Mapping the Mal Web

The World's Riskiest Domains

Mapping the Mal Web

By:
Shane Keats, Senior Research Analyst
Dan Nunes, Research Engineer
Paula Greve, Director of Research

CONTENTS

Introduction

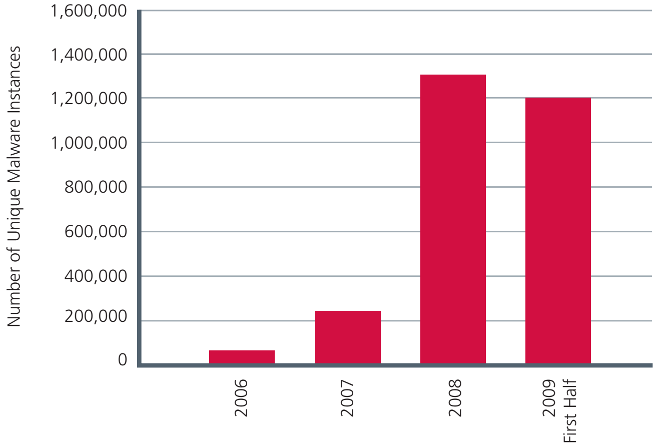
Here is a typical scenario. You hear about a free file-sharing program that will allow you to download copyrighted music for free, or a file that contains cheat codes for your favorite game. You search for the file, select a website that offers it, and begin downloading. What is the chance that the site you select will host some form of malware?

If the file comes from a site that ends in .KR (South Korea)—the chance that the site is risky is 2.8%. If you choose a site that ends in .RO (Romania)—the chance is 21.0%, an increase of 748.0%. One out of five Romanian-registered websites with downloadable files contains some form of potentially unwanted software.

Why is that? When scammers and hackers consider where to register their malicious websites, they take into account a variety of factors.

- **Lowest price**—All things being equal, scammers prefer registrars with inexpensive registrations, volume discounts, and generous refund policies.
- **Lack of regulation**—All things being equal, scammers prefer registrars with "no questions asked" registration. The less information a scammer needs to provide, the better. Similarly, scammers prefer registrars who act slowly, if at all, when notified of malicious domains.
- **Ease of registration**—All things being equal, scammers prefer registrars that allow them to register in bulk. This is especially true of phishers and spammers who need large volumes of sites to offset the high rate of takedowns by top-level domain (TLD) managers.

Malware Growth



According to McAfee Labs™, malware has exploded this year, with almost as much unique malware in the first half of 2009 as in all of 2008.

In less than a generation, the web has grown into an indispensible part of our personal and professional lives. But with each advance, scammers, criminals, and malicious hackers have not been far behind. According to McAfee Labs, malware has exploded this year. And the security industry is in general agreement that the web has grown to become the primary delivery mechanism for malware and other malicious activity.

We should not be surprised. The evolution of malware delivery toolkits has given even the novice hacker the ability to easily create a fake bank site that challenges all but the most careful consumer to tell the difference. The persistence and proliferation of these phishing sites is in itself proof of this; absent of hacker profitability, phishing would disappear. Likewise, the explosion in the use of social networking sites and communication tools has exposed even more consumers to malware authors.

Mapping the mal web

Since 2007, McAfee has analyzed its vast data to create *Mapping the Mal Web*, a portrait of the world's riskiest domains. This is the third annual report to analyze the relative risk of top-level domains (TLD). A TLD is one of the organizers of the web. It is the letter code at the end of a website that tells us where the site is registered. A website with a .DE suffix is registered in Germany while .MX signifies Mexico.

Note: The TLD tells us only where a site is registered. The website itself—its content, the servers, the owners—is often located elsewhere.

Our goals remain simple:

- For the domain registrar and registry community, we hope this report acknowledges those who work hard at reducing scammer registrations and that it spurs others to reach out to these strong leaders to adopt best practices.
- For site owners, we hope the report can be a useful guide to consult when deciding on the public-facing "location" for their registrations.
- Finally, for consumers, we hope the report acts as a reality check, a warning that risk is widely distributed throughout the web and that even the most experienced users need the assistance of a comprehensive security software suite with safe search functionality to more safely search and surf.

Key Findings

The third annual report contains some dramatic reversals with formerly risky domains significantly improving and others becoming "no surfing" zones. But the overall travel advisory for web travelers remains "use the web widely, but use it wisely."

- Overall, an unweighted 5.8% of all domains we tested for this report were risky. In 2007 and 2008, we found 4.1% of websites to be risky—rated red (avoid) and yellow (use caution). Because of changes to the methods used in this year's report, however, we cannot say for *certain* that risk has increased.
- Web-based risk remains widely distributed. Seven of the 20 riskiest TLDs were from the Asia-Pacific region, six were so-called generic TLDs like .COM (Commercial), one was from the Americas, two from Africa, and three were from former Soviet republics.
- The five TLDs with the greatest risky registrations are:
  - .CM (Cameroon) with a weighted risk of 36.7%
  - .COM (Commercial) with a weighted risk of 32.2%
  - .CN (People's Republic of China) with a weighted risk of 23.4%
  - .WS (Samoa) with a weighted risk of 17.8%
  - .INFO (Information) with a weighted risk of 15.8%
- Hong Kong (.HK), which soared in 2008 to become the country TLD with the most risky registrations, dropped dramatically in overall risk to 34th place. Given changes to this year's methodology, this improvement is even more significant.
- Sites registered to TLDs from the Americas are significantly less risky than the web overall, with an average risk of 1.6%. The United States TLD (.US) is the riskiest Americas TLD with a weighted risk of 5.7% and a ranking of 17th worldwide.
- Sites registered to Asia-Pacific TLDs are significantly riskier than the web overall, with an average risk of 13.0%. The People's Republic of China (.CN) is the riskiest TLD in the region at 23.4%. The region also includes Japan (.JP), the web's safest country level TLD.
- Europe, the Middle East, and Africa register, on average, relatively fewer risky sites than the web as a whole at 2.2%. Ireland (.IE) is the region's least risky TLD.
- With a weighted risk of 32.2%, .COM (Commercial—the most heavily trafficked TLD) is the second riskiest TLD and the most risky generic TLD.

The overall travel advisory for web travelers remains "use the web widely, but use it wisely."

- The five TLDs with the least risky registrations, each with 0.3% or fewer domains rated risky, are:

  – Governmental (.GOV)

  – Japan (.JP)

  – Educational (.EDU)

  – Ireland (.IE)

  – Croatia (.HR)

  However, it is important to make two distinctions. First, we note that McAfee bases its ranking on domains rather than individual uniform resource locators (URLs). This is important because McAfee has found numerous examples of malicious *individual* URLs within .HR and .EDU *domains*. Second, we have also found malicious or risky content served from Croatia but registered to non-Croatian TLDs.

