DOMAINTOOLS

THE DOMAINTOOLS REPORT

A PROFILE OF MALICIOUS DOMAINS
2015 EDITION

SUMMARY

Much of the malicious activity on the Internet is classified and tracked in domain blacklists and reputation scores. But these do little to profile and predict cybercrime to proactively protect against domains that have yet to exhibit illicit behavior. **Malicious actors behave in a predictable manner, and the more thoroughly we profile that behavior, the better we can defend against them.**

With that purpose in mind, we analyzed domains from several popular blacklists. This report uses DomainTools' leading Whois and DNS data to define attributes of those malicious domains and begin to create a profile of locations and privacy preferences of cybercriminals.

KEY FINDINGS

TOP-LEVEL DOMAINS
Cybercriminals, especially spammers, seem to favor familiar TLDs; .com clearly dominates by volume. This makes logical sense, in that the goal of spam and phishing is to make the offending domain appear legitimate.

WHOIS PRIVACY
Whois Privacy doesn't correlate any more strongly with maliciousness than does open registration. Often a paid service, Whois Privacy is not a tactic utilized by cybercriminals. However, certain privacy providers are favored over others.

FREE EMAIL PROVIDERS
Malicious domains are more frequently registered using Gmail addresses. But for reasons that aren't clear, several Japanese free email providers make up the highest concentration of malicious domains. From an investigative standpoint, certain email domains, found in Whois records, correlate with high risk.

HOSTING LOCATION
By volume of malicious domains hosted on infrastructure within a country, the US dominates. By concentration of malicious domains, four countries have malicious domain concentrations over 10%, with one topping 50%.

OVERVIEW

WHERE DOES CYBERCRIME "LIVE?"

Analysis of specific threat actors often uncovers their bases of operation; real-time as well as historical attack maps give broad information about the IP addresses that originate attacks; positively attributed attacks give a clear picture of at least the locus of direction and authority for the attacks. But a comprehensive map of where cybercrime "lives," from a logical as well as a geographical viewpoint, can help the global cybercrime fight. Specifically, we envision these benefits:

IMPROVING AWARENESS

Mapping connected webs of domains can help develop a better view of cybercrime networks from a semantic/organizational standpoint, which is valuable for defenders and white-hat attackers alike. Because malicious domains--sources of malware, phishing, spam, botnets, and the like--are in service of larger cybercrime operations, these maps of Internet holdings help characterize and map the organizations themselves.

FIGHT IT AT THE SOURCE

Attacking the attackers: Mapping cybercrime locations can assist law enforcement and governmental agencies in their efforts to shut down cybercrime at its source, or to curtail its activities by strangling funding and other assistance sources. Particularly from the standpoint of concentration of badness, certain targets may merit further scrutiny or action.

FIGHT IT AT THE DESTINATION

Defending the target: Pinpointing "hotspots" of activity and clusters of connected domains can help organizations fine-tune their perimeter defenses against attacks from the mapped entities. With the ability to carefully inspect or block connections that would otherwise be allowed, organizations can better defend against these "hotspots" of badness.

For this report, we set out to develop logical maps of cybercrime volume and concentration, broken down by four attributes: **Top-Level Domain (TLD), Whois Privacy Provider, Free Email Provider, Geography of Hosting.**

We looked at malicious activity identified on trusted blacklists to see where its volumes and its concentrations were highest. Concentration is measured as the number of malicious domains exhibiting that attribute divided by the total number of domains that exhibit that attribute.

For example: of all known domains, 30 million were registered with a Gmail.com address, and of those 30 million registered using Gmail, 1.37% were found on blacklists.

Why focus on concentration, when the raw numbers of attacks may be more relevant?

>> Identifying hotspots and patterns can help build a better risk assessment, enabling defensive measures such as reputation scores. While these don't promise to shut down all malicious activity, they do filter out some of the "noise," raising the efficiency of preventive and detection postures.

>> It also helps us better profile criminal networks. A great portion of malicious activity is in service of a larger criminal enterprise, rather than hacking for its own sake. Understanding the actors, preferences and connections helps in fighting them.

METHODOLOGY AND CHARTING

We analyzed records in the DomainTools database of around 270 million domains, in conjunction with well-known spam, phishing, and malware reputation/blacklist sources. Our parsing of the Whois records made it simple for us to analyze various fields in the registration data—registrant physical addresses, email addresses, and the like. Our domain profile information also includes data beyond canonical Whois records, such as IP addresses.

Overlaying the domain data with data on malicious activity gave us quantitative insights into where the malicious and innocuous domains "live," logically as well as geographically. While we know there may be gaps in the data, DomainTools has amassed the world's largest database of domains; the dataset is complete enough for us to be comfortable drawing inferences about the relative concentrations and absolute numbers of malicious domains.

Each analysis will contain a **DomainTools Report VCP Chart** (Volume, Concentration, Proportion), which show the following data for each attribute:

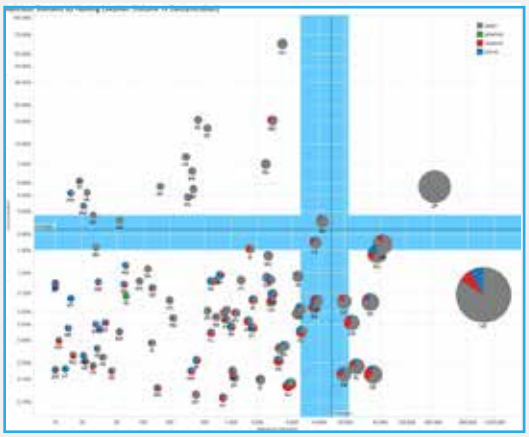
>> Ranking of overall numbers of malicious domains
>> Ranking of concentration of malicious domains
>> How each item stacks up against the overall averages
>> Proportions of each type of badness within each item

In the VCP Charts, items in the upper right quadrant are of particular interest, as they are both above average in volume and concentration. These are the best indicators of malicious domains when looking at that attribute.

WHAT CONSTITUTES "MALICIOUS?"

We used several well-known sources of blacklist/reputation information to build our counts of "bad" domains. A total of nearly 1.75M domains fell on blacklists for:

>> Spam
>> Phishing
>> Botnet
>> Malware



Each chart plots the total number of malicious domains on the X-axis vs the concentration of malicious domains on the Y-axis, using a logarithmic scale. Each mark is a pie chart showing the relative proportion of types of malicious activity found in each of those items. The total size of the pie charts represents the relative volume of malicious domains. The crossing blue lines show 95% confidence intervals around the averages for each axis.

TOP-LEVEL DOMAIN (TLD): TRUST LEADS TO DECEPTION

Spammers and phishers love .com addresses, since they tend to draw a lot of traffic. Additionally, they can be registered easily, inexpensively, and perhaps most importantly, anonymously (either through privacy services or through falsified registrant information). In raw numbers, .com dominates the numbers of malicious domains. However, from the standpoint of concentration of badness, .com doesn't even make the top 10; the TLD with the most illicit domains by proportion is .link.

Certainly, in terms of absolute numbers .com is the head-and-shoulders winner, with the runner-up (.net) at less than 20% as many bad domains. The tail-off is dramatic: the 10th-ranked TLD (.in) shows a bit under 14,000 bad domains—that's just under 1.4% as many evil domains as .com.

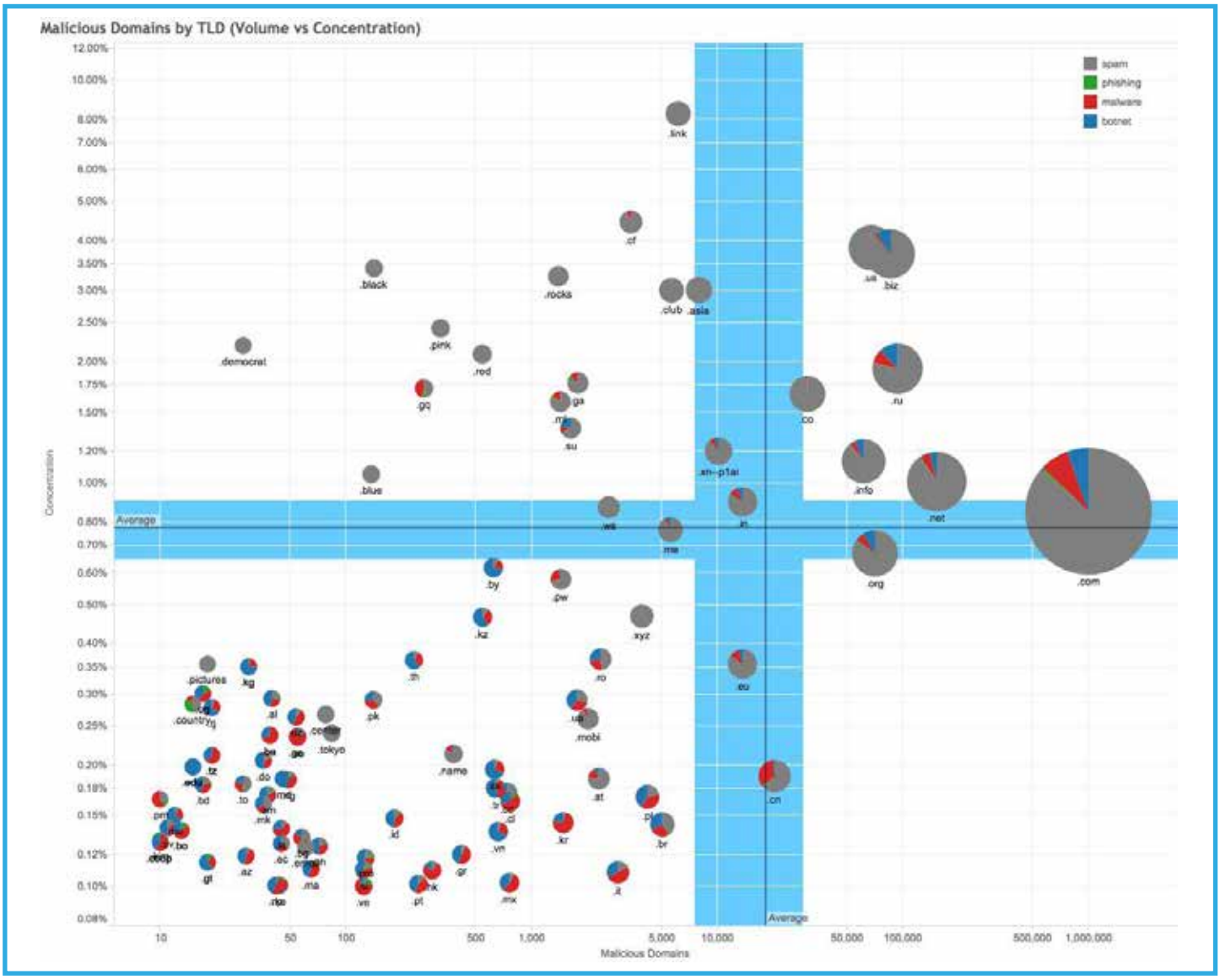
The VCP Chart for top level domains shows that a vast majority of the TLDs are below the average for both volume and concentration (a pattern which held true for all 4 attributes we examined, since the averages are swayed dramatically by high volume TLDs).

In this case, the "big six" (.com, .net, .org, .biz, .info, .us) plus 2 ccTLDs (Russia and Colombia) are above average in volume. This may be because the big six have been around longer and are perceived as trustworthy to victims of malicious activity. Of those 8 TLDs, .us and .biz rank much higher than the others in concentration, but neither of those are near the concentration of .link. This TLD leads mostly because of the sheer volume of spam that contain .link domains.

KEY TAKEAWAYS: Cybercriminals exhibit a preference for domains that appear trustworthy to the recipient, where they can blend in with the crowd of non-nefarious domains. This is primarily true for spam. Malware and botnets show a higher proportion among the smaller TLDs, which makes sense, as those domain names aren't necessarily intended to deceive a human eye.

	TOP LEVEL DOMAIN	MALICIOUS	%
1	.com	1,003,177	0.85%
2	.net	152,661	1.01%
3	.ru	93,985	1.92%
4	.biz	86,073	3.70%
5	.org	70,977	0.67%
6	.us	67,717	3.84%
7	.info	61,609	1.13%
8	.co	30,713	1.66%
9	.cn	20,447	0.19%
10	.in	13,737	0.90%

	TOP LEVEL DOMAIN	%
1	.link	8.25%
2	.cf	4.44%
3	.us	3.84%
4	.biz	3.70%
5	.rocks	3.26%
6	.asia	3.01%
7	.club	3.01%
8	.ru	1.92%
9	.ga	1.77%
10	.co	1.66%



WHOIS PRIVACY SERVICES: COST-CONSCIOUSNESS OF CRIMINALS

Even though there's little to prevent criminals from registering domains under clearly false information (for example, Batman tops the list of fake registrants), many criminals still opt for privacy services. Since they're often using other people's money, the extra cost might not be much of a deterrent. Still, not all privacy services seem to be equal. Incidentally, since there are many extremely small operators who could skew the numbers, we ranked providers with at least 10,000 serviced domains. In fact, with the number of privacy services out there, the relative distribution of malicious domains across these services is the most uniform of all the attributes we examined.

In total, privately-registered domains have a lower incidence of malicious domains than non-private registrations. In our data, **0.67%** *of domains without privacy protection* were observed on a blacklist, whereas a lower **0.65%** *of privacy-protected domains* were malicious. While these concentrations are very close, it still disproves the misconception that Privacy-Protected domains are more likely malicious. Therefore, **Privacy Protection alone is not a good indicator of maliciousness.**

However, when we look at the comparison among providers, there are a few that land notably above both averages. While domain profile information doesn't tell us why, it may be that certain providers offer lower prices, better convenience features, or, in certain cases, may be less responsive to legal requests to release data.

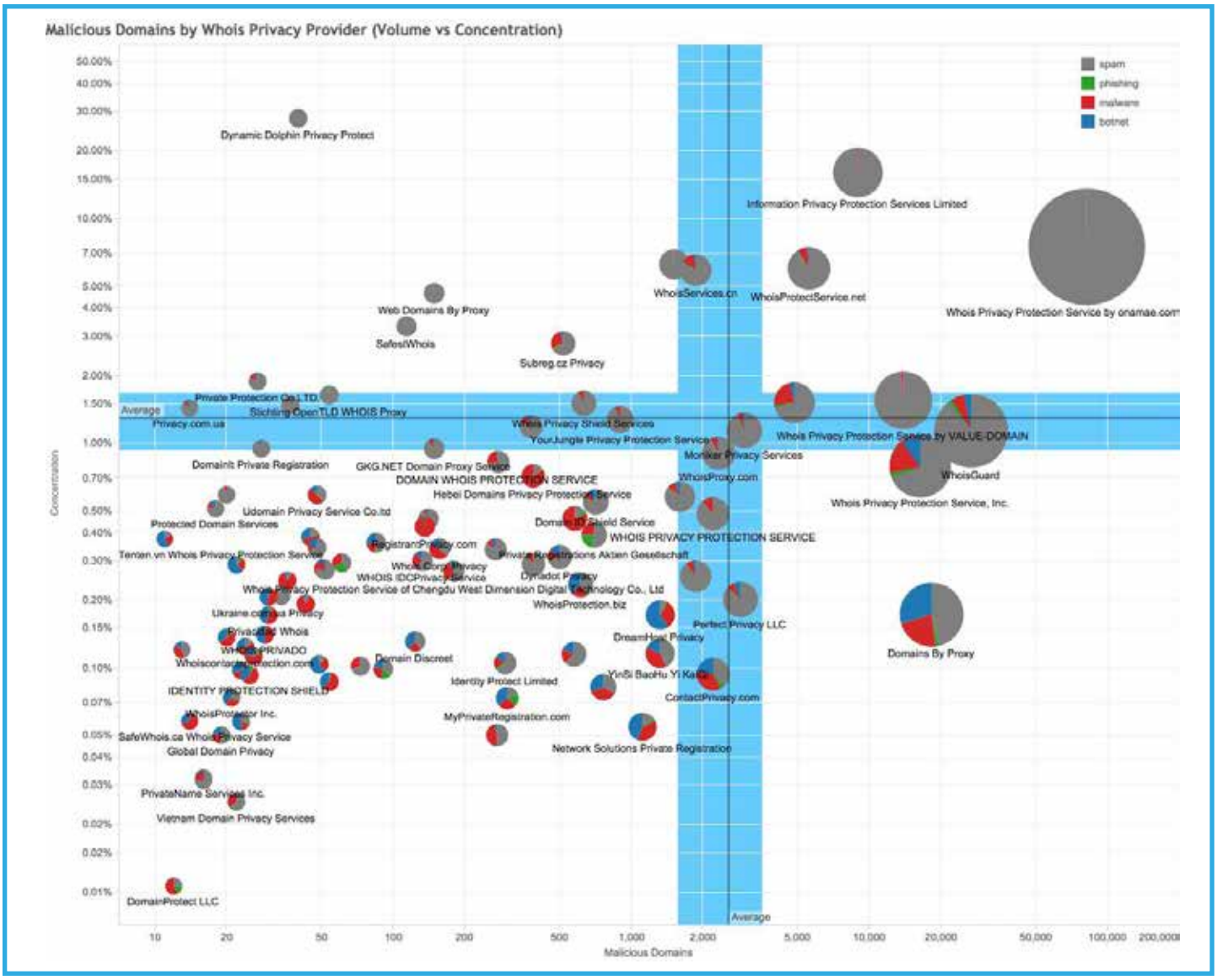
The largest privacy service by volume, and well above average in concentration, is tied to a Japanese domain registration and hosting company. Some other services, such as WhoisGuard and Domains by Proxy, also show high volumes (as we might expect, since they are tied to major registrars such as GoDaddy and Namecheap).

KEY TAKEAWAYS:

Certain outlying privacy services have higher-than-average concentrations of malicious domains registered with them, and thus might bear deeper scrutiny, especially from those tasked with stopping cybercrime at its source. By and large, though, the use of privacy services does not correlate strongly with spam, phishing, malware, or botnet activity.

	PRIVACY PROVIDER	MALICIOUS	%
1	Whois Privacy by onamae.com	82,067	7.50%
2	WhoisGuard	26,835	1.13%
3	Domains By Proxy	18,303	0.17%
4	PrivacyProtect.org	16,393	0.78%
5	Whois Privacy Protection Service, Inc.	16,372	0.80%
6	Whois Privacy by VALUE-DOMAIN	13,923	1.55%
7	Information Privacy Protection Svc Ltd	8,971	16.05%
8	WhoisProtectService.net	5,590	6.00%
9	Whois Privacy Corp.	4,860	1.51%
10	Moniker Privacy Services	2,992	1.14%

	PRIVACY PROVIDER	%
1	Information Privacy Protection Svc Ltd	16.05%
2	Whois Privacy by onamae.com	7.50%
3	Whois Proof LLP	6.26%
4	WhoisProtectService.net	6.00%
5	WhoisServices.cn	5.89%
6	Subreg.cz Privacy	2.78%
7	Whois Privacy by VALUE-DOMAIN	1.55%
8	Whois Privacy Corp.	1.51%
9	Whois Privacy Shield Services	1.51%
10	YourJungle Privacy Protection Services	1.27%



FREE EMAIL PROVIDERS: ANONYMITY ON THE CHEAP

Without paying for privacy protection, a quick and easy way to gain at least partial anonymity is to use a free email provider such as Yahoo, Google, China's 163, or countless others, for domain registration contact information. We looked at which email providers were connected to the highest-volume and most concentrated occurrences of badness.

Our data shows email providers by email domains. For example, yahoo appears several times because of the multiple domains it offers for email (Yahoo.com, Yahoo.co.jp, Yahoo.co.uk, etc). We find it important to split these out as the process of registering a free email address may be easier in some countries over others—for example, if they don't require additional identity verification.

The top 10 by volume of malicious domains shows all major global personal/free email providers. However, we do see an overrepresentation of 4 providers from Asia in this list.

Concentration of evil showed something of a surprise: 5 of the top 6 all come from the same country (Japan). In fact, domains registered with a yahoo.co.jp email address land second in total volume of malicious activity.

The VCP Chart for this attribute shows, as we would expect, a higher-than-average number of domains registered by the major providers (Gmail, Yahoo, Outlook/Hotmail, QQ, and 163). In the above average concentrations, the Japanese email domains stand out. Additionally, within the Microsoft free email domains, cybercriminals seem to prefer Outlook.com over Hotmail.com and Live.com.

KEY TAKEAWAYS:

Since certain email providers correspond to strong concentrations of malicious or suspicious activity, the presence of these email domains in Whois records can be a marker of a higher risk tied to the domain. It is not actionable in and of itself, but can contribute to the risk profile, much as various traits or behaviors contribute to actuarial risk pools in the insurance industry.

	EMAIL PROVIDER	MALICIOUS	%
1	gmail.com	419,646	1.37%
2	yahoo.co.jp	199,620	28.70%
3	qq.com	109,084	1.58%
4	yahoo.com	59,887	0.78%
5	163.com	52,068	1.45%
6	outlook.com	43,974	7.11%
7	hotmail.com	41,430	0.60%
8	126.com	16,689	0.99%
9	aol.com	12,887	0.44%
10	mail.com	8,923	4.98%

	EMAIL PROVIDER	%
1	yahoo.co.jp	28.70%
2	outlook.jp	24.65%
3	docomo.ne.jp	23.12%
4	excite.co.jp	19.62%
5	out1ook.com	14.66%
6	inter7.jp	13.46%
7	live.cn	12.23%
8	yandex.com	10.31%
9	gmx.com	9.74%
10	inbox.com	9.20%

NOTE: The Japan dominance is broken up in the 5th spot by one with a purely phishy name: out1ook[.]com (with a numeral 1 instead of an l, in case it's too hard to tell by the font). In fact, this out1ook[.]com domain itself has been listed as malicious, a strong indicator of why nearly 15% of the domains registered using that as an email address. For an idea of what this means, Imagine the domain of a legitimate email provider such as Gmail.com falling onto a blacklist.

IP ADDRESS GEO-LOCATION: WHERE'S THE LAIR?

There are many attack maps that show the origins and targets of cyberattacks. However, these tend to be oriented mainly or purely toward volume or real-time. As with the other attributes, in addition to the volume analysis, we looked for where the highest concentrations of evil domains are hosted. By focusing on concentration, we can infer things about where cybercriminals might congregate, where deterrence of cybercrime might be lower, or both.

In terms of volume, we see that the top 10 is a listing of countries with the largest network infrastructures. There are no surprises in this list, except perhaps the distribution. Number 1, The United States, has nearly 40 times the number of malicious domains as Number 10, the UK.

For malicious domain concentration, get your atlas out. The top ten countries, in terms of concentration of malicious domains hosted on IP infrastructure there, aren't necessarily the most familiar. Don't confuse the countries here with the TLDs that correspond to them: for example, Tuvalu, the country, has only two domains in our database hosted there (and one of them has been observed as malicious), but the .tv TLD has many domains registered to it. For the purposes of this list, we included only countries that have more than 1000 hosted. Cambodia (KH) sits significantly higher than the others on the list. Nearly 60% of the sites hosted there have landed on a blacklist.

That the US dominates the volume of malicious domain hosting while remaining below average on concentration of badness speaks to the enormous volume of domains (good and bad) hosted within the country. Meanwhile, Japan hosts a relatively high volume and an above-average concentration of bad (mainly spam) domains. It is possible that this correlates with the higher-than-average numbers of domains associated with free email providers in Japan (even though domain registration and hosting location do not automatically go together). There are a few smaller countries represented above the average for concentration, but the volume of malicious domains hosted in those countries is fairly low (mostly 500 or below).

KEY TAKEAWAYS:

By volume of malicious domains hosted on infrastructure within its national boundaries, the US dominates. By concentration of malicious domains, four countries have malicious domain concentrations over 10%, with one topping 50% (though on low absolute numbers).

	HOSTING COUNTRY	MALICIOUS	%
1	United States (US)	753,128	0.68%
2	Japan (JP)	208,872	4.67%
3	Hong Kong (HK)	53,366	1.67%
4	Russia (RU)	46,084	1.41%
5	Germany (DE)	41,711	0.16%
6	France (FR)	38,595	0.59%
7	Netherlands (NL)	27,065	0.19%
8	China (CN)	23,877	0.41%
9	Canada (CA)	19,475	0.60%
10	United Kingdom (GB)	19,373	0.16%

	HOSTING COUNTRY	%
1	Cambodia (KH)	59.67%
2	Belize (BZ)	15.36%
3	Moldova (MD)	15.26%
4	Seychelles (SC)	13.26%
5	Lebanon (LB)	7.95%
6	Panama (PA)	7.00%
7	Macedonia (MK)	6.16%
8	Bahamas (BS)	4.69%
9	Japan (JP)	4.67%
10	Bosnia/Herzegovina (BA)	4.47%

CONCLUSIONS

This report did, in the aggregate and at scale, what DomainTools customers fighting cybercrime do on smaller data sets every day: we examined domain profile information in order to find patterns and gain insights based on various attributes of registration and hosting.

We observed datapoints that stood out strongly in three of our four attributes. Whois Privacy by onamae, registrant emails from yahoo.co.jp, and Japan as a hosting location, are all in the top 2 for malicious domain volume and concentration rankings for their respective attributes. The .jp TLD doesn't even fall in the top 200 of concentration of malicious domains, whereas every other attribute points, intriguingly, to Japan. We make no assumptions; it may in fact be that there are innocuous or non-obvious explanations for these numbers. In all of the attributes, we identified hotspots of relatively concentrated malicious/suspicious activity.

NEXT STEPS

We found the results enlightening, and we hope they will be informative to all in the fight against global cybercrime. And, because we will repeat the analysis on a regular basis going forward, future editions of the report will show trends and evolutions of these cybercrime concentration patterns.

While it has already provided some interesting insights, we expect to carry out further analysis on this data set, and to incorporate additional data into future editions of the DomainTools Report. Expansions of the data and analysis might include:

- >> Analysis of other attributes in Whois and the domain profile
- >> Analysis of active vs dormant domains
- >> Addition of other blacklists and reputation scores
- >> Closer analysis of individual type of malicious activity (i.e. malware vs phishing)
- >> Analysis across combinations of multiple attributes (for example, domains with more than one attribute associated with above-average rates of malicious activity)

Stay tuned to see what we find next. If you have ideas for additional data points, please email us at **team@domaintools.com.**

For more information about DomainTools' data and products please visit **www.domaintools.com** and request a demo.

DISCLAIMER

This report does not intend to implicate any registries, registrars, privacy providers, email providers, hosting providers, or countries as complicit with cybercrime. It is merely a profile of tendencies and preferences of cybercriminals, and is intended as an illustration of the depth and coverage of DomainTools' data.

ABOUT US

ABOUT DOMAINTOOLS

DomainTools is the leader in domain name, DNS and Internet OSINT-based cyber threat intelligence and cybercrime forensics products and data. With over 14 years of domain name, DNS and related 'cyber fingerprint' data across the Internet, DomainTools helps companies assess security threat risks, profile attackers, investigate online fraud and crimes, and map cyber activity in order to stop attacks.

Our goal is to stop security threats to your organization before they happen, using domain/DNS data, predictive analysis, and monitoring of trends on the Internet. We collect Open Source Intelligence (OSINT) data from many sources, along with historical records, in a central database. We index and analyze the data based on various connection algorithms to deliver actionable intelligence, including domain scoring and forensic mapping.

DomainTools has over 9 billion related DNS data points to build a map of 'who's doing what' on the Internet. Government agencies, Fortune 500 companies and leading security firms use our data as a critical ingredient in their threat investigation and cybercrime forensics work.

OUR HISTORY

For over 14 years, DomainTools has been the most popular Whois research service on the internet because we have the most comprehensive coverage of generic and country code Top Level Domains. We have also collected and stored Whois and related hosting/DNS data to provide the most complete historical records in the industry.

OUR PRODUCTS

In addition to Whois, parsed Whois, Bulk Whois and Whois History products, we offer many other domain related research products to help you create a profile of all domains associated with an organization and all attribution information available through OSINT data.

WORLD'S LARGEST DNS FORENSICS DATABASE**

>> **9 Billion+** current and historical Whois records

>> **4.5 Billion+** IP address change events

>> **1.8 Billion+** Registrar change events

>> **3 billion+** name server change events

>> **580 million+** screenshots

*** These figures are from Q2 2015, but they are inherently out of date, as we add over 4M records a day.*