Mapping the Mal Web

The world's riskiest domains

McAfee

Mapping the Mal Web

The world's riskiest domains

By:
Barbara Kay, CISSP, Secure by Design Group
Paula Greve, Director of Research, McAfee Labs™

CONTENTS

Introduction

Bonanza or botnet? Next time you search for a celebrity photo or "how to" hint, pay special attention to the top-level domains (TLDs), the last few characters at the end of the URL in the search results. In this year's *Mapping the Mal Web* study, McAfee found that web risk climbed to a record 6.2% of more than 27 million live domains we evaluated for this report. If users don't click with care, simply viewing a page can return much more than they bargained for. This year, more websites contain malicious code that steals passwords and identity information, takes advantage of security holes in browsers, or secretly installs the ingredients that turn computers into zombies.

If you knew in advance that three out of five sites in a certain TLD were risky, you would probably choose a different download location for that photo you're searching for. For instance, despite Vietnam's growing allure as a vacation destination, visitors to sites registered in Vietnam (.VN) should consider it a "no fly" zone. This year, .VN splashed into our top five as one of the riskiest TLDs on the Internet, with 58% of the sites we track containing malicious or potentially dangerous content and activities including:

- **Malware—**Code that can damage a system, steal data, or perform malicious activities on another computer (includes keyloggers, password stealers, and zombie kits).
- **Browser exploits—**Attacks and malware that take advantage of vulnerable software.
- **Phishing—**Fake sites that appear to be legitimate but are designed to "phish" for information or install malicious code.
- **Spamminess—**Sign-up forms that will cause the person to receive large amounts of commercial email, or spam.
- **Risky affiliations—**Sites with links that take the user to a malicious site, and sites that have suspicious associations, such as their site ownership, registration, or hosting service.

Security Threats Evaluated by McAfee® Global Threat Intelligence™

We determine risk level based upon the ways multiple characteristics relate to each website.

The .INFO and .CM TLDs have almost as many risky sites as safe ones, while .VN has *more* risky sites than safe ones.

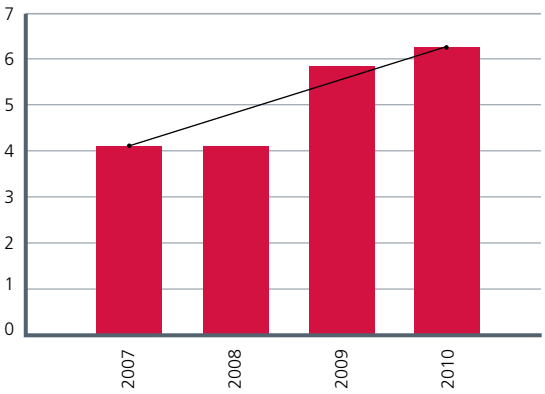
Key Findings: *Mapping The Mal Web IV*

In this fourth annual analysis of the relative risk of TLDs, McAfee has found overall web risk is up from last year. We saw increasing risk in some already risky portions of the web, such as .INFO; some significant reductions in risk within last year's riskiest TLDs, especially Singapore (.SG) and Venezuela (.VE); and some new areas of concern, including Vietnam (.VN), Armenia (.AM), and Poland (.PL).

Note: All risk statistics refer to weighted risk, unless otherwise stated.

- **Increasing risk**—The overall weighted average of risky sites rose from 5.8% (2009) to 6.2% (2010). In 2007 and 2008, we found 4.1% of websites to be rated red (avoid) or yellow (use caution). Although we used a different methodology in the first two years, the trend line—up and to the right—seems to be holding. The web is getting trickier to navigate safely.

Percentage of Risky Sites on the Web



- **Top five riskiest TLDs**—With a weighted risk of 31.3%, .COM (Commercial—the most heavily trafficked TLD) was the most risky TLD. It took this title from .CM (Cameroon), which fell to fourth place this year, while .INFO jockeyed for a more risky position, up to second place from fifth place last year. The five TLDs with the greatest percentage of risky registrations were:
  - .COM (Commercial) 31.3%
  - .INFO (Information) 30.7%
  - .VN (Vietnam) 29.4%
  - .CM (Cameroon) 22.2%
  - .AM (Armenia) 12.1%
- **Global distribution**—The Europe, Middle East, and Africa (EMEA) regions again won the dubious distinction of having the most risky TLDs in the top 20, with seven entrants, including top 20 newcomers Armenia (.AM) and Poland (.PL). The Asia-Pacific (APAC) region followed with six TLDs, while generic domains, such as Network (.NET), captured five of the top 20 riskiest slots. The sole Americas entrant was the United States (.US) at number 14.

- **Generic leadership**—Contrasting risk by region, the generic and sponsored TLDs carried the highest average risk. At 7.9%, these TLDs exceeded the overall average, while all three regional groups fell below the average of 6.2%. APAC fell from last year's average of 13% to 4.9%; the Americas averaged 2.7%; EMEA just 1.9%.
- **Some big improvements**—Singapore (.SG) deserves recognition for falling in risk from last year's number 10 slot to number 81 this year; Venezuela (.VE) dropped from 21 to 88 this year; and the Philippines (.PH) moved from number six in 2009 to number 25 this year.
- **Ones to watch**—We only evaluated TLDs for which we had results for 2,000 or more live sites. However, two low-volume TLDs would have made our top five if we had included all TLDs:
  - Senegal (.SN) at 33% risk would lead at number one, perhaps since it has no registration restrictions (http://en.wikipedia.org/wiki/.sn).
  - British Indian Ocean Territory (.IO) would have been in fifth place (11.5% risk). It may be a popular TLD because it has no second level registration restrictions limiting the names that can appear before the TLD, so it offers clever reuse possibilities: ".IO is used in domain hacks such as eugen.io, moustach.io, or pistacch.io, as well as by the file hosting service drop.io" (http://en.wikipedia.org/wiki/.io).
- **Squeaky clean**—The five TLDs with the fewest risky registrations, each with 0.1% or fewer domains rated risky, were:
  - .TRAVEL (Travel and Tourism Industry) .02%
  - .EDU (Educational) .05%
  - .JP (Japan) .08%
  - .CAT (Catalan) .09%
  - .GG (Guernsey) .10%

Note: The ratings are based on overall site assessments, rather than ratings of individual pages. Users should be aware that there are still risks within individual URLs on generally safe domains; we find quite a few risky page-level URLs on .EDU, for instance.

- **Governmental loses its lead**—The safest TLD in 2009, Governmental (.GOV), was relegated to twenty-third least risky this year; however, it stayed at the same degree of riskiness, a mere 0.3%. All of the risky sites we found there were rated red.

Why Mapping Matters

McAfee publishes the *Mapping the Mal Web* report for three different communities, with three different goals:

- For the domain registrar and registry community, we hope this report acknowledges those who work hard to reduce scammer registrations and shut down malicious sites, and that it spurs others to reach out to these leaders to adapt best practices to their unique challenges. One reward is risk reduction. In the past, we have worked to assist registries on the "worst offender" list, providing our research on risk data. Subsequently, we have seen dramatic reductions in the number of risky sites in their TLDs.
- For site owners, we hope the report can be a useful guide to consult when deciding on the public-facing "location" for their registrations.
- For consumers and enterprise IT managers, we hope the report acts as a reality check, a warning that risk is widely distributed throughout the web, that risks are growing and getting more subtle, and that even the most experienced users need the assistance of comprehensive, up-to-date security software with safe search functionality.

How Criminals Abuse Top-Level Domains

A TLD is one of the organizers of the web, the letter code at the end of a website that tells us where the site is registered. While it is likely that everyone recognizes .COM and .GOV, many TLDs are harder to interpret, such as .AM for Armenia or .CM for Cameroon. Scammers profit from this ignorance, as well as the reality that many consumers just do not pay attention to the TLD suffix when they search. Many consumers click on the first result that sounds interesting, falling prey to criminals that take time to optimize their sites for search engines.

