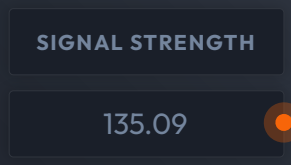
DomainTools

The DomainTools Report

Patterns of Malicious Infrastructure

Spring 2023



Introduction

Welcome to the Spring 2023 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 350 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 (of course, that doesn't mean that any given SOC couldn't have an encounter with a domain from one of those hotspots).

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).

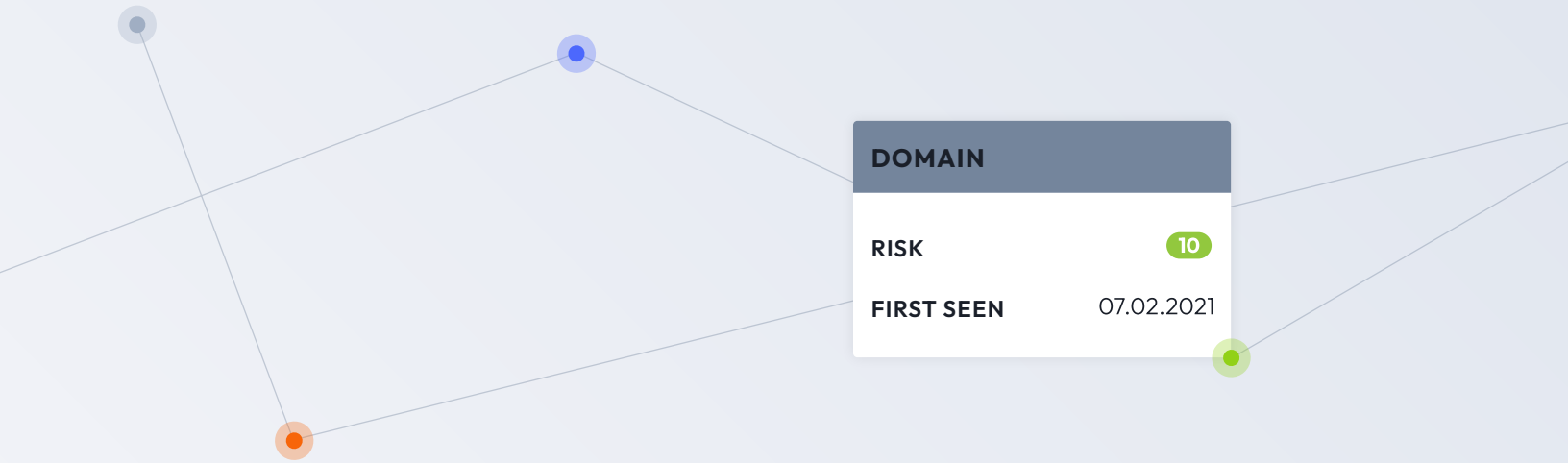
Signal Strength

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.

Snapshot in Time

For our calculations, **we took a snapshot of the domains in existence and active as of late March, 2023.**

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.



Interpreting the Data

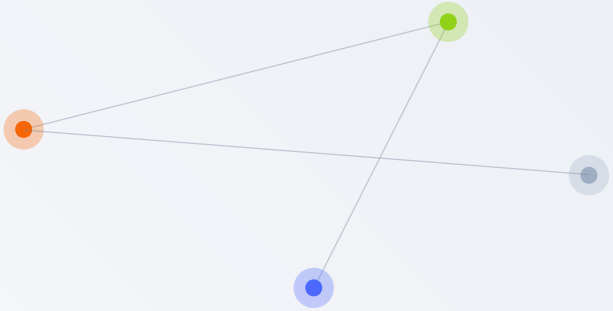
In each of the following six sections, we show "Top-Ten" tables, sorted by the signal strength, for each of the three threat types (phishing, malware, spam). Each table also includes the actual counts of domains associated with the item. As an example, consider this row of data from the TLD section:

	Signal Strength	Malware	Phishing	Spam	Neutral
.cyou	**135.09**	21,683	18,834	409	18,834

The TLD ***.cyou*** has a malware signal strength of **135.09**, and there are 21,683 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 Q4 of 2021 are shown in **bold**. In the example above, the .cyou TLD is not in bold because it wasn't 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 (IP Geolocation, for spam domains).**

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, many 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 (.tk, .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. Speaking of .ga—along with .gq, those two TLDs were represented in each of the three Top 10 lists this time around.

