

Spring 2022



# The DomainTools Report

Internet-Scale Patterns in Malicious  
Infrastructure



## Introduction

Welcome to the Spring 2022 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 edition in the [Fall of 2021](#). 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 which we studied in the first DomainTools Report, are dramatically less relevant in the post-GDPR world of default privacy for most registrations.

But 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 and Methodology

### Domain Characteristics Evaluated

For this edition of the 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
- **Nameserver ASN**; these represent the hosting of the nameserver 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; for example, we will see that when it comes to SSL certificate issuers, some readers may be surprised by what this large-scale analysis shows—and does not show—about where the danger lies. (We first saw these surprises in our Fall 2021 edition.)

## Methodology

### *Candidate Domains*

The DomainTools Iris database includes around 380 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 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.

An implication of this thresholding is that **there are 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.

*NOTE: We decided to make two minor changes to our thresholding methodology for this edition. 1) In the previous report, we would include any feature (TLD, registrar, etc) that had a total of at least 1,000 (or 100 for IP geolocation) malicious domains of any kind. For this edition, it was required to have 1,000 of the **specific threat type** under examination. 2) We set the IP geolocation threshold at 1,000, matching the others (it previously was 100).*

### *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 nameserver, a registrar, etc) the higher our confidence that any unknown domain from that population may be involved in the threat in question. And 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 actually 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 late May, 2022.

## 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
.xyz	108.60	323,439	91,575	55,757	43,320

The TLD .xyz has a malware signal strength of **108.60**, and there are 323,439 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 10 list, the individual entities on the list that were repeats from the previous report in Q4 of 2021 are shown in **bold**. In the example above, the .xyz TLD is in bold because it was also a top 10 TLD for malware domains in the last report.

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 always 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

### Hotspots Abound

Any seasoned network defender or cybersecurity researcher knows that there are certain “areas” of the Internet that raise more suspicion than others. Traffic flows or alerts seen in a SOC where an IP address or domain is seen to have a particular characteristic—for example the domain's TLD, or the region in which the IP address is hosted—are given different scrutiny once that characteristic becomes known. Our findings reinforce that there are certain domain features that ought to be considered markers of potential risk. Since this report focuses on those, it speaks to the concept of risk overall. However, data has a way of helping us keep our biases in check, or at least constrained. In the previous edition of this report, we uncovered a fascinating set of findings: for the category of SSL certificate issuers, some of the top-ten signal strength figures were below 1.00, which is the threshold for neutrality—meaning that **those certificate issuers were actually more associated with neutral or even known-good domains than malicious ones**. Not only does this report corroborate those findings, it uncovers a different category in which the same thing occurs.

In some categories, the findings this time around are remarkably similar to those in the previous report; the domain feature of SSL certificate issuer stands out in this respect, because for each of the three threat types, nine of the top 10 issuers were the same as in the Q4 2021 report. In other categories, the lineup changes quite a bit.

### 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 (.ml, .ga), and new generic (.bar, .cyou) 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 10 lists will show.

## Phishing

Following are the top ten TLDs ranked by signal strength for phishing. Even with our thresholding change, there are a lot of repeat appearances compared to the previous Report. The TLDs .buzz, .rest, .ml, .top, .monster, and .cyou were all in the previous Top 10 list for phishing. The highest signal strength, 245.35 for the .buzz TLD, is almost twice the highest signal strength from last time around (which was 131.03 for .rest). More notable, perhaps, is that we observed a large uptick in the absolute numbers of phishing domains in .buzz, with over 13,000 domains this time versus ~9,000 in the previous report. In fact, even though our new thresholding rule would have eliminated only one contender from the previous Top 10 (.rest, with a total of 426 phishing domains), the absolute numbers were substantially higher this time around across the TLDs.

May 2022	Signal Strength	Phishing	Malware	Spam	Neutral
.buzz	245.35	13,388	7,792	500	1,293
.gq	190.27	16,606	5,916	885	2,068
.ga	160.14	24,228	7,146	1,156	3,585
.rest	157.84	3,657	705	539	549
.ml	156.69	27,667	6,535	1,427	4,184
.top	149.81	80,302	41,721	5,223	12,701
.cf	118.83	18,425	4,086	1,115	3,674
.monster	116.59	3,759	1,366	461	764
.cyou	114.96	5,497	6,149	633	1,133
.quest	73.49	2,971	1,483	409	958

Nov 2021	Signal Strength	Phishing	Malware	Spam	Neutral
.rest	131.03	426	229	498	167
.cyou	81.20	9,759	1,257	414	6,173
.bar	65.20	3,064	6,321	2,648	2,414
.rest	62.89	2,407	909	1,119	1,966
.monster	43.97	2,687	1,334	179	3,139
.casa	43.65	1,760	2,072	2,529	2,071
.buzz	39.61	9,253	4,321	1,809	11,999
.ml	28.11	26,237	3,331	1,818	47,945
.live	25.10	12,787	4,420	1,575	26,164
.top	21.27	34,005	58,486	4,329	82,113

## Malware

Sorry, .xyz, but your reputation in the infosec community is what it is for a reason. In the Malware category, we observed over 323,000 domains in .xyz, a significant uptick from its previous showing of a still-substantial ~207,000. Couple this with the signal strength of 108.60, and it becomes especially clear why this TLD has the reputation it does. Elsewhere across the Malware scoreboard, there were four repeat appearances: the TLDs .xyz, .cc, .top, and .bar. The range of signal strengths in the top 10 was similar to last time, topping out at 108.60 (vs 108.93) and flooring at 26.01 (vs 19.33).