Certain TLDs are riskier to visit than others. Scammers and hackers register their operations in the places where it is easiest to do business, or where they see a financial opportunity from misspellings or logical associations. Since it is easy to leave out the "O" in a .COM address, an unscrupulous player might register in Cameroon for the www.mcafee.cm address, hoping to garner traffic from consumers and business users concerned about security. For instance, this would be a likely site on which to plant a rogue anti-virus program, with the expectation that a consumer was susceptible to an alert message stating: "you have a virus, install this software."

Registrars work diligently to squelch this activity, known as "typosquatting." Typosquatting runs the gamut from sites that generate ad revenue from your typo to parked sites that would love to sell you that address to full-fledged phishing sites that harvest personal information or install malicious software.

The most dangerous software (sometimes referred to as a "drive-by") is invisible to the user—the user does not have to click or consciously accept a download to be infected or exploited. Most malware and attacks do their best to remain undetected. Consumers may not notice for days or weeks that there is a problem, while criminals empty bank accounts, access online gaming accounts, infect social network "friends," or skim CPU cycles for their botnets.

Similarly, the average user does not know if a .COM site is hosted in the U.S.A. or China. Unless they use a rating advisory tool, viewers need to do extra research to determine if a location is one they should be comfortable visiting. Does .VN stand for Vietnam or Venezuela? The answer can make a big difference in your risk.

As the good guys work to improve policing and registration oversight,[1] criminals invest in nimble software and resilient infrastructure (see zombies sidebar). When the noose tightens on one TLD, they quickly move their Internet front doors to more forgiving and flexible homes, without necessarily relocating physical servers or altering content.

Beware of Zombies

Zombies are corrupted computers located in homes and businesses. Criminals connect them together to launch different attacks: spam, phishing, and data theft. Botnets are groups of zombies that distribute the activity, so they help bot owners stay "under the radar," avoiding detection and policing, such as takedowns at ISP facilities. They gain a business-class infrastructure for cybercrime at negligible cost.

Along with being cheap to operate, zombies help bot masters maintain their anonymity. The success of this strategy may explain the differing impacts of the McColo takedown, which slashed global spam volumes in 2008,[2] and the Zeus botnet takedown in March 2010, which lasted just a few hours.[3]

The TLD tells us only where a site is registered. The website itself, including its content, servers, and owners, can be located elsewhere. One trend is for criminals to place content within free consumer file-sharing services, then serve the content out to TLDs as needed. Since files stored on services such as BitTorrent, YouTube, and RapidShare change constantly, policing this content has proven very difficult.

Several factors affect how criminals pick a TLD:

- **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 TLD managers.

1 *McAfee 2010 Threat Predictions*, p. 9, available for download in multiple languages at http://www.mcafee.com/us/threat_center/white_paper.html

2 http://arstechnica.com/security/news/2009/01/two-months-after-mccolo-takedown-spam-levels-yet-to-recover.ars

3 http://www.thetechherald.com/article.php/201010/5363/ISP-takedown-deals-smashes-Zeus-botnet-%E2%80%93-for-a-few-hours

Methodology

There were no changes to this year's methodology. As in last year's report, this report uses the McAfee Global Threat Intelligence database, which reflects data 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 mid-sized businesses, enterprise customers, educational institutions, and governmental agencies.

Our approach is to identify risk by analyzing web traffic patterns, site behavior, hosted content, and links. We assess individual sites for malicious or risky content and behavior and also analyze what might be called site context—how the site is registered, referenced, used, and accessed.

- **Websites** are evaluated 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 consumers' computers 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 on many freeware and shareware sites, such as RapidShare, and we test P2P and BitTorrent client software. The same sort of services that are used for free file-sharing work great for malware distribution.
- **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 filter software.

In addition, McAfee Global Threat Intelligence 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.

We give red ratings to websites that contain malicious code (such as Trojans, viruses, and spyware) or browser exploits that have earned a dangerous reputation because of their correlated file, email, web, and network reputations. Yellow ratings are given to sites that merit caution before using, often due to spamminess, aggressive popups, or links to risky sites. Almost all TLDs have a mix of red and yellow sites.

More creative criminals, more sophisticated countermeasures

Each year, criminals develop more intricate and innovative techniques for hiding their activities. This year, for example, botnets drove a huge spike in new malicious site categories, one of our analysis classifications that includes viruses, Trojans, and botnets.

As criminals get craftier, we get craftier. McAfee has more than 400 researchers devoted to threat analysis. This global team builds new tools for sensing changes on the web, analyzes data from these sensors, and identifies the behavior and fingerprints that signal risk. Each new insight is folded back into our global threat intelligence network for even more refined analysis. So, while our methodology remains the same, there are constant changes within our technology to ensure that we capture an accurate assessment of the real risk today's web users face.

The rankings

As before, we restricted our analysis to TLDs for which we track at least 2,000 sites. For this report, we included 106 TLDs from the 271 we track, representing two more domains than in 2009.

	Unweighted Method		Weighted 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%

All domains versus live domains

We included only live domains, those that were active at the time the survey was run: 27,304,797 domains. This live data is a neutral snapshot that captures the state of the TLD system on the day we captured our data. There is risk variation that is natural, such that a survey run a week later would show different results.

Unscheduled and unannounced

We do not time this study or average the results using multiple samples. Additionally, we do not announce the date. By taking a random, unscheduled sample, we can ensure that there is no gaming of the process.

Weighted risk

As in last year's report, the risk rating is weighted: 50% of the rating comes from the ratio of a TLD's risky sites to its total sites, and 50% from the ratio of a TLD's risky sites to all risky sites. We believe this ranking methodology reflects the level of risk a typical user faces when traveling the entire web. Put a different way, we believe a web user would be more reluctant to visit a TLD knowing that it contained 50% of the entire web's risky sites, even if those risky sites represented just 1% of that TLD's total domains.

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%*100/10 ,000)+(50%*100/200)=25.5%] would be ranked riskier than the TLD with 10 risky sites out of 100 [(50%*(10/100)+(50%*(10/200)=7.5%].

This 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*:* 6.1% of the 15.5 million .COM (Commercial) sites we analyzed were rated risky, a bit less than our overall average of 6.2%. However, when we weighted .COM's risk by the total number of risky sites worldwide, its ratio increased to 31.3%, making it the most risky TLD. By contrast, 58% of the 24,988 .VN (Vietnam) websites we evaluated were risky, but when we weighted that risk by their share of the number of risky sites worldwide, the ratio decreased to 29.4%, placing .VN behind .COM in risk.

