

McAfee®



Protect what you value.

Mapping the Mal Web, Revisited

May 2008

Shane Keats
Research Analyst, McAfee

Table of Contents

Introduction and Key Findings.....	3
Methodology.....	4
Category Breakouts.....	5
TLD Breakouts.....	7
Detailed Discussion of the Data.....	8
Conclusion.....	9
Complete Data Matrices.....	10

Mapping the Mal Web, Revisited

Introduction and Key Findings

In March 2007, McAfee released the first comprehensive map of malicious web sites across the world. For the first time, *Mapping the Mal Web* offered a comprehensive guidebook for web tourists—where it was safe to surf and where searchers should avoid. A year later, we revisited the data and found both remarkable continuity—and remarkable change—in the web safety landscape.

- Overall risk in 2008 remains roughly constant compared to 2007, with 4.1 percent of web sites in these 74 domains rated red (avoid) and yellow (use caution), the same percentage as last year.
- At 5.26 percent, .com (the most heavily trafficked top-level domain, or TLD) is riskier than the average web site by 1.16 percentage points, or 28.3 percent.
- Hong Kong (.hk) soared in 2008 to become the most risky country TLD, with 19.2 percent of all sites tested rated red or yellow. China (.cn) was second with 11.8 percent. By comparison, last year, Tokelau (.tk) was first with 10.1 percent.
- The most risky generic TLD remains .info, with 11.8 percent of all sites tested rated red or yellow. The most popular domain, .com, is rated ninth riskiest overall with 5.3 percent, and is the fourth riskiest generic TLD.
- In the Europe, Middle East, and Africa regions, Romania (.ro) and Russia (.ru) continue to be risky surfing destinations; 6.8 percent of Romanian and 6.0 percent of Russian domains are rated risky.
- In the North, South, and Latin America regions, the United States (.us) domain is riskiest, with 2.1 percent. The Americas TLDs remain relatively safe to surf.
- The five least-risky TLDs are Slovenia (.si), Norway (.no), Japan (.jp), Governmental (.gov), and Finland (.fi), each with 0.2 percent or fewer domains rated risky.
- Risk is distributed very unevenly. Of the 74 TLDs we rated, just 10 are riskier than average: Hong Kong (.hk), China (.cn), Information (.info), the Philippines (.ph), Romania (.ro), Network (.net), Families and Individuals (.name), Russia (.ru), Commercial (.com), and Business (.biz).
- The prevalence of exploit code—sites with malicious, drive-by downloads—remains very rare. On average, just 0.0717 percent (seven-hundredths of 1 percent) of sites rated included malicious exploits. In other words, during a series of random visits to 10,000 web sites, an average surfer would encounter just seven with exploit code.
- While exploits remain exceedingly rare, they are also exceedingly dangerous. Some domains are dramatically more risky than others. We found exploit code on 1.1 percent of all Romania (.ro) sites we tested. The surfer to a Romanian (.ro) web site is 1,559 percent more likely to encounter malicious drive-by code than the surfer to an average web site anywhere in the world.
- Email registration is slightly more risky than last year. Of those sites tested for email, we found 7.6 percent to be at risk for high volume, highly commercial email, compared to 7.0 percent last year, an increase of 0.6 percentage points or 8.4 percent.
- As with exploits, wide disparities were found with email risk. Registering an email address at a Chinese (.cn) web site is dramatically more risky than it was last year. Test registrations receiving high volume, spammy email more than doubled, from 17.2 percent to 39.7 percent. Information (.info) registrations improved by 14.9 percentage points, but remained very risky, going from 73.2 percent to 58.3 percent.

- Sites that offered downloads with viruses, spyware, and adware increased over last year: 4.7 percent of sites offering downloads were rated red or yellow for those payloads, compared to 3.3 percent last year, an increase of 1.4 percentage points or 41.5 percent.
- While some TLDs remained dramatically more risky to download from (21.9 percent of .info download sites were risky), some TLDs improved. For example, downloading a program from a random Venezuelan (.ve) web site is significantly less risky than it was last year. In 2007, 4.5 percent of Venezuelan sites were risky for downloads. In 2008, just 0.5 percent were risky, a decrease of 4.0 percentage points or almost 90 percent improvement.

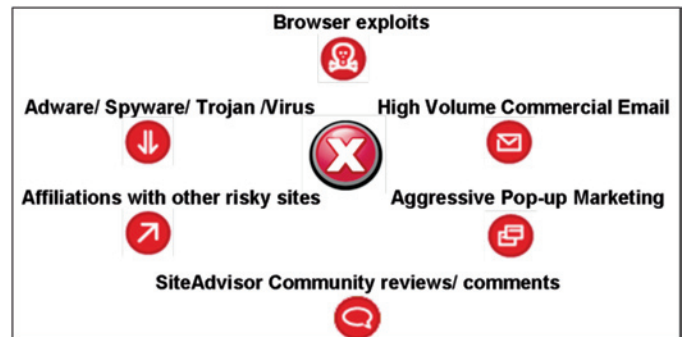
Methodology

Like last year, this report compares the ratings of sites found in each of 265 *country* (example: .br for Brazil) and *generic* (example: .com) TLDs. These domains are then ranked by their risk.

Our site safety assessments come from the McAfee® SiteAdvisor® web safety database. Last year at this time, we had rated 8.1 million of the most trafficked web sites that together accounted for more than 95 percent of web traffic. This year, our rankings are based on 9.9 million site reports, an increase of 23 percent. These sites have been tested for a wide variety of unwanted behaviors.