May 2022	Signal Strength	Malware	Phishing	Spam	Neutral
.xyz	108.60	323,439	91,575	55,757	43,320
.cc	106.95	53,242	4,762	408	7,241
.buzz	87.65	7,792	13,388	500	1,293
.cfd	84.43	1,695	915	220	292
.cyou	78.94	6,149	5,497	633	1,133
.top	47.78	41,721	80,302	5,223	12,701
.gq	41.61	5,916	16,606	885	2,068
.bar	40.17	2,535	2,730	4,196	918
.ga	28.99	7,146	24,228	1,156	3,585
.monster	26.01	1,366	3,759	461	764

Nov 2021	Signal Strength	Malware	Phishing	Spam	Neutral
.bar	108.93	6,321	3,064	2,648	2,414
.quest	57.04	229	426	498	167
.cc	51.93	28,411	4,145	696	22,758
.casa	41.62	2,072	1,760	2,529	2,071
.xyz	33.90	207,726	70,178	51,693	254,882
.top	29.63	58,486	34,005	4,329	82,113
.bid	27.78	1,035	244	131	1,550
.surf	22.02	378	289	1,229	714
.club	21.52	43,017	15,233	2,388	83,156
.icu	19.33	6,637	4,445	362	14,280

## Spam

Among TLDs with the highest signal strength for spam, .cam made a major jump, from the 8th position to 1st. Its signal strength increased by more than an order of magnitude, as well (370.12 vs 23.98), while in absolute numbers it nearly doubled. Second-place .bar also increased in signal quite a bit (295.72 vs 80.18), while .surf repeated in third place, with a much higher signal strength (249.18 vs 125.81) but a similar spam domain count (1,244 vs 1,229). TLDs repeating from last time were .cam, .bar, .surf, and .xyz. Another data point that stands out about .xyz is its high overall count of spam domains, with almost 56,000 as of our snapshot time.

May 2022	Signal Strength	Spam	Phishing	Malware	Neutral
.cam	370.12	6,373	735	1,145	1,114
.bar	295.72	4,196	2,730	2,535	918
.surf	249.18	1,244	326	210	323
.xyz	83.27	55,757	91,575	323,439	43,320
.click	43.51	1,384	2,047	1,804	2,058
.top	26.61	5,223	80,302	41,721	12,701
.tk	22.81	1,699	14,902	6,866	4,819
.ml	22.07	1,427	27,667	6,535	4,184
.ga	20.86	1,156	24,228	7,146	3,585
.cf	19.63	1,115	18,425	4,086	3,674

Nov 2021	Signal Strength	Spam	Phishing	Malware	Neutral
.quest	217.97	498	426	229	167
.work	148.61	50,152	4,092	4,327	24,667
.surf	125.81	1,229	289	378	714
.casa	89.26	2,529	1,760	2,072	2,071
.bar	80.18	2,648	3,064	6,321	2,414
.fit	50.45	2,166	404	573	3,138
.rest	41.60	1,119	2,407	909	1,966
.cam	23.98	3,288	557	3,228	10,020
.xyz	14.82	51,693	70,178	207,726	254,882
.uno	12.87	384	186	477	2,181



## 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 Fall 2021 edition, **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 41564 has 1713 malware domains vs just 50 neutral). With each AS in this and the following section, we provide its country code of registration in parentheses.

For Malware and Spam, as you will see, the top signal strengths are considerably lower than they were in the previous edition of the report. This may be attributable to our change in methodology, where we now require at least 1,000 domains of the threat type being examined. An effect of this change is that there is less skewing toward high signal strengths for some features when relatively small counts of domains can swing the strengths substantially.

### *Phishing*

Following are the top ten IP ASNs ranked by signal strength for phishing. You will note the dramatically higher signal strengths in this category compared to the TLD category: whereas the highest Phishing signal in TLDs was 245.35, the highest among IP ASNs is 50,665.41—an over 200x increase! The spread at the bottom of the chart (10th position) is not as great: 132.56 in IP ASN vs 73.49 in TLDs. (The massive signal strength for 49447 flies in the face of the reasoning around the more modest top signal strengths for the other two threat types, but the low overall domain counts are at play here in creating that huge value.)

A quick glance at the domain counts shows why AS 49447 has such an astronomical signal strength: while it does not have a huge overall number of phishing domains (1,125), it has but **one** domain showing as neutral. This means that, to put it mildly, one would be well advised to treat any traffic from this AS as suspicious. Nor is this a new phenomenon, at least compared with our last report in the fall of 2021: 49447 also topped out that list, albeit with a substantially lower signal strength owing to the 15 neutral domains that appeared that time. Overall, five of these ASNs were repeaters in the Top 10.

May  
2022

		Signal Strength	Phishing	Malware	Spam	Neutral
49447	Nice IT Services Group Inc (DM)	50665.41	1,125	119	28	1
140803	HQDATA-AS-VN 8, 195 St, Thang Town, Hiep Hoa, Bac Giang, Viet Nam (VN)	21024.27	5,602	10	0	12
209813	Fast Content Delivery LTD (SC)	3571.35	3,172	301	223	40
211193	ZHUSUP-AS (KG)	2592.07	2,072	16	60	36
41564	Orion Network Limited (SE)	1418.63	1,575	1,713	7	50
58065	Packet Exchange, LTD (SE)	1131.06	2,411	1,619	30	96
9002	RETN-AS (GB)	653.63	1,074	944	2	74
31624	VFMNL-AS Amsterdam Location BGP Setup (NL)	513.71	57,900	15,059	1,694	5,076
59447	SAYFANET (TR)	194.03	2,641	983	67	613
262254	DDOS-GUARD CORP (BZ)	132.56	1,769	181	175	601

Nov 2021

		Signal Strength	Phishing	Malware	Spam	Neutral
49447	Nice IT Services Group Inc (DM)	8,047.06	1,572	131	46	15
24295	Internap Japan Co., Ltd. (JP)	2,167.04	254	394	923	9
211390	Cloud Solutions Ltd (RU)	805.74	808	91	453	77
132827	GATEWAY INC (JP)	649.86	347	141	1,608	41
58065	Packet Exchange, LTD (SE)	621.96	1,134	1,354	421	140
41564	Orion Network Limited (SE)	409.52	608	877	99	114
262254	DDOS-GUARD CORP (BZ)	404.55	2,550	90	147	484
59447	Istanbuldc Veri Merkezi Ltd Sti (TR)	303.38	1,857	2,964	126	470
209813	Fast Content Delivery LTD (SC)	290.33	2,314	726	294	612
200313	INTERNET IT COMPANY (SC)	180.91	589	185	447	250

## Malware

The top signal strengths among IP ASNs for malware were dramatically more modest than for phishing (787.46 for malware vs 50,665.41 for phishing), though at 10th position, they were much closer (178.40 vs 132.56). In general, in this category the counts of malicious domains are relatively low, but fourth-place AS 46261 stands out, with over 37,000 malware domains (vs a bit under 3,000 neutral). Given the signal strengths, traffic from the protected environment to any of these AS should be considered suspicious.