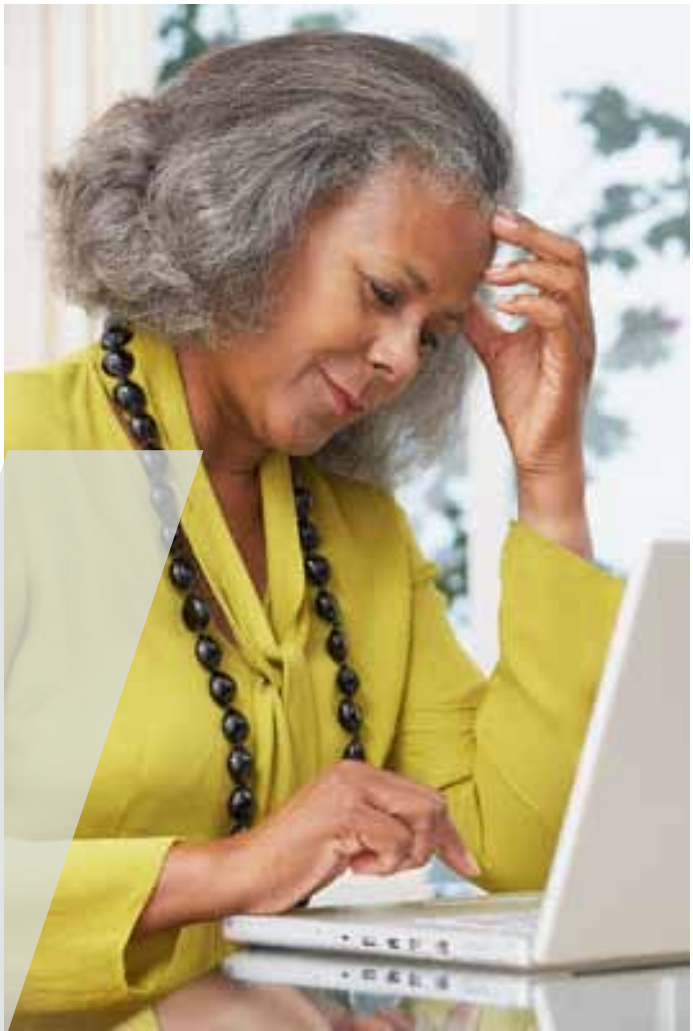
Some Caveats About the Rankings

No weighting by traffic

Our risk ratings are not weighted by the traffic a TLD receives. We do not distinguish between a very popular TLD that receives a great deal of traffic to its risky sites and a less popular TLD that receives little traffic. This approach matches the reality that malicious sites often climb rapidly into the Internet top one million (as measured by traffic), staying there for a few weeks while users are infected. A user who simply sticks to the popular sites, or the top search results, is still at risk.

No weighting by type of risk

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. A site sign-up that results in spam email is weighted equally with a site with a virus-infected download.



No weighting by TLD 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 considered 297,946 .PL (Poland) domains. Of those, we found 17,398 to be risky, or 5.8% of the total. Assuming the total population of .PL domains is 2,970,000, our sample size is roughly 10.0%. At a 95% confidence level, our confidence interval is +/- 0.08%. In other words, we can be 95% confident that the actual percentage of risky sites is between 5.72% and 5.88%.

Domains not URLs

This study incorporates only domain-level rankings, not individual URLs within a domain. This is important because McAfee has found numerous examples of malicious *individual* URLs within otherwise safe *domains*, such as .HR (Croatia) and .EDU (Educational).

No adjustments for delisting of 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

Finally, our rankings do not take into account domains that we do not track.

Breakdown of the Rankings

Overall rankings

HIGH RISK **LOW RISK**

Country or Name	Region	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	Total Domains Tracked	Total Risky Domains
Commercial	Generic	COM	1	31.3%	6.1%	2	32.2%	-2.8% ↓	15,530,183	948,995
Information	Generic	INFO	2	30.7%	46.6%	5	15.8%	94.5% ↑	533,711	248,806
Vietnam	APAC	VN	3	29.4%	58.0%	39	0.9%	3,107.9% ↑	24,988	14,492
Cameroon	EMEA	CM	4	22.2%	44.2%	1	36.7%	-39.5% ↓	3,947	1,746
Armenia	EMEA	AM	5	12.1%	24.2%	23	2.0%	512.9% ↑	3,145	760
Cocos (Keeling) Islands	APAC	CC	6	10.5%	20.2%	14	3.3%	215.4% ↑	58,713	11,869
Asia-Pacific	APAC	ASIA	7	10.3%	20.6%	N/A	N/A	N/A	3,122	642
Network	Generic	NET	8	10.1%	10.5%	7	5.8%	73.7% ↑	1,556,813	163,466
Russia	EMEA	RU	9	10.1%	16.8%	9	4.6%	116.7% ↑	329,136	55,373
Western Samoa	APAC	WS	10	8.6%	16.9%	4	17.8%	-51.8% ↓	22,070	3,734
Tokelau	APAC	TK	11	8.4%	15.9%	19	2.3%	262.0% ↑	91,876	14,630
Organization	Generic	ORG	12	6.4%	7.4%	11	4.2%	50.3% ↑	1,224,870	90,290
Business	Generic	BIZ	13	6.3%	11.8%	13	3.6%	74.3% ↑	121,622	14,350
United States	Americas	US	14	6.0%	11.2%	17	3.1%	95.7% ↑	119,861	13,365
People's Republic of China	APAC	CN	15	4.8%	8.3%	3	23.4%	-79.5% ↓	261,298	21,711
Former Soviet Union	EMEA	SU	16	4.6%	9.2%	8	5.2%	-9.8% ↓	8,478	784
São Tomé and Príncipe	EMEA	ST	17	3.7%	7.3%	12	3.8%	-1.6% ↓	11,997	880
Romania	EMEA	RO	18	3.7%	7.1%	20	2.2%	63.5% ↑	56,312	3,982
Georgia	EMEA	GE	19	3.5%	7.0%	N/A	N/A	N/A	2,311	162
Poland	EMEA	PL	20	3.4%	5.8%	60	0.5%	574.2% ↑	297,946	17,398
India	APAC	IN	21	3.4%	6.5%	22	2.0%	67.8% ↑	49,368	3,218
Montserrat	EMEA	MS	22	3.2%	6.3%	N/A	N/A	N/A	3,382	213
Pakistan	APAC	PK	23	2.8%	5.5%	18	2.8%	0.5% ↑	4,947	273
Niue	APAC	NU	24	2.5%	5.0%	24	1.9%	32.3% ↑	27,420	1,362
Philippines	APAC	PH	25	2.2%	4.3%	6	13.1%	-83.4% ↓	9,625	418
Montenegro	EMEA	me	26	2.1%	4.3%	N/A	N/A	N/A	5,465	233
Tonga	APAC	TO	27	2.1%	4.2%	33	1.1%	94.5% ↑	13,150	550
Trinidad and Tobago	Americas	TT	28	1.9%	3.8%	51	0.6%	217.6% ↑	4,287	165
Families and Individuals	Generic	NAME	29	1.7%	3.3%	16	3.1%	-45.9% ↓	6,726	223
Tuvalu	APAC	TV	30	1.7%	3.2%	38	0.9%	80.1% ↑	40,770	1,316
Kazakhstan	EMEA	KZ	31	1.5%	3.1%	15	3.1%	-50.2% ↓	4,708	144
Turks and Caicos Islands	Americas	TC	32	1.5%	3.0%	40	0.9%	74.8% ↑	11,187	338
Mobile Devices	Generic	MOBI	33	1.5%	3.0%	25	1.7%	-14.4% ↓	6,861	204
Morocco	EMEA	MA	34	1.5%	3.0%	N/A	N/A	N/A	2,024	60
Laos	APAC	LA	35	1.5%	2.9%	26	1.6%	-8.7% ↓	4,143	122
Colombia	Americas	CO	36	1.5%	2.9%	68	0.4%	249.0% ↑	3,618	106
Belize	Americas	BZ	37	1.3%	2.5%	30	1.2%	2.2% ↑	3,472	88

Overall rankings (cont.)