Threat-specific findings

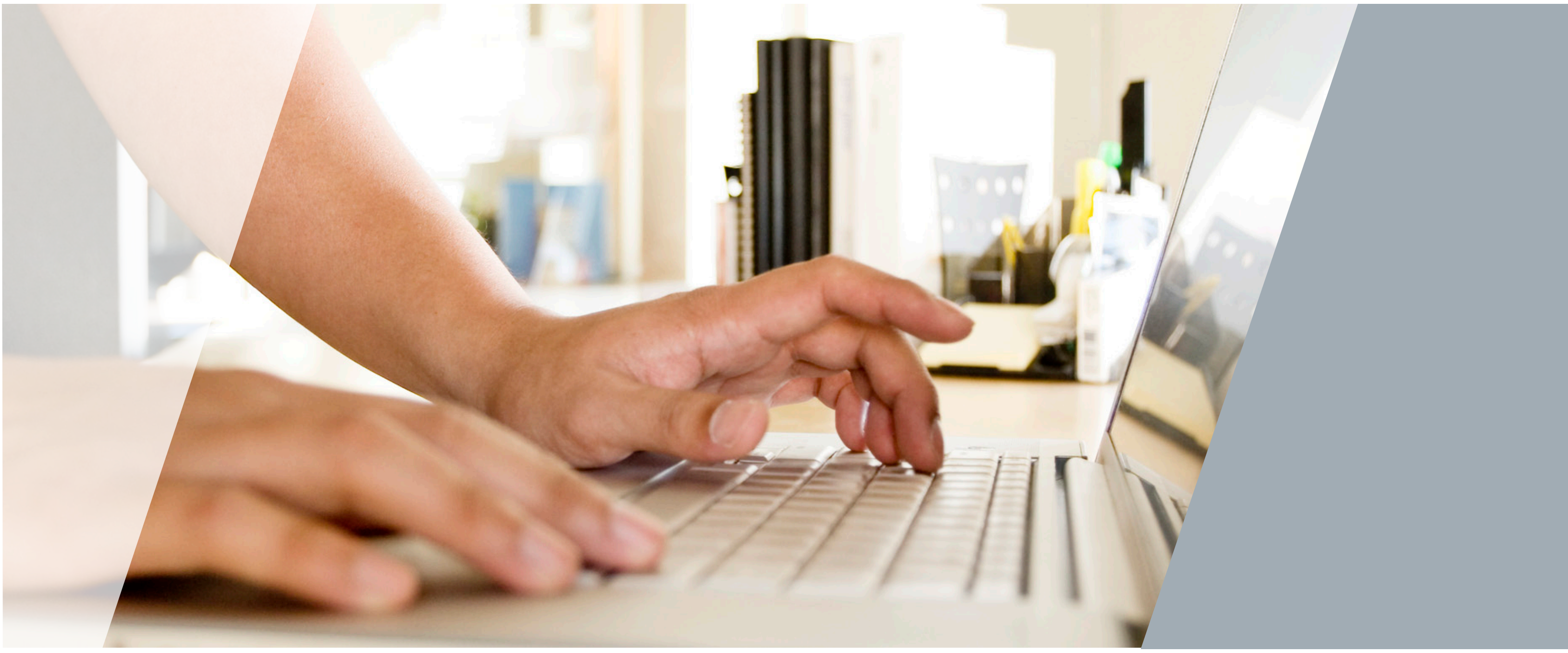
- The risk of registering an email address and receiving spam or high-volume email declined this year. Of the 331,112 domains we tested for email, just 2.8% were at risk for high-volume, highly commercial email, compared to 7.6% last year.

  Note: This does not mean that the volume or amount of spam has decreased, however, only that the number of websites with "spammy signups" declined. Other McAfee research shows the *volume* of spam increasing significantly as botnets (bot networks) proliferate.

- Sites that delivered downloads with viruses, spyware, and adware, or other potentially unwanted programs (PUPs) decreased slightly over last year. Of the 688,861 sites for which we tested downloads, 4.5% of them delivered downloads rated red or yellow for malicious payloads. Last year, 4.7% were rated risky for downloads.

  Note: This does not mean that there are fewer of them out there—but rather that they are getting more difficult to find via standard testing measures. As noted previously, McAfee Labs has seen almost as much unique malware in the first half of 2009 as it did in all of 2008.

- Romania (.RO) was the riskiest TLD for downloads, with 21.0% of domains with downloads testing risky for those files. .INFO (Information) was the riskiest email TLD with 17.2% of sites with sign-ups resulting in unwanted email.



Changes to This Year's Report

Of the slightly more than 27 million domains we rated for this report, 5.8% were risky. In 2007 and 2008, we found 4.1% of websites to be risky—rated red (avoid) and yellow (use caution). However, we cannot automatically conclude that the web has gotten riskier because of a change we made to our methodology.

The top five least risky domains are:

- .GOV
- .JP
- .EDU
- .IE
- .HR

Adding McAfee® TrustedSource™ ratings

This is the first year this study includes data from McAfee TrustedSource technology, a web reputation service focused on protecting businesses. The TrustedSource reputation system actively seeks out risky parts of the web. That means that its data for a particular TLD may be disproportionately risky. This is important when comparing this year's results to prior years.

One possibility is that this new data reflects risky parts of the web that have been in existence for some time. Another possibility is that the web has, in fact, gotten riskier. Additional tests over time will help us better understand these changes.

Changing how we rank

Another change is the way we rank different TLDs. In earlier reports, we conducted a simple ratio analysis and then ranked those with the highest "risk ratios" at the top.

In an effort to better distinguish the risk faced when visiting massive TLDs like .COM (Commercial) compared to smaller TLDs like .PH (Philippines), we have adjusted the calculation we use to rank TLDs. In general, this change has caused some larger TLDs with many risky sites to move up in the "riskier" rankings.

These changes were made as a result of extensive feedback from the registry community to the 2008 report, and we hope the result is a more accurate assessment and presentation of this map of risk.

More information about these changes can be found in the methodology section.

We expect more changes to the report next year, as the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation that oversees domain system management, debates major additions to the current, tightly proscribed list of available TLDs.

Methodology

As noted, this is the third year McAfee has issued the *Mapping the Mal Web* report and changes in methodology were employed. As in previous years, this report uses data from McAfee SiteAdvisor® technology. This technology crawls the web and tests domains for a variety of security threats.