May 2022

		Signal Strength	Malware	Phishing	Spam	Neutral
41564	Orion Network Limited (SE)	787.46	1,713	1,575	7	50
58065	Packet Exchange, LTD (SE)	387.63	1,619	2,411	30	96
59037	ZHIYUNET Hangzhou ZhiYu Network Technology Co.,Ltd. (CN)	323.66	1,211	0	0	86
46261	QUICKPACKET (US)	288.69	37,366	608	545	2,975
20248	TAKE2 (US)	278.81	5,216	111	4	430
399077	TERAEXCH (US)	241.37	3,497	563	13	333
136970	YISUCLOUDLTD-AS-AP YISU CLOUD LTD, (HK)	226.67	1,282	279	10	130
18779	EGIHOSTING (US)	193.95	143,664	8,275	10,400	17,025
54600	PEG TECH Inc (US)	181.56	81,117	5,813	3,987	10,269
398823	PEG TECH Inc (US)	178.40	17,898	715	2,506	2,306

Nov 2021

		Signal Strength	Malware	Phishing	Spam	Neutral
136574	Shanghai Zheye Network Technology Co.Ltd (CN)	3,379.93	573	13	1230	9
24295	Internap Japan Co., Ltd. (JP)	2,324.07	394	254	923	9
58065	Packet Exchange, LTD (SE)	513.44	1354	1134	421	140
49447	Nice IT Services Group Inc (DM)	463.63	131	1572	46	15
41564	Orion Network Limited (SE)	408.40	877	608	99	114
59447	Istanbuldc Veri Merkezi Ltd Sti (TR)	334.79	2964	1857	126	470
398478	PEG TECH Inc (US)	333.31	992	9	172	158
135097	LUOGELANG (FRANCE) LIMITED (HK)	318.87	919	6	93	153
398823	PEG TECH Inc (US)	186.21	6559	55	1853	1870
132827	GATEWAY INC (JP)	182.57	141	347	1608	41

## Spam

As in the malware category, the top signal strengths for spam domains were more modest in this edition of the report than in the previous. This Top 10 list had more turnover than the others we've examined thus far, with only one AS (23881, UDomain Web Hosting Company Ltd (HK) repeating.

May 2022		Signal Strength	Spam	Phishing	Malware	Neutral
45382	EHOSTIDC-AS-KR EHOSTICT (KR)	779.43	1,409	17	142	163
23881	UDomain Web Hosting Company Ltd (HK)	296.10	4,824	14	2,617	1,469
17941	BIT-ISLE Equinix Japan Enterprise K.K. (JP)	197.33	2,357	0	1,110	1,077
32097	WII (US)	146.76	3,130	581	571	1,923
9919	New Century InfoComm Tech Co. Ltd. (TW)	131.88	3,402	15	247	2,326
62904	AS62904 (US)	101.40	5,148	2,525	4,424	4,578
46573	LAYER-HOST (US)	98.80	2,679	453	7,596	2,445
398823	PEG TECH Inc (US)	97.99	2,506	715	17,898	2,306
397423	TIER-NET (US)	96.71	3,283	143	324	3,061
137951	Clayer Ltd (HK)	79.87	5,390	1,470	18,805	6,085

Nov 2021		Signal Strength	Spam	Phishing	Malware	Neutral
136574	Shanghai Zheye Network Technology Co.Ltd (CN)	9,585.49	1230	13	573	9
18046	DongFong Technology Co. Ltd. (TW)	7,947.24	6232	0	15	55
24295	Internap Japan Co., Ltd. (JP)	7,193.01	923	254	394	9
132827	GATEWAY INC (JP)	2,750.77	1608	347	141	41
9311	HITRON TECHNOLOGY INC (TW)	1,955.94	3458	78	42	124
16578	Lanset America Corporation (US)	1,238.82	1466	16	64	83
208006	Softqloud GmbH (DE)	805.31	1263	82	278	110
209371	Cenk Aksit (TR)	567.22	1019	45	162	126
23881	UDomain Web Hosting Company Ltd (HK)	552.70	15193	8	844	1928
211390	Cloud Solutions Ltd (RU)	412.63	453	808	91	77

## Nameserver ASNs

At a glance, these will look similar to the previous category, but in this case, we're looking at the AS associated with the **nameserver** IPs for the domains, rather than the hosting IPs. Sometimes registrants use nameservers 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 nameservers.

### Phishing

The top signal strengths among Nameserver ASNs for phishing domains are in the same ballpark as the phishing domains for IP ASNs. AS 39845 sports over 2,000 phishing domains, against just two neutral (and just about a

third of the domains associated with that nameserver AS are spam). The signal strength of this AS, over 30,000, is also dramatically higher than the top signal strength for this category and threat type in the last edition of the report. As you will read below, however, this pattern does not hold for malware or spam. There were three ASNs that repeated in this list compared to the previous (ASNs 200313, 44592, and 57724).