HIGH RISK **LOW RISK**

Country or Name	Region	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	Total Domains Tracked	Total Risky Domains
South Korea	APAC	KR	38	1.1%	2.2%	28	1.5%	-26.7% ↓	70,261	1,530
Christmas Island	APAC	CX	39	1.1%	2.2%	74	0.4%	195.6% ↑	6,084	136
Latvia	EMEA	LV	40	1.1%	2.1%	71	0.4%	163.1% ↑	10,015	210
Canada	Americas	CA	41	0.9%	1.6%	64	0.5%	90.5% ↑	169,543	2,777
Slovakia	EMEA	SK	42	0.9%	1.7%	45	0.8%	11.4% ↑	37,643	649
Serbia	EMEA	RS	43	0.9%	1.7%	N/A	N/A	N/A	2,031	35
European Union	EMEA	EU	44	0.8%	1.6%	59	0.5%	60.3% ↑	80,278	1,288
Ukraine	EMEA	UA	45	0.8%	1.6%	36	1.0%	-19.7% ↓	38,619	615
Federated States of Micronesia	APAC	FM	46	0.7%	1.5%	66	0.4%	69.7% ↑	4,075	60
Malaysia	APAC	MY	47	0.7%	1.5%	80	0.3%	122.1% ↑	15,200	221
Thailand	APAC	TH	48	0.7%	1.5%	32	1.1%	-34.8% ↓	8,912	130
United Kingdom	EMEA	UK	49	0.7%	0.9%	55	0.6%	30.3% ↑	898,229	8,503
Moldova	EMEA	MD	50	0.7%	1.4%	N/A	N/A	N/A	2,644	38
Belarus	EMEA	BY	51	0.7%	1.4%	29	1.3%	-44.8% ↓	4,372	62
South Georgia and the South Sandwich Islands	EMEA	GS	52	0.6%	1.2%	48	0.6%	-7.1% ↓	4,578	55
Peru	Americas	PE	53	0.6%	1.2%	41	0.9%	-32.9% ↓	5,176	60
Czech Republic	EMEA	CZ	54	0.6%	1.0%	54	0.6%	-4.7% ↓	101,781	1,068
Iran	EMEA	IR	55	0.5%	1.1%	37	0.9%	-42.5% ↓	17,874	191
Lithuania	EMEA	LT	56	0.5%	1.1%	44	0.8%	-36.9% ↓	11,517	121
Ecuador	Americas	EC	57	0.5%	1.0%	49	0.6%	-18.8% ↓	2,496	26
United Arab Emirates	EMEA	AE	58	0.5%	1.0%	65	0.5%	7.9% ↑	4,123	42
Uruguay	Americas	UY	59	0.5%	1.0%	75	0.4%	35.0% ↑	3,277	33
Hong Kong	APAC	HK	60	0.5%	1.0%	34	1.1%	-53.8% ↓	17,960	176
Republic of China (Taiwan)	APAC	TW	61	0.5%	1.0%	52	0.6%	-16.3% ↓	56,000	534
Belgium	EMEA	BE	62	0.5%	0.9%	81	0.3%	49.2% ↑	123,606	1,124
Liechtenstein	EMEA	LI	63	0.5%	1.0%	90	0.2%	110.3% ↑	3,000	29
East Timor	APAC	TL	64	0.5%	1.0%	58	0.5%	-11.6% ↓	5,309	51
Hungary	EMEA	HU	65	0.4%	0.9%	53	0.6%	-23.9% ↓	71,650	614
Germany	EMEA	DE	66	0.4%	0.5%	83	0.3%	43.8% ↑	1,504,163	7,052
Saudi Arabia	EMEA	SA	67	0.4%	0.9%	42	0.9%	-48.7% ↓	2,630	23
Bosnia	EMEA	BA	68	0.4%	0.9%	46	0.8%	-43.9% ↓	2,671	23
Indonesia	APAC	ID	69	0.4%	0.8%	56	0.6%	-23.7% ↓	6,138	52
Brazil	Americas	BR	70	0.4%	0.7%	70	0.4%	5.0% ↑	290,350	2,084
Finland	EMEA	FI	71	0.4%	0.8%	85	0.3%	41.5% ↑	35,046	283
Argentina	Americas	AR	72	0.4%	0.8%	50	0.6%	-36.7% ↓	80,324	603
Spain	EMEA	ES	73	0.4%	0.7%	27	1.6%	-75.6% ↓	103,555	749
New Zealand	APAC	NZ	74	0.4%	0.7%	94	0.2%	86.8% ↑	56,240	416
France	EMEA	FR	75	0.4%	0.7%	61	0.5%	-24.8% ↓	244,237	1,626
Austria	EMEA	AT	76	0.4%	0.7%	89	0.2%	58.4% ↑	139,244	966
Israel	EMEA	IL	77	0.4%	0.7%	31	1.2%	-70.4% ↓	29,113	209

Overall rankings (cont.)

HIGH RISK **LOW RISK**

Country or Name	Region	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	Total Domains Tracked	Total Risky Domains
Nauru	APAC	NR	78	0.4%	0.7%	62	0.5%	-29.9% ↓	8,199	58
Turkey	EMEA	TR	79	0.4%	0.7%	47	0.7%	-46.6% ↓	36,466	252
Sweden	EMEA	SE	80	0.4%	0.7%	88	0.3%	35.8% ↑	102,870	684
Singapore	APAC	SG	81	0.3%	0.7%	10	4.6%	-92.6% ↓	15,632	105
Norway	EMEA	NO	82	0.3%	0.6%	77	0.4%	-8.5% ↓	50,089	317
Greece	EMEA	GR	83	0.3%	0.6%	73	0.4%	-22.7% ↓	41,357	243
Governmental	Generic	GOV	84	0.3%	0.6%	104	0.0%	1,188.3% ↑	6,415	38
Mexico	Americas	MX	85	0.3%	0.6%	69	0.4%	-26.7% ↓	49,601	284
Luxembourg	EMEA	LU	86	0.3%	0.6%	98	0.1%	102.4% ↑	6,750	38
Italy	EMEA	IT	87	0.3%	0.5%	78	0.3%	-17.6% ↓	314,171	1,495
Venezuela	Americas	VE	88	0.3%	0.5%	21	2.1%	-86.7% ↓	5,842	32
Estonia	EMEA	EE	89	0.3%	0.5%	76	0.4%	-30.1% ↓	11,302	58
South Africa	EMEA	ZA	90	0.3%	0.5%	96	0.2%	50.6% ↑	72,629	357
Portugal	EMEA	PT	91	0.2%	0.5%	86	0.3%	-13.2% ↓	38,869	189
Vanuatu	APAC	VU	92	0.2%	0.5%	97	0.2%	49.1% ↑	15,211	70
Netherlands	EMEA	NL	93	0.2%	0.3%	84	0.3%	-24.4% ↓	583,943	1,980
Bulgaria	EMEA	BG	94	0.2%	0.5%	43	0.8%	-73.1% ↓	17,974	81
Denmark	EMEA	DK	95	0.2%	0.4%	91	0.2%	0.7% ↑	151,472	627
Iceland	EMEA	IS	96	0.2%	0.4%	87	0.3%	-19.8% ↓	6,102	26
Slovenia	EMEA	SI	97	0.2%	0.4%	79	0.3%	-36.6% ↓	11,339	48
Australia	APAC	AU	98	0.2%	0.3%	93	0.2%	-4.3% ↓	256,103	871
Switzerland	EMEA	CH	99	0.1%	0.3%	95	0.2%	-13.3% ↓	217,863	572
Ireland	EMEA	IE	100	0.1%	0.2%	101	0.1%	-5.7% ↓	32,120	71
Croatia	EMEA	HR	101	0.1%	0.2%	100	0.1%	-11.1% ↓	22,511	50
Guernsey	EMEA	GG	102	0.1%	0.2%	57	0.6%	-81.1% ↓	12,092	25
Catalan	Sponsored	CAT	103	0.1%	0.2%	99	0.1%	-31.6% ↓	3,936	7
Japan	APAC	JP	104	0.1%	0.1%	103	0.1%	6.6% ↑	464,408	547
Educational	Generic	EDU	105	0.1%	0.1%	102	0.1%	-48.6% ↓	14,002	15
Travel and Tourism Industry	Generic	TRAVEL	106	0.0%	0.0%	92	0.2%	-88.6% ↓	2,013	1

Note: Entries marked "N/A" were new TLDs in the report this year, so there is no year-over-year change.