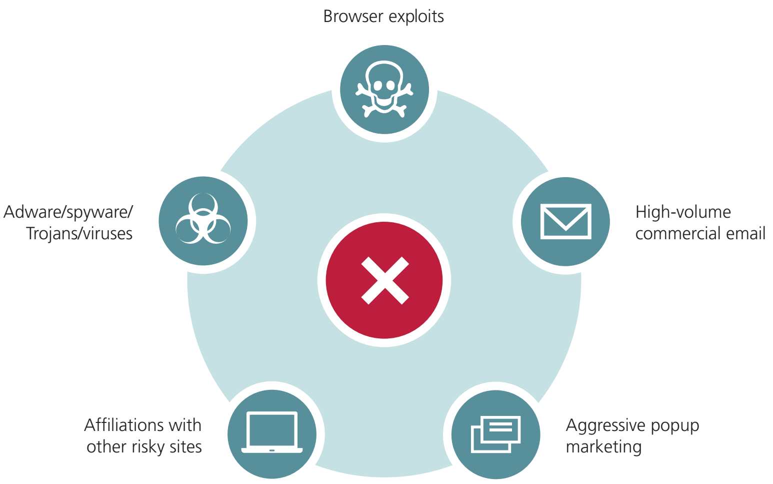
McAfee SiteAdvisor methodology

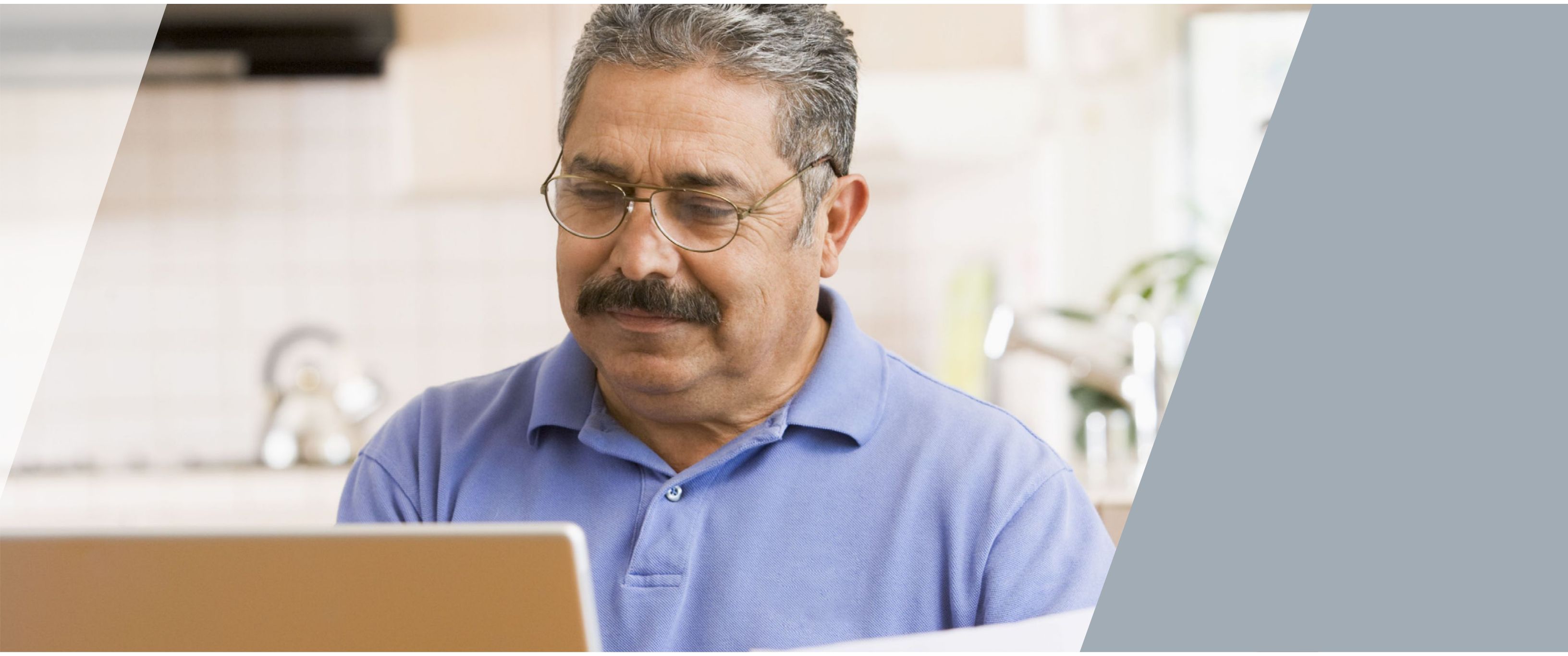
- **Websites** are tested for browser exploits, phishing, and excessive popups. Browser exploits, also known as drive-by-downloads, enable viruses, keystroke loggers (keyloggers), or spyware to install on a consumer's computer without their consent and often without their knowledge. We also examine outbound links to see if they direct visitors to other sites rated risky by McAfee.
- **Downloads** are analyzed by installing software on our test computers and checking for viruses and any bundled adware, spyware or other potentially unwanted programs. McAfee does not test individual files offered via peer-to-peer (P2P) and BitTorrent file-sharing programs or content platforms like iTunes or Rhapsody. We do test files found for download from many freeware and shareware sites, and we test P2P and BitTorrent client software.
- **Sign-up forms** are completed using a one-time use email address so the volume and "spamminess" of any subsequent email can be tracked. Spamminess refers to the commercial content of email, as well as the use of tactics to trick spam filtering software.

Red ratings are given to websites that fail one or more of these tests. Yellow ratings are given to sites that merit caution before using.

SiteAdvisor software tests for a variety of security threats and warns you of a website's safety rating before you access it.

Security Threats Tested by SiteAdvisor


Browser exploits
Adware/spyware/ Trojans/viruses
High-volume commercial email
Affiliations with other risky sites
Aggressive popup marketing



The top five riskiest domains are:

- .CM
- .COM
- .CN
- .WS
- .INFO

McAfee TrustedSource methodology

As previously mentioned, this is the first report incorporating data from McAfee TrustedSource technology. TrustedSource is a comprehensive Internet reputation system that analyzes web traffic patterns, site behavior, hosted content, and more, to provide insight into site security risk. TrustedSource data is collected from more than 150 million sensors located in more than 120 countries. These sensors—individual computers, gateway network devices, endpoint software, in-the-cloud hosted services—come from consumers, small- and medium-size businesses, enterprise customers, educational institutions, and governmental agencies.

Like SiteAdvisor technology, TrustedSource tests individual sites for malicious or risky content and behavior. TrustedSource goes beyond those tests, however, to analyze what might be called site context—how the site is registered, referenced, used, and accessed. It also correlates available information from other threat vectors, including email traffic, network intrusion traffic, and malware analysis, to arrive at a comprehensive reputation score for a website.

The rankings

There are currently 280 top-level domains. For this report, we looked at 104 top-level domains, 30 more than in our previous report. As before, we restricted our analysis to top-level domains for which we had at least 2,000 site test results. For our threat-specific analysis, we also limited our rankings to TLDs for which we had 2,000 or more threat-specific test results. In other words, a TLD needed to have 2,000 or more domains that had been tested for email or downloads in order to be ranked. (This is a change from prior reports when we ranked the email and download risk for all TLDs in our study, even if we had only a small number of threat-specific test results.)

In the 2008 report, we based our rankings on test results for 9.9 million domains. This year, our rankings are based on 27,002,629 domain ratings, an increase of 173.0%. Of these, a little more than 37.0% came from McAfee TrustedSource technology.

In the 2008 report, the entire risk rating came from the ratio of a TLD's risky sites to the TLD's total sites. A TLD with 10 risky sites out of 100 total domains would have a risk rating of 10.0%. A TLD with 100 risky sites out of 10,000 would have a risk rating of 1.0%.

For this year's report, the risk rating was weighted. Half of the rating came from the ratio of a TLD's risky sites to its total sites and half from the ratio of a TLD's risky sites to all risky sites.

Example: A TLD with 100 risky sites out of 10,000, where those 100 risky sites were part of 200 total risky sites across all TLDs [(50.0%x100/10,000)+(50.0%x100/200)=25.5%] would be ranked riskier than the TLD with 10 risky sites out of 100 [(50.0%x(10/100)+(50.0%x (10/200)=7.5%].

This change in ranking methodology means that, in a few cases, a TLD with many risky sites but a lower overall risk rating, can be ranked higher (riskier) than a small TLD with a relatively higher proportion of risky sites.

Example: 6.0% of the 15.4 million .COM (Commercial) sites we analyzed were rated as risky, but when we weight .COM's risk by the number of risky sites worldwide, its ratio increases to 32.2%. By contrast, 26.1% of the 8,700 Philippines (.PH) websites we tested were risky, but when we weight that risk by their share of the number of risky sites worldwide, the ratio decreases to 13.1%.

We believe this new ranking methodology better reflects the level of risk a typical user faces when traveling the entire web.

	2008 METHOD		2009 METHOD	
	TLD #1	TLD #2	TLD #1	TLD #2
Risky Sites	10	100	10	100
Total Sites	100	10,000	100	10,000
All Risky Sites	Not relevant	Not relevant	200	200
Risk Rating	10.0%	1.0%	7.5%	25.5%

Some Caveats About the Rankings

Weighting by traffic

Our risk ratings are not weighted by the traffic a TLD receives. We don't distinguish between a very popular TLD that receives much more traffic to its risky sites and a less popular TLD that receives less.

Weighting by type of risk

Our ratings do not distinguish between types of risk. A site sign-up that results in spam email is weighted equally with a site with a virus-infected download. We discuss this in more detail later in the report.

Weighting by top-level domain size

McAfee does not have access to each registrar's "zone file" or list of all registered public domains. We are therefore unable, in certain cases, to assess the percentage of a TLD's public websites for which we have ratings. However, by restricting ourselves to ranking only those TLDs for which we have a large sample, we believe our overall risk assessments and, therefore, our rankings are statistically significant.

Example: We tested 17,630 .SG (Singapore) domains. Of those, we found 1,607 to be risky. If we assume that the total number of domains for .SG is 175,000, we have tested approximately 10.0% of the total .SG population. At a 95.0% confidence level, our confidence interval is +/- 0.4%. In other words, we can be 95.0% confident that the actual percentage of risky sites is between 8.7% and 9.5%. If we assume the total population of .SG is an order of magnitude larger (1,750,000), our confidence interval increases slightly to 0.42%.

The confidence interval—the margin of error—may be somewhat higher due to TrustedSource technology's tendency to seek out risky sites.

We remind readers that a TLD's risk rank is weighted and is not based solely on that TLD's ratio of risky sites to its total sites.

Domains versus URLs

SiteAdvisor technology rates entire domains, not individual URLs within that domain. If we find exploit code on 1.foo.bar but not on 2.foo.bar, we rate all of foo.bar as risky. TrustedSource technology rates both individual URLs and entire domains. For consistency, this study only incorporates domain-level TrustedSource ratings.

Delisting risky sites

We know that TLD operators are sometimes under contractual obligations that prevent them from being able to delist certain types of domains that McAfee may consider risky. Moreover, website behavior that leads to delisting by one registry may not be considered inappropriate in another. McAfee does not distinguish among these different rules.