A development that preceded this report (but not by long enough to make much of a difference in the statistics) may have an impact on the next edition: Freenom, the domain registrar behind some of the TLDs in these lists including .ga, .gq, .tk, .ml, and .cf, shut down its registrations after being sued by Meta. Stay tuned for the next edition to find out what the impact might be on these numbers.

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, .cyou, .top, .monster, and .live were all in the previous Top 10 list for phishing. The highest signal strength, 102.49 for the .cyou TLD, is modestly below 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 .cyou, with over 35,000 domains this time versus just under 10,000 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 many of the TLDs.

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

November 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

Well, we didn't expect to .cyou again so soon! (Sorry, not sorry.) This TLD has topped both the Phishing and Malware lists this time around, clocking in with over 21,000 malware domains (and it was not even in the Malware top 10 last time). Absolute numbers in this category are interesting: notably, while .xyz has repeated in the top 10 for malware by signal strength, the absolute numbers of malware domains in that TLD have dropped greatly, from over 207,000 last time to 32,687 in this snapshot. Elsewhere across the Malware scoreboard, there were three repeat appearances: the TLDs .top, .icu, and .xyz. The range of signal strengths in the top 10 was similar to last time, topping out at 135.09 (vs 108.93) and flooring at 15.06 (vs 19.33).

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

November 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

This Top 10 list had 100% turnover from last time—not one of the Top 10 TLDs for Spam appeared on the November 2021 list. The dynamics are somewhat different, as well, with a significantly larger range of signal strengths (692.36/24.15 this time vs 217.97/12.87 last time). As in the other two Top 10 lists, .ga and .gq are first-timers on this list, with a few tens of thousands of spam domains in each of those TLDs.

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

November 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 102.49, the highest among IP ASNs is 33,632.73—an over 300x increase! The spread at the bottom of the chart (10th position) is not as great: 111.81 in IP ASN vs 26.87 in TLDs. (The massive signal strength for 133955 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 133955 has such an astronomical signal strength: while it does not have a huge overall number of phishing domains (1,404), it has but **3** domains showing as neutral. This means that, to put it mildly, one would be well advised to treat any traffic from this AS as potentially suspicious. Nor is this a new phenomenon, at least compared with our last report in the fall of 2021: Nice IT Services (AS 49447) topped out that list, with a substantially lower—but still immensely high—signal strength of 8047.06. Overall, this category had 90% turnover, with only AS 59447 repeating in the Top 10.

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

November 2021	Signal Strength	Phishing	Malware	Spam	Neutral
Nice IT Services Group Inc (DM)	**8,047.06**	1,572	131	46	15
Internap Japan Co., Ltd. (JP)	**2,167.04**	254	394	923	9
Cloud Solutions Ltd (RU)	**805.74**	808	91	453	77
GATEWAY INC (JP)	**649.86**	347	141	1,608	41
Packet Exchange, LTD (SE)	**621.96**	1,134	1,354	421	140
Orion Network Limited (SE)	**409.52**	608	877	99	114
DDOS-GUARD CORP (BZ)	**404.55**	2,550	90	147	484
Istanbuldc Veri Merkezi Ltd Sti (TR)	**303.38**	1,857	2,964	126	470
Fast Content Delivery LTD (SC)	**290.33**	2,314	726	294	612
INTERNET IT COMPANY (SC)	**180.91**	589	185	447	250

Malware

This Top 10 list had 100% turnover since the November 2021 snapshot. The top signal strengths among IP ASNs for malware were dramatically more modest than for phishing (3,769.73 for malware vs 33,632.73 for phishing), though at 10th position, they were much closer (19.86 for malware vs 111.81 for phishing). In general, in this category the counts of malicious domains are low, but the third-, sixth-, and tenth-place finishers all sported tens of thousands of domains. Given the signal strengths, traffic from the protected environment to any of these AS, with the possible exception of 206834, should be considered suspicious.