May 2022		Signal Strength	Phishing	Malware	Spam	Neutral
39845	LV-2CLOUD (LV)	31,033.54	2,075	18	1105	2
140947	SnTHostings (IN)	6,586.59	2,202	32	62	10
212913	TIMEHOST-AS (RU)	1,017.79	1,293	69	117	38
<b>200313</b>	<b>INTERNET IT COMPANY (SC)</b>	<b>923.53</b>	1,235	108	440	40
18049	Taiwan Infrastructure Network Technologie (TW)	247.08	1,016	196	6	123
<b>44592</b>	<b>SkyLink Data Center BV (NL)</b>	<b>40.53</b>	1,286	555	162	949
54990	AS-1337 (KN)	32.12	1,265	910	44	1,178
39287	ABSTRACT (FI)	29.75	1,267	912	44	1,274
<b>57724</b>	<b>DDoS-Guard Ltd (RU)</b>	<b>15.98</b>	1,169	353	904	2,188
38283	SiChuan Telecom Internet Data Center (CN)	14.70	9,056	19,490	3,057	18,422

Nov 2021		Signal Strength	Phishing	Malware	Spam	Neutral
24295	Internap Japan Co.,Ltd. (JP)	897.09	283	346	827	23
200313	INTERNET IT COMPANY (SC)	449.97	611	124	1187	99
44592	SkyLink Data Center BV (NL)	393.88	1799	322	737	333
30860	Virtual Systems LLC (UA)	134.23	637	90	684	346
395839	HOSTKEY (US)	109.36	6	105	7155	4
17623	China Unicom Shenzhen network (CN)	66.02	5373	4114	1021	5934
57724	DDoS-Guard Ltd (RU)	49.53	2188	309	1124	3221
43317	FISHNET COMMUNICATIONS LLC (RU)	37.33	831	58	308	1623
140227	Hong Kong Communications International Co., Limited (HK)	36.08	145	140	770	293
133199	SonderCloud Limited (HK)	34.66	145	136	772	305

## Malware

The signal strengths associated with malware domains among nameserver ASNs are much more modest than those in the phishing and spam threat types in this category. It is worth noting that there are more than two orders of magnitude difference in numbers of malware domains for the different ASNs, with the largest having nearly a half-million domains and the smallest having fewer than 2,000. Four of the ASNs are repeaters from our last report.

May 2022		Signal Strength	Malware	Phishing	Spam	Neutral
134762	CHINANET Liaoning province Dalian MAN network (CN)	213.08	3,762	62	4098	205
139201	CHINANET Jiangxi Jiujiang IDC (CN)	174.19	18,107	630	2093	1,207
21859	Zenlayer Inc (US)	43.29	498,708	29,551	29,955	133,779
134543	China Unicom Guangdong IP network (CN)	28.67	254,590	19,100	25,641	103,126
60592	Gransy s.r.o. Gransy.com (CZ)	22.72	4,668	214	1,201	2,386
9808	China Mobile Communication Co.Ltd. (CN)	19.55	287,285	21,783	31,934	170,635
58519	CHINATELECOM Cloud Computing Corp (CN)	17.05	1,714	120	42	1,167
4837	CHINA UNICOM China169 Backbone (CN)	14.78	63,733	11,786	3,670	50,081
7979	SERVERS-COM (US)	13.13	5,150	640	837	4,554
40824	WZCOM (US)	12.36	1,804	118	51	1,695

Nov 2021		Signal Strength	Malware	Phishing	Spam	Neutral
395839	HOSTKEY (US)	855.24	105	6	7,155	4
24295	Internap Japan Co.,Ltd. (JP)	490.12	346	283	827	23
200313	INTERNET IT COMPANY (SC)	40.81	124	611	1,187	99
44592	SkyLink Data Center BV (NL)	31.50	322	1,799	737	333
40065	CNSERVERS LLC (US)	30.42	4,158	85	244	4,453
17623	China Unicom Shenzen network (CN)	22.59	4,114	5,373	1,021	5,934
134543	China Unicom Guangdong IP network (CN)	21.27	155,133	13,159	68,638	237,662
21859	Zenlayer Inc (US)	20.81	172,624	14,648	80,632	270,254
4837	CHINA UNICOM China169 Backbone (CN)	16.16	168,034	16,602	74,860	338,780
9808	China Mobile Communication Co.Ltd. (CN)	15.60	177,030	16,117	88,604	369,803

## Spam

The top signal strength for spam, at nearly 28,000, looks very high until we compare it with the #1 spot in our last edition, which had a signal strength of over 90,000. As you will anticipate by this point without even looking at the table, the nameserver ASNs in these top positions have very low overall numbers of domains, with the top spot in this edition having only 1,105 domains (vs 7,155 domains for the #1 slot in the previous edition). Among nameserver ASNs, we don't see nearly as many high domain counts as we did in the malware category; the largest set of spam domains (AS 134762) was 4,098, versus that half-million we saw for malware). Three of these ASNs also appeared in the prior edition.

May 2022		Signal	Spam	Phishing	Malware	Neutral
39845	LV-2CLOUD (LV)	27,922.07	1,105	2,075	18	2
137443	Anchnet Asia Limited (HK)	9,176.20	1,271	9	228	7
<b>57043</b>	<b>HOSTKEY B.V. (NL)</b>	<b>2,481.03</b>	2,651	30	76	54
57344	TELEHOUSE (BG)	2,376.67	1,693	0	6	36
134762	CHINANET Liaoning province Dalian MAN network (CN)	1,010.26	4,098	62	3,762	205
<b>44901</b>	<b>BELCLOUD (BG)</b>	<b>766.13</b>	2,471	28	134	163
135377	UCCLOUD INFORMATION TECHNOLOGY HK LIMITED (HK)	222.85	4,467	63	605	1,013
<b>4686</b>	<b>BEKKOAME BEKKOAME INTERNET INC. (JP)</b>	<b>182.34</b>	1,519	9	114	421
58466	CHINANET Guangdong province network (CN)	117.32	4,492	184	784	1,935
12586	ASGHOSTNET (DE)	98.61	3,165	58	146	1,622

Nov 2021		Signal	Spam	Phishing	Malware	Neutral
395839	HOSTKEY (US)	90,200.93	7,155	283	346	4
327790	Wirels Connect (PTY) (ZA)	5,166.45	1,127	611	124	11
24295	Internap Japan Co.,Ltd. (JP)	1,813.17	827	1,799	322	23
18068	Dream Wave Shizuoka Co. Ltd. (JP)	1,103.34	4,923	637	90	225
57043	HOSTKEY B.V. (NL)	1,063.89	3,671	6	105	174
200313	INTERNET IT COMPANY (SC)	604.61	1,187	5,373	4,114	99
44901	BELCLOUD (BG)	316.19	3,806	2,188	309	607
4686	BEKKOAME BEKKOAME INTERNET INC. (JP)	292.90	3,909	831	58	673
61272	IST-AS (LT)	220.85	3,749	145	140	856
134771	CHINATELECOM-ZHEJIANG-WENZHOU-IDC (CN)	189.63	1,775	145	136	472