Other

Our analysis does not distinguish among minor, moderate, and trivial threats. In other words, a domain rated yellow for a slightly risky download counts as heavily as one rated red for hosting drive-by-download exploit code.

Our rankings do not take into account domains that we have not tested.

Breakdown of Rankings

Overall rankings

COUNTRY OR NAME	REGION	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Cameroon	EMEA	CM	1	36.7%	69.7%	n/a	n/a	82,087	57,210
Commercial	Generic	COM	2	32.2%	6.0%	5.3%	5.5%	15,440,225	918,873
People's Republic of China	APAC	CN	3	23.4%	34.5%	11.8%	3.7%	561,517	193,917
Samoa	APAC	WS	4	17.8%	34.6%	3.8%	5.8%	43,829	15,178
Information	Generic	INFO	5	15.8%	22.8%	11.7%	7.5%	601,629	137,403
Philippines	APAC	PH	6	13.1%	26.1%	7.7%	2.1%	8,707	2,272
Network	Generic	NET	7	5.8%	5.9%	6.3%	4.4%	1,554,136	91,049
Former Soviet Union	EMEA	SU	8	5.2%	10.3%	n/a	n/a	7,349	754
Russia	EMEA	RU	9	4.6%	7.6%	6.0%	4.5%	344,434	26,234
Singapore	APAC	SG	10	4.6%	9.1%	0.3%	0.3%	17,630	1,607
Organization	Generic	ORG	11	4.2%	4.8%	2.3%	1.8%	1,179,864	57,148
São Tomé and Príncipe	EMEA	ST	12	3.8%	7.5%	n/a	n/a	10,449	779
Business	Generic	BIZ	13	3.6%	6.8%	4.7%	4.9%	111,492	7,557
Cocos (Keeling) Islands	APAC	CC	14	3.3%	6.5%	3.8%	3.7%	32,430	2,108
Kazakhstan	EMEA	KZ	15	3.1%	6.1%	n/a	n/a	3,155	194
Families and Individuals	Generic	NAME	16	3.1%	6.1%	6.1%	4.2%	8,116	497
United States	Americas	US	17	3.1%	5.7%	2.1%	2.1%	109,152	6,231
Pakistan	APAC	PK	18	2.8%	5.5%	n/a	n/a	4,335	238
Tokelau	APAC	TK	19	2.3%	4.4%	1.4%	10.1%	85,310	3,754
Romania	EMEA	RO	20	2.2%	4.3%	6.8%	5.6%	52,717	2,280
Venezuela	Americas	VE	21	2.1%	4.1%	0.5%	1.5%	6,601	272
India	APAC	IN	22	2.0%	3.9%	3.1%	2.1%	40,218	1,568
Armenia	EMEA	AM	23	2.0%	3.9%	n/a	n/a	2,104	83
Niue	APAC	NU	24	1.9%	3.7%	1.4%	2.1%	36,709	1,369
Mobile Devices	Generic	MOBI	25	1.7%	3.5%	n/a	n/a	5,781	201
Laos	APAC	LA	26	1.6%	3.2%	n/a	n/a	3,563	115
Spain	EMEA	ES	27	1.6%	3.0%	2.0%	0.6%	99,254	2,936
South Korea	APAC	KR	28	1.5%	3.0%	2.4%	2.6%	65,054	1,934
Belarus	EMEA	BY	29	1.3%	2.6%	n/a	n/a	3,813	98
Belize	Americas	BZ	30	1.2%	2.5%	n/a	n/a	3,590	89
Israel	EMEA	IL	31	1.2%	2.4%	0.7%	0.5%	26,973	655
Thailand	APAC	TH	32	1.1%	2.2%	1.0%	0.6%	7,958	178
Tonga	APAC	TO	33	1.1%	2.2%	2.3%	3.0%	10,451	225
Hong Kong	APAC	HK	34	1.1%	2.1%	19.2%	1.2%	16,870	358
Ascension Island	EMEA	AC	35	1.0%	2.1%	n/a	n/a	8,671	178
Ukraine	EMEA	UA	36	1.0%	2.0%	3.2%	1.7%	33,884	673
Iran	EMEA	IR	37	0.9%	1.9%	2.1%	n/a	15,490	288
Tuvalu	APAC	TV	38	0.9%	1.8%	2.4%	3.0%	40,270	721
Vietnam	APAC	VN	39	0.9%	1.8%	2.0%	1.2%	8,218	150
Turks and Caicos Islands	Americas	TC	40	0.9%	1.7%	n/a	n/a	8,842	153
Peru	Americas	PE	41	0.9%	1.7%	n/a	n/a	4,627	80
Saudi Arabia	EMEA	SA	42	0.9%	1.7%	n/a	n/a	2,406	41
Bulgaria	EMEA	BG	43	0.8%	1.7%	2.0%	1.9%	15,847	266
Lithuania	EMEA	LT	44	0.8%	1.7%	0.6%	0.5%	9,536	159
Slovakia	EMEA	SK	45	0.8%	1.5%	0.7%	3.9%	37,529	580
Bosnia	EMEA	BA	46	0.8%	1.5%	n/a	n/a	2,605	40

Overall rankings—continued

COUNTRY OR NAME	REGION	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Turkey	EMEA	TR	47	0.7%	1.3%	0.8%	0.5%	30,629	397
South Georgia and the South Sandwich Islands	EMEA	GS	48	0.6%	1.3%	n/a	n/a	4,561	59
Ecuador	Americas	EC	49	0.6%	1.3%	n/a	n/a	2,338	30
Argentina	Americas	AR	50	0.6%	1.2%	1.0%	1.0%	74,693	886
Trinidad and Tobago	Americas	TT	51	0.6%	1.2%	n/a	n/a	3,713	45
Taiwan	APAC	TW	52	0.6%	1.1%	1.5%	1.0%	49,475	565
Hungary	EMEA	HU	53	0.6%	1.1%	1.0%	1.6%	63,513	717
Czech Republic	EMEA	CZ	54	0.6%	1.1%	0.9%	1.0%	85,649	949
United Kingdom	EMEA	UK	55	0.6%	0.7%	0.5%	0.5%	802,178	5,923
Indonesia	APAC	ID	56	0.6%	1.1%	0.6%	n/a	5,041	56
Guernsey	EMEA	GG	57	0.6%	1.1%	n/a	n/a	10,130	111
East Timor	APAC	TL	58	0.5%	1.1%	n/a	n/a	4,783	52
European Union	EMEA	EU	59	0.5%	1.0%	2.2%	n/a	66,916	673
Poland	EMEA	PL	60	0.5%	0.9%	1.2%	1.0%	276,920	2,401
France	EMEA	FR	61	0.5%	0.9%	1.3%	1.2%	231,320	2,046
Nauru	APAC	NR	62	0.5%	1.0%	n/a	n/a	7,230	73
French Southern and Antarctic Lands	EMEA	TF	63	0.5%	0.9%	n/a	n/a	2,111	20
Canada	Americas	CA	64	0.5%	0.9%	0.6%	0.7%	154,048	1,328
United Arab Emirates	EMEA	AE	65	0.5%	0.9%	n/a	n/a	3,601	34
Federated States of Micronesia	APAC	FM	66	0.4%	0.9%	n/a	n/a	3,803	33
Saint Helena	EMEA	SH	67	0.4%	0.8%	n/a	n/a	8,474	71
Colombia	Americas	CO	68	0.4%	0.8%	0.2%	0.3%	7,405	62
Mexico	Americas	MX	69	0.4%	0.8%	0.6%	0.9%	47,276	369
Brazil	Americas	BR	70	0.4%	0.7%	0.8%	0.9%	277,436	1,891
Latvia	EMEA	LV	71	0.4%	0.8%	1.3%	0.7%	8,779	70
Yugoslavia	EMEA	YU	72	0.4%	0.8%	0.5%	0.7%	4,564	36
Greece	EMEA	GR	73	0.4%	0.8%	0.4%	0.4%	35,030	267
Christmas Island	APAC	CX	74	0.4%	0.8%	1.8%	2.6%	5,553	42
Uruguay	Americas	UY	75	0.4%	0.7%	n/a	n/a	2,949	22
Estonia	EMEA	EE	76	0.4%	0.7%	0.5%	2.3%	10,349	76
Norway	EMEA	NO	77	0.4%	0.7%	0.1%	0.2%	47,417	328
Italy	EMEA	IT	78	0.3%	0.6%	1.6%	1.0%	286,926	1,663
Slovenia	EMEA	SI	79	0.3%	0.7%	0.2%	0.3%	9,725	65
Malaysia	APAC	MY	80	0.3%	0.7%	0.4%	0.3%	12,973	85
Belgium	EMEA	BE	81	0.3%	0.6%	0.8%	1.5%	113,730	694
Chile	Americas	CL	82	0.3%	0.6%	0.6%	0.7%	44,194	280
Germany	EMEA	DE	83	0.3%	0.3%	0.6%	1.0%	1,428,423	4,625
Netherlands	EMEA	NL	84	0.3%	0.4%	0.5%	1.1%	543,937	2,443
Finland	EMEA	FI	85	0.3%	0.6%	0.1%	0.1%	29,914	171
Portugal	EMEA	PT	86	0.3%	0.6%	0.5%	0.4%	34,409	193
Iceland	EMEA	IS	87	0.3%	0.5%	0.3%	0.2%	5,837	31
Sweden	EMEA	SE	88	0.3%	0.5%	0.3%	0.2%	95,349	467
Austria	EMEA	AT	89	0.2%	0.4%	0.5%	0.6%	126,404	555
Liechtenstein	EMEA	LI	90	0.2%	0.5%	n/a	n/a	2,828	13
Denmark	EMEA	DK	91	0.2%	0.4%	0.3%	0.6%	145,337	596
Travel and Tourism Industry	Generic	TRAVEL	92	0.2%	0.4%	n/a	n/a	2,061	9
Australia	APAC	AU	93	0.2%	0.4%	0.3%	0.2%	219,980	790

