BLUE COAT®

Security
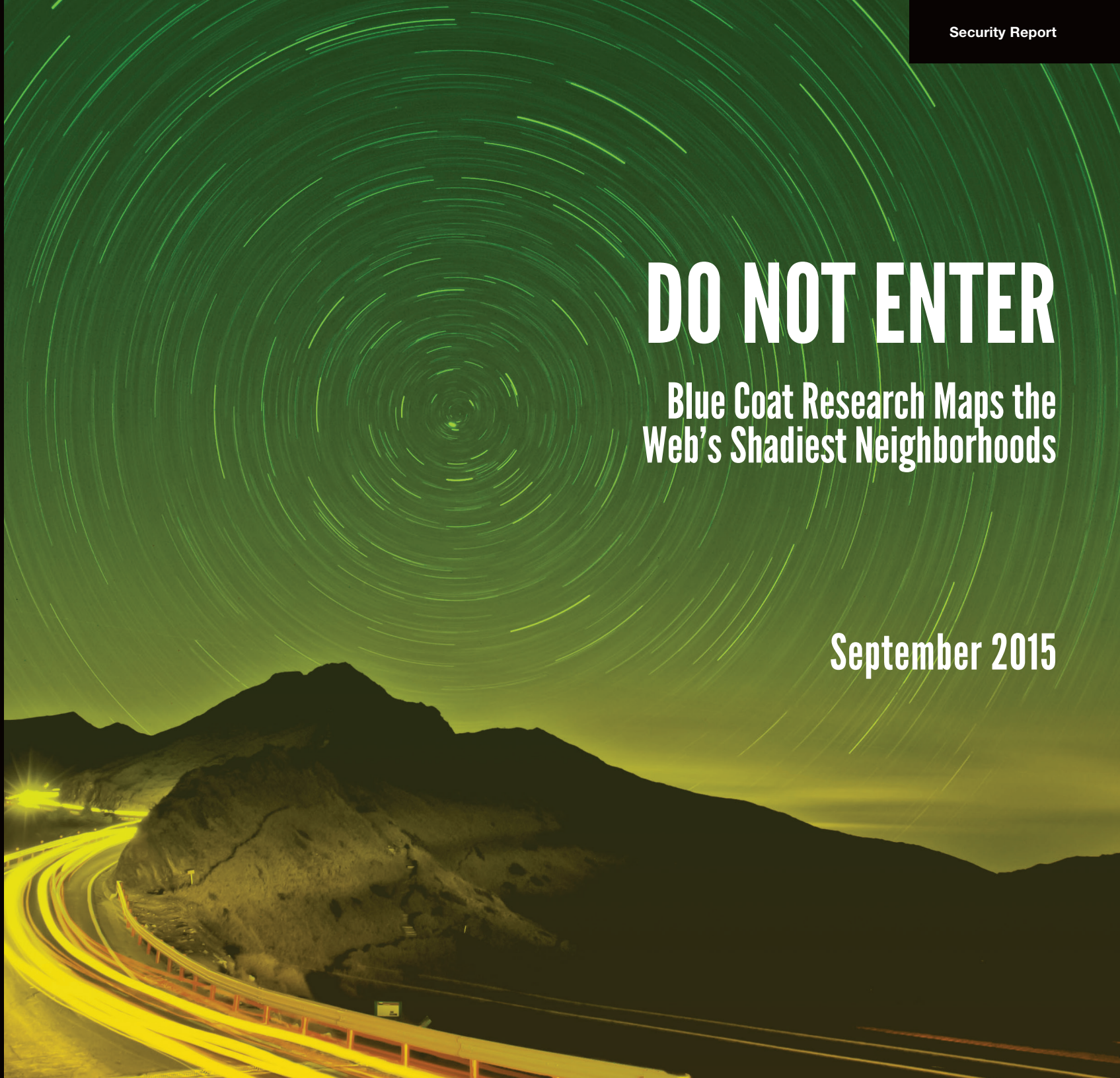**Empowers**
Business

DO NOT ENTER

Blue Coat Research Maps the Web's Shadiest Neighborhoods

September 2015

KEY FINDINGS

- There has been an explosion of new Top Level Domains over the past two years.
- Lax policies in some managing organizations breed shady neighborhoods.
- Malicious activity continues to increase.
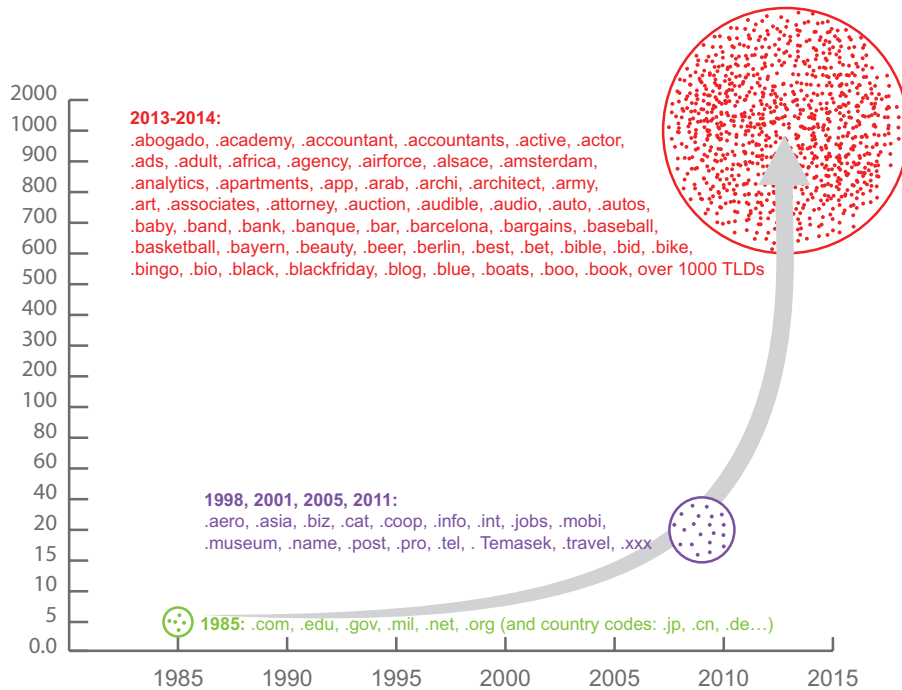- Bad guys always need a new supply of domains to do bad things.

Introduction

Many users may not pay much attention to the letters following the "." in a website address when clicking on a link. What they may not realize is that those simple letters represent a Top Level Domain (TLD) – essentially a "neighborhood" of addresses – that are maintained by a specific company or group. Much like the physical world, the relative risk of visiting a website in one of these neighborhoods can vary dramatically depending on who is managing the "residents" there.

Over the past two years, there has been an explosion of new neighborhoods on the web, many of which are neither safe nor friendly. Much has changed since the early days of the Internet, when the web had only six common top level domains (TLDs). Back then, what most consumers and businesses encountered were a few standard TLDs, such as .com, .net, .org, .edu and .gov, and some "country code" domains such as .fr (France), and .jp (Japan).

However, since 2013, the sheer number of new TLDs has skyrocketed. By 2015, the count of validly issued TLDs stood at over one thousand. As the number of TLDs has increased, so have the opportunities for attackers. Businesses and consumers need additional guidance to understand how