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

November 2021	Signal Strength	Malware	Phishing	Spam	Neutral
Shanghai Zheye Network Technology Co.Ltd (CN)	**3,379.93**	573	13	1230	9
Internap Japan Co., Ltd. (JP)	**2,324.07**	394	254	923	9
Packet Exchange, LTD (SE)	**513.44**	1354	1134	421	140
Nice IT Services Group Inc (DM)	**463.63**	131	1572	46	15
Orion Network Limited (SE)	**408.40**	877	608	99	114
Istanbuldc Veri Merkezi Ltd Sti (TR)	**334.79**	2964	1857	126	470
PEG TECH Inc (US)	**333.31**	992	9	172	158
LUOGELANG (FRANCE) LIMITED (HK)	**318.87**	919	6	93	153
PEG TECH Inc (US)	**186.21**	6559	55	1853	1870
GATEWAY INC (JP)	**182.57**	141	347	1608	41

Spam

As in the malware category, this list had 100% turnover. Also 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. Here again the total numbers of malicious domains tended to be low—but so were the numbers of neutral domains, relatively speaking—so there were still some strong signals (especially compared to some of the other features such as IP geolocation, domain registrars, or certificate issuers.

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

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

Of the 30 ASNs represented in the three Top 10 lists for the Nameserver ASN feature, only one (in the spam category) repeated from the November 2021 snapshot. This was a higher turnover rate than we've seen in previous years from report to report, but again is likely attributable to the thresholding change.

Nameserver ASNs show a much smaller spread of signal strengths than IP ASNs. The spam category had the highest signal strength of any of the three threat types, with 1473.11 for the #1 ASN—but even in this category, the strengths then dropped off substantially, as you will see.

Phishing

This category shows dramatic differences between two "neighboring" categories: the November 2021 snapshot of this same category had much higher signal strengths, and the Phishing category for IP ASN had astronomically higher signal strengths—around 1000x! As we have seen in some of the other Top 10 lists, this one also had 100% turnover.

The careful reader may note what looks like either a data error or an extraordinary coincidence in the malicious domain counts for the first two nameserver ASNs for phishing (54990 and 39287). There is an explanation: the hosting provider Njalla, well-known for providing robust privacy around its hosting services, provisions many domains with one nameserver in each of these two ASNs. So the grouping of phishing, malware, and spam domains seen here is a set that would all appear to tie back to Njalla.

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

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

Malware

The story for malware is similar to what we saw for phishing: we have a modest spread of signal strengths in this snapshot, again likely attributable to the thresholding.

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

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

Spam

The top signal strength for spam, at 1773.11, 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 fairly low overall numbers of domains, with the top spot in this edition having only 4,207 spam domains (vs 7,155 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 and phishing categories.

Spam was the only Top 10 list for Nameserver ASNs that had a repeater from the previous snapshot: AS 4686 from Japan.

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
4686 BEKKOAME BEKKOAME INTERNET INC. (JP)	**1473.11**	4,207	69	15	1,003
7684 SAKURA-A SAKURA Internet Inc. (JP)	**107.28**	5,935	10	393	19,430
45102 ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (CN)	**12.19**	1,795	12274	7415	51,734
9370 SAKURA-B SAKURA Internet Inc. (JP)	**11.40**	5,280	141	181	162,714
51167 CONTABO Contabo GmbH (DE)	**9.34**	4,416	18553	760	166,062
38283 CHINANET-SCIDC-AS-AP CHINANET SiChuan Telecom Internet Data Center (CN)	**7.55**	2,093	3572	2043	97,395
397213 SECURITYSERVICES (US)	**7.23**	21,622	53175	24860	1,050,967
19318 IS-AS-1 (US)	**6.66**	4,345	18101	467	229,141
397220 SECURITYSERVICES (US)	**6.34**	21,625	53452	24959	1,198,951
134543 UNICOM-DONGGUAN-IDC China Unicom Guangdong IP network (CN)	**6.25**	5,628	11868	7860	316,436

November 2021	Signal Strength	Spam	Phishing	Malware	Neutral
HOSTKEY (US)	**90,200.93**	7,155	283	346	4
Wirels Connect (PTY) (ZA)	**5,166.45**	1,127	611	124	11
Internap Japan Co.,Ltd. (JP)	**1,813.17**	827	1,799	322	23
Dream Wave Shizuoka Co. Ltd. (JP)	**1,103.34**	4,923	637	90	225
HOSTKEY B.V. (NL)	**1,063.89**	3,671	6	105	174
INTERNET IT COMPANY (SC)	**604.61**	1,187	5,373	4,114	99
BELCLOUD (BG)	**316.19**	3,806	2,188	309	607
BEKKOAME BEKKOAME INTERNET INC. (JP)	**292.90**	3,909	831	58	673
IST-AS (LT)	**220.85**	3,749	145	140	856
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. This feature also had relatively high turnover. Taking all of the Top 10 lists in aggregate, there were only six repeaters in the entire set. Seychelles, Mauritius, the Philippines, Moldova, and Panama all dropped entirely off of our lists.