Americas region

HIGH RISK **LOW RISK**

Country or Name	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	2010 Total Domains Tracked	2010 Total Risky Domains
United States	US	14	6.0%	11.2%	17	3.1%	95.7% ↑	119,861	13,365
Trinidad and Tobago	TT	28	1.9%	3.8%	51	0.6%	217.6% ↑	4,287	165
Turks and Caicos Islands	TC	32	1.5%	3.0%	40	0.9%	74.8% ↑	11,187	338
Colombia	CO	36	1.5%	2.9%	68	0.4%	249.0% ↑	3,618	106
Belize	BZ	37	1.3%	2.5%	30	1.2%	2.2% ↑	3,472	88
Canada	CA	41	0.9%	1.6%	64	0.5%	90.5% ↑	169,543	2,777
Peru	PE	53	0.6%	1.2%	41	0.9%	-32.9% ↓	5,176	60
Ecuador	EC	57	0.5%	1.0%	49	0.6%	-18.8% ↓	2,496	26
Uruguay	UY	59	0.5%	1.0%	75	0.4%	35.0% ↑	3,277	33
Brazil	BR	70	0.4%	0.7%	70	0.4%	5.0% ↑	290,350	2,084
Argentina	AR	72	0.4%	0.8%	50	0.6%	-36.7% ↓	80,324	603
Mexico	MX	85	0.3%	0.6%	69	0.4%	-26.7% ↓	49,601	284
Venezuela	VE	88	0.3%	0.5%	21	2.1%	-86.7% ↓	5,842	32

- .CO (Colombia) showed one of the biggest increases in risk, moving from number 68 to number 36 in risk this year. We found that the primary risks associated with .CO relate to malicious activity: URLs serving as intermediaries for other malicious hosts, such as botnets of compromised systems and the command-and-control centers that manipulate them.
- .VE (Venezuela) was one of our most improved TLDs this year, moving from number 21 riskiest in 2009 to risk position 88 this year.

Asia-Pacific (APAC) region

HIGH RISK **LOW RISK**

Country or Name	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	2010 Total Domains Tracked	2010 Total Risky Domains
Vietnam	VN	3	29.4%	58.0%	39	0.9%	3,107.9% ↑	24,988	14,492
Cocos (Keeling) Islands	CC	6	10.5%	20.2%	14	3.3%	215.4% ↑	58,713	11,869
Western Samoa	WS	10	8.6%	16.9%	4	17.8%	-51.8% ↓	22,070	3,734
Tokelau	TK	11	8.4%	15.9%	19	2.3%	262.0% ↑	91,876	14,630
People's Republic of China	CN	15	4.8%	8.3%	3	23.4%	-79.5% ↓	261,298	21,711
India	IN	21	3.4%	6.5%	22	2.0%	67.8% ↑	49,368	3,218
Pakistan	PK	23	2.8%	5.5%	18	2.8%	0.5% ↑	4,947	273
Niue	NU	24	2.5%	5.0%	24	1.9%	32.3% ↑	27,420	1,362
Philippines	PH	25	2.2%	4.3%	6	13.1%	-83.4% ↓	9,625	418
Tonga	TO	27	2.1%	4.2%	33	1.1%	94.5% ↑	13,150	550
Tuvalu	TV	30	1.7%	3.2%	38	0.9%	80.1% ↑	40,770	1,316
Laos	LA	35	1.5%	2.9%	26	1.6%	-8.7% ↓	4,143	122
South Korea	KR	38	1.1%	2.2%	28	1.5%	-26.7% ↓	70,261	1,530
Christmas Island	CX	39	1.1%	2.2%	74	0.4%	195.6% ↑	6,084	136
Federated States of Micronesia	FM	46	0.7%	1.5%	66	0.4%	69.7% ↑	4,075	60
Malaysia	MY	47	0.7%	1.5%	80	0.3%	122.1% ↑	15,200	221
Thailand	TH	48	0.7%	1.5%	32	1.1%	-34.8% ↓	8,912	130
Hong Kong	HK	60	0.5%	1.0%	34	1.1%	-53.8% ↓	17,960	176
Republic of China (Taiwan)	TW	61	0.5%	1.0%	52	0.6%	-16.3% ↓	56,000	534
East Timor	TL	64	0.5%	1.0%	58	0.5%	-11.6% ↓	5,309	51
Indonesia	ID	69	0.4%	0.8%	56	0.6%	-23.7% ↓	6,138	52
New Zealand	NZ	74	0.4%	0.7%	94	0.2%	86.8% ↑	56,240	416
Nauru	NR	78	0.4%	0.7%	62	0.5%	-29.9% ↓	8,199	58
Singapore	SG	81	0.3%	0.7%	10	4.6%	-92.6% ↓	15,632	105
Vanuatu	VU	92	0.2%	0.5%	97	0.2%	49.1% ↑	15,211	70
Australia	AU	98	0.2%	0.3%	93	0.2%	-4.3% ↓	256,103	871
Japan	JP	104	0.1%	0.1%	103	0.1%	6.6% ↑	464,408	547

Note: Entries marked "N/A" were new TLDs in the report this year, so there is no year-over-year change.

- Overall, the Asia-Pacific region dominated the "most improved" category, occupying four of the top five positions, led by Singapore (.SG) in number one, then the People's Republic of China (.CN), the Philippines (.PH), and Western Samoa (.WS). This achievement is especially impressive since all four of these TLDs were in last year's list of top ten riskiest TLDs.
- However, Vietnam (.VN) moved from number 39 riskiest in 2009 to third riskiest in 2010. Similar to Colombia (.CO), the predominant risks associated with .VN relate to malicious activity, sites being used to proxy to other malicious hosts, as well as command-and-control activity.
- Japan returned as one of the world's least risky TLDs, and once again was the least riskiest in APAC.

Europe, Middle East, and Africa (EMEA) region

HIGH RISK **LOW RISK**

Country or Name	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	2010 Total Domains Tracked	2010 Total Risky Domains
Cameroon	CM	4	22.2%	44.2%	1	36.7%	-39.5% ↓	3,947	1,746
Armenia	AM	5	12.1%	24.2%	23	2.0%	512.9% ↑	3,145	760
Russia	RU	9	10.1%	16.8%	9	4.6%	116.7% ↑	329,136	55,373
Former Soviet Union	SU	16	4.6%	9.2%	8	5.2%	-9.8% ↓	8,478	784
São Tomé and Príncipe	ST	17	3.7%	7.3%	12	3.8%	-1.6% ↓	11,997	880
Romania	RO	18	3.7%	7.1%	20	2.2%	63.5% ↑	56,312	3,982
Georgia	GE	19	3.5%	7.0%	N/A	N/A	N/A	2,311	162
Poland	PL	20	3.4%	5.8%	60	0.5%	574.2% ↑	297,946	17,398
Montserrat	MS	22	3.2%	6.3%	N/A	N/A	N/A	3,382	213
Montenegro	ME	26	2.1%	4.3%	N/A	N/A	N/A	5,465	233
Kazakhstan	KZ	31	1.5%	3.1%	15	3.1%	-50.2% ↓	4,708	144
Morocco	MA	34	1.5%	3.0%	N/A	N/A	N/A	2,024	60
Latvia	LV	40	1.1%	2.1%	71	0.4%	163.1% ↑	10,015	210
Slovakia	SK	42	0.9%	1.7%	45	0.8%	11.4% ↑	37,643	649
Serbia	RS	43	0.9%	1.7%	N/A	N/A	N/A	2,031	35
European Union	EU	44	0.8%	1.6%	59	0.5%	60.3% ↑	80,278	1,288
Ukraine	UA	45	0.8%	1.6%	36	1.0%	-19.7% ↓	38,619	615
United Kingdom	UK	49	0.7%	0.9%	55	0.6%	30.3% ↑	898,229	8,503
Moldova	MD	50	0.7%	1.4%	N/A	N/A	N/A	2,644	38
Belarus	BY	51	0.7%	1.4%	29	1.3%	-44.8% ↓	4,372	62
South Georgia and the South Sandwich Islands	GS	52	0.6%	1.2%	48	0.6%	-7.1% ↓	4,578	55
Czech Republic	CZ	54	0.6%	1.0%	54	0.6%	-4.7% ↓	101,781	1,068
Iran	IR	55	0.5%	1.1%	37	0.9%	-42.5% ↓	17,874	191
Lithuania	LT	56	0.5%	1.1%	44	0.8%	-36.9% ↓	11,517	121
United Arab Emirates	AE	58	0.5%	1.0%	65	0.5%	7.9% ↑	4,123	42
Belgium	BE	62	0.5%	0.9%	81	0.3%	49.2% ↑	123,606	1,124
Liechtenstein	LI	63	0.5%	1.0%	90	0.2%	110.3% ↑	3,000	29
Hungary	HU	65	0.4%	0.9%	53	0.6%	-23.9% ↓	71,650	614
Germany	DE	66	0.4%	0.5%	83	0.3%	43.8% ↑	1,504,163	7,052
Saudi Arabia	SA	67	0.4%	0.9%	42	0.9%	-48.7% ↓	2,630	23
Bosnia	BA	68	0.4%	0.9%	46	0.8%	-43.9% ↓	2,671	23
Finland	FI	71	0.4%	0.8%	85	0.3%	41.5% ↑	35,046	283
Spain	ES	73	0.4%	0.7%	27	1.6%	-75.6% ↓	103,555	749
France	FR	75	0.4%	0.7%	61	0.5%	-24.8% ↓	244,237	1,626
Austria	AT	76	0.4%	0.7%	89	0.2%	58.4% ↑	139,244	966
Israel	IL	77	0.4%	0.7%	31	1.2%	-70.4% ↓	29,113	209
Turkey	TR	79	0.4%	0.7%	47	0.7%	-46.6% ↓	36,466	252
Sweden	SE	80	0.4%	0.7%	88	0.3%	35.8% ↑	102,870	684
Norway	NO	82	0.3%	0.6%	77	0.4%	-8.5% ↓	50,089	317
Greece	GR	83	0.3%	0.6%	73	0.4%	-22.7% ↓	41,357	243
Luxembourg	LU	86	0.3%	0.6%	98	0.1%	102.4% ↑	6,750	38
Italy	IT	87	0.3%	0.5%	78	0.3%	-17.6% ↓	314,171	1,495
Estonia	EE	89	0.3%	0.5%	76	0.4%	-30.1% ↓	11,302	58
South Africa	ZA	90	0.3%	0.5%	96	0.2%	50.6% ↑	72,629	357
Portugal	PT	91	0.2%	0.5%	86	0.3%	-13.2% ↓	38,869	189