- **Web sites** are tested for browser exploits, phishing, and excessive pop-ups. Browser exploits, also known as drive-by downloads, enable viruses, keystroke loggers, or spyware to install on a consumer’s computer without their consent and often without their knowledge.
- **Downloads** are analyzed by installing software on our test computers and checking for viruses and any bundled adware, spyware, or other unwanted programs.
- **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.

- **Feedback** from individual users and site owners, plus analysis by McAfee SiteAdvisor staff, enhance McAfee SiteAdvisor’s automated testing.



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

Our analysis measures risk in four ways:

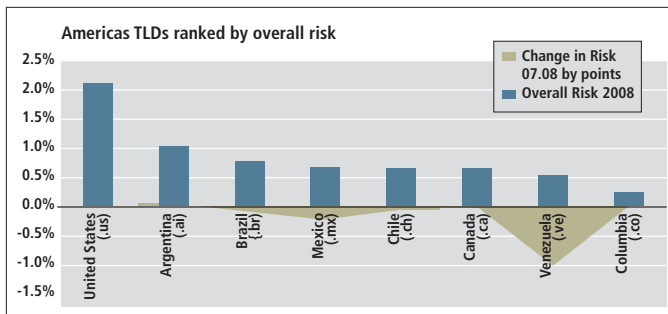
- Percent of red- and yellow-rated sites
- Percent of red- and yellow-rated sites, of those with tested downloads
- Percent of red- and yellow-rated sites, of those with tested email practices
- Percent of sites in that domain rated red for exploits

The rankings are restricted to 74 top level domains, each containing at least 2,000 sites tested by SiteAdvisor. Last year, we ranked 71 TLDs. The European Union (.eu), Indonesia (.id), and Iran (.ir) TLDs are new this year. Additional discussion of data collection can be found below.

Category Breakouts

The Americas TLDs

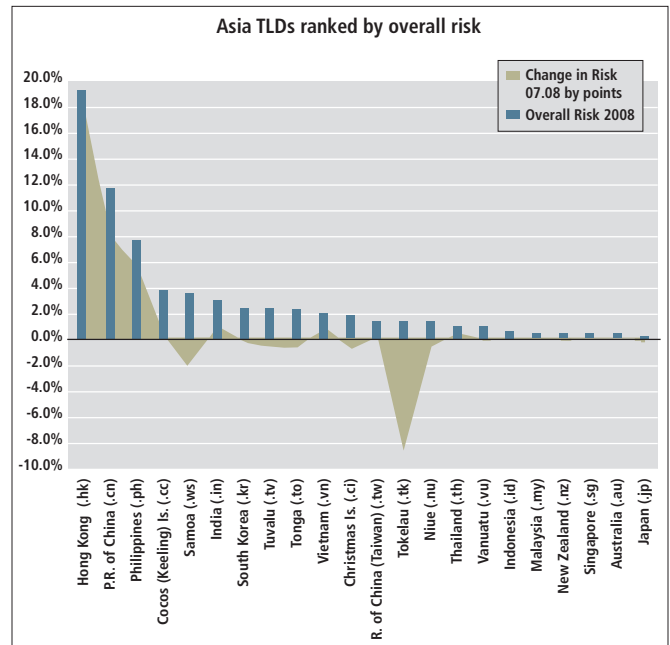
- In general, TLDs from the Americas are less risky than average. Aside from the United States and Canada, no countries from the Americas have more than [50 percent Internet access penetration](#). Since economically motivated scammers seek the largest potential victim pool, that may explain why they target Americas TLDs relatively less frequently.



[Complete Americas results](#)

Asia/Pacific TLDs

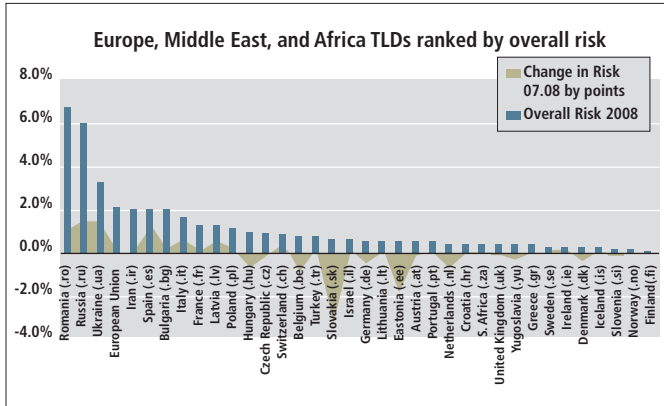
- Asia is a study in contrasts with both the most (.hk) and one of the least (.jp) risky TLDs.
- Hong Kong (.hk), which was ranked twenty-eighth most risky overall in 2007, is now the most risky TLD.
- China (.cn) also experienced a big increase in overall risk, from 3.7 percent risky sites to 11.8 percent, a jump from eleventh place to second. The Philippines (.ph) also experienced a major increase in risk of 270.1 percent.
- Part of the increase in relative risk for .hk, .cn, and .ph is due to improved data collection. Real-time data feeds on phishing and spammer domains added significant numbers of new risky domains to these TLDs.
- Countries with restrictive registration policies like Japan (.jp) and Australia (.au) continue to enjoy safe surfing environments.
- Tokelau (.tk) and Samoa (.ws) are notably safer this year, with declines of 85.8 percent and 35.4 percent respectively.