As we noted in the previous edition, IP hosting region is not generally a strong indicator of maliciousness, as you can see by the mild signal strength values—but we were surprised this time to see something we had only previously seen in the SSL Certificate Issuer section before—**some hosting countries actually had signal strengths that were positive relative to neutral.** Specifically, we saw this with the US, the UK, and Brazil in the Spam category.

Phishing

Two of the hosting regions in the phishing category are repeaters from the previous report: Luxembourg and Hong Kong. Unsurprisingly, with our change of thresholding, the range of signal strengths is narrower, topping out at just 10.74, 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.

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
LU (Luxembourg)	**10.74**	6,852	2507	3719	45,919
HK (Hong Kong)	**5.08**	10,210	4722	5059	144,766
TW (Taiwan)	**2.48**	1,728	746	400	50,079
RU (Russia)	**2.18**	13,862	5014	3886	457,399
CN (China)	**2.09**	3,930	1643	456	135,266
LT (Lithuania)	**1.58**	1,099	844	491	50,105
VN (Vietnam)	**1.54**	1,921	475	202	89,824
BR (Brazil)	**1.54**	7,775	3870	1064	364,573
NL (Netherlands)	**1.43**	27,907	12215	6808	1,408,415
US (United States)	**1.23**	205,543	109958	42041	12,036,790

November 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

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 (under 5k 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.

March 2023	Signal Strength	Malware	Phishing	Spam	Neutral
CA (Canada)	**7.41**	40,315	5056	610	655,830
LU (Luxembourg)	**6.58**	2,507	6852	3719	45,919
HK (Hong Kong)	**3.93**	4,722	10210	5059	144,766
AU (Australia)	**3.18**	13,045	4397	281	494,694
CN (China)	**1.46**	1,643	3930	456	135,266
CZ (Czech Republic)	**1.39**	4,021	2365	188	348,230
RU (Russia)	**1.32**	5,014	13862	3886	457,399
BR (Brazil)	**1.25**	3,780	7775	1064	364,573
US (United States)	**1.10**	109,958	205543	`42041	12,036,790
NL (Netherlands)	**1.05**	12,215	27907	6808	1,408,415