Europe, Middle East, and Africa (EMEA) region (cont.)

HIGH RISK **LOW RISK**

Country or Name	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	2010 Total Domains Tracked	2010 Total Risky Domains
Netherlands	NL	93	0.2%	0.3%	84	0.3%	-24.4% ↓	583,943	1,980
Bulgaria	BG	94	0.2%	0.5%	43	0.8%	-73.1% ↓	17,974	81
Denmark	DK	95	0.2%	0.4%	91	0.2%	0.7% ↑	151,472	627
Iceland	IS	96	0.2%	0.4%	87	0.3%	-19.8% ↓	6,102	26
Slovenia	SI	97	0.2%	0.4%	79	0.3%	-36.6% ↓	11,339	48
Switzerland	CH	99	0.1%	0.3%	95	0.2%	-13.3% ↓	217,863	572
Ireland	IE	100	0.1%	0.2%	101	0.1%	-5.7% ↓	32,120	71
Croatia	HR	101	0.1%	0.2%	100	0.1%	-11.1% ↓	22,511	50
Guernsey	GG	102	0.1%	0.2%	57	0.6%	-81.1% ↓	12,092	25

Note: Entries marked "N/A" were new TLDs in the report this year, so there is no year-over-year change.

- Two EMEA TLDs increased significantly in risk this year compared to 2009: .PL (Poland) moved from number 60 to number 20 this year, and .AM (Armenia) moved from number 23 to number five in risk.
- .PL has domains associated with all of the various risks, including malicious activity, malicious downloads, and hosting URLs affiliated with spam attacks and campaigns.
- The risks associated with .AM are more focused, concentrating on malicious activities, including command-and-control and other such services.

Generic and sponsored TLDs

HIGH RISK **LOW RISK**

Name	Region	TLD	2010 Worldwide Risk Rank	2010 Weighted Risk Ratio	2010 Unweighted Risk Ratio	2009 Worldwide Risk Rank	2009 Weighted Risk Ratio	Year-to-Year Change in Weighted Risk	2010 Total Domains Tracked	2010 Total Risky Domains
Commercial	Generic	COM	1	31.3%	6.1%	2	32.2%	-2.8% ↓	15,530,183	948,995
Information	Generic	INFO	2	30.7%	46.6%	5	15.8%	94.5% ↑	533,711	248,806
Asia-Pacific	Generic	ASIA	7	10.3%	20.6%	N/A	N/A	N/A	3,122	642
Network	Generic	NET	8	10.1%	10.5%	7	5.8%	73.7% ↑	1,556,813	163,466
Organization	Generic	ORG	12	6.4%	7.4%	11	4.2%	50.3% ↑	1,224,870	90,290
Business	Generic	BIZ	13	6.3%	11.8%	13	3.6%	74.3% ↑	121,622	14,350
Families and Individuals	Generic	NAME	29	1.7%	3.3%	16	3.1%	-45.9% ↓	6,726	223
Mobile Devices	Generic	MOBI	33	1.5%	3.0%	25	1.7%	-14.4% ↓	6,861	204
Governmental	Generic	GOV	84	0.3%	0.6%	104	0.0%	1,188.3% ↑	6,415	38
Catalan	Sponsored	CAT	103	0.1%	0.2%	99	0.1%	-31.6% ↓	3,936	7
Educational	Generic	EDU	105	0.1%	0.1%	102	0.1%	-48.6% ↓	14,002	15
Travel and Tourism Industry	Generic	TRAVEL	106	0.0%	0.0%	92	0.2%	-88.6% ↓	2,013	1

- Almost half (47%) of the evaluated Information (.INFO) sites were red or yellow, with most of those sites (43%) being red. Many of the risks identified within the .INFO TLD are associated with the hosting of content used for spam campaigns. This content may be about goods, malware, or fake anti-virus. In addition, there were many sites within the .INFO TLD that were affiliated with other malicious domains and servers. Many of these sites later became evident in fake anti-virus campaigns and Zeus botnet activity.
- More than 14% of Koobface URLs (45,213) were within Commercial (.COM), with no significant presence within other TLDs.

Red versus yellow risk bias

Red ratings are given to websites that contain malicious code (such as Trojans, viruses, and spyware) or browser exploits or have earned a dangerous reputation as a result of their correlated file, email, web, and network reputation. Yellow ratings are given to sites that merit caution before using, often due to spamminess, aggressive popups, or links to risky sites.

Most TLDs have a mix of red and yellow sites. Some, however, have a strong bias toward yellow or red. For example, of Asia-Pacific region's (.ASIA) 642 risky domains, 619 were yellow. In contrast, 100% of the domains that were risky in Governmental (.GOV), Iceland (.IS), Educational (.EDU), and Travel and Tourism Industry (.TRAVEL) were red. As it happens, we do not need to worry about these four TLDs very much. None of these four TLDs had more than 40 risky sites total, and they are all generally safe. However, Vietnam (.VN) had 14,492 red sites, representing 99.89% of its risky sites, and helping to justify its position as third riskiest TLD.