Overall rankings—continued

COUNTRY OR NAME	REGION	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
New Zealand	APAC	NZ	94	0.2%	0.4%	0.3%	0.6%	50,708	201
Switzerland	EMEA	CH	95	0.2%	0.3%	0.9%	0.5%	197,361	600
South Africa	EMEA	ZA	96	0.2%	0.3%	0.5%	0.5%	60,400	198
Vanuatu	APAC	VU	97	0.2%	0.3%	0.9%	1.1%	13,604	42
Luxembourg	EMEA	LU	98	0.1%	0.3%	n/a	n/a	5,750	16
Catalan	Sponsored	CAT	99	0.1%	0.3%	n/a	n/a	3,460	9
Croatia	EMEA	HR	100	0.1%	0.3%	0.5%	0.5%	18,781	47
Ireland	EMEA	IE	101	0.1%	0.2%	0.3%	0.1%	27,683	65
Educational	Generic	EDU	102	0.1%	0.2%	0.4%	0.3%	9,584	20
Japan	APAC	JP	103	0.1%	0.1%	0.1%	0.4%	395,615	446
Governmental	Generic	GOV	104	0.0%	0.0%	0.1%	0.0%	4,345	2

Americas region

COUNTRY	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Unweighted Risk Ratio (Worldwide TLDs)				5.8%				
Unweighted Risk Ratio (Americas TLDs)				1.6%				
United States	US	17	3.1%	5.7%	2.1%	2.1%	109,152	6,231
Venezuela	VE	21	2.1%	4.1%	0.5%	1.5%	6,601	272
Belize	BZ	30	1.2%	2.5%	n/a	n/a	3,590	89
Turks and Caicos Islands	TC	40	0.9%	1.7%	n/a	n/a	8,842	153
Peru	PE	41	0.9%	1.7%	n/a	n/a	4,627	80
Ecuador	EC	49	0.6%	1.3%	n/a	n/a	2,338	30
Argentina	AR	50	0.6%	1.2%	1.0%	1.0%	74,693	886
Trinidad and Tobago	TT	51	0.6%	1.2%	n/a	n/a	3,713	45
Canada	CA	64	0.5%	0.9%	0.6%	0.7%	154,048	1,328
Colombia	CO	68	0.4%	0.8%	0.2%	0.3%	7,405	62
Mexico	MX	69	0.4%	0.8%	0.6%	0.9%	47,276	369
Brazil	BR	70	0.4%	0.7%	0.8%	0.9%	277,436	1,891
Uruguay	UY	75	0.4%	0.7%	n/a	n/a	2,949	22
Chile	CL	82	0.3%	0.6%	0.6%	0.7%	44,194	280

- Risky sites registered with the .US (United States) TLD are fairly evenly distributed among malicious activity, spam activity, and phishing. Of course, the United States itself is host to a great many more malicious or risky sites than just those with the .US TLD.
- .VE (Venezuela) registered sites tend to be risky for malicious activity like exploits, viruses, and re-directs to drive-by sites rather than for spam or phishing.
- McAfee has seen a recent uptick in phishing sites registered in Belize (.BZ).

Asia-Pacific (APAC) region

COUNTRY	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Unweighted Risk Ratio (Worldwide TLDs)				5.8%				
Unweighted Risk Ratio (APAC TLDs)				13.0%				
People's Republic of China	CN	3	23.4%	34.5%	11.8%	3.7%	561,517	193,917
Samoa	WS	4	17.8%	34.6%	3.8%	5.8%	43,829	15,178
Philippines	PH	6	13.1%	26.1%	7.7%	2.1%	8,707	2,272
Singapore	SG	10	4.6%	9.1%	0.3%	0.3%	17,630	1,607
Cocos (Keeling) Islands	CC	14	3.3%	6.5%	3.8%	3.7%	32,430	2,108
Pakistan	PK	18	2.8%	5.5%	n/a	n/a	4,335	238
Tokelau	TK	19	2.3%	4.4%	1.4%	10.1%	85,310	3,754
India	IN	22	2.0%	3.9%	3.1%	2.1%	40,218	1,568
Niue	NU	24	1.9%	3.7%	1.4%	2.1%	36,709	1,369
Laos	LA	26	1.6%	3.2%	n/a	n/a	3,563	115
South Korea	KR	28	1.5%	3.0%	2.4%	2.6%	65,054	1,934
Thailand	TH	32	1.1%	2.2%	1.0%	0.6%	7,958	178
Tonga	TO	33	1.1%	2.2%	2.3%	3.0%	10,451	225
Hong Kong	HK	34	1.1%	2.1%	19.2%	1.2%	16,870	358
Tuvalu	TV	38	0.9%	1.8%	2.4%	3.0%	40,270	721
Vietnam	VN	39	0.9%	1.8%	2.0%	1.2%	8,218	150
Taiwan	TW	52	0.6%	1.1%	1.5%	1.0%	49,475	565
Indonesia	ID	56	0.6%	1.1%	0.6%	n/a	5,041	56
East Timor	TL	58	0.5%	1.1%	n/a	n/a	4,783	52
Nauru	NR	62	0.5%	1.0%	n/a	n/a	7,230	73
Federated States of Miconesia	FM	66	0.4%	0.9%	n/a	n/a	3,803	33
Christmas Island	CX	74	0.4%	0.8%	1.8%	2.6%	5,553	42
Malaysia	MY	80	0.3%	0.7%	0.4%	0.3%	12,973	85
Australia	AU	93	0.2%	0.4%	0.3%	0.2%	219,980	790
New Zealand	NZ	94	0.2%	0.4%	0.3%	0.6%	50,708	201
Vanuatu	VU	97	0.2%	0.3%	0.9%	1.1%	13,604	42
Japan	JP	103	0.1%	0.1%	0.1%	0.4%	395,615	446

- The risky or malicious activity associated with sites registered with the .CN (China) TLD is overwhelmingly related to spam sites as opposed to malicious downloads.
- By contrast, Samoan (.WS) registered domains are rated risky primarily for phishing and malicious download activity.
- Philippines (.PH) registered sites are more similar to China than Samoa, with the preponderance of risk weighted towards spam and phishing than risk related to downloads.
- Singapore (.SG) registered sites were evenly distributed between spam and download activity, but the preponderance of the ratings were yellow (use caution) rather than red (avoid).