November 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

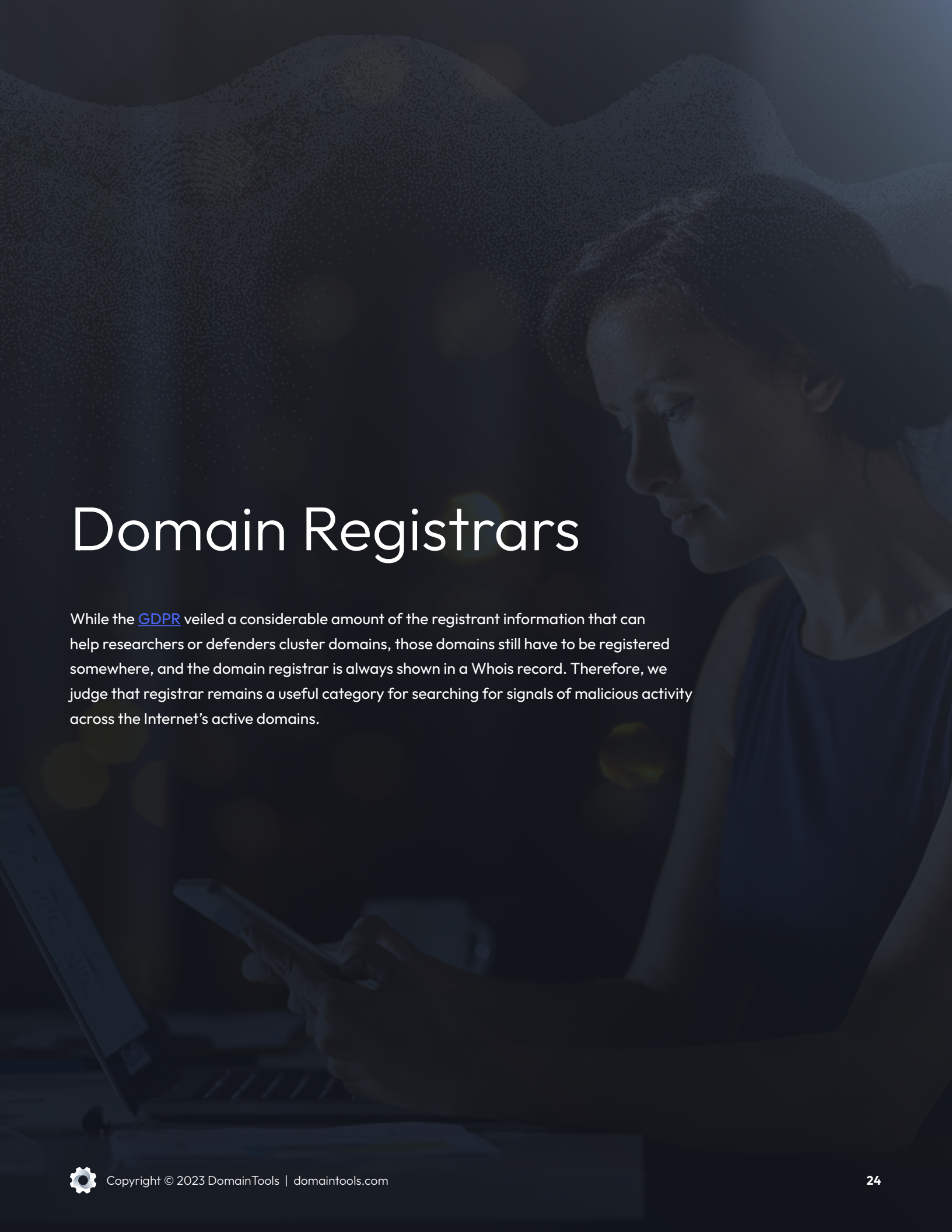
Spam

We won't bury the lede: for the first time in any domain feature other than SSL certificate issuers, we saw several hosting regions which actually showed a relative **underrepresentation** of spam 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.

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.

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
LU (Luxembourg)	**23.22**	3,719	6852	2507	45,919
HK (Hong Kong)	**10.02**	5,059	10210	4722	144,766
JP (Japan)	**8.82**	6,677	993	739	217,153
BG (Bulgaria)	**2.60**	1,128	1446	377	124,490
RU (Russia)	**2.44**	3,886	13862	5014	457,399
NL (Netherlands)	**1.39**	6,808	27907	12215	1,408,415
TR (Turkey)	**1.14**	1,454	2096	1000	365,450
US (United States)	1.00	42,041	205543	109958	12,036,790
BR (Brazil)	0.84	1,064	7775	3780	364,573
GB (United Kingdom)	0.75	3,422	12286	5140	1,316,678

November 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 140,000 phishing domains observed in this snapshot. This is a substantial increase.

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
3765 NICENIC INTERNATIONAL GROUP CO., LIMITED	**53.41**	6,769	3017	544	5,412
1915 West263 International Limited	**32.84**	33,850	4130	261	44,014
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	**30.78**	24,015	8645	1502	33,314
1868 Eranet International Limited	**21.24**	7,538	1361	185	15,153
1556 Chengdu West Dimension Digital Technology Co., Ltd.	**15.74**	40,205	20642	529	109,094
3806 Beget LLC	**13.05**	2,425	515	28	7,933
609 Sav.com, LLC	**10.82**	37,967	23273	17467	149,890
1479 NameSilo, LLC	**9.64**	140,781	29130	17196	623,435
1449 URL Solutions, Inc.	**9.40**	8,287	5110	186	37,637
1606 Registrar of Domain Names REG.RU LLC	**9.33**	17,315	4778	843	79,285

November 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

This Top 10 list is a 100% change from last time around—there is not one repeating registrar. 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 rank highly on the basis of signal strength.

March 2023	Signal Strength	Malware	Phishing	Spam	Neutral
3765 NICENIC INTERNATIONAL GROUP CO., LIMITED	**48.21**	3,017	6769	544	5,412
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	**22.44**	8,645	24015	1502	33,314
3824 Cloud Yuqu LLC	**20.93**	3,297	1161	28	13,620
1556 Chengdu West Dimension Digital Technology Co., Ltd.	**16.36**	20,642	40205	529	109,094
609 Sav.com, LLC	**13.43**	23,273	37967	17467	149,890
1449 URL Solutions, Inc.	**11.74**	5,110	8287	186	37,637
1555 22net, Inc.	**9.57**	2,781	1710	47	25,140
1250 OwnRegistrar, Inc.	**9.10**	9,192	9218	1043	87,355
1915 West263 International Limited	**8.12**	4,130	33850	261	44,014
1868 Eranet International Limited	**7.77**	1,361	7538	185	15,153

November 2021	Signal Strength	Malware	Phishing	Spam	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.