Biased toward yellow

Country or Name	TLD	Total Risky Sites	Percent Yellow	Percent Red
Asia-Pacific	ASIA	642	96.4%	3.6%
Armenia	AM	760	94.2%	5.8%
Finland	FI	283	89.1%	11.0%
Tokelau	TK	14,630	86.3%	13.7%
Cocos (Keeling) Islands	CC	11,869	85.5%	14.5%
Canada	CA	2,777	82.0%	18.0%
United Kingdom	UK	8,503	77.8%	22.2%
Tuvalu	TV	1,316	77.7%	22.3%
Mobile Devices	MOBI	204	76.0%	24.0%
Malaysia	MY	221	74.7%	25.3%
Niue	NU	1,362	73.3%	26.7%
Sweden	SE	684	65.2%	34.8%
Federated States of Micronesia	FM	60	65.0%	35.0%
New Zealand	NZ	416	61.8%	38.2%
Colombia	CO	106	56.6%	43.4%
Western Samoa	WS	3,734	55.8%	44.2%
China	CN	21,711	55.5%	44.5%
Russia	RU	55,373	55.4%	44.6%
Peru	PE	60	51.7%	48.3%
Australia	AU	871	51.7%	48.3%

Biased toward red

Country or Name	TLD	Total Risky Sites	Percent Yellow	Percent Red
Governmental	GOV	38	0.0%	100.0%
Iceland	IS	26	0.0%	100.0%
Educational	EDU	15	0.0%	100.0%
Travel and Tourism Industry	TRAVEL	1	0.0%	100.0%
Vietnam	VN	14,492	0.1%	99.9%
Turks and Caicos Islands	TC	338	3.3%	96.8%
Poland	PL	17,398	3.5%	96.5%
Trinidad and Tobago	TT	165	4.2%	95.8%
East Timor	TL	51	5.9%	94.1%
Croatia	HR	50	8.0%	92.0%
Serbia	RS	35	8.6%	91.4%
Information	INFO	248,806	8.6%	91.4%
Nauru	NR	58	8.6%	91.4%
Saudi Arabia	SA	23	8.7%	91.3%
Hungary	HU	614	9.1%	90.9%
United Arab Emirates	AE	42	9.5%	90.5%
Business	BIZ	14,350	9.8%	90.2%
São Tomé and Príncipe	ST	880	10.3%	89.7%
Thailand	TH	130	10.8%	89.2%
Georgia	GE	162	11.1%	88.9%
Turkey	TR	252	11.5%	88.5%
Christmas Island	CX	136	11.8%	88.2%
Guernsey	GG	25	12.0%	88.0%
Uruguay	UY	33	12.1%	87.9%
Laos	LA	122	12.3%	87.7%
Montserrat	MS	213	13.6%	86.4%

A Different Type of Zombie: Malware That Never Dies

One of the biggest news items from early June was a massive SQL-injection attack. A "spatter" attack across tens of thousands of websites inserted an iFrame that redirected users to a malicious page, which then downloaded and executed a file. These attacks happen periodically—at least once a quarter.

Once the malicious domain is taken down, the news and concern over that particular attack fades into the background. But what we don't hear about are the number of sites that fail to clean up after such an attack. One month after the June attack, known as ww.robint.us, we counted 51,900 sites that were still infected with this SQL injection.

This lack of housecleaning is not unique. The attack 2677.in still redirects users on 26,800 web pages, yahoosite.ru still impacts 1,380 sites, the killpp.cn exploit from 2008 is still present on 680 pages, and k.18xn.com plagues another 538 sites. These problems will likely become much worse as the dynamic and fluid nature of the web makes it easy to inject and hide attacks.

—McAfee Threats Report: Second Quarter 2010

The Changing Threatscape

Malware volumes continue to climb in 2010, with the first six months of 2010 being the most active half year ever for total malware production.[4] The types of malware are evolving, with more auto-run software (started from USB devices), more rogue anti-virus (fake-alert software), more social networking malware, and much more personalized and credible spam. Advanced persistent threats (APTs) can combine several techniques to work their swindles or execute their attacks, so a website is just one part of the threat puzzle.

Social networking sites make a criminal's work easier, since malicious or disguised links can be included in posts and messages from friends who enjoy "transitive trust." I trust you, so I can trust your "friend," right? Since 2008, the Koobface worm has been exploiting these trust networks to find new victims for their malicious code and new zombie bots for their botnets.[5] There was significant Koobface worm activity in 2010. We categorized 315,415 URLs as malicious in relation to Koobface. More than 14% of these URLs (45,213) were within our riskiest TLD, .COM, with no significant concentration within other TLDs.

A microcosm of this malware maelstrom was this year's second riskiest TLD: .INFO. Clicking on a link to this domain had a 47% chance of landing you on a risky page. When we researched the threat types for .INFO, the vast majority were flagged as risky because of how they registered themselves and their domain reputations, drawn from our database of suspicious activities observed over time.

The next .INFO risk factor was malicious sites. Some of these sites serve malware, exploits, or a variety of both. Some serve as a command-and-control server, a compromised server, or a domain on a bot-owned server. Many sites contained downloads for rogue anti-virus (also known as scareware and fake alert software) and Zeus botnet malware, reflecting the dominant activities in the overall threatscape.

The Zeus botnets use especially sophisticated techniques to circumvent strong authentication systems used for online banking, including single-use passwords, so they pose a particularly thorny and serious threat to consumers and businesses. Finally, phishing sites represented a significant percentage of .INFO's red sites.

The more we work, the more work we have

As TLD registrars tighten restrictions on using their domains, criminals look for other ways to exploit the web. Readily available malware toolkits hook into weak security in Web 2.0 technologies, such as AJAX, XML, Flash, iFrames, and JavaScript, and poorly configured or maintained browsers, computers, and websites. Infinite combinations of tools and software vulnerabilities make it easy to plant risky content within otherwise legitimate domains. This user-invisible content requires no user "click to download" to exploit vulnerabilities in the browser.

For example, a hacker might use a special attack called a SQL injection to implant a specific type of invisible code called an iFrame. The iFrame, which can be as small as a pixel and hidden behind other images or popup screens, includes a URL that silently redirects users to a site where they receive the malicious payload.

In an attempt to thwart browser detections of faked URLs, the embedded iFrame may use URL shortening services such as bit.ly or Tinyurl to disguise the URL.

URL shortening services are trying to do a better job of recognizing this abuse, but their efforts so far have been easy to circumvent. For example, criminals can detect the place of origin of visitors and select only the traffic they want to connect to their site.

[4] *McAfee Threats Report: Second Quarter 2010*, available for download in multiple languages at http://www.mcafee.com/us/threat_center/white_paper.html

[5] Craig Schmugar, "Koobface remains active on Facebook," McAfee Labs Blog. www.avertlabs.com/research/blog/index.php/2008/12/03/ koobface-remains-active-on-facebook/

By using cross-site redirection, the attacker separates the content from the initial line of attack. The content can thus be reused in serial efforts, as well as versioned or changed slightly to avoid frequency-based detection tools. Is that flavor of Koobface or Zeus getting too well known? Try this one instead.

Fast moving, topical targets

It is possible to insert malicious material in poorly protected sites, as well as any user-generated content, whether a JPEG file, a blog, or a forum. Although poorly maintained sites often host known malware for months or years (see sidebar on page 21), some of the most clever threat actors appear and disappear within a few hours. A botnet command-and-control center might be "awake" for just five minutes a day.

To protect against these fleeting—but lucrative—activities, URL-level or path-level evaluations must be updated frequently. That's why web users benefit from content inspection (scans for the latest malware) performed in real-time.

After planting malware on a site, poisoned search terms remain one of the most popular—and subtle—ways for criminals to drive traffic to their sites. Criminals pay attention to disasters, celebrity shenanigans, sporting events, and other hot topics. They build ads and fabricate websites with popular terms, get them indexed by search engines, then use botnets and click engines to elevate their content to the first page of search results. When users click on these items in the search results, they travel to sites where they collect malicious downloads. A malicious site could be a new one, created for the purpose with topical content, or an innocent site that has been hacked.

Any and all of these approaches pay off with personal information, account logins, account data on friends, passwords, and botnet zombies.

Going mobile

Ranking number 33 in risk, Mobile Devices (.MOBI) was one of the safer TLDs on the web this year, but we are tracking it and overall mobile web usage closely. For example, more attacks now incorporate mobile devices. The Zeus botnet can ask users for their mobile numbers and an authorization number, and then use that information in a financial transaction. If a spam message or web form collects a mobile number, that number can be used in subsequent efforts, sending more spam, phishing lures, or links to sites hosting malware. The millions of web-enabled smartphones out there simply amplify the opportunities for clever crooks.

"In 2009, 6% of the malicious URLs that McAfee identified and protected our users from were at the path level. Already in 2010, that percentage has increased to 16%."