[Complete AsiaPacific results](#)

Europe, the Middle East, and Africa TLDs

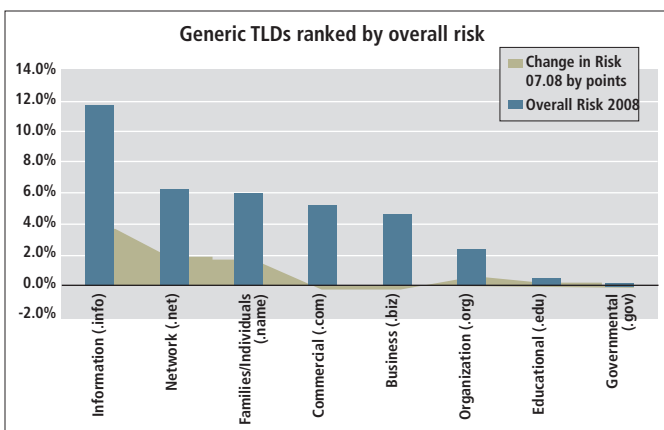
- Romania (.ro) and Russia (.ru) remain the riskiest TLDs in Europe, are more risky than the web in general, and became riskier from 2007 to 2008.
- The European Union (.eu), one of three new TLDs to be added to the list, is the nineteenth most risky TLD but at 2.2 percent is almost half as risky as the 4.1 percent average.
- Spain (.es), a major country with significant web traffic, experienced a sharp 91 percent increase in risk, from 0.6 percent to 2.0 percent of all tested sites earning a red or yellow rating. Spain remains relatively less risky than the web on average.
- Some of the increase in risk for .es is due to real-time data feeds on phishing and spammer domains, which added significant numbers of new risky domains to this TLD.
- Two other web traffic powerhouses, Germany (.de) and the Netherlands (.nl) experienced strong declines in risk, 42.3 percent and 54.9 percent respectively. Big declines in major countries like these suggest that on a weighted traffic basis, surfing European web sites may have gotten somewhat less risky over 2007.



[Complete Europe, the Middle East, and Africa results](#)

Generic TLDs

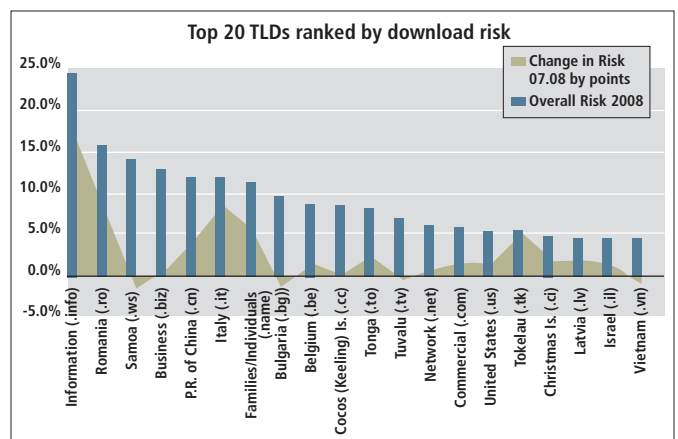
- The riskiest generic TLD remained .info from 2007 to 2008 and increased its percentage of risky sites from 7.5 percent to 11.7 percent.
- Real-time data feeds on phishing and spammer domains added significant numbers of new risky domains to .info, .net, and .org. This accounts for some of the increase in risk for these TLDs.
- The .com and .biz TLDs both improved slightly, by 4.8 percent and 5.6 percent respectively. Because they are responsible for so much web traffic, the weighted chance of surfing to a risky generic TLD is probably slightly less likely in 2008 than 2007.
- The .gov TLD remains exceedingly safe. However, our test results showed a few risky sites in 2008, unlike last year where we did not find any red- or yellow-rated sites.



[Complete generic results](#)

Top 20 TLDs ranked by percentage of sites with red and yellow download ratings

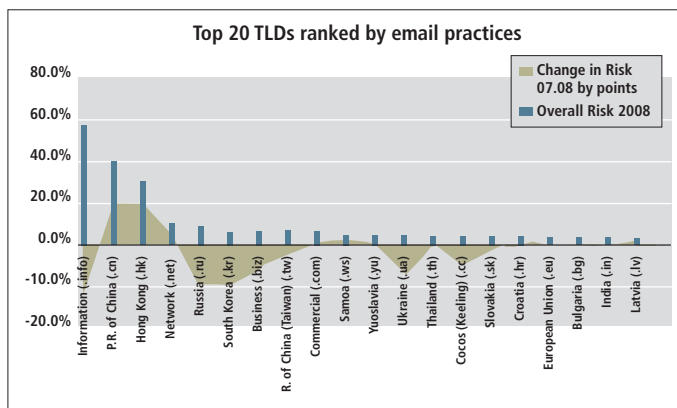
- Overall, the chance of downloading spyware, adware, viruses or other unwanted software increased 41.5 percent over 2007, from 3.3 percent of tested sites to 4.7 percent.
- Significant 100+ percent increases in risky downloads were recorded for the Information (.info), Romania (.ro), and Italy (.it) TLDs. Of those .it sites for which we tested downloads, 10.6 percent were risky, an increase of 7.5 percentage points, or 236 percent. Overall, however, Italy (.it) remains quite safe, with just 1.6 percent of all sites rated risky.
- A casual surfer who downloads at random has a one-in-five chance of downloading from a risky .info site, a one-in-seven chance of downloading from a risky .ro site, and nearly a one-in-10 chance of downloading from a risky .it site.
- Downloaders from the next three most risky TLDs—Samoa (.ws), Business (.biz), and China (.cn)—are, on average, 235 percent more likely to do so from a risky site than downloaders on average, and 830 percent more likely than downloaders from sites in Australia (.au), Mexico (.mx), and the United Kingdom (.uk), the fifty-third, fifty-fourth, and fifty-fifth most risky.
- Note that not all downloads from sites rated red or yellow are risky. A site with a mix of green-, yellow-, and red-rated downloads will be rated red for overall download risk.