## IP Geolocation

This category examines hotspots of malicious activity by the country code of the IP address hosting the domains in question. Consistent with the Q4 2021 snapshot, **this category showed much milder spreads in signal strength**, compared with other features such as IP and nameserver ASN. But the big surprise this time around is that, for the first time since we have studied these concentrations of badness, for one of the threat types (malware) **we did not find 10 regions with positive signal strengths**, which means that the last four regions on the malware list show a stronger signal toward neutrality than toward malware. This is similar to our findings with SSL certificate issuers, but was a surprise to see in this feature. As we noted in the previous edition, IP hosting region is not generally a strong indicator of maliciousness anyway. Still, in an incident response scenario, a traffic flow to a specific hosting location may have significance in the context of that particular connection, if the location does not make sense for other aspects of the connection in question.

### Phishing

Only two of the hosting regions in the phishing category are repeaters from the previous report: Luxembourg and Hong Kong. Why so much turnover? This is the category in which our methodology change had the greatest effect. As a reminder, for this edition, to be a candidate for the top 10 list, the region had to contain at least 1,000 domains of the threat type under examination. In our previous report, the top 10 list included regions with as few as 59 domains—but they were included on the basis of signal strength. This time around, the region with the fewest phishing domains (Ukraine) has 1,215. Unsurprisingly, with this change of thresholding, the range of signal strengths is narrower, topping out at 32.30 compared to 76.86 in the prior edition. As you will see later, this heavy turnover in the top 10 population holds true in the malware and spam categories as well.

May 2022	Signal Strength	Phishing	Malware	Spam	Neutral
<b>LU (Luxembourg)</b>	<b>32.30</b>	3,461	3,493	137	4840
VN (Vietnam)	18.32	4,591	500	264	11,320
AE (United Arab Emirates)	4.64	2,842	2,134	979	27,649
<b>HK (Hong Kong)</b>	<b>4.59</b>	2,625	11,714	4,774	25,807
NL (Netherlands)	4.21	21,410	9,455	4,479	229,475
RU (Russia)	3.95	12,875	5,532	3,810	147,053
IN (India)	3.34	1,962	1,078	1,154	26,531
BR (Brazil)	2.40	4,638	3,497	864	87,198
UA (Ukraine)	1.90	1,215	603	1,872	28,865
SG (Singapore)	1.43	2,212	2,714	460	70,038



Nov 2021	Signal Strength	Phishing	Malware	Spam	Neutral
SC (Seychelles)	76.86	617	285	80	612
BZ (Belize)	54.15	2780	167	263	3914
PA (Panama)	23.20	399	95	132	1311
KH (Cambodia)	14.77	105	17	50	542
HK (Hong Kong)	7.52	21627	133,780	77807	219340
LU (Luxembourg)	5.41	990	1093	796	13962
BE (Belgium)	4.38	8156	1616	543	141805
MU (Mauritius)	4.24	59	1496	356	1061
MD (Moldova)	4.15	325	364	1661	5965
NG (Nigeria)	3.93	77	33	9	1495

## Malware

We won't bury the lede: for the first time in any domain feature other than SSL certificate issuers, we saw several ASNs which actually showed a relative **underrepresentation** of malware domains—and remember, these are in the top 10—so all of the other hosting regions around the world that had at least 1,000 malware domains were even less likely, statistically, to host malware. These regions are noted with the green signal strength color.

Like the phishing category, for malware we saw only three repeat regions compared to the last report: Luxembourg, Hong Kong, and China. For Hong Kong, the number of malware domains we observed was less than one-tenth of the number seen last time (11k vs nearly 134k). Because Hong Kong repeated, our inclusion criterion of at least 1,000 malware domains per AS does not explain the change in numbers. It is possible that some of the inputs, in terms of how domains landed on the blocklists we consulted, could have changed.

May 2022	Signal Strength	Malware	Phishing	Spam	Neutral
LU (Luxembourg)	16.79	3,493	3,461	137	4,840
HK (Hong Kong)	10.56	11,714	2,625	4,774	2,5807
KR (South Korea)	8.62	4,311	636	206	11,636
CN (China)	4.25	4,432	708	303	24,284
AE (United Arab Emirates)	1.80	2,134	2,842	979	27,649
CZ (Czech Republic)	1.05	4,394	355	1,295	97,305
NL (Netherlands)	0.96	9,455	21,410	4,479	229,475
IN (India)	0.95	1,078	1,962	1,154	26,531
BR (Brazil)	0.93	3,497	4,638	864	87,198
SG (Singapore)	0.90	2,714	2,212	460	70,038

Nov 2021	Signal Strength	Malware	Phishing	Spam	Neutral
MU (Mauritius)	73.60	1496	59	356	1061
HK (Hong Kong)	31.84	133780	21627	77807	219340
SC (Seychelles)	24.31	285	617	80	612
MN (Mongolia)	14.72	470	16	927	1667
LU (Luxembourg)	4.09	1093	990	796	13962
PA (Panama)	3.78	95	399	132	1311
CN (China)	3.37	13119	3329	3016	203108
MD (Moldova)	3.19	364	325	1661	5965
PH (Philippines)	2.52	193	17	2571	3998
BZ (Belize)	2.23	167	2780	263	3914

## Spam

Only one region, Hong Kong, repeated in this top 10 list compared to the last edition. The ranges of signal strengths we observed were generally comparable, but were lower across the board than last time around. But our thresholding change is part of this story, since fully half of the top 10 regions from the prior report had fewer than 1,000 spam domains.

