Fall 2021

The DomainTools Report

Internet-Scale Patterns in Malicious Infrastructure

DOMAINTOOLS®

Introduction

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 and email privacy providers (2015) to affixes in domain names (2016) to domain "blooms" and "spikes" (Spring 2021).

For this edition, we chose to go "back to basics," and focus on concentrations of malicious activity by six categories, several of which were also studied in earlier reports. 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 get better 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 characteristics 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 characteristics 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 characteristic, 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.

Methodology

Candidate Domains

The DomainTools Iris database includes around 380 million currently-registered domains. However, not all of these domains are active. In the interest of understanding real and current threats, **we chose to exclude 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.

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.

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 a count of known-malicious domains above the following thresholds:

- IP Geolocation: 100
- TLD: 1000
- IP ASN: 1000
- Nameserver ASN: 1000
- Registrar: 1000
- SSL Certificate Authority: 1000

The threshold of 100 for IP Geolocation is different from the others because we chose to remain consistent with earlier editions of the DomainTools Report that used the same threshold.

The 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.

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 (which is a DomainTools Report first).

> *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 September, 2021**. Of course, the Internet is in a constant state of flux, but as with most big-data analyses, large-scale trends tend to have some stability and durability. Future DomainTools Reports that examine the same criteria as this report will likewise be built on snapshots in time.

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
.bar	108.93	**6,321**	3,064	2,648	2,414

The TLD ***.bar*** has a Malware signal strength of **108.93** (the highest malware signal of any TLD on the Internet, by our methodology). There are 6,321 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.

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 typically 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

Some Confirmations, Some Surprises

Defenders and researchers have come to expect certain patterns when they look into suspicious or known-bad infrastructure. Certain TLDs, for example, have poor reputations in the infosec community, and indeed, some of those are represented in the top-ten lists for phishing, malware, and spam signal strength. The newer generic TLDs, such as ***.live, .top***, and ***.xyz*** are examples of these. And, indeed, within the top 10 lists in the TLD section, none of the most popular TLDs, such as ***.com***, ***.net***, or ***.org***, nor any of the larger country code TLDs such as ***.co.uk***, ***.de***, ***.fr,*** etc, are anywhere to be found. **All of the top-ten lists are composed of relatively new gTLDs, or country code TLDs (ccTLDs) from comparatively small countries** such as ***.ml***, the ccTLD for Mali (which, it should be noted, allows free, anonymous domain registrations). The findings in the TLD section, then, aren’t likely to surprise most readers.

On the other hand, the results in some of the other categories may be counterintuitive to many readers. In particular, the top-ten lists based on SSL Certificate Authority, were not even entirely “top ten” from the malicious signal perspective—that is, in all three of the categories, 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**. Indeed, two of the certificate providers most often scorned by infosec pros—***Let’s Encrypt*** and ***self-signed*** certificates—**both had sub-1.00 signal strength** in at least one of the top-ten lists! (NOTE: for the sake of this research, we make no distinction between SSL and TLS certificates; we simply use the term SSL because it’s the common parlance among most practitioners and researchers.)

The SSL results reminded us of what many of us considered a surprising finding in the very first DomainTools Report: **the majority of newly-created domains each day do not show strong signals of maliciousness**. It is almost an article of faith among defenders that new domains are dangerous, but the data say otherwise. However, we hasten to add that the inverse of this does comport with expectations: **the majority of malicious domains are, indeed, young**.

And now, on to the categories.

Top-Level Domains (TLDs)

The TLD of a domain often conveys some level of meaning about the domain. By far the most common TLD, .com, tends to connote legitimacy to many Internet users,

Phishing

Following are the top ten TLDs ranked by signal strength for phishing. The range of signal strengths is comparatively modest; as we will see, while the 131.03 for .quest is substantially higher than the second-place TLD, it is a low value compared to some of the other top-ten "winners."

	Signal Strength	Phishing	Malware	Spam	Neutral
.quest	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

The top ten TLDs for Malware signal strength show some overlap with the Phishing list, with four of the Phishing TLDs also seen in Malware. The general range of signal strengths is comparable between the two lists, as well. Notable in this table is the appearance of .xyz, which is a relatively popular TLD, in part because of promotions over the years for relatively inexpensive, or even free, domain registration in .xyz. The numbers of domains in .xyz in this table are among the highest in this report—until we reach the Certificate Authority section.

	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

As with the previous two lists, several of the TLDs are represented more than once. However, note that the signal strength variation is wider in the Spam category than either of the others, with both the highest and lowest values of any of the three lists. The TLD .xyz, with its high domain counts, makes this top ten list as well.

	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 **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 category and another (for example, in the Malware category, ASN 49447, NICEIT, DM, has 1572 phishing domains versus just 15 neutral). With each AS in this and the following section, we provide its country code of registration in parentheses.

Phishing

Following are the top ten IP ASNs ranked by signal strength for phishing. As noted above, **see the wide range in Signal Strength**, from over 8,000 at the top to about 181 at the bottom—the latter number not far from the highest signal strengths we recorded for TLDs across that whole category! To save you the math, that spread is more than a 44:1 ratio from highest to lowest signal strength. (Spoiler alert, however: that spread is not the overall winner for this study; in fact, it's not even close!)

		Signal Strength	Phishing	Malware	Spam	Neutral
49447	Nice IT Services Group Inc (DM)	**8,047.06**	1572	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	1608	41
58065	Packet Exchange, LTD (SE)	**621.96**	1134	1354	421	140
41564	Orion Network Limited (SE)	**409.52**	608	877	99	114
262254	DDOS-GUARD CORP (BZ)	**404.55**	2550	90	147	484
59447	Istanbuldc Veri Merkezi Ltd Sti (TR)	**303.38**	1857	2964	126	470
209813	Fast Content Delivery LTD (SC)	**290.33**	2314	726	294	612
200313	INTERNET IT COMPANY (SC)	**180.91**	589	185	447	250

Malware

Signal strength for Malware in the IP ASN was not quite as broad as in the Phishing category, but still a more than order-of-magnitude spread. And note, too, some of the extreme spreads in absolute numbers of domains. Some of these ASNs seem to 'specialize' in certain kinds of malicious activity. Note, too, that PEG TECH makes it into this list twice, for two different AS under their control.

		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

This category plays out similarly to the other two, with a very wide range of signal strengths, and similarly wide spreads in absolute numbers of domains. Of course, as in all of the top-ten lists in this category, **the rule of small numbers is very much in play**, with many of these IP ASNs hosting comparatively low overall numbers of domains.

		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 as the data show, there's not a direct correspondence. Any domain registrant, legitimate or evil, may have their own preferences for nameservers. In the Phishing and Malware threat types, the signal strengths are not dramatically different than what we have seen in some of the other top ten lists. But when we look at the Spam list, that changes!

Phishing

Underscoring that the Venn diagram between IP ASNs and nameserver ASNs is not a circle, only two of the ASNs in this table (AS-PNAPOSK Internap Japan Co.,Ltd., JP and INTERNET-IT from Seychelles) are also in the Phishing table for IP ASN. In most respects, the signal strengths and the counts are relatively modest in this table.

		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 Shenzen 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

There is not a great deal of overlap in this category with the Phishing nameserver ASNs nor with the Malware IP ASNs. There are a couple of outliers on this list in terms of the domain counts,, with the last four ASNs on the list having six-digit counts of both Malware and Neutral domains.

		Signal Strength	Malware	Phishing	Spam	Neutral
395839	HOSTKEY (US)	**855.24**	105	6	7155	4
24295	Internap Japan Co.,Ltd. (JP)	**490.12**	346	283	827	23
200313	INTERNET IT COMPANY (SC)	**40.81**	124	611	1187	99
44592	SkyLink Data Center BV (NL)	**31.50**	322	1799	737	333
40065	CNSERVERS LLC (US)	**30.42**	4158	85	244	4453
17623	China Unicom Shenzen network (CN)	**22.59**	4114	5373	1021	5934
134543	China Unicom Guangdong IP network (CN)	**21.27**	155133	13159	68638	237662
21859	Zenlayer Inc (US)	**20.81**	172624	14648	80632	270254
4837	CHINA UNICOM China169 Backbone (CN)	**16.16**	168034	16602	74860	338780

9808	China Mobile Communication Co.Ltd. (CN)	15.60	177030	16117	88604	369803

Spam

The Spam signal strength for HOSTKEY-USA is not a typo. That signal of over 90,000, is almost ten times as strong as the next-highest, the #1 IP ASN for Spam. A look at the domain counts explains it: we found over 7,000 spam domains using this ASN for their nameservers, and only 4 neutral domains.

		Signal Strength	Spam	Phishing	Malware	Neutral
395839	HOSTKEY (US)	90,200.93	7155	283	346	4
327790	Wirels Connect (PTY) (ZA)	5,166.45	1127	611	124	11
24295	Internap Japan Co.,Ltd. (JP)	1,813.17	827	1799	322	23
18068	Dream Wave Shizuoka Co. Ltd. (JP)	1,103.34	4923	637	90	225
57043	HOSTKEY B.V. (NL)	1,063.89	3671	6	105	174
200313	INTERNET IT COMPANY (SC)	604.61	1187	5373	4114	99
44901	BELCLOUD (BG)	316.19	3806	2188	309	607
4686	BEKKOAME BEKKOAME INTERNET INC. (JP)	292.90	3909	831	58	673
61272	IST-AS (LT)	220.85	3749	145	140	856
134771	CHINATELECOM-ZHEJIANG-WENZHOU-IDC (CN)	189.63	1775	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. Unlike the ASN categories for both IP and nameserver, **this category showed much milder spreads in signal strength**. This may qualify to some readers as another myth busted: that IP hosting region is a strong indicator of maliciousness. There are much higher numbers of malicious domains hosted in Russia and the United States, for example, than in any of the countries in any of the following three tables. However, relative to the numbers of neutral domains also hosted in Russia and the US, the malicious ones are not particularly strongly represented.