March 2023	Signal Strength	Spam	Phishing	Malware	Neutral
Sav.com, LLC	**24.34**	17,467	37967	23273	149,890
GMO Internet, Inc. d/b/a Onamae.com	**17.25**	54,529	13501	6244	660,360
3775 ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	**9.42**	1,502	24015	8645	33,314
3855 Hong Kong Juming Network Technology Co., Ltd	**6.60**	1,740	2995	1373	55,097
1479 NameSilo, LLC	**5.76**	17,196	140781	29130	623,435
1599 Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	**5.43**	4,192	16838	5873	161,257
Namecheap, Inc.	**4.52**	52,490	124890	56528	2,426,272
OwnRegistrar, Inc.	**2.49**	1,043	9218	9192	87,355
Dynadot, LLC	**2.40**	4,601	23326	24704	401,274
1923 Gname.com Pte. Ltd.	**2.27**	1,604	14414	6190	147,642

November 2021	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. 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 certificate authorities (CAs) associated with domains, however, fewer than ten had a positive correlation with maliciousness for any of the threat types.

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 March 2023 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—some 8,000 phishing domains vs 81,000, respectively—but they are associated with enough malicious activity that th**e Let's Encrypt E1 certificates took second place in 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 fans of the new certificate type, relative to creators of neutral domains.) 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.

Notable in the spam category is that our "Top 10" list only has four rows. This is because there are only four issuers that had 1,000 or more spam domains—regardless of signal strength.

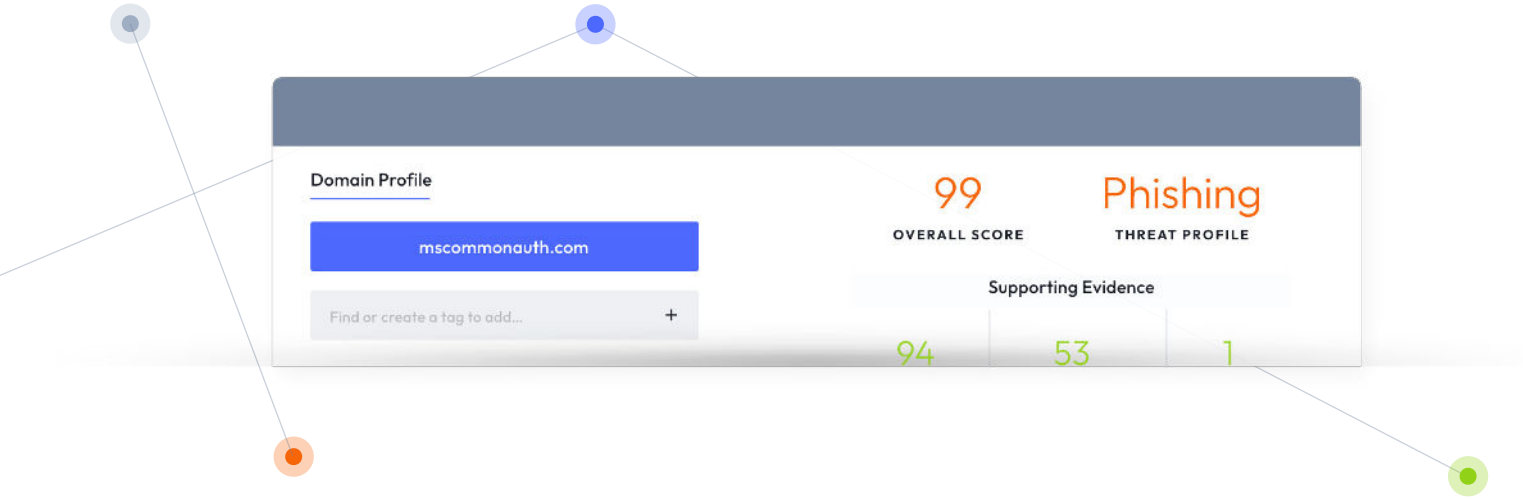
Readers of our November 2021 report may wonder why **self-signed certificates make no appearance** in our Top 10 lists this time around. There is a two-part explanation: first, our thresholding eliminates any issuer with fewer than 1,000 domains of the threat type under examination. Second, some of the tuning that 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, self-signed certificates were not tied to more than 1,000 domains in any of the three categories.