—McAfee Threats Report: Second Quarter 2010

Comments From Top-Level Domain Registrars and Operators

In addition to our ideas, we wanted to bring you some perspective from the TLD community on the frontline of managing risk. We solicited comments from some of the TLDs we mentioned in this report, providing experiences, color, and context for our analysis.

.INFO (Information)

"As the steward of the .INFO registry, Afilias is committed to curbing abusive activity in the .INFO domain. That's why we established our industry-leading Anti-Abuse Policy in 2008 and have been working proactively with our registrars (who sell directly to the end registrants) to proactively fight phishing and other abuses.

Unfortunately, .INFO's growth in popularity has attracted the attention of spammers, and we have started deploying some new tactics accordingly; there is more to do. The challenge is made difficult because as a gTLD registry operator, Afilias is not allowed to decide who sells .INFO domain names, or to whom.

.INFO is home to millions of useful and legitimate sites, so blocking email simply based on the TLD address is inadvisable and can unfairly harm more innocent victims. Rather, more sophisticated email filtering methods can provide relief without undesirable side effects."

—Roland LaPlante
Senior Vice President
and Chief Marketing Officer
Afilias

.JP (Japan)

"I believe that our ongoing efforts to improve safety of the JP domain names have led to the increase of the registrants' and users' confidence in JP domain.

To register a JP domain name, you need to satisfy eligibility requirements. Especially, Organizational Type JP domain name registration (e.g., EXAMPLE.CO.JP) has different requirements depending on the type of domain (e.g., only companies incorporated in Japan can register EXAMPLE.CO.JP).

If a registered JP domain name is found to be short of these requirements, the registration is invalidated following proper procedures.

In this case, in the past, JPRS as the registry checked the status and took action to invalidate the name if appropriate, through the JP Registrars. In June 2008, JPRS reinforced the JP domain name registration rule for CO.JP and made it possible for the registry to cancel the false registrations if the cancellation by the Registrars does not work. Furthermore, in November 2009, we extended the scope of the rule to all Organizational and Geographic Type JP domain names.

By enhancing these rules and through continuous cooperation with the JP Registrars, JPRS rigorously and expeditiously addresses the issue of false registrations.

We also take measures to tackle the problem of domain names which are registered and used for fraudulent activities like phishing. Through cooperation with JPCERT/CC and the other related organizations, JPRS examines the degree of malevolence of the allegedly abused domain name. If it is confirmed the name is abused, JPRS request the JP Registrar to invalidate the name.

In addition, JPRS has continuously implemented, since 2006, deletion of DNS server registration in the case where the host name contains non-existing JP domain name.

With regard to Domain Name System Security Extensions (DNSSEC), we plan to start signing JP zone in October 2010 and to introduce DNSSEC to the JP domain name services in January 2011. Moreover, with an aim to promote community-wide introduction and spread of DNSSEC, a forum called 'DNSSEC Japan' was established in November 2009. One of the staff members of JPRS serves as the vice chair of the forum.

These persistent efforts have worked well; for example, the number of phishing complaints which JPRS receives has been at a very low level, about one complaint a month."

—Yumi Ohashi
International and Government Relations Manager
JPRS

.SG (Singapore)

"The Singapore Network Information Centre (SGNIC) encourages the adoption and usage of '.SG' domain names by businesses and individuals. Besides better identifying themselves with users and customers in Singapore, they could also extend their presence to the global market.

Visitors to a '.SG' website can be assured that it is governed by SGNIC's registration requirements to ensure accountability. This is because a '.SG' domain name applicant is required to show appropriate documentation when it seeks to register a domain name under the various categories of '.sg' names, which reflect their entity status. For instance, a '.com.sg' registrant would need to provide proof that it is a commercial entity registered with the Accounting Regulatory Authority of Singapore (ACRA) or any professional body, while a '.EDU.SG' registrant has to register with the Ministry of Education (MOE) or be recognised by other relevant agencies. For registrations by foreign corporations, the applications have to be supported by a Singapore contact address.

When SGNIC receives adverse feedback about the usage of a '.SG' domain name, it will investigate immediately, work closely with its registrars, and where appropriate, consult relevant agencies to ensure compliance with its registration rules. Any name involved in cases of misrepresentation or fraud, or is used to host material that breaches the laws or rules of the regulatory authorities are rectified by registrants, failing which, they are liable to be suspended or deleted by SGNIC. As Internet content can be hosted anywhere, even after a name has been registered in Singapore, SGNIC works actively with the international Internet community, including specialised groups in Internet security and stability, to monitor and prevent potential abuse of '.SG' domain names.

SGNIC believes that these measures have helped ensure that the '.SG' domain names continue to be secure and used for lawful purposes."

—Mr. Lim Choon Sai
General Manager
Singapore Network Information Centre Pte Ltd.

.WS (Western Samoa)

"Over the course of the last year, we have focused on reducing the number of risky domains under our .WS TLD by employing additional verification and security modules to our registry's infrastructure. The proactive monitoring of domain registrations allows us to prevent malicious content from becoming public.

We have also partnered with established online security and safety companies to implement an enhanced feedback system that will quickly notify us of potentially malicious domains that may be later detected by website visitors. As we become more aware of how new threats online are created and deployed, we are able to identify and neutralize potential issues before they cause any damage. Combined with this information and strengthening ties with our .WS-accredited registrars, we have succeeded in developing a notification system to advise registrars of potentially malicious domain name registrations. Similarly, a service for notifying web hosts that provide hosting services for .WS domains is also active. To combat email spam, advanced monitoring of email activity from our servers allows for spammers to be recognized quickly, and their efforts prevented.

As the official Registry for the .WS top-level domain, we have always valued our reputation throughout the online community since we launched the zone over a decade ago. Global Domains International was one of the first companies to become part of the Conficker Working Group at the Registry level. We worked closely with them assisting their efforts to identify the worm and mitigate its damage, and we continue doing so to ensure our .WS TLD is not used to proliferate the Conficker threat.

The modifications made to our Registry system are constantly transforming to appear congruent with ever-changing abuse tactics. As a result of becoming familiar with popular methods employed by those attempting to engage in malicious activity online, we can ensure integrity and safety within the .WS zone."

—Alan Ezeir
President
Global Domains International

Conclusion

The level of risk is rising while the types of risk on the web change faster every day. As more criminals find ways to bury and disguise their activities, web users must find new ways to stay on top of these threats while preserving the joy and value of surfing the web.

Consumers may not be able to remember all of the risky places in this report. Even if they could, we have demonstrated that one year's riskiest TLD may be the next year's most improved. Consumers can avoid the dangerous places on the web by using reputable, actively updated computer security software with safe search functionality, such as McAfee Total Protection™. This is one case where it is an especially good idea to let technology help.

Businesses today know that the web is integral to operations, and that many employees feel that they have the right to web access while working. This expectation will increase as work and home life become blurred with a more mobile and remote workforce, more use of personal devices, and a relentless shift to constant connectivity. The simplest way to help users navigate web risks is to add web reputation functionality to their other defenses. Visual cues updated in real-time can help educate them about risk while actively protecting them against it.

Operators of risky TLDs should find hope in this report. It is very possible to turn around a risky reputation or maintain a good one. Dedicated security companies like McAfee are committed to helping you. With the world's most extensive global threat intelligence network, we can offer you fresh data on what is happening and clever ideas for what you can do to reduce your exposure.

Next year, we may find that botnets of zombies have been superseded by a new tactic that hinges on the hundreds of millions of data-capable mobile devices in hands worldwide. We look forward to reporting their progress—and the countermeasures of TLD registrars and the security community—next year.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by unrivaled McAfee Global Threat Intelligence, 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. McAfee secures your digital world.

http://www.mcafee.com

McAfee, Inc.
2821 Mission College Blvd
Santa Clara, CA 95054
1.866.622.3911
www.mcafee.com

10902rpt_mapping-mal-web_0910