May 2022	Signal Strength	Spam	Phishing	Malware	Neutral
IE (Ireland)	20.11	3,758	480	376	17,784
<b>HK (Hong Kong)</b>	17.61	4,774	2,625	11,714	25,807
JP (Japan)	13.23	10,510	413	2,299	75,598
UA (Ukraine)	6.17	1,872	1,215	603	28,865
TR (Turkey)	4.77	2,552	1,259	1,403	50,912
IN (India)	4.14	1,154	1,962	1,078	26,531
RU (Russia)	2.47	3,810	12,875	5,532	147,053
NL (Netherlands)	1.86	4,479	21,410	9,455	229,475
CZ (Czech Republic)	1.27	1,295	355	4,394	97,305
DE (Germany)	1.10	7,061	13,145	7,453	610,734

Nov 2021	Signal Strength	Spam	Phishing	Malware	Neutral
PH (Philippines)	46.94	2571	17	193	612
MN (Mongolia)	40.59	927	16	470	3914
HK (Hong Kong)	25.89	77807	21627	133780	1311
MU (Mauritius)	24.49	356	59	1496	542
MD (Moldova)	20.33	1661	325	364	219340
TW (Taiwan)	9.97	6592	300	667	13962
SC (Seychelles)	9.54	80	617	285	141805
PA (Panama)	7.35	132	399	95	1061
KH (Cambodia)	6.73	50	105	17	5965
KR (South Korea)	6.71	6673	2122	2729	1495

## 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

Five of the registrars with the highest signal strengths for phishing are repeaters from the last report. The range of signal strengths for phishing is also relatively comparable to the last report; overall, in the phishing category, our inclusion threshold change did not seem to have a large effect. In fact, only two of the top 10 from the Q4 2021 report had fewer than 1,000 domains, so under our current criteria most of the registrars would have been candidates for inclusion.

In absolute numbers, NameSilo leads with more than 138,000 phishing domains observed in this snapshot. This is a substantial, but not inordinate, increase from our last snapshot, when there were a little under 77,000.

May 2022	Signal Strength	Phishing	Malware	Spam	Neutral
NICENIC INTERNATIONAL GROUP CO., LIMITED	84.73	2,096	2,647	466	488
Eranet International Limited	67.22	5,197	8,883	4,436	1,525
ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	50.60	26,499	25,823	1,646	10,330
West263 International Limited	36.42	7,328	56,620	1,165	3,969
OwnRegistrar, Inc.	35.15	5,414	5,208	1,927	3,038
NameSilo, LLC	28.16	138,236	137,930	14,383	96,837
Beget LLC	21.31	1,610	859	143	1,490
Chengdu West Dimension Digital Technology Co., Ltd.	19.95	15,555	31,617	1,057	15,381
DNSPod, Inc.	17.93	8,925	19,502	696	9,818
Sav.com, LLC	16.62	19,662	18,142	6,057	23,336

Nov 2021	Signal Strength	Phishing	Malware	Spam	Neutral
Eranet International Limited	70.49	3534	6976	3027	2038
NICENIC INTERNATIONAL GROUP CO., LIMITED	51.92	1041	2253	212	815
ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	40.33	30366	41637	5343	30608
Squarespace Domains LLC	21.63	1899	416	3	3569
Shinjiru Technology Sdn Bhd	15.59	1050	137	140	2737
NameSilo, LLC	12.04	76846	96161	21443	259336
CNOBIN INFORMATION TECHNOLOGY LIMITED	11.40	382	363	585	1362
Beget LLC	11.29	1049	1010	90	3776
Registrar of Domain Names REG.RU LLC	10.25	15649	10317	2263	62085
DOMAINNAME BLVD, INC.	9.44	49	1099	73	211

## Malware

Only one registrar, Global Domain Name Trading Center Ltd, repeats from the last report on this top 10 list. If a number of the registrars in this top 10 list look curiously similar, that is no coincidence. A larger company called "17Domain," based in Hong Kong, has a number of subsidiary registrars that each have their own [IANA registrar IDs](#). So it is indeed the case that a single overall entity represents fully half of the registrar top 10 list for malware. In general, the numbers of malware domains associated with individual registrars are comparatively low, at least for those with high signal strengths. There are certainly other, well-known registrars, with many more malware

domains, but because they also have high numbers of neutral domains, they do not register highly on the basis of signal strength.

May 2022	Signal Strength	Malware	Spam	Phishing	Neutral
Crystal Coal, LLC	2,225.65	1,364	22	3	4
Guangzhou Yunxun Information Technology Co., Ltd.	21.34	1,115	0	12	24
17 Domain 2, Limited	41.35	1,321	0	8	33
17 Domain 4, Limited	39.40	1,236	2	12	35
17 Domain 3, Limited	39.76	1,203	0	5	38
17 Domain 1, Limited	37.62	1,271	1	7	44
17 Domain Limited	38.98	1,320	0	12	49
<b>Global Domain Name Trading Center Ltd</b>	<b>28.07</b>	12,491	1,623	204	478
Gname 004 Inc	43.84	1,196	0	17	46
Gname 006 Inc	41.55	1,133	1	18	45

Nov 2021	Signal Strength	Malware	Spam	Phishing	Neutral
Tname Group Inc.	929.93	1522	0	0	45
Global Domain Name Trading Center Ltd	331.07	4672	1167	56	388
DOMAINNAME BLVD, INC.	143.21	1099	73	49	211
DomainName Highway LLC	119.36	1832	19	75	422
FLAPPY DOMAIN, INC.	114.91	1747	86	61	418
DOMAINNAME FWY, INC.	111.57	909	48	44	224
DotMedia Limited	102.30	1053	57	57	283
DomainName Path, Inc.	99.61	1826	86	71	504
Xiamen Domains, Inc.	99.30	1600	68	78	443
Domain International Services Limited	97.81	9480	387	181	2665

## Spam

While there are a lot of spam domains on the Internet—as any email user can attest—there are not many registrars that stand out as strongly associated with spam, especially in terms of a combination of signal strength and numbers. For the second Report running, **Global Domain Name Trading Center Ltd** shows a strong (for the category) signal, but as before, has a relatively low number (1,623) of Spam domains associated with it. Also similar to the last Report, **GMO Internet, Inc. d/b/a Onamae.com** has a large number of Spam domains associated

with it, albeit substantially fewer than last time (91k in Spring 2022 vs 150k in Fall 2021). Five of the registrars in this top 10 list were also in the Fall 2021 list for this category.