safe, or how shady, these new TLDs may be considered for web security purposes. Ideally, TLDs would all be run by security-conscious operators who diligently review new domain name applications, and reject those that don't meet a stringent set of criteria. The reality for many of these new neighborhoods is that this is not happening.

Based on analysis of web requests from more than 15,000 worldwide businesses and 75 million users, Blue Coat researchers have created a list rating the web's shadiest and safest neighborhoods.

The Great TLD Explosion

2013-2014:
.abogado, .academy, .accountant, .accountants, .active, .actor, .ads, .adult, .africa, .agency, .airforce, .alsace, .amsterdam, .analytics, .apartments, .app, .arab, .archi, .architect, .army, .art, .associates, .attorney, .auction, .audible, .audio, .auto, .autos, .baby, .band, .bank, .banque, .bar, .barcelona, .bargains, .baseball, .basketball, .bayern, .beauty, .beer, .berlin, .best, .bet, .bible, .bid, .bike, .bingo, .bio, .black, .blackfriday, .blog, .blue, .boats, .boo, .book, over 1000 TLDs

1998, 2001, 2005, 2011:
.aero, .asia, .biz, .cat, .coop, .info, .int, .jobs, .mobi, .museum, .name, .post, .pro, .tel, . Temasek, .travel, .xxx

1985: .com, .edu, .gov, .mil, .net, .org (and country codes: .jp, .cn, .de…)

Back in its early days, the web was limited to six normal TLDs and roughly 100 "country code" TLDs. This continued for over a decade, with a few additional TLDs being added in 1998, 2001, 2005 – some of which are likely familiar to many users (.info, .biz, .mobi, .name, .pro) and some less-familiar (.aero, .asia, .cat, .coop, .int, .jobs, .museum, .tel, .travel, .post). The infamous ".xxx" was added in 2011.