Europe, Middle East, and Africa (EMEA) region

COUNTRY	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Unweighted Risk Ratio (Worldwide TLDs)				5.8%				
Unweighted Risk Ratio (EMEA TLDs)				2.2%				
Cameroon	CM	1	36.7%	69.7%	n/a	n/a	82,087	57,210
Former Soviet Union	SU	8	5.2%	10.3%	n/a	n/a	7,349	754
Russia	RU	9	4.6%	7.6%	6.0%	4.5%	344,434	26,234
São Tomé and Príncipe	ST	12	3.8%	7.5%	n/a	n/a	10,449	779
Kazakhstan	KZ	15	3.1%	6.1%	n/a	n/a	3,155	194
Romania	RO	20	2.2%	4.3%	6.8%	5.6%	52,717	2,280
Armenia	AM	23	2.0%	3.9%	n/a	n/a	2,104	83
Spain	ES	27	1.6%	3.0%	2.0%	0.6%	99,254	2,936
Belarus	BY	29	1.3%	2.6%	n/a	n/a	3,813	98
Israel	IL	31	1.2%	2.4%	0.7%	0.5%	26,973	655
Ascension Island	AC	35	1.0%	2.1%	n/a	n/a	8,671	178
Ukraine	UA	36	1.0%	2.0%	3.2%	1.7%	33,884	673
Iran	IR	37	0.9%	1.9%	2.1%	n/a	15,490	288
Saudi Arabia	SA	42	0.9%	1.7%	n/a	n/a	2,406	41
Bulgaria	BG	43	0.8%	1.7%	2.0%	1.9%	15,847	266
Lithuania	LT	44	0.8%	1.7%	0.6%	0.5%	9,536	159
Slovakia	SK	45	0.8%	1.5%	0.7%	3.9%	37,529	580
Bosnia	BA	46	0.8%	1.5%	n/a	n/a	2,605	40
Turkey	TR	47	0.7%	1.3%	0.8%	0.5%	30,629	397
South Georgia and the South Sandwich Islands	GS	48	0.6%	1.3%	n/a	n/a	4,561	59
Hungary	HU	53	0.6%	1.1%	1.0%	1.6%	63,513	717
Czech Republic	CZ	54	0.6%	1.1%	0.9%	1.0%	85,649	949
United Kingdom	UK	55	0.6%	0.7%	0.5%	0.5%	802,178	5,923
Guernsey	GG	57	0.6%	1.1%	n/a	n/a	10,130	111
European Union	EU	59	0.5%	1.0%	2.2%	n/a	66,916	673
Poland	PL	60	0.5%	0.9%	1.2%	1.0%	276,920	2,401
France	FR	61	0.5%	0.9%	1.3%	1.2%	231,320	2,046
French Southern and Antarctic Lands	TF	63	0.5%	0.9%	n/a	n/a	2,111	20
United Arab Emirates	AE	65	0.5%	0.9%	n/a	n/a	3,601	34
Saint Helena	SH	67	0.4%	0.8%	n/a	n/a	8,474	71
Latvia	LV	71	0.4%	0.8%	1.3%	0.7%	8,779	70
Yugoslavia	YU	72	0.4%	0.8%	0.5%	0.7%	4,564	36
Greece	GR	73	0.4%	0.8%	0.4%	0.4%	35,030	267
Estonia	EE	76	0.4%	0.7%	0.5%	2.3%	10,349	76
Norway	NO	77	0.4%	0.7%	0.1%	0.2%	47,417	328
Italy	IT	78	0.3%	0.6%	1.6%	1.0%	286,926	1,663
Slovenia	SI	79	0.3%	0.7%	0.2%	0.3%	9,725	65
Belgium	BE	81	0.3%	0.6%	0.8%	1.5%	113,730	694
Germany	DE	83	0.3%	0.3%	0.6%	1.0%	v	4,625
Netherlands	NL	84	0.3%	0.4%	0.5%	1.1%	543,937	2,443
Finland	FI	85	0.3%	0.6%	0.1%	0.1%	29,914	171
Portugal	PT	86	0.3%	0.6%	0.5%	0.4%	34,409	193
Iceland	IS	87	0.3%	0.5%	0.3%	0.2%	5,837	31
Sweden	SE	88	0.3%	0.5%	0.3%	0.2%	95,349	467
Austria	AT	89	0.2%	0.4%	0.5%	0.6%	126,404	555

- Risk associated with Cameroon (.CM) registered sites tends to be for malicious download activity rather than email or phishing. Also, some scammers have exploited the fact that .CM is one of the most common "typo" errors made by consumers trying to directly navigate to .COM (Commercial).
- Risky registrations using the former Soviet Union (.SU) TLD are evenly distributed between phishing and risky download activity.
- By contrast, Russian (.RU) registered site risk is distributed in a roughly 3:2:1 ratio for malicious downloads, phishing and spam.
- It appears to be mainly phishers who are targeting São Tomé and Príncipe (.ST) registered domains.

Europe, Middle East, and Africa (EMEA) region—continued

COUNTRY	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Liechtenstein	LI	90	0.2%	0.5%	n/a	n/a	2,828	13
Denmark	DK	91	0.2%	0.4%	0.3%	0.6%	145,337	596
Switzerland	CH	95	0.2%	0.3%	0.9%	0.5%	197,361	600
South Africa	ZA	96	0.2%	0.3%	0.5%	0.5%	60,400	198
Luxembourg	LU	98	0.1%	0.3%	n/a	n/a	5,750	16
Croatia	HR	100	0.1%	0.3%	0.5%	0.5%	18,781	47
Ireland	IE	101	0.1%	0.2%	0.3%	0.1%	27,683	65

Generic and sponsored top-level domains

NAME	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Commercial	COM	2	32.2%	6.0%	5.3%	5.5%	15,440,225	918,873
Information	INFO	5	15.8%	22.8%	11.7%	7.5%	601,629	137,403
Network	NET	7	5.8%	5.9%	6.3%	4.4%	1,554,136	91,049
Organization	ORG	11	4.2%	4.8%	2.3%	1.8%	1,179,864	57,148
Business	BIZ	13	3.6%	6.8%	4.7%	4.9%	111,492	7,557
Families and Individuals	NAME	16	3.1%	6.1%	6.1%	4.2%	8,116	497
Mobile Devices	MOBI	25	1.7%	3.5%	n/a	n/a	5,781	201
Travel and Tourism Industry	TRAVEL	92	0.2%	0.4%	n/a	n/a	2,061	9
Catalan	CAT	99	0.1%	0.3%	n/a	n/a	3,460	9
Educational	EDU	102	0.1%	0.2%	0.4%	0.3%	9,584	20
Governmental	GOV	104	0.0%	0.0%	0.1%	0.0%	4,345	2

- As indicated, the raw ratio of risky .COM (Commercial) sites to all .COM sites is 6.0%—above the worldwide average of 5.8%. But, because .COM accounts for such a large proportion of all risky sites, its weighted risk ratio climbs to 32.2%, giving it the dubious distinction of second place to Cameroon (.CM).
- The risk associated with .INFO (Information) registered domains is primarily spam related.
- By contrast, the risk associated with .BIZ (Business) registered domains is primarily malicious download activity.
- We note that some .EDU (Educational) sites have many risky URLs that do not affect the overall rating of that domain. For example, we may find risky activity on universityXYZ.edu/risky_download and universityXYZ.edu/malicious_redirect, but because the vast majority of URLs associated with universityXYZ.edu are not risky, our overall score for the site is green (safe).

Email risk

COUNTRY OR NAME	TLD	DOMAINS WITH RISKY EMAIL PRACTICES	EMAIL DOMAINS TESTED
Information	INFO	17.2%	3,029
Commercial	COM	3.9%	207,415
Network	NET	1.9%	16,389
Switzerland	CH	1.1%	2,114
Denmark	DK	0.8%	2,096
Organization	ORG	0.8%	21,142
Russia	RU	0.6%	3,419
Italy	IT	0.6%	3,406
Canada	CA	0.6%	2,929
Poland	PL	0.4%	2,687
Brazil	BR	0.4%	4,078
United Kingdom	UK	0.3%	14,430
Bosnia	BA	0.3%	5,687
France	FR	0.2%	2,818
Netherlands	NL	0.2%	6,828
Germany	DE	0.2%	14,959
Japan	JP	0.1%	2,062

McAfee conducted some threat specific analysis. Of those TLDs for which we had 2,000 or more email tests, we measured the percentage of those email tests that were risky.