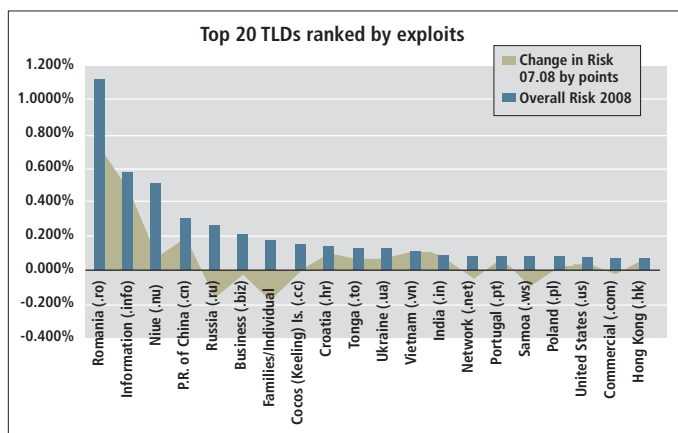
[Complete download results](#)

Top 20 TLDs ranked by percentage of sites with red and yellow email practices ratings

- Overall, users faced a slight increase in risk of high volume email, highly commercial email, or both; 7.6 percent of sites tested for email practices were rated risky this year compared to 7.0 percent last year, a change of 0.6 percentage points, or 8.4 percent.
- China (.cn) grew significantly worse over the year, increasing 22.5 percentage points, from 17.2 percent risky registrations to 39.7 percent. And while .info improved this year, dropping 14.9 percentage points, or 20.3 percent, it remains the most risky TLD to register at. Of the sites tested 58.3 tested, were risky for email practices.



[Complete email results](#)



[Complete exploit results](#)

Top 20 TLDs ranked by percentage of sites with exploits

- Overall, the number of sites we encountered with exploit or drive-by code remained roughly constant, at under one-tenth of 1 percent of all sites included in this study.
- Romania (.ro) grew even riskier, increasing 197.2 percent to take the "most exploited" slot from Niue (.nu) which dropped to third. The .info TLD increased 411 percent to take second place.
- Exploits remain very rare, but because a single visit to one of these sites can permanently disable a computer, they are very dangerous.

TLD Breakouts

Hong Kong

Hong Kong (.hk) experienced the most dramatic increase in overall risk this year, increasing 18.0 percentage points from 1.18 percent to 19.18 percent, an increase of 1,527.9 percent.

McAfee is not the only security company to find this. Reports of waves of .hk malware and spam came in throughout 2007, including a June notice from [Sunbelt](#) about greeting cards that carried the [Storm Worm](#). More broadly, in its "[Security Report 2007](#)," security firm [Sop'hos](#) ranked Hong Kong ninth for malicious code and second (in conjunction with China) for spam.

Bonnie Chun, an official with the [Hong Kong Domain Name Registration](#) Company, the registrar of the TLD, acknowledged that they had made some decisions that inadvertently encouraged the scammers:

1. "We enhanced our domain registration online process thus making it more user-friendly. Instances include the capability for registering several domains at one time, auto-copying of administrative contact to technical contact and billing contact, etc. Phishers usually registered eight or more domains at one time.
2. We offered great domain registration discounts, such as buy-one, get-two domains.
3. Our overseas service partners promoted .hk domains in overseas markets."

In a [presentation](#) at the Asia Pacific Computer Emergency Response Teams (APCERT) Conference in March 2008, Ms. Chun says that the registrar took strong action in the summer of 2007 to tighten policies that led to a dramatic decline in use of the .hk domain for spam and phishing.

According to Geok Meng, head of McAfee Avert® Labs Asia Pacific Malware Research Team, “Spam and malware syndicates seek paths of least resistance. When cybercriminals meet with resistance in the form of additional rules and regulations, they just move on to an easier target. I suspect .hk is a classic example.” His McAfee Avert Labs colleague, Vu Nguyen, speculates that, “One reason for .hk’s popularity could also be its access into and out of China. We know that China monitors traffic outbound through some very big Cisco routers, but I believe they do not apply the same filters for traffic bound to Hong Kong.” This difference could be a loophole that scammers exploited in 2007.

Registration cost as a predictor of risk

According to Michael Levine, author of *The Internet for Dummies* and a former member of ICANN’s *At-Large Advisory Committee*, one of the main reasons for a given TLD’s popularity among scammers is cost. Levine is not surprised, for example, that Tokelau (.tk) was the most risky TLD in McAfee’s first *Mapping the Mal Web* study last year. Domain registration there was free.

This tiny island of 1,500 inhabitants sold its TLD to a Dutch entrepreneur and the fees from the sale *generate 10 percent of the island’s GDP*. McAfee’s report *spurred* Dot TK, the country’s TLD manager, to reexamine its policies. The registrar installed software designed to weed out scam registrations, and, notes Levine, “They no longer offer unlimited free anonymous registration, with the free stuff now limited to URL and email forwarding.”

According to McAfee’s results, these changes are working. The amount of risky Tokelauan web sites dropped 8.7 percentage points, from 10.1 percent to 1.43 percent, an improvement of 85.8 percent.