May 2022	Signal Strength	Spam	Phishing	Malware	Neutral
Global Domain Name Trading Center Ltd	161.91	1,623	204	12,491	478
Eranet International Limited	138.71	4,436	5,197	8,883	1,525
CNOBIN INFORMATION TECHNOLOGY LIMITED	58.20	2,004	1,149	13,228	1,642
MAT BAO CORPORATION	43.97	4,402	905	5,968	4,774
OwnRegistrar, Inc.	30.25	1,927	5,414	5,208	3,038
Domain International Services Limited	24.08	1,034	724	38,766	2,048
GMO Internet, Inc. d/b/a Onamae.com	23.77	91,446	6,128	118,359	183,444
Hongkong Domain Name Information Management Co., Ltd.	22.07	1,353	719	15,363	2,924
Jiangsu Bangning Science & Technology Co. Ltd.	18.61	2,262	1,603	9,741	5,797
West263 International Limited	14.00	1,165	7,328	56,620	3,969

Nov 21	Signal Strength	Spam	Phishing	Malware	Neutral
Global Domain Name Trading Center Ltd	158.18	1167	56	4672	388
Hongkong Domain Name Information Management Co., Ltd.	106.29	8153	239	5663	4034
Eranet International Limited	78.11	3027	3534	6976	2038
Hong Kong Juming Network Technology Co., Ltd	43.27	4759	303	5652	5784
Gname.com Pte. Ltd.	22.77	3136	251	1865	7242
CNOBIN INFORMATION TECHNOLOGY LIMITED	22.59	585	382	363	1362
Zhengzhou Century Connect Electronic Technology Development Co., Ltd	22.39	487	16	552	1144
Cloud Yuqu LLC	20.32	1906	561	2973	4934
GMO Internet, Inc. d/b/a Onamae.com	19.86	149964	8182	71635	397130
DOMAINNAME BLVD, INC.	18.19	73	49	1099	211

## SSL Certificate Authorities

For the second time in DomainTools Report history, we have explored a **category 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. 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 certificate authorities (CAs) associated with domains, however, fewer than ten had a positive correlation with maliciousness for any of the threat types. In Phishing and Spam, fully half of the CAs were more associated with good domains than bad, and in Malware, four of the ten also had sub-1.00 signals.

That a big and popular CA such as GoDaddy had a “green” signal may not have been especially surprising, but one of the CAs most often pilloried for associations with malicious domains—**Let’s Encrypt**—actually had *positive* signals in every threat type, **except where it didn’t**. Each of the Top 10 tables in this section for the May 2022 data snapshot actually has **two** entries for Let’s Encrypt—one with the CN E1, and one with the CN R3. E1 refers to a relatively new certificate type, using a different cryptographic algorithm. There are not nearly as many of these certificates in circulation as the previously existing R3 type, but they are associated with enough malicious activity that **the Let’s Encrypt E1 certificates topped our lists for each threat type**. (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 early adopters of the new certificate type.) The more common R3 certificates correlated slightly with more neutral domains, as they did in the previous report. E1 certificates are going to become more common over time, so it will be worth watching what happens with concentrations of malicious domains using these certificates.

Almost as surprising were the results for the “non-CA”: **self-signed certificates**, which showed a weak signal of 5.36 for Spam, but had a perfectly neutral 1.00 for Phishing and a barely-registering malicious signal of 1.09 for Malware. So, as we saw earlier, a given data point for a domain—in this case, a self-signed certificate or the older R3 type from Let’s Encrypt—does not have the forensic significance, in and of itself, that many practitioners might assume it does.

Having said this, it is very important to note that **such certificates can, in certain contexts, absolutely be a signal of maliciousness**: consider a domain that spoofs a well-known brand or resource with a look-alike domain name. If this domain has a self-signed or any “flavor” of Let’s Encrypt certificate, then within this specific context, the certificate absolutely *does* take on an incriminating aspect.

Compared to all of the other domain features, SSL issuer had remarkable consistency report-over-report in the top 10 issuers for signal strength across all three threat types. 9 of the top 10 were the same in each threat category; also of interest, the newcomer to each list was the same for all three threat types: Sectigo. Within the

top 10, the different issuers moved up and down compared to Q4 2021; it was their presence in the top 10 that was unchanged.

## Phishing

Because the issuers with better-than-neutral signal strengths are such an important part of the story, we will note that for the May 2022 snapshot, there were three issuers of this description, as opposed to five in the previous edition. Still, the signal strengths are generally low. The self-signed certificate, which is often associated with malicious domains, is indeed overrepresented in phishing domains compared to neutral domains—but just barely. As we will see in all three threat categories, in Phishing, the top place goes to the Let’s Encrypt E1 certificate type. Also holding true across all three is that the more familiar Let’s Encrypt R3 certificates have a (very) mildly non-malicious signal.

May 2022	Signal Strength	Phishing	Malware	Spam	Neutral
CN=E1,O=Let's Encrypt,C=US	20.79	28,391	23,598	4,304	110,161
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	6.11	51,804	47,160	8,438	683,524
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	2.99	1,117	1,076	145	30,159
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	1.38	11,697	7,257	4,481	685,501
CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com,O=DigiCert Inc,C=US	1.33	3,033	2,613	91	184,490
CN=GTS CA 1D4,O=Google Trust Services LLC,C=US	1.28	828	1,128	551	52,067
Self-signed	1.07	789	821	428	59,649
CN=Amazon,OU=Server CA 1B,O=Amazon,C=US	0.64	806	970	72	100,915
CN=R3,O=Let's Encrypt,C=US	0.61	47,086	62,459	15,372	6,250,250
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	0.16	7,030	5,245	277	3,510,866