Then an explosion happened – In 2013-2014, over 600 new TLDs were approved and the pace has continued in 2015. In early 2015, the count of valid TLDs was 795 (including the country codes), and by mid August, the count was over 1000.
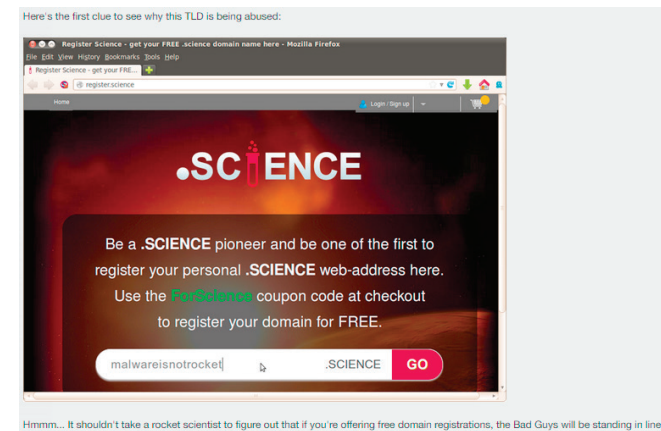
Lax Policies for Purchasing TLDs Breeds Danger

The dramatic rise in new TLDs can be attributed to a new generic Top-Level Domains (gTLDs) initiative launched by the Internet Corporation for Assigned Names and Numbers (ICANN) in 2012. ICANN's Frequently Asked Questions document for gTLDs outlines the original goal for the initiative:

> "One of ICANN's key commitments is to promote competition in the domain name market while ensuring Internet security and stability. New generic Top-Level Domains (gTLDs) help achieve that commitment by paving the way for increased consumer choice by facilitating competition among registry service providers. Soon entrepreneurs, businesses, governments and communities around the world will be able to apply to operate a Top-Level Domain registry of their own choosing."

Each new TLD is under the control of an organization that has to pay a $185,000 evaluation fee to ICANN and also has to prove that it has the infrastructure and expertise to run a new TLD registry.

Ideally, all of these new registries (and all of the country code registries), would exercise the same level of caution in who they allow to purchase domains in their new space – but many do not, and the Bad Guys know where to shop.

Here's the first clue to see why this TLD is being abused:

Hmmm... It shouldn't take a rocket scientist to figure out that if you're offering free domain registrations, the Bad Guys will be standing in line...

For this research, we counted a domain as "shady" if it was rated in our database with a category such as:

Most Common	Less Common
Spam	Malware
Scam	Botnet
Suspicious	Phishing
Potentially Unwanted Software (PUS)	

Any domain in the database that did not have one of these categories was counted as "non-shady." It is our hope that the TLDs rated as shady will learn from the example of the Safest TLDs; with a little effort it is possible to keep most of the bad players out.

The Web's Top 10 TLDs with Shady Sites*

Rank	Top-Level Domain Name	Percentage of Shady Sites
1	.zip	100.00%
2	.review	100.00%
3	.country	99.97%
4	.kim	99.74%
5	.cricket	99.57%
6	.science	99.35%
7	.work	98.20%
8	.party	98.07%
9	.gq (Equatorial Guinea)	97.68%
10	.link	96.98%

As of August 15, 2015 - Percentages are based on categorizations of web sites actually visited by our 75 million users. A TLD having 100 percent shady sites correlates to sites categorized by Blue Coat.

Blue Coat researchers analyzed tens of millions of websites requested by 75 million global users to rank the TLDs that pose the greatest potential threat to visitors. All of the TLDs listed above have more than 95 percent of their sites with shady ratings in our main database – that is, most of the sites using these TLDs that have earned a rating in the database have a shady one (e.g., malware, spam, scam, phishing, suspicious, etc.). Each of these TLDs has hundreds, or thousands, or tens of thousands of rated websites, less than five percent of which are rated with a normal category.

Examples of Risky Activity

Shady TLDs are providing fertile ground for malicious activity. Most of these websites are being leveraged by attackers in spam and scams and to distribute potentially unwanted software. Others are related to search engine optimization/positioning or other "junk sites" that would be classified as suspicious.

Bad guys always need a new supply of domains to do bad things. Previous Blue Coat research, "One-Day Wonders: How Malware Hides Among the Internet's Short-Lived Websites," explored in depth how many sites on the web only exist for less than 24 hours.

Links to these locations are included in spam campaigns, and they are changed rapidly to increase the chances that they will evade security defenses before they are updated. The explosion of new TLDs has provided a nearly limitless supply of "One-Day Wonders" for the taking.

