. We acknowledge that as forensic indicators, some of these data points are not likely to make too big an impact for most organizations, as the odds of coming across any of the domains tied to them are low. On the other hand, we do consistently observe some data points with meaningful numbers of malicious domains, and in some cases, these come with meaningful signal strengths. Such data points represent clusters of activity where a real impact is being felt by victims.

We hope that this and future editions will be useful to others who, like the DomainTools team, are passionate about making the Internet a safer place for everyone.