By contrast, China (.cn) grew considerably riskier over the last year, increasing 8.0 percentage points from 3.73 percent to 11.76 percent, an increase of 215.2 percent. Similarly, .info grew 56.4 percent more risky, going from 7.50 percent to 11.73 percent. According to Levine, cost plays a role. “The very high numbers of bogus sites in .cn and .info makes sense because they are among the cheapest places to register, with the wholesale price for .cn now being about 15 cents.”

Detailed Discussion of the Data

Broader coverage

McAfee’s SiteAdvisor crawl improved significantly this year, adding both breadth (number of domains tested) and depth (number of pages tested within a domain). *Mapping the Mal Web* ranks only those TLDs where we’ve tested 2,000 or more domains. That subset of the larger McAfee SiteAdvisor dataset grew 15 percent, from 7.7 million to 8.8 million rated domains.

Our coverage of certain domains increased significantly. For example, the six TLDs with the biggest increases in rated domains were China (.cn) domains by 280 percent, Hong Kong (.hk) by 76 percent, Spain (.es) by 58 percent, Portugal (.pt) by 50 percent, Mexico (.mx) by 45 percent, and India (.in) by 44 percent. In each of these cases, the percent of overall red- and yellow-rated sites also increased.

We have not conducted deeper statistical analysis on this year’s data. Margins of error for our risk ratings for certain TLDs might be useful, particularly for those with significant increases in coverage or TLDs that just make our cutoff. Note that while 2,000 rated domains is our cutoff for inclusion in this study, last year, we tested more than 5,000 domains for each of the TLDs above.

Better detection

In the past year, McAfee has continued to improve both our download and exploit detections, and is now more accurate in the detection and flagging of *rogue anti-spyware programs*. In general, most improvements increase the number of risky actions we find (since we place the highest importance on improving areas of detecting bad things, as one would expect). It is worth noting that some part of the increase in the risk of a given TLD may be due to finding unsafe or undesirable activity that was already present.

New detections

For the first time, this study includes real-time data on phishing and spammer domains that have long been incorporated into the McAfee SiteAdvisor system but not this study. In particular, this new data had a measurable effect on increasing the overall risk of China (.cn), Hong Kong (.hk), Network (.net), Organization (.org), Information (.info), Philippines (.ph), Switzerland (.ch), and Spain (.es).

Mass attacks

One thoughtful, independent observer who was asked to preview this year’s data expressed concern that a mass attack could distort our risk rating for a particular TLD. The observer explained that perpetrators are becoming more and more crafty in their efforts and will rotate through domain names

quickly. If a perpetrator were to register *1a0000a1.example* through *1a9999a1.example* and cycle through their use in activity that SiteAdvisor would flag, and SiteAdvisor was not aware of these 10,000 domains prior to the campaign, it would create 10,000 more sites that SiteAdvisor is aware of and 10,000 more sites that are flagged.

The observer went on to note that if SiteAdvisor only monitored that the .example domain had 20,000 sites before that campaign, of which 1,000 were flagged, it would be 1,000/20,000 or 1/20 or 5 percent of the .example TLD being flagged domains. After the campaign, SiteAdvisor would be aware of 30,000 domains, of which 11,000 were flagged. This changes the numbers materially to where 11,000/30,000 or 11/30 or roughly 37 percent. This would then translate into a sevenfold increase in flagged domains in a given TLD.

We acknowledge the concern but note that if a mass attack altered a TLD's risk, this would only be inaccurate if those sites are really unlikely to be visited. Typically, a mass attack involves hijacking either existing sites and/or use of spam and advertising to promote these unsafe sites, in which case the mass attack should affect our results. For example, if we added the 10,000 new "attack" domains described above, and we found these sites at a higher proportional rate than "normal" domains, then it is accurate to say that the TLD has just become more unsafe to browse than before.

We believe our crawl techniques do generate an exceptionally accurate sampling of what the typical user will encounter during his or her use of the web. Among other techniques, we test sites based on third-party popularity, the sites visited by our user base (now many millions strong and distributed across the globe), the top results from search engines, and the top links we find on sites. These are, by definition, the most likely set of sites users will encounter.

Still, if we tested all or most of these "attack" sites at a higher priority than other sites, a case could be made that our overall risk rating for the TLD was skewed. However, we note that while we do try to find the bad domains as often as possible, our system is highly balanced—we focus more of our resources on testing popular domains than on focusing on the specialized "bad" domains (like a mass hijacking). Of course, we cover those attacks as well. With our resources, we can cover a 10,000-domain attack in a short time.

In subsequent years, we look forward to having more time to invite more in depth analysis of our data.

Conclusion

The web is remarkably diverse across so many dimensions. The *Mapping the Mal Web* study shows that this diversity extends to risk. Vast parts of the web are quite safe to visit, but many neighborhoods—big ones and small ones—put every visitor at risk of an online mugging. Whether that attack comes in the relatively mild form of a pop-up trap or something extremely serious like an unwitting experience with a keystroke logger, the web is dangerous to the user who does not exercise common sense.

And even a cursory glance at the data show that surfing based on past experience or conventional wisdom is not enough to stay safe online. Malicious and risky activity is remarkably fluid. A number of domains that were very risky or very safe in 2007 reversed in 2008. Improvements and declines in overall risk of 10 percent, 20 percent, or even 30 percent were not uncommon.

The bottom line is that whether the user is an IT expert or a computer novice, web use requires proper protection in the form of an up-to-date computer security suite and a comprehensive web site safety guide.

Complete Data Matrices

Legend

Risky Sites	Relative Risk
12%+	
9% 11.99%	
6% 8.99%	
3% 5.99%	
0.0% 0.99%	

Americas TLDs ranked by overall percentage of red and yellow sites

Name	% sites rated red and yellow 2008	% sites rated red and yellow 2007	Point change 2007-2008	% change 2007-2008	Red and yellow rank 2008	Red and yellow rank 2007	Change direction 2007-2008
United States (.us)	2.09%	2.07%	0.02%	1.1%	20	20	Worse
Argentina (.ar)	1.01%	0.98%	0.04%	3.6%	33	37	Worse
Brazil (.br)	0.76%	0.87%	-0.11%	-12.5%	41	40	Better
Mexico (.mx)	0.65%	0.88%	-0.23%	-26.3%	44	39	Better
Chile (.cl)	0.64%	0.69%	-0.06%	-8.0%	45	41	Better
Canada (.ca)	0.64%	0.68%	-0.04%	-5.9%	46	42	Better
Venezuela (.ve)	0.52%	1.54%	-1.01%	-65.9%	52	26	Better
Colombia (.co)	0.25%	0.26%	-0.01%	-2.3%	69	64	Better

Asia TLDs ranked by overall percentage of red and yellow sites

Name	% sites rated red and yellow 2008	% sites rated red and yellow 2007	Point change 2007-2008	% change 2007-2008	Red and yellow rank 2008	Red and yellow rank 2007	Change direction 2007-2008
Hong Kong (.hk)	19.15%	1.18%	18.0%	1,527.9%	1	28	Worse
P.R. of China (.cn)	11.76%	3.73%	8.0%	215.2%	2	11	Worse
Philippines (.ph)	7.72%	2.09%	5.6%	270.1%	4	19	Worse
Cocos (Keeling) Is. (.cc)	3.80%	3.67%	0.1%	3.6%	11	12	Worse
Samoa (.ws)	3.76%	5.82%	-2.1%	-35.4%	12	3	Better
India (.in)	3.07%	2.13%	0.9%	43.8%	14	18	Worse
South Korea (.kr)	2.39%	2.64%	-0.2%	-9.5%	15	15	Better
Tuvalu (.tv)	2.38%	3.03%	-0.7%	-21.5%	16	13	Better
Tonga (.to)	2.30%	3.01%	-0.7%	-23.6%	18	14	Better
Vietnam (.vn)	1.96%	1.16%	0.8%	69.2%	24	29	Worse
Christmas Is. (.cx)	1.83%	2.64%	-0.8%	-30.4%	25	16	Better
R. of China (Taiwan) (.tw)	1.47%	1.01%	0.5%	46.0%	27	34	Worse
Tokelau (.tk)	1.43%	10.10%	-8.7%	-85.8%	28	1	Better
Niue (.nu)	1.38%	2.05%	-0.7%	-32.8%	29	21	Better
Thailand (.th)	0.95%	0.55%	0.4%	71.9%	35	49	Worse
Vanuatu (.vu)	0.89%	1.08%	-0.2%	-17.8%	37	32	Better
Indonesia (.id)	0.61%	n/a	n/a	n/a	47	n/a	N/A
Malaysia (.my)	0.40%	0.30%	0.1%	35.1%	60	61	Worse
New Zealand (.nz)	0.34%	0.57%	-0.2%	-40.4%	62	48	Better
Singapore (.sg)	0.27%	0.26%	0.0%	4.4%	67	63	Worse
Australia (.au)	0.27%	0.22%	0.1%	23.8%	68	65	Worse
Japan (.jp)	0.13%	0.41%	-0.3%	-67.3%	72	57	Better

Europe, Middle East, and Africa TLDs ranked by overall percentage of red and yellow sites

Name	% sites rated red and yellow 2008	% sites rated red and yellow 2007	Point change 2007-2008	% change 2007-2008	Red and yellow rank 2008	Red and yellow rank 2007	Change direction 2007-2008
Romania (.ro)	6.76%	5.58%	1.2%	21.3%	5	4	Worse
Russia (.ru)	6.00%	4.50%	1.5%	33.3%	8	7	Worse
Ukraine (.ua)	3.22%	1.69%	1.5%	91.0%	13	24	Worse
European Union (.eu)	2.17%	n/a	n/a	n/a	19	n/a	N/A
Iran (.ir)	2.09%	n/a	n/a	n/a	21	n/a	N/A
Spain (.es)	2.05%	0.64%	1.4%	218.2%	22	45	Worse
Bulgaria (.bg)	2.04%	1.89%	0.1%	7.7%	23	22	Worse
Italy (.it)	1.63%	0.97%	0.7%	68.8%	26	38	Worse
France (.fr)	1.33%	1.16%	0.2%	14.8%	30	30	Worse
Latvia (.lv)	1.26%	0.67%	0.6%	87.9%	31	44	Worse
Poland (.pl)	1.18%	0.99%	0.2%	18.4%	32	35	Worse
Hungary (.hu)	0.99%	1.57%	-0.6%	-36.8%	34	25	Better
Czech Republic (.cz)	0.91%	0.99%	-0.1%	-8.0%	36	36	Better
Switzerland (.ch)	0.86%	0.48%	0.4%	81.1%	38	54	Worse
Belgium (.be)	0.84%	1.53%	-0.7%	-45.0%	39	27	Better
Turkey (.tr)	0.80%	0.54%	0.3%	48.3%	40	50	Worse
Slovakia (.sk)	0.69%	3.93%	-3.2%	-82.4%	42	10	Better
Israel (.il)	0.69%	0.50%	0.2%	36.7%	43	52	Worse
Germany (.de)	0.60%	1.05%	-0.4%	-42.3%	48	33	Better
Lithuania (.lt)	0.58%	0.49%	0.1%	17.0%	49	53	Worse
Estonia (.ee)	0.55%	2.30%	-1.8%	-76.2%	50	17	Better
Austria (.at)	0.53%	0.63%	-0.1%	-15.3%	51	46	Better
Portugal (.pt)	0.52%	0.38%	0.1%	36.7%	53	59	Worse
Netherlands (.nl)	0.49%	1.09%	-0.6%	-54.9%	54	31	Better
Croatia (.hr)	0.49%	0.47%	0.0%	3.8%	55	55	Worse
S. Africa (.za)	0.47%	0.46%	0.0%	2.3%	56	56	Worse
United Kingdom (.uk)	0.47%	0.53%	-0.1%	-10.9%	57	51	Better
Yugoslavia (.yu)	0.45%	0.67%	-0.2%	-32.5%	58	43	Better
Greece (.gr)	0.40%	0.39%	0.0%	2.3%	61	58	Worse
Sweden (.se)	0.33%	0.21%	0.1%	55.3%	63	66	Worse
Ireland (.ie)	0.30%	0.11%	0.2%	185.3%	64	69	Worse
Denmark (.dk)	0.30%	0.61%	-0.3%	-51.2%	65	47	Better
Iceland (.is)	0.29%	0.19%	0.1%	47.4%	66	67	Worse
Slovenia (.si)	0.21%	0.27%	-0.1%	-22.2%	70	62	Better
Norway (.no)	0.15%	0.16%	0.0%	-10.9%	71	68	Better
Finland (.fi)	0.05%	0.10%	0.0%	-46.8%	74	70	Better