Phishing

These are the top ten countries of hosting, as sorted by Phishing signal strength. Hong Kong stands out with a relatively high number of domains in each of the categories compared to the others. However, its signal strength of 7.52 is not particularly strong. **Takeaway: you may be more likely, statistically, to see a phishing domain that is hosted in Hong Kong, but if you're doing forensic work on a Hong Kong-hosted domain whose nature is**

unknown, there's not an especially strong indication that it is a phishing domain. As the Malware and Spam tables show, in fact, that Hong Kong domain is more likely to be involved in one of those other threat types.

	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	133780	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

Using Hong Kong as an example again, here we see a datapoint that has both a relatively high signal strength and a relatively high count of domains compared to its peers in the category. In fact, while the law of small numbers is fairly pervasive in this study, Hong Kong's representation in all three threat types is an outlier.

	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

If you're looking for quick ways to identify domains as being "spammy," IP hosting geolocation is not the way to go about it. Neither the signal strengths nor the absolute numbers in this category will do much to (statistically speaking) forecast whether a domain is involved with spam. Compare this, for example, to that Spam signal we saw in the previous category (Nameserver ASN), which was over 90,000, and you see what we mean.

	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 has 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 judged that registrar would be a useful category for searching for signals of malicious activity across the Internet's active domains.

We found a modest level of overlap among the top-ten registrars in each of the threat types. In fact, only one registrar, **DOMAINNAME BLVD, INC**, was represented in all three categories—perhaps surprising, since it is a very small registrar with fewer than 1,500 domains in total. (The largest registrar in our lists by domain count, **GMO Internet, Inc. d/b/a Onamae.com**, registered over 600,000 domains.) Signal strengths in this category are not extreme, though in terms of counts, there are some registrars with many thousands of malicious domains associated.

Phishing

Three registrars in our top-ten list have over 10,000 domains associated with them; the largest, **NameSilo, LLC**, has nearly 77,000. NameSilo, in fact, has five-digit counts of malicious domains in all three threat types, and the total number of malicious domains registered through them is not dramatically lower than the number of neutral domains. So in terms of overall impact, it outweighs the others in the list; but from a signal strength perspective, it is not particularly notable.

	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

While there were no dramatic outliers among the registrars, we did see a substantially higher maximum signal strength in Malware than with the other two threat types. That said, this was the most extreme case of small numbers in the entire report: there were exactly zero Phishing or Spam domains associated with **Tname Group Inc**, a fairly small registrar with fewer than 1,600 domains all-in. But of those, only 45 were neutral, with the remainder all in the Malware category.

	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. **Global Domain Name Trading Center Ltd** shows a strong (for the category) signal of 158.18, but has only 1167 Spam domains associated with it. The aforementioned **GMO Internet, Inc. d/b/a Onamae.com** has almost 150,000 Spam domains associated with it; but it also has a lot of neutral domains. It has some impact, therefore, but is not a strong forensic signal to the investigator or analyst faced with a domain of unknown intent.

	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 first 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 have an unfamiliar color in them: green. 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. 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 one 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 a Let's Encrypt certificate, then within this specific context, the certificate absolutely *does* take on an incriminating aspect.)

Phishing

If it were not for the five "green" CAs in the list, the Phishing table would be unremarkable. Neither the absolute numbers of domains nor the malicious signal strengths particularly stand out.

	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

For this threat type, the overall picture is very similar to Phishing. Let's Encrypt shows a slightly non-malicious signal in Malware, but we'll acknowledge that for anyone who fell victim to one of the roughly 44,000 Malware, 38,000 Phishing, or 20,000 Spam domains using that certificate, its relative innocence might be a hard sell.

	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

While this observation is true across all three threat types, we'll mention it here: **the CAs are the same set of ten across all three threat types**. The Venn diagram is a circle. Most of the categories earlier in the report had some degree of overlap, in some cases quite a bit. This is the first time in DomainTools Report history, though, where the exact same entities were in the top ten in every threat type (albeit in different orders).

	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

We consider the DomainTools Report an effort to identify "hotspots" of malicious activity across the Internet. We do this in part to help 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 research and development efforts, as we seek to develop ever-more-accurate algorithms for predicting the nature of a given domain.

But some of these hotspots are like neutron stars: very high "heat" and density (Signal Strength), very low size (number of domains). As forensic indicators, 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.

This edition of the report represents a milestone: we have developed an automated means of recording the data that underpins this study. In figure reports, we expect to provide trend information, showing where there is growth or recession in the numbers and signals of malicious domains across the Internet. 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.