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 this edition of the report.

Phishing

Because the issuers with better-than-neutral signal strengths are such an important part of the story, we will note that for the March 2023 snapshot, there were four issuers of this description, as opposed to five in the previous edition. Still, the signal strengths are generally low, topping out at 10.95. As we will see in all three threat categories, in Phishing, the top place goes to the 1P5 Google Trust Services certificate type. Also holding true across all three lists is that the more familiar Let's Encrypt R3 certificates have a (very) mildly non-malicious signal.

March 2023	Signal Strength	Phishing	Malware	Spam	Neutral
CN=**GTS CA 1P5,O=Google Trust Services LLC**,C=US	**10.95**	49,888	23098	6630	681,628
CN=**E1,O=Let's Encrypt**,C=US	**5.06**	8,161	5587	1521	241,103
CN=**Cloudflare Inc ECC CA-3**, O=Cloudflare\, Inc.,C=US	**2.84**	31,931	17374	3504	1,683,623
CN=Encryption Everywhere DV TLS CA - G2,OU=www.digicert.com,O=DigiCert Inc,C=US	**2.31**	1,497	443	79	97,115
CN=**ZeroSSL RSA Domain Secure Site CA**,O=ZeroSSL,C=AT	**1.91**	2,413	1344	193	189,379
CN=**GTS CA 1D4,O=Google Trust Services LLC**,C=US	**1.32**	2,465	1534	112	279,858
CN=**cPanel\, Inc. Certification Authority**,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.65	11,758	5763	818	2,708,969
CN=**R3,O=Let's Encrypt**,C=US	0.63	81,563	71733	18516	19,520,458
CN=**Encryption Everywhere DV TLS CA - G1**,OU=www.digicert.com,O=DigiCert Inc,C=US	0.57	3,133	1814	77	821,459
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	0.49	6,708	4510	235	2,038,567



November 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: four "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. The Let's Encrypt R3 issuer moved into the "green" category this time around (whereas Let's Encrypt E1 is in second place). However, in general it's noteworthy that the strongest signal strength, 7.58, is very modest compared to many of the other Top 10 lists in this report.

March 2023	Signal Strength	Malware	Spam	Phishing	Neutral
CN=GTS CA 1P5,O=Google Trust Services LLC,C=US	**7.58**	23,098	6630	49888	681,628
CN=E1,O=Let's Encrypt,C=US	**5.18**	5,587	1521	8161	241,103
CN=**Cloudflare Inc ECC CA-3**, O=Cloudflare\, Inc.,C=US	**2.31**	17,374	3504	31931	1,683,623
CN=**ZeroSSL RSA Domain Secure Site CA**,O=ZeroSSL,C=AT	**1.59**	1,344	193	2413	189,379
CN=**GTS CA 1D4,O=Google Trust Services LLC**,C=US	**1.23**	1,534	112	2465	279,858
CN=**R3,O=Let's Encrypt**,C=US	0.82	71,733	18516	81563	19,520,458
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	0.50	4,510	235	6708	2,038,567
CN=**Encryption Everywhere DV TLS CA - G1**,OU=www.digicert.com,O=DigiCert Inc,C=US	0.49	1,814	77	3133	821,459
CN=**cPanel\, Inc. Certification Authority**,O=cPanel\, Inc.,L=Houston,ST=TX,C=US	0.48	5,763	818	11758	2,708,969

November 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

As mentioned earlier, there is a general dearth of spam domains associated with certificate issuers, which is why there are only four entries in this "Top 10." Most of the issuers have fewer than 1,000 spam domains associated with them. This makes a certain amount of sense, in that spammers don't necessarily have much reason to use SSL certificates. Overall, there was one weaker-than-neutral (i.e. "green") signal for spam in this snapshot, compared to five in the previous. As with the Malware threat category, the 1P5 "flavor" of Google Trust Services, and Let's Encrypt E1, were newcomers to this list.

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	681,628
CN=E1,O=Let's Encrypt,C=US	**6.00**	1,521	8161	5587	241,103
CN=**Cloudflare Inc ECC CA-3**, O=Cloudflare\, Inc.,C=US	**1.98**	3,504	31931	17374	1,683,623
CN=**R3,O=Let's Encrypt**,C=US	0.90	18,516	81563	71733	19,520,458

November 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

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.