A recent malware campaign shows how the .kim TLD is being leveraged for nefarious activity:

Sites like buu.kim and newido.kim were recently found to be serving up pages built of obfuscated Javascript that produced pages like the one below:
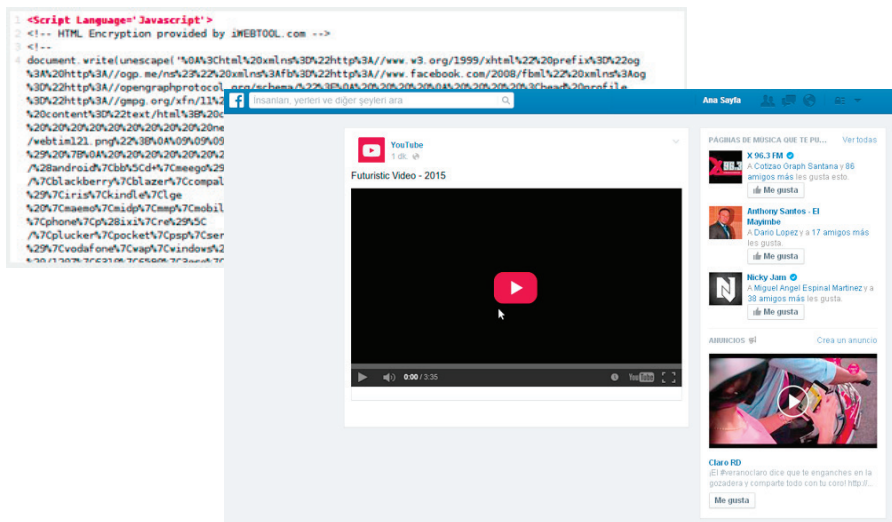
Most of the content on these pages actually consists of image files, hosted on a malicious site called fourapp.info. Unprotected visitors to these pages are prompted to download malware.

In a different twist on a fake video attack, the highest-trafficked ".country" site observed by Blue Coat on a day in mid-June was part of a "shocking video" scam network:

This increasingly common scam leads visitors to a "teaser page," usually designed to make them believe they are visiting YouTube, when in reality they are on a fake site that has no legitimate tie to YouTube. The non-working video includes fake comments immediately below it from someone wanting to know how to get the video to play, and someone else explaining that you have to "share" or "like" the video first, or take an online survey. When visitors follow these instructions, they either divulge personal data in the survey, or the scammers spam their Facebook friends.

Image #1 is an example of what users were led to believe was a "shocking" pornographic video. The teaser image has been blacked out.
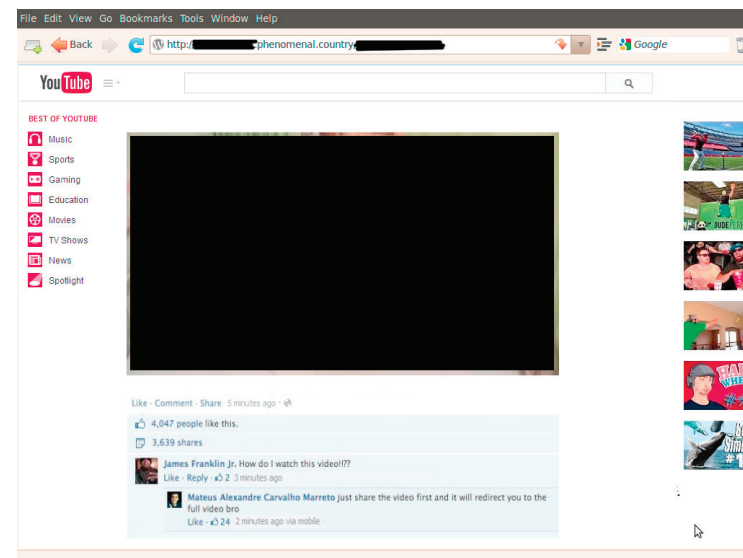

Image #1

FAKE VIDEO ATTACKS ARE INCREASINGLY COMMON AS A SUCCESSFUL THREAT TARGETING SOCIAL MEDIA USERS.

Many of shady TLDs are used solely for the purposes of scams and spam. Image #2 is what visitors would see if they viewed the main page of the website hosting this scam.
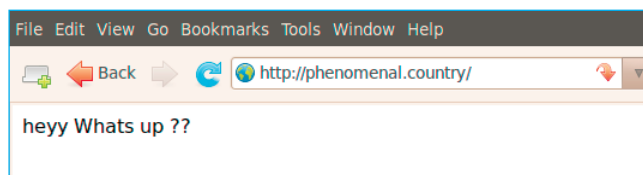

Image #2

Images #3, #4, and #5 are representative examples of the scam surveys that users are directed to from the non-working video page based on its associated traffic.
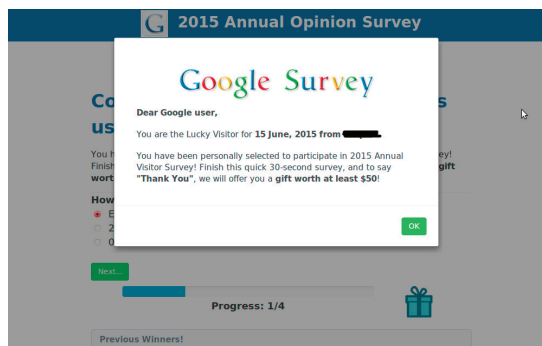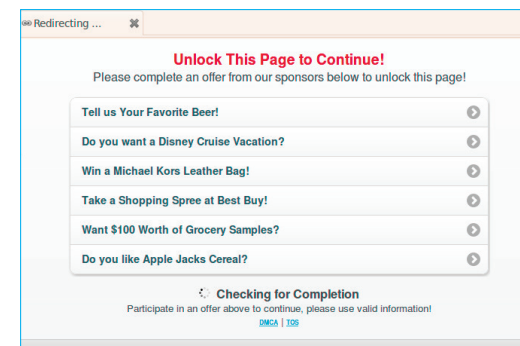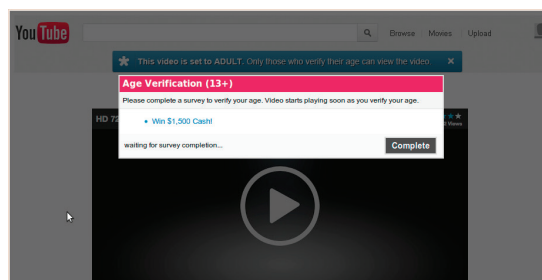

Image #3

Image #4

Image #5

We see this campaign frequently, often with sites that get hundreds of attempted visits per day, so people are clicking on it. Nearly all of that traffic is coming from Facebook, so the scammers' scheme works.

The Web's "Safest" Neighborhoods

Rank	Top-Level Domain Name	Percentage of Shady Sites
10	.jp (Japan)	1.95%
9	.london	1.85%
8	.kw (Kuwait)	1.61%
7	.tel	1.60%
6	.gi (Gibraltar)	1.26%
5	.gov	0.96%
4	.church	0.84%
3	.ck (Cook Islands)	0.52%
2	.jobs	0.36%
1	.mil	0.24%

For comparison, the above list includes the Bottom Ten Shady TLDs – or the "safest" TLDs historically. All of these TLDs have less than two percent of their sites classified with shady ratings to date.

However, we should beware of reading too much into this section.

Only a few of these (.jp, .gov, and .mil) have large numbers of sites in Blue Coat's database. For example, .london has just over 100 sites so far. There are also no guarantees that TLDs that currently have lower risk levels will maintain them. We have seen plenty of small church websites get hacked in the past, so over time, .church may not remain as much of a sanctuary.

As good general purpose TLDs, .tel and .jobs appear to be obvious targets for attackers in the future. In addition, .ck is a concern now that we've publicly identified it as a fairly safe place, since whoever is running their registry may not have the resources to keep out the bad guys.

Meanwhile, the new .sucks registry could soon join the "safest" list. Although that TLD has created some controversy recently in charging brands $2,000 or more a year to pre-register, the cost will also likely reduce the number of domains registered by attackers.

Still, this list highlights that a registry that puts forth the effort to keep its neighborhood clean really can make a difference on the web.

How to Minimize the Risk for Businesses and Consumers

In summary everyone, whether a business user or consumer, should be aware and vigilant about the online neighborhoods they visit. Even the "safest" TLD's are not without risk of threats from nefarious players, and it remains as critical as ever to have strong digital security protection and policies in place.

- Businesses should consider blocking traffic that leads to the riskiest TLDs. For example, Blue Coat has previously recommended that businesses consider blocking traffic to .work, .gq, .science, .kim and .country. The remaining five TLDs in the Top 10 Shadiest TLDs list deserve similar consideration.

- Users should use caution to click on any links that have these TLDs in them if they encounter them in search results, e-mail, or social network environments.

- If unsure about the source, hover the mouse over a link to verify that it leads to the address displayed in the text of the link.

- Remember that you can "press and hold" a link on a mobile device (not just click) to verify it leads to where it says it does.

BLUE COAT®