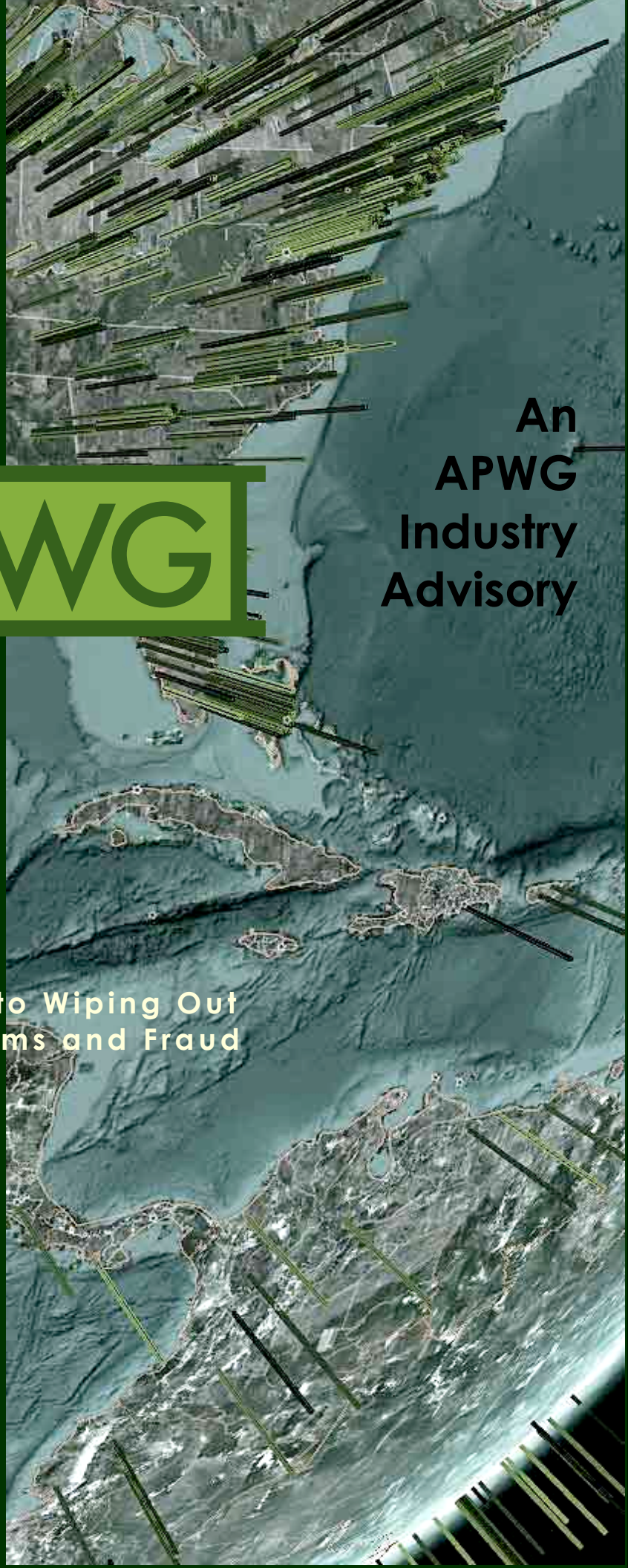
Global Phishing Survey: Trends and Domain Name Use in 2H2010



An APWG Industry Advisory

APWG

Committed to Wiping Out Internet Scams and Fraud

April 2011

Authors:

Greg Aaron
Afilias
<gaaron at afilias.info>

Rod Rasmussen
Internet Identity
<rod.rasmussen at internetidentity.com>

Research, Analysis Support, and Graphics:
Aaron Routt, Internet Identity

Published April 27, 2011

Table of Contents

Disclaimer: *PLEASE NOTE: The APWG and its cooperating investigators, researchers, and service providers have provided this study as a public service, based upon aggregated professional experience and personal opinion. We offer no warranty as to the completeness, accuracy, or pertinence of these data and recommendations with respect to any particular company's operations, or with respect to any particular form of criminal attack. This report contains the research and opinions of the authors. Please see the APWG web site – apwg.org – for more information.*

Overview

The e-crime landscape is a constantly shifting battlefield, where phishers are always moving toward ripe targets and away from well-defended Internet assets. We saw this dynamic play out in several different ways in late 2010, with implications for phishing targets, service providers, and anti-phishing responders.

This report seeks to understand trends and their significances by quantifying the scope of the global phishing problem. Specifically, this new report examines all the phishing attacks detected in the second half of 2010 ("2H2010", or July 1, 2010 through December 31, 2010).

The data was collected by the Anti-Phishing Working Group and supplemented with data from several phishing feeds and private sources. The APWG phishing repository is the Internet's most comprehensive archive of phishing and e-mail fraud activity.[1] We hope that bringing new trends to light will lead to improved anti-phishing measures. The authors' major findings in this report include:

1. **In 2H2010, the average and median uptimes of all phishing attacks spiked significantly from previous periods, and were higher than any time period since we began our uptime measurements three years ago.** *(Page 7)*
2. **Phishers are attacking Chinese e-commerce sites and banks aggressively. These phishers prefer to register domain names, rather than using compromised Web servers like most phishers do.** *(Pages 5-6)*
3. **Shutting down the availability of .CN domain names did not stop phishing that victimizes Chinese Internet users and Chinese institutions. Rather, it seems to have merely shifted the phishing to other top-level domains.** *(Page 6)*
4. **Malicious use of subdomain services by phishers nearly doubled in the second half of 2010. Phishers use such services as often as they register domain names.** This activity shows phishers using services that cannot be taken down by domain registrars or registry operators. *(Page 14)*
5. **Two free services were heavily abused by phishers in order to create phishing sites:** the .TK domain registration service and the CO.CC subdomain service. Nearly 11percent of all phishing attacks utilized these relatively little-known services. (Pages 12,14)

[1] This new report is a follow-up to our earlier studies of data stretching back to January 2007. The previous studies are available at: http://www.apwg.org/resources.html#apwg

Basic Statistics

Millions of phishing URLs were reported in 2H2010, but the number of unique phishing attacks and domain names used to host them was much smaller.[2] The 2H2010 data set yields the following statistics:

- **There were at least 67,677 phishing attacks worldwide.** This is greater than the 48,244 we observed in 1H2010, but significantly less than the record 126,697 observed in 2H2009 at the height of phishing on the Avalanche botnet**. The increase in 2H2010 is mainly due to new data about phishing attacks on Chinese targets.** An "attack" is defined as a phishing site that targets a specific brand or entity. One domain name can host several discrete attacks against different banks, for example. The decrease in attacks was due to reduced activity by the Avalanche phishing gang.
- The attacks occurred on **42,624 unique domain names**.[3] This is a high in our reports going back to 2007, and the increase is due to new data about Chinese phishing. The number of domain names in the world grew from 196 million in May 2010 to 205.6 million in October 2010.[4]
- In addition, 3,051 attacks were detected on **2,318 unique IP addresses, rather than on domain names.** (For example: http://96.56.84.42/ClientHelp/ssl/index.htm.) This is comparable to the 2,018 unique IPs seen in 1H2010. We did not observe any phishing on IPv6 addresses.
- Of the 42,624 phishing domains, **we identified 11,769 that we believe were registered maliciously, by the phishers (28%). Of those, 6,382 were registered to phish Chinese targets.** The other 30,855 domains were hacked or compromised on vulnerable Web hosting. Malicious registrations apparently took place in 56 TLDs.
- **Phishing remains concentrated in certain namespaces.** Sixty percent of attacks occurred in just four TLDs: .COM, .CC, .NET, and .ORG. And 89 percent of malicious domain registrations were made in four TLDs: .COM, .TK, .NET, and .INFO.

---

[2] This is due to several factors: A) Some phishing involves customized attacks by incorporating unique numbers in the URLs, often to track targeted victims, or to defeat spam filters. A single phishing attack can therefore manifest as thousands of individual URLs, while leading to essentially one phishing site. Counting all URLs would therefore inflate some phishing campaigns. Our counting method de-duplicates in order to count unique attacks, and has remained consistent across this and our previous reports. For an example of an apparently different tallying method, see page 4 at: http://apwg.org/reports/apwg_report_h1_2009.pdf
B) Phishers often use one domain name to host simultaneous attacks against different targets. Some phishers place several different phishing attacks on each domain name they register.
C) A phishing site may have multiple pages, each of which may be reported.

[3] "Domain names" are defined as second-level domain names, plus third-level domain names if the relevant registry offers third-level registrations. An example is the .CN (China) registry, which offers both second-level registrations and third-level registrations (in zones such as com.cn, gov.cn, zj.cn, etc.). However, see the "Subdomains Used for Phishing" section for commentary about how these figures may undercount the phishing activity in a TLD.

[4] As per our research, and VeriSign Industry Briefs: http://www.verisign.com/domain-name-services/domain-information-center/industry-brief/index.html

- **Only about 9 percent of all domain names that were used for phishing contain a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations" on page 15.)
- Only 10 of the 42,624 domain names we studied were IDNs, and only one was a homographic attack. See "Use of Internationalized Domain Names" below for more details.

Basic Statistics

	2H2010	1H2010	2H2009	1H2009	2H2008
Phishing domain names	42,624	28,646	28,775	30,131	30,454
Attacks	67,677	48,244	126,697	55,698	56,959
TLDs used	183	177	173	171	170
IP-based phish (unique IPs)	2,318	2,018	2,031	3,563	2,809
Maliciously registered domains	11,769	4,755	6,372	4,382	5,591
IDN domains	10	10	12	13	10

Each domain name's registrar of record was not reported at the time the phish was live. Obtaining accurate registrar sponsorship data for a domain name requires either time-of-attack WHOIS data, or historical registry-level data. These data have not been collected in a comprehensive manner by the anti-phishing community.

Phishing in China

This report contains a valuable new data contribution from CNNIC. CNNIC not only operates the .CN domain registry, but is also the secretariat of the Anti-Phishing Alliance of China (APAC, http://en.apac.cn/). APAC has more than 140 member institutions in the country, including banks, e-commerce sites, and domain registrars, and has an efficient reporting and domain suspension program. The authors are grateful to CNNIC and APAC for sharing data in cooperation with the APWG.

APAC's data provides a fascinating look at phishing that targets Chinese institutions. We compared APAC's data to our other sources, and it became immediately clear that observers outside of China detected only about 20 percent of the Chinese-target phishing that APAC did. We suspect that security observers in Europe and the Americas are not receiving and/or parsing many of the Chinese-language phishing lure e-mails and instant messages that advertise these phishing attacks, while APAC members are detecting and reporting such attacks far more effectively.

Attacks on Chinese institutions did not involve many .CN domain names. In December 2009, new rules barred individuals from registering .CN domains, and required all potential registrants to present a paper application form with a copy of a company business license and a copy of the registrant's personal identification. As a result, the number of names in

the .CN registry fell from 13.5 million in late 2009 to just 3.4 million in March 2011. In the second half of 2009, we observed 2,826 phishing attacks on 228 .CN names. Through the first half of 2010, the numbers dropped to just 162 attacks on 120 domains. In 2H2010, our data shows 352 attacks on 278 .CN domains, with the increase due to CNNIC's superior data contribution. Half of those domains were used to attack non-Chinese targets.

Historically, about 80 percent of phishing attacks have used the hacked Web servers of innocent domain registrants. In contrast, the Chinese phishers prefer to register domain names and subdomains for their malicious work. **In 2H2010 we counted 12,282 attacks on Chinese institutions, utilizing 6,382 unique domain names plus a staggering 4,737 free CO.CC subdomains.** Of the 6,382 domain names, just 487 looked hacked.

What seems clear is that when .CN's registration policy became more restrictive, **the phishers simply went to other TLDs and services to find resources.** Through 2010, attacks against Chinese targets showed up in increasing numbers in .COM, .TK, .INFO, .US, .IN, and CO.CC. Of the 2,429 .TK domains used for phishing in 2H2010, 2,001 were used to phish Chinese institutions. In another example, the .INFO registry observed a noticeable upswing of attacks against Taobao.com in the second half of 2010. The phishers always provided addresses located in China, and often used Chinese freemail services such as QQ.com. Based on URL patterns and the domain strings registered, a small number of phishers were probably responsible for creating dozens of registrant accounts over time. The .INFO domains used in these attacks were all purchased via one registrar, and the phishers used a new registrant name and address for each batch of domains they registered. A few of the registrant accounts contained domains used for other malicious purposes, including malware and sites used to sell counterfeit brand name goods.

Of the 12,282 attacks, 9,087 (74%) targeted Taobao.com. Taobao is a Chinese-language Web site for online shopping and auctions, similar to eBay, with the great majority of products being new merchandise sold at a fixed price.

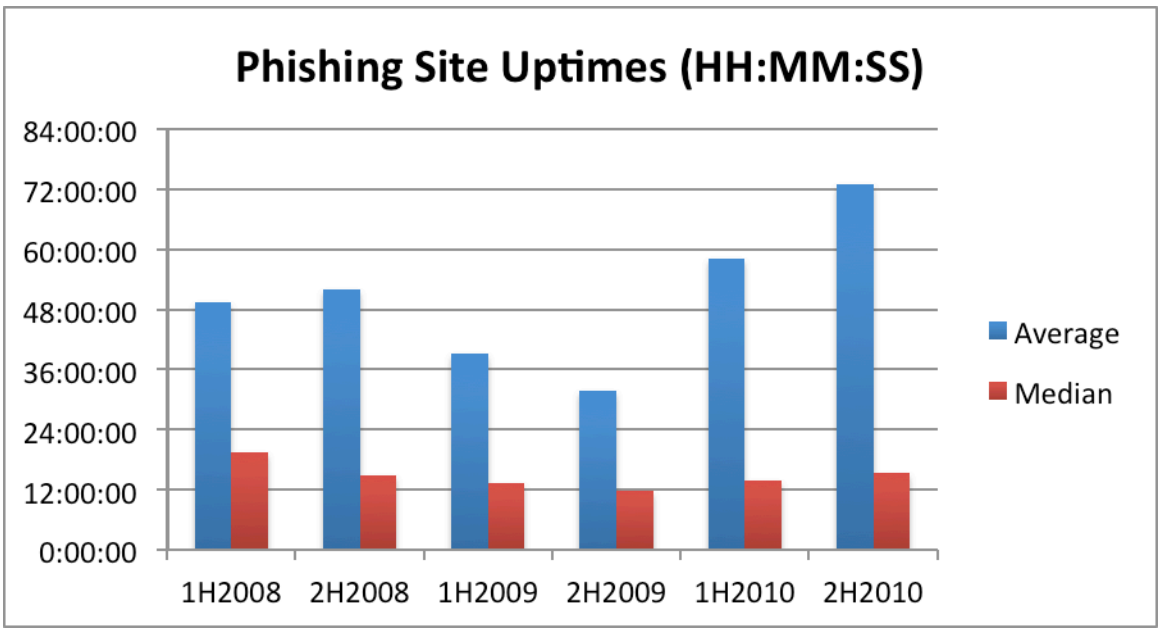
Left: A phish that mimics Taobao's order con-firmation process.

Phishing By Uptime

After reaching an historical low in 2H2009, the average and median uptimes of phishing attacks rose throughout 2010. The average uptime was 73 hours, the longest average for any time period since we began our uptime measurements three years ago. The median uptime was 15 hours 19 minutes, one of the higher medians we have recorded.

The "uptimes" or "live" times[5] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a measure of the success of mitigation efforts. The longer a phishing attack remains active, the more money the victims and target institutions lose. The first two days of a phishing attack are believed to be the most lucrative for the phisher, so quick takedowns are essential. Long-lived phish can skew the averages since some phishing sites may last weeks or even months, so medians are also a useful barometer of overall mitigation efforts. CNNIC did not record the uptimes of the phish it documented, so those phish were not part of our uptime calculations.

The historical trend is:



[5] The system used to track the uptimes automatically monitored the phishing sites, and monitoring began as soon as the system became aware of a phish via feeds or honeypots. Each phish was checked several times per hour to confirm its availability, and was not declared "down" until it had stayed down for at least one hour. (This requirement was used because some phish, especially those hosted on botnets, may not resolve on every attempt but in general remain live.) This estimate tends to under-count the "real" uptime of a phishing site, since more than 10% of sites "re-activate" after one hour of being down. However, our method is a consistent measure that allows direct comparison across incidents and should be fair for relative comparisons.

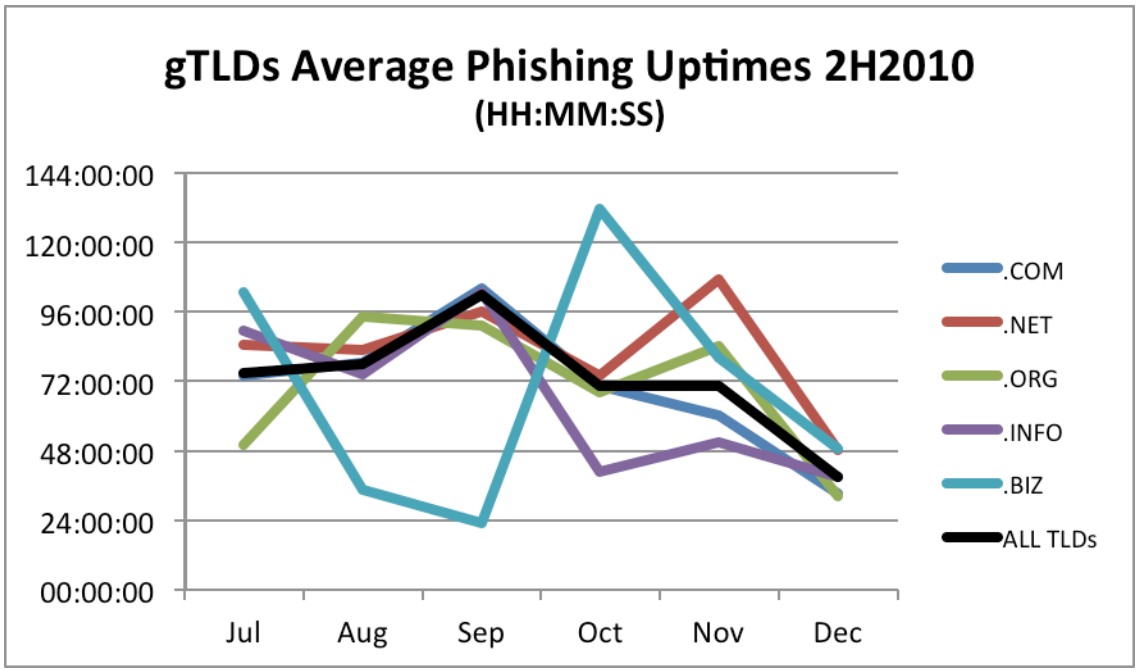
It is logical that 2010's uptimes would be higher than 2009's. In 2009, the Avalanche gang registered large numbers of domain names that were taken down aggressively. The field in 2010 consisted mainly of phish on compromised domains, which are more difficult to mitigate than maliciously registered domain names.

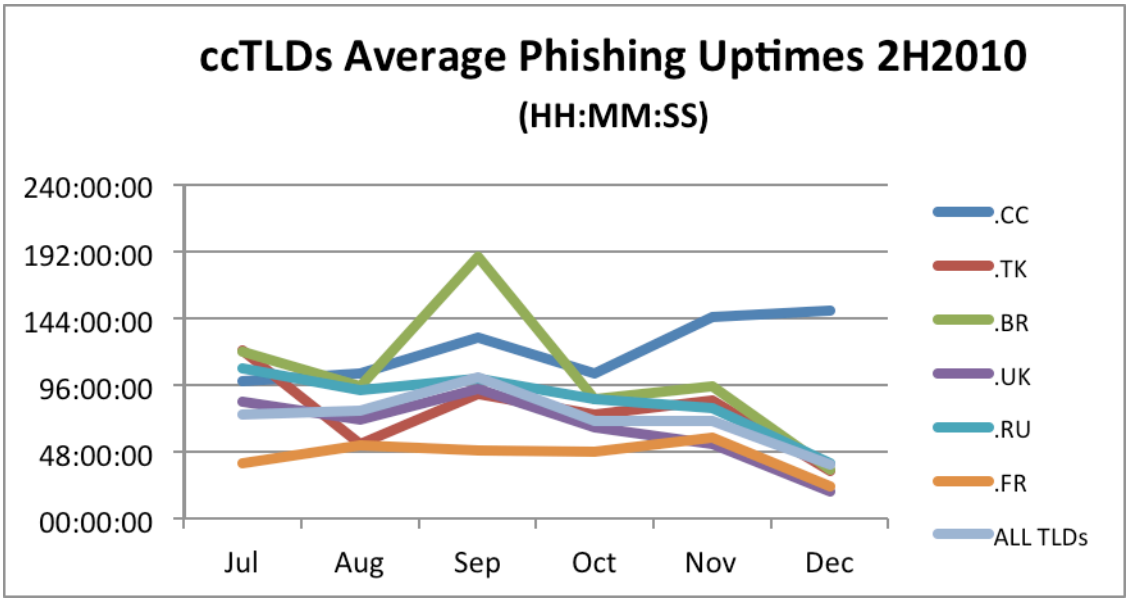
What is not clear is why uptimes jumped so dramatically during 2H2010. This is a worrying trend we will continue to monitor.

The uptimes for the last three years were:

All Phish, All TLDs	Average (HH:MM:SS)	Median (HH:MM:SS)
Dec 2010	38:54:53	11:35:02
Nov 2010	70:38:07	15:37:53
Oct 2010	70:24:08	17:13:35
Sep 2010	101:57:45	14:44:43
Aug 2010	78:02:08	18:23:03
Jul 2010	74:56:01	14:05:05
2H2010	**73:05:31**	**15:19:41**
1H2010	**58:10:16**	**13:42:16**
2H2009	**31:38:00**	**11:44:15**
1H2009	**39:11:00**	**13:15:32**
2H2008	**52:01:58**	**14:43:15**
1H2008	**49:30:00**	**19:30:00**

The uptimes for all phishing attacks in 2H2010, and for phish in some large TLDs, were:





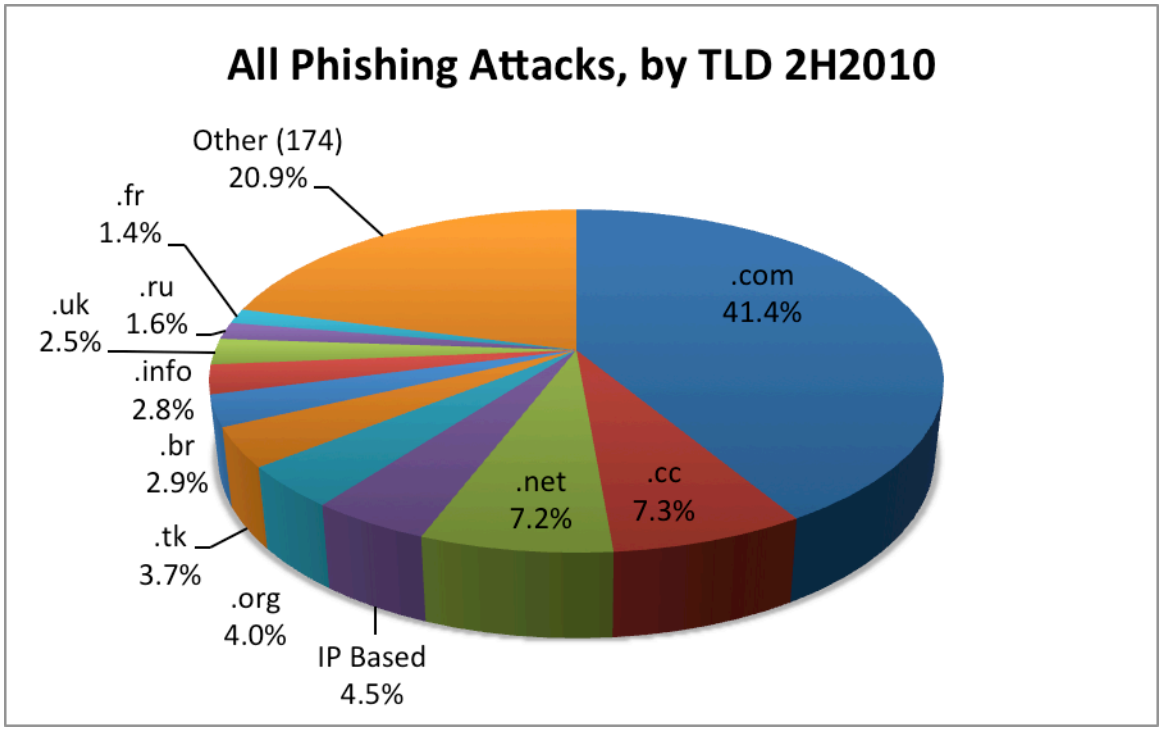
Uptimes by TLD, 2H2010

TLD	Average (HH:MM:SS)	Median (HH:MM:SS)
.COM	71:20:56	13:36:34
.NET	82:01:17	16:51:27
.ORG	71:46:41	13:08:33
.INFO	67:26:52	14:14:23
.BIZ	67:33:56	09:49:20
.UK	64:09:21	14:41:26
.CN	75:41:47	18:27:28
.EU	64:06:09	10:26:54
.RU	86:48:24	18:47:00
.BE	72:44:09	17:44:19
.KR	60:56:24	21:33:45
.PL	70:24:56	16:21:39
.BR	88:20:39	23:07:04
.DE	61:58:40	12:42:51
.FR	46:47:21	12:34:11
.CZ	64:33:34	12:49:00
.CC	129:13:33	54:00:05
.TK	77:27:54	21:54:16

Prevalence of Phishing by Top-Level Domain (TLD)

We analyzed the phishing domains and attacks to see how they were distributed among the TLDs. The complete tables are presented in the Appendix. We were able to obtain the domain count statistics for TLDs containing 99.5 percent of the phishing domains in our data set, and a total of 205,615,855 domain names overall. [6]

The majority of phishing continues to be concentrated in just a few namespaces. Except for .TK and CO.CC, which were taken advantage of more extensively by phishers, phishing was roughly distributed by market share. Sixty percent of the attacks occurred in just four TLDs: .COM, .NET, .TK, and .CC. And 78 percent of the world's malicious domain registrations were made in just three TLDs: .COM, .TK, and .NET.



To put the numbers in context and measure the prevalence of phishing in a TLD, we use the metrics "Phishing Domains per 10,000" and "Phishing Attacks per 10,000." "Phishing Domains per 10,000"[7] is a ratio of the number of domain names used for phishing in a TLD to the number of registered domain names in that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of phishing relative to others.

[6] For the purposes of this study, we used the number of domain names in each registry as of October 2010. Sources: ICANN.org (monthly registry reports), ccTLD registry operators.
[7] Score = (phishing domains / domains in TLD) x 10,000

The metric "Phishing Attacks per 10,000" is another useful measure of the pervasiveness of phishing in a namespace. It especially highlights what TLDs are predominantly used by phishers who use subdomain services, and where high-volume phishers place multiple phish on one domain.

The complete tables are presented in the Appendix, including the scores and the number of phish in each TLD.

- **The median domains-per-10,000 score was 3.2**.
- **The average domains-per-10,000 score of 7.8** was skewed by a few high-scoring TLDs.
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 2.1.** .COM contains 48 percent of the phishing domains in our data set, and 45 percent of the domains in the TLDs for which we have domains-in-registry statistics.

We therefore suggest that domains-per-10,000 scores between .COM's 2.1 and the median of 3.2 occupy the middle ground, with scores above 3.2 indicating TLDs with increasingly prevalent phishing. [8]

Top 10 Phishing TLDs by Domain Score

Minimum 25 phishing domains and 30,000 domain names in registry

RANK	TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010
1	.th	Thailand	125	65	51,438	12.6
2	.ir	Iran	295	169	175,600	9.6
3	.ma	Morocco	73	34	36,669	9.3
4	.ie	Ireland	112	96	151,023	6.4
5	.tk	Tokelau	2,533	2,429	4,030,709	6.0
6 (tie)	.kz	Kazakhstan	49	28	50,534	5.5
6 (tie)	.cc	Cocos Islands	4,963	55	100,000	5.5
7	.in	India	523	421	791,165	5.3
8	.my	Malaysia	68	55	108,211	5.1
9	.hu	Hungary	365	255	542,000	4.7

With the exception of .TH (Thailand), the TLDs above are all newcomers to the top-10 list. .TH has been at the top of our list for two-and-a-half years. Phishing in .TH takes place

[8] Notes regarding the statistics:

- A small number of phish can increase a small TLD's score significantly, and these push up the study's median score. The larger the TLD, the less a phish influences its score, and the largest TLDs tend to appear lower in the rankings.
- A registry's score can be increased by the action of just one busy phisher, or one vulnerable or inattentive registrar.
- For more background on factors that can affect a TLD's score, please see "Factors Affecting Phishing Scores" in our earlier studies.

mostly on compromised academic (AC.TH) and government (GO.TH) Web servers. The phishing on the other TLDs was on compromised domains almost exclusively, with the exceptions of .IN and .TK. .IN was used by Chinese phishers, who registered at least 212 .IN domains to attack Chinese e-commerce sites and banks.

.TK had more phishing domains than any TLDs except .COM and .NET. .TK is a liberalized country code domain; the registry is a joint venture of the small Pacific nation of Tokelau and BV Dot TK, a privately held company. By offering free domain names, .TK has become the third-largest ccTLD in the world after Germany's .DE and Great Britain's .UK.

The downside is that the free domain names have become a popular resource for phishers. Every .TK domain used for phishing was maliciously registered. .TK was used to phish 54 different targets across the globe, but most of the domains—2,001 of the 2,429—were used to phish Chinese institutions.

BV Dot TK notes that: "Dot TK is a very open service, available for everyone in all countries. Because of this we are also used by fraudsters—and we are very aware of this. Dot TK operates a dedicated abuse and copyright infringement department in London that handles efficiently all spam, phishing, abuse and copyright infringement problems within one day, 7 days a week. Because of Dot TK's policies, domains that are registered for free can be cancelled immediately, reducing the harm of a possible threat. Dot TK works closely with many governmental law enforcement agencies, trademark organizations and anti-spam agents worldwide, resulting in an effective way to fight fraud."

If TLDs are ranked by Attacks per 10,000, then .CC is easily #1, due to the 4,803 attacks that used CO.CC subdomains. (See "Use of Subdomain Services for Phishing" on page 14). Even if those subdomains were factored out, .CC's score would still come in at 5.5 attacks per 10,000, a high score.[9]

The "generic" TLDs (gTLDs) and sponsored TLDs all had average-to-below-average scores.

Compromised Domains vs. Malicious Registrations

We performed an analysis of how many domain names were registered by phishers, versus phish that appeared on compromised (hacked) domains. These different categories are important because they present different mitigation options for responders, and offer insights into how phishers commit their crimes. We flagged a domain as malicious if it was reported for phishing within a very short time of being registered (this is an indicator that their sites were not compromised), and/or contained a brand name or misleading string, and/or was registered in a batch or in a pattern that indicated common ownership or intent.

Of the 42,624 domains used for phishing, **we identified 11,769 that we believe were registered by phishers, or 29 percent.** The number and percentage is far higher than usual; we saw only 4,775 maliciously registered domains (for 16% of the total) in 1H2010. There are two major reasons for the increase. First, this is the first report for which we have had

[9] VeriSign operates the .CC registry but does not disclose its registration numbers. We used passive DNS replication observations to estimate the approximate size of the .CC zone.

CNNIC's rich data about phishing attacks on Chinese markets. It turns out that phishers who attack Chinese targets prefer to register domain names, rather than using hacked domains. Second, .TK was abused extensively by phishers. (See "Prevalence of Phishing by Top-Level Domains," above). All the phishing sites in .TK were on malicious domains, 2,429 total.

What's also clear is that some phishers like to play games—massively multiplayer online games (MMOGs), that is. A full 18 percent of the malicious domains (2,066) were registered to phish World of Warcraft and Battle.net (the online gaming service that supports Warcraft). Online gaming credentials are valuable items for criminals, who sell them on the black market, with prices governed by how well the associated characters are developed. In-game items can also be sold for real-world cash.

The maliciously registered domains were spread over 56 different TLDs, but 89 percent of them were found on just four TLDs (.COM, .TK, .NET, and .INFO). .COM had nearly half of all maliciously registered names. Many of the malicious domains were found in TLDs whose operators run active anti-abuse programs, including .INFO, .US, .ORG, .CN, and .UK. This highlights the importance of getting reports of malicious domains to the relevant registries quickly, so they and the sponsoring registrar can take action.

Top 10 TLDs for Maliciously Registered Phishing Domains, 2H2010

Rank	TLD	TLD Location	Total Attacks
1	.com	generic TLD	5,617
2	.tk	Tokelau	2,429
3	.net	generic TLD	1,258
4	.info	generic TLD	1,164
5	.us	United States	255
6	.org	generic TLD	254
7	.in	India	251
7	.cn	China	131
9	.uk	United Kingdom	57
10	.nl	Netherlands	39

The bulk of the remaining 28,537 domains used for phishing were "compromised" or hacked domains. Phishing most often takes place on compromised Web servers, where the phishers place their phishing pages unbeknownst to the site operators. This method gains the phishers free hosting, and complicates takedown efforts because suspending a domain name or hosting account also disables the resolution of the legitimate user's site. Less than 1 percent of the domains used for phishing were domains operated by subdomain resellers and sites that offer virtual Web site hosting (such as ISPs, ovh.net, etc.).

Of the maliciously registered domains, 3,826 contained a relevant brand name or variation thereof—often a misspelling.[10] This represents 9 percent of all domains that were used for phishing, and 32.5 percent of all maliciously registered domains. These percentages

[10] Examples of domain names we counted as containing brand names included: ardwords-n.com (Google Adwords), bid-pagz-yahoo.com (Yahoo!), battleuswow.net (World of Warcraft), ntwestsc.com (Natwest), and fbphonenumbers.tk (Facebook).

historically have been about half as large, but in 2H2010 phishers registered many variations of Taobao.com, Battle.net, and World of Warcraft.

Most maliciously registered domain strings offered nothing to confuse a potential victim. Placing brand names or variations thereof in the domain name itself is not a favored tactic, since brand owners are proactively scanning Internet zone files for such names. As we have observed in the past, **the domain name itself usually does not matter to phishers, and a hacked domain name of any meaning, in any TLD, will usually do.** Instead, phishers almost always place brand names in subdomains or subdirectories. This puts the misleading string somewhere in the URL, where potential victims may see it and be fooled. Internet users are rarely knowledgeable enough to be able to pick out the "base" or true domain name being used in a URL.

Use of Subdomain Services for Phishing

As we've tracked for the past few years, phishers make significant use of subdomain registration services to host phishing Web sites. **Malicious use of these services nearly doubled in the second half of 2010, and accounted for the majority of phishing in many TLDs.** There were 11,768 phish hosted on subdomain services in the second half of 2010, while there were only 6,761 in 1H2010, 6,734 in 2H2009, 6,441 in 1H2009, and 6,339 in 2H2008. **The 2H2010 total is slightly less than the number of phish found on maliciously registered domain names purchased by phishers at regular domain name registrars in 2H2010** (12,971). **If we counted these unique subdomains as "regular" domain names, they would represent around 22 percent of all domains involved in phishing.**

We define "subdomain registration services" as providers that give customers subdomain "hosting accounts" beneath a domain name the provider owns. These services offer users the ability to define a "name" in their own DNS space for a variety of purposes. Thus a customer will obtain a hostname to use for his/her own Web site and/or e-mail of the form:

<customer_term>.<service_provider_sld>.TLD

Use of subdomain services continues to be a challenge, because only the subdomain providers themselves can effectively mitigate these phish.[11] While many of these services are responsive to complaints, very few take proactive measures to keep criminals from abusing their services in the first place.

This behavior is exemplified by the top victim of subdomain service abuse—the CO.CC service, based in Korea. **Over 40 percent of attacks using subdomain services occurred on CO.CC**, despite the fact that CO.CC is very responsive to abuse reports. Phishers are probably attracted to CO.CC because CO.CC registrations are free, easy to sign up for, come with DNS service, and there are features to assist with bulk signups. As of this writing, CO.CC supports more than 9,400,000 subdomains in more than 5,000,000 user accounts.

To its credit, CO.CC Inc, acts quickly to mitigate abuse when they are told about it.

[11] Standard domain name registrars or registry operators usually cannot mitigate these phish by suspending the main or "parent" domains as doing so would neutralize every subdomain hosted on the parent, thereby affecting innocent users as well. If extensive abuse happens on a single domain, a registrar may still opt to suspend the domain based on numerous complaints. This has been observed on occasion.

Despite that though, the median site uptime of CO.CC phish is still nearly 60 hours, possibly due to a lack of effective reporting by victims. CO.CC even runs a "whois" service for subdomain owners, which helps the anti-abuse community track down subdomain users who have had their sites hacked. However, the growing popularity of the service, especially in China, seems to have brought a very large abuse problem along with it that CO.CC hasn't been able to address on the front-end. We have seen this pattern play out with other services, and hope that they will be able to address these issues similarly.

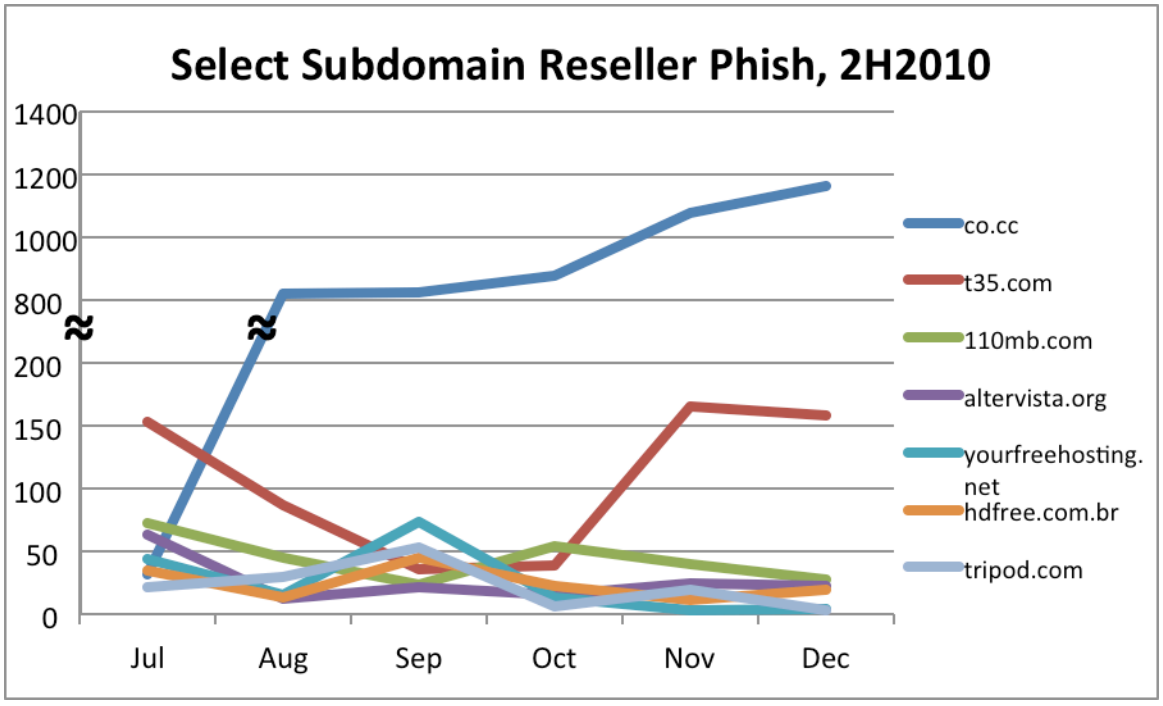
We have identified nearly 700 subdomain registration providers, which offer services on more than 3,200 domain names. This is a space as rich as the current "regulated" domain space as each subdomain service is effectively its own "domain registry." The subdomain services have many business models, and are unregulated. It is not surprising to see criminals gravitating towards this space as registries and registrars in the gTLD and ccTLD spaces implement better anti-abuse policies and procedures. We are seeing some interesting changes in this market space as well. For example, many subdomain resellers now offer WHOIS services and anti-abuse support, and we've even seen "failures" of such services.

Top 20 Subdomain Services Used for Phishing, 2H2010

Rank	Domain	Total Attacks	Provider
1	co.cc	4803	CO.CC, Inc.
2	t35.com	642	t35.com
3	110mb.com	265	110mb.com
4	altervista.org	163	altervista.org
5	yourfreehosting.net	156	yourfreehosting.net
6	hdfree.com.br	147	hdfree.com.br
7	tripod.com	132	tripod.com
7	somee.com	132	somee.com
9	my3gb.com	128	my3gb.com
10	freewebhostx.com	125	freewebhostx.com
11	hd1.com.br	123	hdfree.com.br
12	justfree.com	111	justfree.com
13	solidwebhost.com	102	blackapplehost.com
14	001webs.com	97	001webs.com
15	x10.mx	92	x10hosting.com
16	webs.com	86	webs.com
17	webcindario.com	83	miarroba.es
18	zxq.net	78	zymic.com
19	notlong.com	74	notlong.com
20	hut2.ru	67	hut2.ru

The good news in 2H2010 was that a subdomain service that had been a perennial abuse target—the Russian free email provider Pochta.ru—almost completely eliminated phishing on its service, dropping from 189 attacks in 1H2010 to only 14 attacks for the remainder of 2010. That's great news that proves that attending to these problems can pay off handsomely.

The American provider **t35.com** fell from first place in 1H2010 to second place in 2H2010 due to the rise of CO.CC phishing. Third place was occupied by 110mb.com, representing yet another listing in the top three for this provider, but abuse on its sites was down from 401 attacks in 1H2010 to 265 in 2H2010.



For more information about subdomain resellers and the unique challenges they pose for abuse mitigation, please see the APWG paper "Making Waves in the Phishers' Safest Harbors: Exposing the Dark Side of Subdomain Registries."[12]

Use of Internationalized Domain Names (IDNs)

An area of growing interest on the Internet is Internationalized Domain Names, or IDNs. **Data continues to show that the unique characteristics of IDNs are not being used to facilitate phishing.**

IDNs are domain names that contain one or more non-ASCII characters. Such domain names can contain letters with diacritical marks such as ă and ü, or characters from non-Latin scripts such as Arabic, Chinese, Cyrillic, or Hindi. Over the past six years, IDNs have been available at the second and third levels in many domain name registries, with the majority registered in Asia. IDN TLDs allow the entire domain name to be in non-Latin characters, including the TLD extension. ICANN and IANA enabled the first IDN TLDs in May 2010, and as of this writing there are 36 approved IDN TLDs.

The IDN homograph attack is a means by which a phisher seeks to deceive Internet users by exploiting the fact that characters in different language scripts may be nearly (or

[12] http://apwg.com/reports/APWG_Advisory_on_Subdomain_Registries.pdf

wholly) indistinguishable. Since January 2007, we have found only one true homograph attack. It appeared on January 16, 2009 and was the domain name "xn--hotmal-t9a.net", which appeared as "hotmaıl.net" when rendered in enabled browser address bars. Note that the lower-case "i" has been replaced with a similar-looking substitute character.

In 2H2010, we finally saw another homographic attack in the wild. It was detected on July 12, 2010 on the domain name:

http://xn--fcebook-hwa.com

When rendered in IDN-enabled browsers it appeared as:

http://fácebook.com

Otherwise, only nine other of the 42,624 domain names we studied in 2H2010 were IDNs, and they were hacked domains.

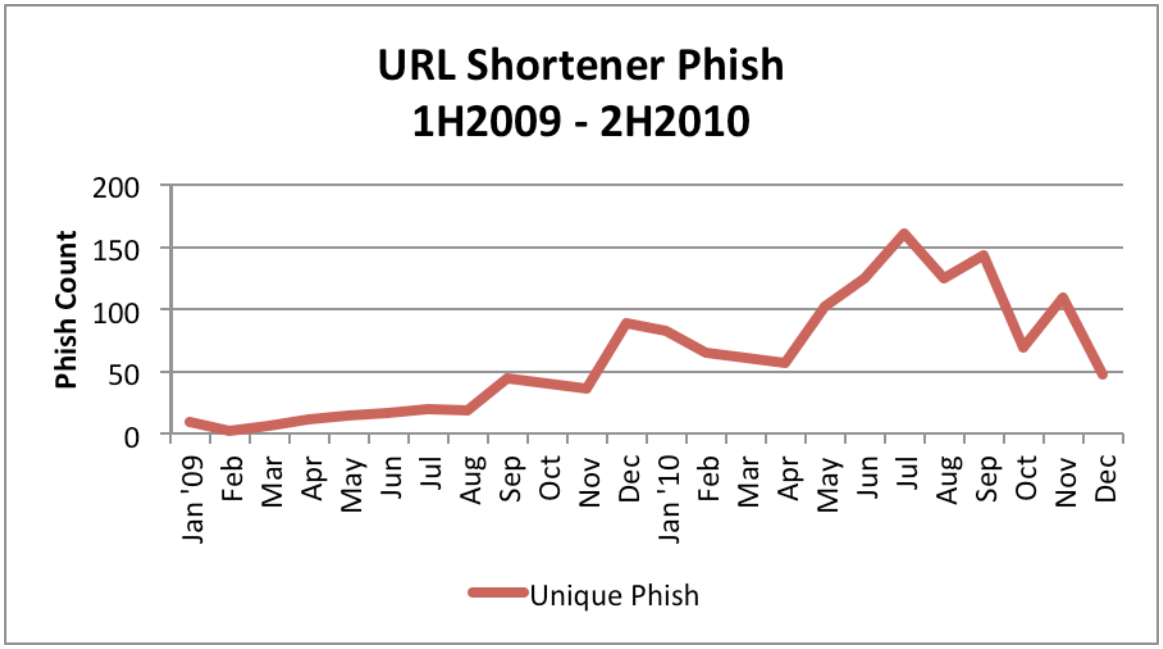
Given that IDNs have been widely available for years, why haven't phishers utilized IDN homograph attacks more often?

1. Phishers don't *need* to resort to such attacks. As noted elsewhere in this report, the domain name itself usually does not matter to a phisher.
2. By default, some browser manufacturers show the punycode version of the domain name (such as "xn--hotmal-t9a.net") in the address bar, instead of the native-character version. Users of those browsers therefore cannot see homographic attacks.