Download risk

Of those TLDs for which we had 2,000 or more download tests, we measured the percentage of those download tests that were risky.

COUNTRY OR NAME	TLD	DOMAINS WITH RISKY DOWNLOADS	DOWNLOAD DOMAINS TESTED
Romania	RO	21.0%	2,941
People's Republic of China	CN	18.6%	16,356
Information	INFO	15.2%	7,494
Business	BIZ	6.8%	2,749
Network	NET	5.2%	56,162
Commercial	COM	5.1%	326,600
France	FR	4.0%	16,606
Russia	RU	3.9%	35,212
United States	US	3.5%	3,460
European Union	EU	3.4%	2,265
Belgium	BE	3.3%	2,543
Slovakia	SK	3.2%	2,285
Netherlands	NL	3.0%	9,669
Hungary	HU	3.0%	3,403
Spain	ES	2.8%	3,358
South Korea	KR	2.8%	4,554
Turkey	TR	2.8%	2,107
Poland	PL	2.7%	10,500
Organization	ORG	2.4%	46,151
Czech Republic	CZ	2.4%	7,096
Ukraine	UA	2.3%	3,920
Argentina	AR	1.9%	3,467
Taiwan	TW	1.8%	3,245
Brazil	BR	1.8%	11,448
Sweden	SE	1.8%	2,503
Italy	IT	1.7%	14,911
Denmark	DK	1.6%	3,975
United Kingdom	UK	1.6%	14,825
Switzerland	CH	1.2%	4,761
Australia	AU	1.1%	4,235
Austria	AT	1.0%	2,723
Canada	CA	1.0%	3,793
Germany	DE	0.9%	41,033
Japan	JP	0.5%	9,660

Red versus yellow risk

All TLDs have a mix of red and yellow sites. Some, however, have a strong bias toward yellow or red. For example, of the 1,607 risky Singapore (.SG) sites we tested, 1,536 were rated yellow. Just 71 were rated red. By contrast, of the 15,178 risky Samoa (.WS) sites we rated, 13,688 were rated red.

Biased toward yellow

COUNTRY OR NAME	TLD	TOTAL RISKY SITES	PERCENT YELLOW	PERCENT RED
Singapore	SG	1,607	95.6%	4.4%
Ascension Island	AC	178	95.5%	4.5%
Venezuela	VE	272	93.8%	6.3%
Niue	NU	1,369	86.8%	13.2%
Spain	ES	2,936	86.2%	13.8%
Tokelau	TK	3,754	83.3%	16.7%
Finland	FI	171	78.9%	21.1%
Saint Helena	SH	71	77.5%	22.5%
Canada	CA	1,328	75.0%	25.0%
Mobile Devices	MOBI	201	74.6%	25.4%
People's Republic of China	CN	193,917	74.1%	25.9%
United Kingdom	UK	5,923	71.8%	28.2%
São Tomé and Príncipe	ST	779	67.7%	32.3%
Armenia	AM	83	67.5%	32.5%
India	IN	1,568	65.6%	34.4%
Iceland	IS	31	61.3%	38.7%
Israel	IL	655	61.2%	38.8%
Cocos (Keeling) Islands	CC	2,108	60.6%	39.4%
Hong Kong	HK	358	59.5%	40.5%
Taiwan	TW	565	59.3%	40.7%

Biased toward red

COUNTRY OR NAME	TLD	TOTAL RISKY SITES	PERCENT YELLOW	PERCENT RED
Saudi Arabia	SA	41	4.9%	95.1%
Kazakhstan	KZ	194	7.7%	92.3%
Turks and Caicos Islands	TC	153	9.2%	90.8%
Former Soviet Union	SU	754	9.5%	90.5%
Samoa	WS	15,178	9.8%	90.2%
Guernsey	GG	111	9.9%	90.1%
Slovakia	SK	580	10.3%	89.7%
Trinidad and Tobago	TT	45	11.1%	88.9%
Cameroon	CM	57,210	12.1%	87.9%
Croatia	HR	47	14.9%	85.1%
French Southern and Antarctic Lands	TF	20	15.0%	85.0%
Nauru	NR	73	15.1%	84.9%
Ukraine	UA	673	15.2%	84.8%
East Timor	TL	52	15.4%	84.6%
Pakistan	PK	238	18.1%	81.9%
Romania	RO	2,280	18.9%	81.1%
Christmas Island	CX	42	19.0%	81.0%
Yugoslavia	YU	36	19.4%	80.6%
Iran	IR	288	20.5%	79.5%
Information	INFO	137,403	20.7%	79.3%

Discussion

Top-level domains ranked high for risk

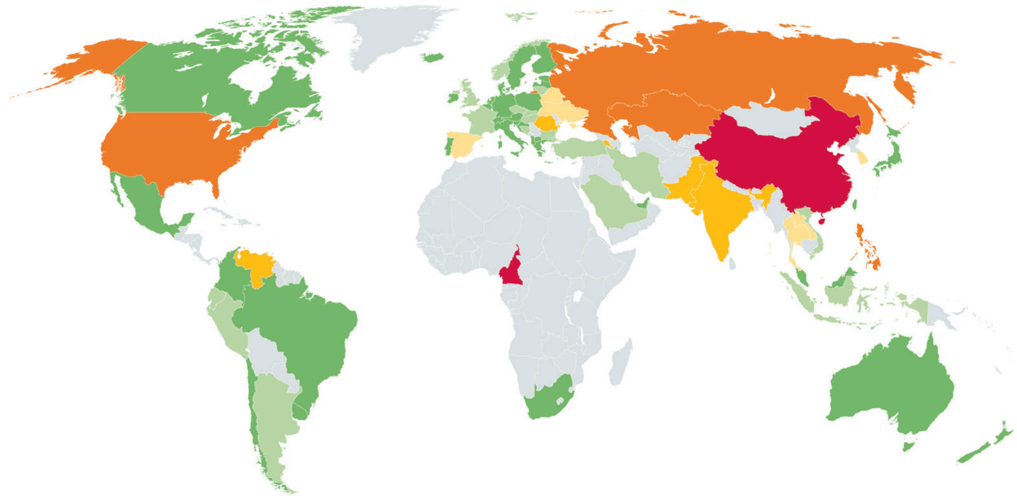
.CM (Cameroon)

The TLD with the highest weighted ratio of risky registrations is .CM. .CM is no stranger to controversy. Starting a few years ago, it became the target of frequent criticism for "wildcarding" the entire .COM (Commercial) TLD. When users mistype a .COM website as .CM and are re-directed to a landing page with advertisements, .CM generates income from clicks on those ads. The controversy continues to this day, with some arguing that .CM typosquatting (erecting a fake site at a commonly misspelled web address) is little different from any other mistype. Our data show that typosquatting is just one of the issues besetting .CM registrations. Our tests find significant malicious download activity—from adware and spyware to aggressive linking to drive-by-download sites. Moreover, we began noticing a spike in malicious activity starting in the second quarter of 2009. We are anxious to see whether this trend continues or if .CM decides to take action.

.SG (Singapore)

Singapore soared over the last year to become the TLD with the biggest increase in risky registrations. While apples to apples comparisons are especially difficult because of changes to our methodology this year, .SG stood out, rising from 0.3% risky registrations to 9.1%. When weighted to reflect .SG's relatively small footprint on total risky registration, the weighted ratio becomes 4.6%. Driving this trend were frequent Chinese pharmacy spam sites. However, we note that of the 1,607 .SG domains we rated risky, more than 95.0% were rated yellow (use caution) rather than red (avoid), meaning that the dangers of visiting risky .SG domains were moderate rather than severe.

What countries are riskiest to visit on the Internet?



This map looks at each country top-level domain (TLD), and rates them based on how many risky websites we found during our safety tests.