Generic TLDs ranked by overall percentage of red and yellow sites

Name	% sites rated red and yellow 2008	% sites rated red and yellow 2007	Point change 2007-2008	% change 2007-2008	Red and yellow rank 2008	Red and yellow rank 2007	Change direction 2007-2008
Information (.info)	11.73%	7.50%	4.2%	56.4%	3	2	Worse
Network (.net)	6.28%	4.35%	1.9%	44.4%	6	8	Worse
Families/Individuals (.name)	6.07%	4.21%	1.9%	44.3%	7	9	Worse
Commercial (.com)	5.26%	5.53%	-0.3%	-4.8%	9	5	Better
Business (.biz)	4.67%	4.94%	-0.3%	-5.6%	10	6	Better
Organization (.org)	2.32%	1.77%	0.5%	31.1%	17	23	Worse
Educational (.edu)	0.44%	0.30%	0.1%	46.6%	59	60	Worse
Governmental (.gov)	0.05%	0.00%	0.1%	n/a	73	71	Worse

Top 20 TLDs ranked by percentage of sites with red and yellow download ratings

Name	Of those sites w/download ratings, % red and yellow 2008	Of those sites w/download ratings, % red and yellow 2007	Point change 2007-2008	% change 2007-2008	Download rank 2008	Download rank 2007	Change direction 2007-2008
Information (.info)	21.95%	5.60%	16.4%	291.9%	1	10	Worse
Romania (.ro)	14.18%	6.05%	8.1%	134.3%	2	8	Worse
Samoa (.ws)	12.50%	13.97%	-1.5%	-10.5%	3	1	Better
Business (.biz)	11.64%	11.44%	0.2%	1.7%	4	2	Worse
P.R. of China (.cn)	10.75%	7.40%	3.4%	45.4%	5	5	Worse
Italy (.it)	10.62%	3.16%	7.5%	236.0%	6	23	Worse
Families/Individuals (.name)	10.32%	5.62%	4.7%	83.7%	7	9	Worse
Bulgaria (.bg)	8.60%	9.91%	-1.3%	-13.1%	8	3	Better
Belgium (.be)	7.83%	6.76%	1.1%	15.8%	9	6	Worse
Cocos (Keeling) Is. (.cc)	7.64%	7.53%	0.1%	1.4%	10	4	Worse
Tonga (.to)	7.39%	5.11%	2.3%	44.6%	11	12	Worse
Tuvalu (.tv)	6.28%	6.69%	-0.4%	-6.2%	12	7	Better
Network (.net)	5.58%	4.69%	0.9%	19.1%	13	13	Worse
Commercial (.com)	5.39%	3.89%	1.5%	38.4%	14	17	Worse
United States (.us)	4.99%	3.67%	1.3%	36.1%	15	18	Worse
Tokelau (.tk)	4.76%	0.00%	4.8%	n/a	16	69	Worse
Christmas Is. (.cx)	4.63%	3.17%	1.5%	45.8%	17	21	Worse
Latvia (.lv)	4.46%	2.63%	1.8%	69.5%	18	26	Worse
Israel (.il)	4.40%	3.21%	1.2%	37.2%	19	19	Worse
Vietnam (.vn)	4.36%	5.19%	-0.8%	-15.9%	20	11	Better

Top 20 TLDs ranked by percentage of sites with red and yellow email practices ratings

Name	Of those sites w/email ratings, % rated red or yellow 2008	Of those sites w/email ratings, % rated red or yellow 2007	Point change 2007-2008	% change 2007-2008	Email rank 2008	Email rank 2007	Change direction 2007-2008
Information (.info)	58.35%	73.24%	-14.9%	-20.3%	1	1	Better
P.R. of China (.cn)	39.71%	17.18%	22.5%	131.1%	2	4	Worse
Hong Kong (.hk)	31.73%	10.00%	21.7%	217.3%	3	11	Worse
Network (.net)	12.83%	12.88%	-0.1%	-0.4%	4	8	Better
Russia (.ru)	11.17%	21.70%	-10.5%	-48.5%	5	2	Better
South Korea (.kr)	9.16%	19.57%	-10.4%	-53.2%	6	3	Better
Business (.biz)	8.84%	13.24%	-4.4%	-33.3%	7	6	Better
R. of China (Taiwan) (.tw)	8.78%	11.57%	-2.8%	-24.1%	8	9	Better
Commercial (.com)	8.09%	6.54%	1.5%	23.6%	9	15	Worse
Samoa (.ws)	5.45%	3.18%	2.3%	71.6%	10	36	Worse
Yugoslavia (.yu)	5.38%	4.69%	0.7%	14.7%	11	24	Worse
Ukraine (.ua)	5.37%	12.92%	-7.5%	-58.4%	12	7	Better
Thailand (.th)	5.36%	4.12%	1.2%	29.9%	13	29	Worse
Cocos (Keeling) Is. (.cc)	5.31%	11.42%	-6.1%	-53.5%	14	10	Better
Slovakia (.sk)	4.47%	6.44%	-2.0%	-30.7%	15	16	Better
Croatia (.hr)	4.31%	3.23%	1.1%	33.6%	16	35	Worse
European Union (.eu)	4.02%	n/a	n/a	n/a	17	n/a	Worse
Bulgaria (.bg)	4.00%	4.62%	-0.6%	-13.3%	18	25	Better
India (.in)	3.84%	4.30%	-0.5%	-10.8%	19	28	Better
Latvia (.lv)	3.81%	1.64%	2.2%	132.4%	20	52	Worse

Top 20 TLDs ranked by percentage of sites with exploits

Name	% of sites with exploits 2008	% of sites with exploits 2007	Point change 2007-2008	% change 2007-2008	Exploit rank 2008	Exploit rank 2007	Change direction 2007-2008
Romania (.ro)	1.119%	0.376%	0.742%	197.2%	1	3	Worse
Information (.info)	0.577%	0.113%	0.464%	411.0%	2	12	Worse
Niue (.nu)	0.514%	0.450%	0.064%	14.2%	3	1	Worse
P.R. of China (.cn)	0.307%	0.113%	0.194%	171.3%	4	11	Worse
Russia (.ru)	0.265%	0.427%	-0.162%	-38.0%	5	2	Better
Business (.biz)	0.205%	0.237%	-0.032%	-13.4%	6	5	Better
Families/Individuals (.name)	0.178%	0.358%	-0.180%	-50.3%	7	4	Better
Cocos (Keeling) Is. (.cc)	0.149%	0.158%	-0.009%	-5.8%	8	8	Better
Croatia (.hr)	0.139%	0.049%	0.090%	184.6%	9	19	Worse
Tonga (.to)	0.130%	0.074%	0.055%	74.8%	10	16	Worse
Ukraine (.ua)	0.127%	0.071%	0.057%	80.1%	11	17	Worse
Vietnam (.vn)	0.109%	0.000%	0.109%	n/a	12	50	Worse
India (.in)	0.090%	0.000%	0.090%	n/a	13	51	Worse
Network (.net)	0.079%	0.134%	-0.056%	-41.4%	14	9	Better
Portugal (.pt)	0.078%	0.017%	0.062%	366.2%	15	30	Worse
Samoa (.ws)	0.077%	0.171%	-0.094%	-55.0%	16	7	Better
Poland (.pl)	0.076%	0.061%	0.014%	23.5%	17	18	Worse
United States (.us)	0.075%	0.045%	0.030%	66.2%	18	21	Worse
Commercial (.com)	0.068%	0.083%	-0.015%	-18.3%	19	13	Better
Hong Kong (.hk)	0.068%	0.000%	0.068%	n/a	20	52	Worse

Pervasive risk: seven TLDs that score in the top 20 for each of our four rankings

Name	TLD	Overall risk rank 2008	Overall risk rank 2007	Change 2007–2008	Email rank 2008	Email rank 2007	Change 2007–2008
Information (.info)	INFO	3	2	Better	1	1	No change
P.R. of China (.cn)	CN	2	11	Worse	2	4	Worse
Business (.biz)	BIZ	10	6	Better	7	6	Better
Cocos (Keeling) Is. (.cc)	CC	11	12	Worse	14	10	Better
Network (.net)	NET	6	8	Worse	4	8	Worse
Samoa (.ws)	WS	12	3	Better	10	36	Worse
Commercial (.com)	COM	9	5	Better	9	15	Worse

Name	TLD	Download rank 2008	Download rank 2007	Change 2007–2008	Ex rank 2008	Ex rank 2007	Change 2007–2008
Information (.info)	INFO	1	10	Worse	2	12	Worse
P.R. of China (.cn)	CN	5	5	No change	4	11	Worse
Business (.biz)	BIZ	4	2	Better	6	5	Better
Cocos (Keeling) Is. (.cc)	CC	10	4	Better	8	8	No change
Network (.net)	NET	13	13	No change	14	9	Better
Samoa (.ws)	WS	3	1	Better	16	7	Better
Commercial (.com)	COM	14	17	Worse	19	13	Better

McAfee, Inc.
 3965 Freedom Circle
 Santa Clara, CA 95054
 888.847.8766
www.mcafee.com

McAfee, SiteAdvisor, Avert, and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US 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.
 © 2008 McAfee, Inc. All rights reserved. 6-cor-mal-web-001-0508