Nov 2021

	Signal Strength	Phishing	Malware	Spam	Neutral
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	5.72	600	918	332	20,014
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	5.47	25,611	28,745	16,380	893,104
CN=TrustAsia TLS RSA CA,OU=Domain Validated SSL,O=TrustAsia Technologies\, Inc.,C=CN	3.36	196	892	3,036	11,127
CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com,O=DigiCert Inc,C=US	1.41	2,215	1,938	779	298,816
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	1.02	8,308	6,063	2,785	1,557,273
Self-signed	1.00	597	708	1,801	114,094
CN=GTS CA 1D4,O=Google Trust Services LLC,C=US	0.91	278	659	329	58,261
CN=R3,O=Let's Encrypt,C=US	0.87	38,478	43,783	20,363	8,462,729
CN=Amazon,OU=Server CA 1B,O=Amazon,C=US	0.56	319	675	158	108,360
CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=Arizona,C=US	0.31	493	777	27	301,303

## Malware

Whereas for phishing domains, we saw a decrease in the number of “green” certificate issuers compared to our last report, for malware it was the opposite: five “green” issuers this time vs three in Q4 2021. Having said this, in Q4 2021, the issuers in the #6 and #7 slots were just barely above neutral, at strengths of 1.09 for both. So the movement is quite minor. Amazon and Let’s Encrypt R3 both moved into the “green” category this time around (whereas Let’s Encrypt E1 is in first place). Compared to other signal strengths we have seen, 17.12 is quite modest, but it qualifies as a slight signal of potential risk.

May 2022

	Signal Strength	Malware	Spam	Phishing	Neutral
CN=E1,O=Let's Encrypt,C=US	17.12	23,598	4,304	28,391	110,161
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	5.52	47,160	8,438	51,804	683,524
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	2.85	1,076	145	1,117	30,159
CN=GTS CA 1D4,O=Google Trust Services LLC,C=US	1.73	1,128	551	828	52,067
CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com,O=DigiCert Inc,C=US	1.13	2,613	91	3,033	184,490
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.85	7,257	4,481	11,697	685,501
CN=R3,O=Let's Encrypt,C=US	0.80	62,459	15,372	47,086	6,250,250
CN=Amazon,OU=Server CA 1B,O=Amazon,C=US	0.77	970	72	806	100,915
CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=Arizona,C=US	0.42	1,096	12	588	206,443
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	0.12	5,245	277	7,030	3,510,866

Nov 2021

	Signal Strength	Malware	Spam	Phishing	Neutral
CN=TrustAsia TLS RSA CA,OU=Domain Validated SSL,O=TrustAsia Technologies\, Inc.,C=CN	14.05	892	3,036	196	11,127
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	8.04	918	332	600	20,014
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	5.64	28,745	16,380	25,611	893,104
CN=GTS CA 1D4,O=Google Trust Services LLC,C=US	1.98	659	329	278	58,261
CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com,O=DigiCert Inc,C=US	1.14	1,938	779	2,215	298,816
CN=Amazon,OU=Server CA 1B,O=Amazon,C=US	1.09	675	158	319	108,360
Self-signed	1.09	708	1,801	597	114,094
CN=R3,O=Let's Encrypt,C=US	0.91	43,783	20,363	38,478	8,462,729
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.68	6,063	2,785	8,308	1,557,273
CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=Arizona,C=US	0.45	777	27	493	301,303

## Spam

Overall, there were four weaker-than-neutral (i.e. “green”) signals for spam in the top 10 for this snapshot, compared to five in the previous. As with the other two threat categories, Sectigo and Let’s Encrypt E1 were the newcomers to this list, though Sectigo’s signal strength is the lowest we have seen in any of our top 10 lists, at 0.03. With 277 spam domains compared to over 3.5 million neutral, it is safe to say that, statistically speaking, a domain with a Sectigo certificate is likely to be relatively safe to visit (or, in this case, to receive email from).

May 2022	Signal Strength	Spam	Phishing	Malware	Neutral
CN=E1,O=Let's Encrypt,C=US	14.20	4,304	28,391	23,598	110,161
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	4.49	8,438	51,804	47,160	683,524
CN=GTS CA 1D4,O=Google Trust Services LLC,C=US	3.85	551	828	1,128	52,067
Self-signed	2.61	428	789	821	59,649
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	2.38	4,481	11,697	7,257	685,501
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	1.75	145	1,117	1,076	30,159
CN=R3,O=Let's Encrypt,C=US	0.89	15,372	47,086	62,459	6,250,250
CN=Amazon,OU=Server CA 1B,O=Amazon,C=US	0.26	72	806	970	100,915
CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com,O=DigiCert Inc,C=US	0.18	91	3,033	2,613	184,490
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	0.03	277	7,030	5,245	3,510,866

Nov 2021	Signal Strength	Spam	Phishing	Malware	Neutral
CN=TrustAsia TLS RSA CA,OU=Domain Validated SSL,O=TrustAsia Technologies\, Inc.,C=CN	92.71	3,036	196	892	11,127
CN=Cloudflare Inc ECC CA-3,O=Cloudflare\, Inc.,C=US	6.23	16,380	25,611	28,745	893,104
CN=ZeroSSL RSA Domain Secure Site CA,O=ZeroSSL,C=AT	5.64	332	600	918	20,014
Self-signed	5.36	1,801	597	708	114,094
CN=GTS CA 1D4,O=Google Trust Services LLC,C=US	1.92	329	278	659	58,261
CN=Encryption Everywhere DV TLS CA - G1,OU=www.digicert.com,O=DigiCert Inc,C=US	0.89	779	2,215	1,938	298,816
CN=R3,O=Let's Encrypt,C=US	0.82	20,363	38,478	43,783	8,462,729
CN=cPanel\, Inc. Certification Authority,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.61	2,785	8,308	6,063	1,557,273
CN=Amazon,OU=Server CA 1B,O=Amazon,C=US	0.50	158	319	675	108,360
CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=Arizona,C=US	0.03	27	493	777	301,303

## Conclusion

This is the second consecutive iteration of the DomainTools Report in what we plan to be an ongoing rhythm of semiannual snapshots. Over time, we intend to glean trending information about the evolving nature of concentrations of malicious activity across the Internet. At the same time, as our change in thresholding methodology demonstrates, we may continue to make small adjustments in order to give what we judge to be the most useful insights.

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 a big 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.