Improved top-level domains

.HK (Hong Kong)

Last year's riskiest TLD improved dramatically since our last report. As .HK's managers noted at the time, they had taken aggressive steps to clamp down on scam-related registrations and had changed policies to prevent new ones. Our data show these actions had a significant impact on .HK registrations. Of the almost 17,000 domains we tested for this report, just 358 were risky. We contacted Jonathan Shea, chief executive officer, Hong Kong Internet Registration Corporation Ltd. (HKIRC), for comment:

"Additional checks are performed to identify applications of '.HK' domain names likely to be used for fraudulent purposes. We request applicants to provide identity proof for suspicious applications. Due to security concerns, we cannot disclose the specifics of the changes in handling applications for new '.HK' domain names.

Also, we have to emphasize that this is a concerted effort of multiple parties. It is not just the registry alone. We have received valuable help from the local CERT, police and the local telecommunication service regulator."

Top-level domains ranked low for risk

.JP (Japan)

In the three years we have conducted this study, McAfee has consistently found .JP to register very few risky websites. This year, .JP ranks 103 out of 104. Only .GOV (Governmental) ranked safer. Of the more than 395,000 websites we tested, just 446 rated risky. We asked Yumi Ohashi, international and government relations manager, business development for Division Japan Registry Services Co., Ltd. (JPRS) to comment:

"To register a .JP domain name, the registrant must satisfy 'local presence' and other requirements (e.g., corporate status) depending on the type of domain he/she applies for. We have two major categories within the .JP domain: General-use JP Domain Name and Organizational-type JP Domain Name.

For some types of .JP domain, we register a name only after we verify in detail that the applicant satisfies registration requirements. Also, we may ask for documented proof in some cases, even after the name is registered. Under .JP registration rules, we as the registry, reserve the right to cancel a registration which does not meet the requirements. We apply a 'one domain name per organization' rule for Organizational-type JP Domain Names.

Through cooperation with CERT and the other relevant entities, we assess the degree of malevolence of the domain name that is allegedly used for abuses like phishing. If it is confirmed that the name is abused, we promptly request the relevant accredited JP Registrar to invalidate the name.

Since the launch of the General-use JP Domain Name, we have accepted the request only from accredited JP Registrars. This is applied to any request including new registration, data modification and deletion. We set the same framework for Organizational-type JP Domain Names. Upon receiving applications, password authentication is required.

In January 2006, JPRS started the measure whereby we delete DNS server registration if its host name contains non-existing JP domain name. We have deleted the concerned DNS settings once a month since then. The following is the English announcement on this: http://jprs.co.jp/en/topics/2005/051213.html. Finally, we are planning to implement DNSSEC by the end of 2010."

.CL (Chile)

.CL ranked as the least risky TLD in the Americas and 82nd least risky out of 104 we ranked. Of the more than 44,000 .CL domains we tested, just 280 tested risky. We asked Patricio Poblete who manages .CL to comment on why the TLD was so effective:

"To register a domain name under .CL one has to be a resident of Chile or be able to provide a contact that resides in Chile. In both cases, the applicant has to provide an identification number (RUT), which is the national ID number for persons and the national tax ID number for companies. An image of this document does not need to be provided at the time of registration, but it is requested when a domain is transferred or in other occasions when the identity of the domain name holder requires validation.

We also try to act quickly when we receive notifications of phishing sites. Our experience is that most, if not all, of these sites are installed in hacked servers, so, as a general rule, we do not take down the domain but contact the domain name holder or the hosting company.

Over the last year we changed our policies for accepting credit card payments, and we are now using a system that requires confirmation using the validation system used by the customer's bank. This made it much harder for people with lists of stolen credit cards to use them to pay for domain names in .CL. We did this mainly to avoid repudiations, but is has also proved to be a deterrent to registration of fraudulent domains.

We also have increased our participation in security working groups and mailing lists, to increase our ability to share information and react to threats."

.IE (Ireland)

.IE has the fewest number of risky registrations in the Europe, Middle East, and Africa region. Of the more than 27,000 domains we tested, just 65 were risky. This earned .IE a rank of 101 out of 104 TLDs. We asked David Curtin, chief executive of .IE Domain Registry Limited for comment:

"The .IE Domain Registry (IEDR) has registration processes in place that discourage spammers from registering their domains with the .IE TLD.

Our objective is to ensure that there is a level of traceability of registrants of .IE addresses. We believe this level of traceability provides confidence to consumers who wish to shop online on a .IE website—and to provide their credit card details or to provide personal information. In other words, we check that 'registrants are who they say they are' so that consumers don't have to.

To achieve our objective of traceability—we ask new registrants to show that they have a 'real and substantive connection' to the island of Ireland. We also ask new registrants to 'authenticate their claim to the domain name' of their choice. Compliance is simple and not at all bureaucratic … Our processes result in less cybercrime and minimal cybersquatting.

We continue to experience strong growth in .IE domain registration numbers—up 37.5% in calendar 2008 and annualized growth of 33.0% to June 2009 … We experience fewer intellectual property disputes and the annual numbers of domains entering the .IE DRP (dispute resolution process) is in single digits."

The best way to protect yourself is by maintaining up-to-date, reputable computer security software with safe search functionality.

Conficker

Conficker is a computer worm that has assembled an army of infected machines called a botnet. Approximately five million strong, this botnet could be used to send waves of spam, conduct denial of service (DoS) attacks on targeted websites, or even attack the Internet backbones of particular countries. The hackers behind this worm have built an impressive auto-update capability that relies on randomly generated domain name/TLD combinations for access to their command and control servers. Hundreds of these domains are generated and accessed by the worm daily in attempts to receive updated code or instructions.

ICANN worked aggressively to help coordinate the security community's response to this serious global threat. ICANN worked closely with the working group of security industry professionals assembled to fight Conficker to coordinate outreach to country TLD managers to block registration of domains used by Conficker and deny their use to the hackers. Dmitri Alperovitch, vice president of threat research at McAfee, represented the company in the Conficker Working Group and notes:

"The assistance provided by ICANN and their close collaborative relationship with the Conficker Working Group was instrumental in a successful mitigation of the Conficker threat to the Internet infrastructure and is a great blueprint for building successful global partnerships to fight cybercrime."

Trends to watch

As TLD managers step up and take action over the issues associated with "risky" domain registrations within their TLDs, we expect to see scammers and malware authors continue to evolve their tactics. For example, we are already seeing aggressive moves to use URL shortening services (e.g., bit.ly, TinyURL) to hide a malicious payload or phishing page. Will these services take some ownership and responsibility of this type of abuse, or are consumers—and TLD managers—in for another period of "Wild West" type domain lawlessness?

Additionally, we continue to see infections of legitimate websites via SQL injection, domain hijacking and cross-site scripting. These often ephemeral infections can still result in massive drive-by exploitations that infect a web server—and the consumers who visit it—without the knowledge of the consumer, webmaster, or registrar.

Conclusion

We find that web-based risk is pervasive and growing, but it is not evenly distributed. We also find that some TLDs are much better at managing risky registrations than others. As consumers and businesses become increasingly interconnected via the web, it is simply not feasible to expect that we can shut the door on the Internet. Even if we could lock the doors on certain parts, malware authors and scammers would start trying to break in through the windows. We see that kind of malicious innovation every day (e.g., malicious use of URL shortening services).

For consumers who want to maximize their protection, it is unrealistic to think they can memorize this map of the mal web, both because it is so complex and because it is ever changing. The best way to protect yourself is by maintaining up-to-date, reputable computer security software with safe search functionality.

For the business that wants to maximize the utility of the web for commerce, it is unwise to try to simply turn off employee web use. The best way for that business to protect itself is to add web reputation functionality to its security to allow workers to use the safer parts of the web and avoid the dark alleys.

And for the operators of risky TLDs, it is unacceptable to simply say "it's too hard" to police the scammers. This report shows that many TLDs have succeeded in maintaining low levels of scammer registrations. Even TLDs that were temporarily inundated have shown they can dramatically improve.

The scammers, spammers, phishers, and hackers have stepped up a notch. We all must do the same.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

www.mcafee.com

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee's customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee and/or other noted McAfee-related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the U.S. and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee-related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners.