

EXECUTIVE SUMMARY

# Mapping the Mal Web

The World's Riskiest Domains





## The Web's Riskiest Domains

Let's say you do a search for a file-sharing program that allows you to download copyrighted music for free. You find a site that offers the program and start downloading it on your computer. What's the chance that along with the program, you are also downloading malware, such as a virus or spyware? As it turns out, it may depend on whether the site's domain ends in .JP (for Japan) or .CM (for Cameroon) because when it comes to risk, not all domains are the same.

In fact, when you do a web search, the chance that you will encounter malware, spam, or other threats from a specific website depends greatly on the site's top-level domain (TLD), or letter code, (for example, .UK or .BR and for a generic TLD, .COM or .NET) at the end of the website address telling you where the site is registered.

When cybercriminals choose where to register their malicious websites, they check for low prices, easy registration, a lack of regulation, or a "no questions asked" policy. In a strange way, they're not much different from you and me—cybercriminals look for the "best deals" too.

### Identifying risky domains

To help you identify potentially risky domains, McAfee just released its third annual *Mapping the Mal Web* report, outlining the world's riskiest and safest domains in terms of whether they contain risky websites and malicious downloads or send out spam.

Our goal in doing this research is to encourage them to become better educated and more aware of risky sites. We also want to celebrate safer domains so that other domains can follow their best practices. We hope that legitimate businesses will decide to register their sites at safer domains, putting further pressure on weak TLD managers to improve their practices. In the end, this benefits you, the consumer, as more domains work to reduce their risks.



So far, our efforts have resulted in several domains improving their rankings. For example, the tiny Pacific island of Tokelau earned a 10.1% risk rating in 2007 and took active steps to increase its safety following our report. By 2008, it earned a risk rating of 1.43%—an improvement of 85.8%.

#### The 2009 rankings

This year's report was produced after analyzing more than 27 million websites and 104 top-level domains using McAfee® SiteAdvisor® technology, which crawls the web and tests domains for a variety of security threats. For the first time this year, we also used data from McAfee TrustedSource™ technology, a web reputation service focused on protecting businesses.

Here is a summary of the results:

- **5.8% of all domains tested were risky**—This is an increase from 2007 and 2008, when 4.1% of sites were rated as risky. (However, we caution that since our rating methodology changed this year, we cannot say for *certain* that the overall risk has increased.)

- **The riskiest TLD was Cameroon (.CM)**—.CM had a risk rating of 36.7%, while last year's riskiest domain, .HK (Hong Kong), dropped to 34th place with a risk rating of 1.1%.
- **Commercial (.COM) is the second-riskiest TLD**—This heavy-trafficked TLD had a risk rating of 32.2% and was also the most risky generic TLD.
- **Romania (.RO) was the riskiest TLD for malicious downloads**—Some 21.0% of the .RO domains with downloads contained risky files such as viruses, spyware, and adware.
- **Information (.INFO) was the most "spammy" TLD**—Of the .INFO sites tested with sign-up forms, 17.2% resulted in unwanted email.
- **The TLDs with the least risky registrations**—Or fewest domains rated risky are:
  - Governmental (.GOV)
  - Japan (.JP)
  - Educational (.EDU)
  - Ireland (.IE)
  - Croatia (.HR)



### Threat findings

In addition to identifying risky domains, the report also sheds light on where online risks are moving. The good news is that your risk of registering an email address and receiving spam declined this year. Of the more than 330,000 domains we tested for email, just 2.8% were at risk for spam, compared to 7.6% last year. It's worth noting, however, that the volume of spam has not decreased—just that the number of sites with “spammy sign-ups” has declined.

Sites offering downloads that contain viruses, spyware, *adware*, and other unwanted programs also decreased compared to last year. Of the nearly 690,000 sites tested for downloads, 4.5% of them were rated as risky or potentially risky for malicious downloads. Last year, 4.7% of the sites tested were declared risky. But once again we must caution that this does not mean that the number of malicious downloads have declined. It could just be that they are getting more difficult to find using standard test measures.

### Conclusion

As our third annual *Mapping the Mal Web* report demonstrates, potential online threats are constantly changing. Cybercriminals will move their malicious activity to regions where registering sites is cheap and convenient and where they are least likely to be caught. That's why it's important that we keep a close eye on where the mal web is moving and where we should take caution.

Of course, we don't expect you to keep track of every potentially risky domain, especially since they are not always easy to trace. You may wind up on a relatively safe .FR (France) domain, for instance, and start downloading a file, only to realize the download is coming from a .RO (Romania) domain, which is quite risky.

The best way to stay safe is to have an up-to-date security suite, like McAfee® Total Protection, which also has safe search technology, like McAfee SiteAdvisor. Through awareness and intelligent technology, we're aiming to make the web a lot less risky.

To read the full *Mapping the Mal Web* report, visit our [Security Advice Center](#).

# Rankings

## Top ten most risky domains

COUNTRY OR NAME	REGION	TLD	WORLDWIDE RISK RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITEADVISOR ONLY)	2007 RISK RATIO (SITEADVISOR ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Cameroon	EMEA	CM	1	36.7%	69.7%	n/a	n/a	82,087	57,210
Commercial	Generic	COM	2	32.2%	6.0%	5.3%	5.5%	15,440,225	918,873
People's Republic of China	APAC	CN	3	23.4%	34.5%	11.8%	3.7%	561,517	193,917
Samoa	APAC	WS	4	17.8%	34.6%	3.8%	5.8%	43,829	15,178
Information	Generic	INFO	5	15.8%	22.8%	11.7%	7.5%	601,629	137,403
Philippines	APAC	PH	6	13.1%	26.1%	7.7%	2.1%	8,707	2,272
Network	Generic	NET	7	5.8%	5.9%	6.3%	4.4%	1,554,136	91,049
Former Soviet Union	EMEA	SU	8	5.2%	10.3%	n/a	n/a	7,349	754
Russia	EMEA	RU	9	4.6%	7.6%	6.0%	4.5%	344,434	26,234
Singapore	APAC	SG	10	4.6%	9.1%	0.3%	0.3%	17,630	1,607

## Top ten least risky domains

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

## Top five domains with risky email practices

COUNTRY OR NAME	TLD	DOMAINS WITH RISKY EMAIL PRACTICES	EMAIL DOMAINS TESTED
Information	INFO	17.2%	3,029
Commercial	COM	3.9%	207,415
Network	NET	1.9%	16,389
Switzerland	CH	1.1%	2,114
Denmark	DK	0.8%	2,096

## Top five domains with risky download practices

COUNTRY OR NAME	TLD	DOMAINS WITH RISKY EMAIL PRACTICES	DOWNLOAD DOMAINS TESTED
Romania	RO	21.0%	2,941
People's Republic of China	CN	18.6%	16,356
Information	INFO	15.2%	7,494
Business	BIZ	6.8%	2,749
Network	NET	5.2%	56,162

### About McAfee, Inc.

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

[www.mcafee.com](http://www.mcafee.com)



McAfee, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054  
888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

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

McAfee and/or other noted McAfee-related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the U.S. and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee-related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners. © 2009 McAfee, Inc. All rights reserved.

MTMW\_Sum-US\_1009