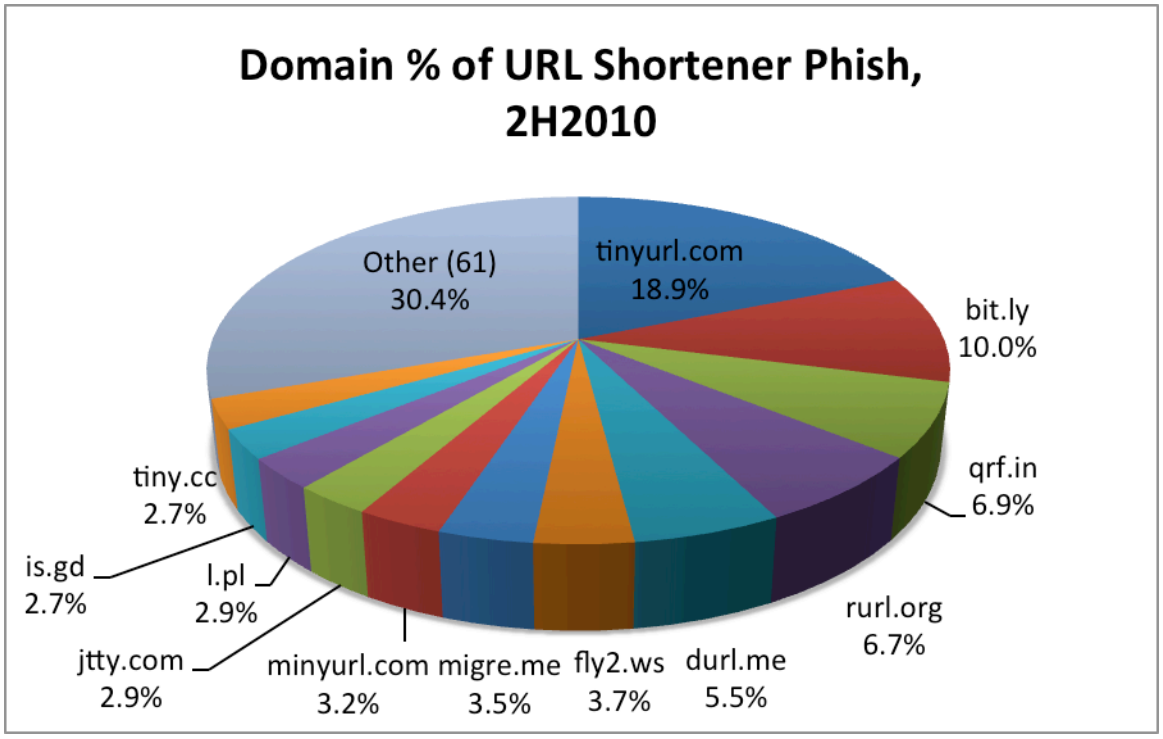
The new IDN TLD registries are being assigned to existing national ccTLD registry operators. We therefore do not believe that they will be more or less vulnerable to abuse than any other domain registry.

Use of URL Shorteners for Phishing

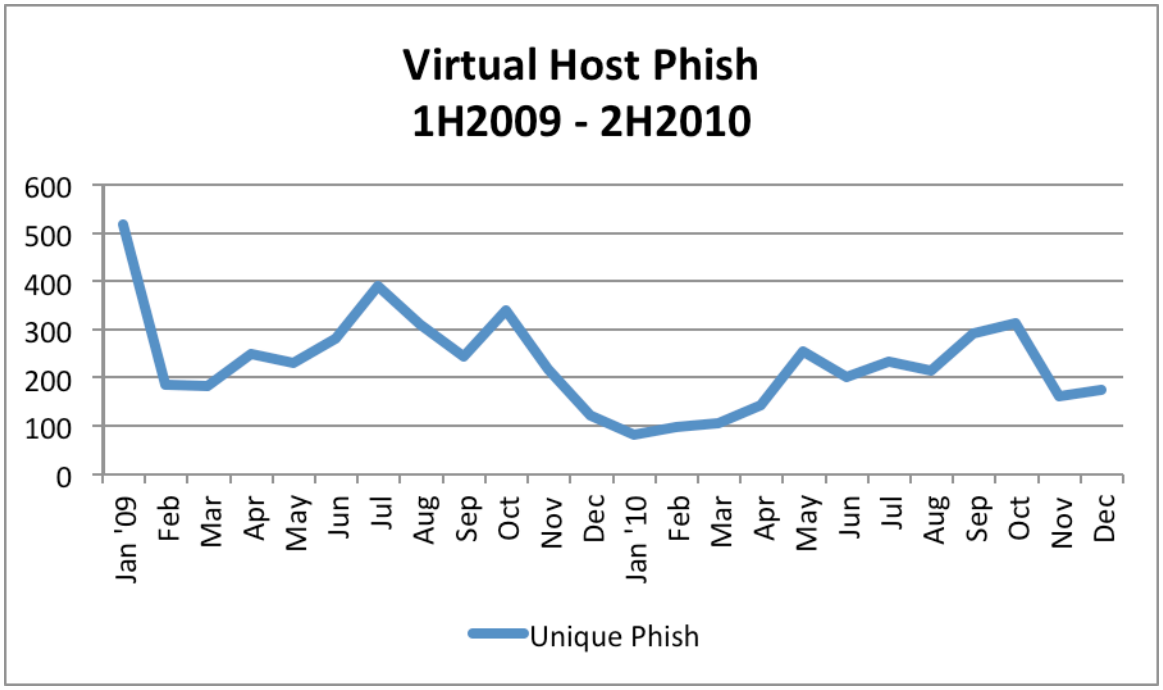
Phishers use other techniques to get their sites onto the Web, or to get past the spam filtering and browser-based protection mechanisms that protect users. As we have reported previously, there is a continuing trend to use "URL shortening" services to obfuscate phishing URLs. Users of those services can obtain a very short URL to put in their limited-space posts, which automatically redirects the visitor to a much longer "hidden" URL. Use of these URL shorteners has been driven by the popularity of Twitter and other social networking sites, and the continued shift to mobile phones and computing devices. A large and growing user base has grown accustomed to seeing and using these short URLs, and trust them regardless of the lack of transparency they provide.



Use of URL shorteners bounced around in 2010 without any apparent reason. The absolute numbers remain small but continue to bear watching. Anecdotal reports indicate that providing URL shortening services has become a competitive field, but the margins are low. In general, these services react fairly quickly to abuse complaints, but are hard-pressed to prevent malicious actors from obtaining resources on their services. Due to the abuse, various enterprises are blocking URL-shortening services from resolving for their employees.



In past reports we also looked at how phishers have used "virtual hosting" services. These services allow Internet users to easily set up Web sites hosted on a central domain, and include providers such as Ripway, OVH,net, FortuneCity, and Multimania. We saw a drop in attacks using such services in 2009, but observed a rise in early 2010. This increase seems to have plateaued through the rest of 2010. While still not a large portion of phishing, this area is still ripe for abuse, as many of these services are "free" to end-users and are a natural place for phishers to move to if significant pressure is applied elsewhere.



The End of Avalanche Phishing?

"Avalanche" is the name given to what had been the world's most prolific phishing gang, and to the botnet infrastructure it used to host phishing sites. In the second half of 2009, this criminal enterprise accounted for two-thirds of all phishing attacks worldwide. Avalanche phishing then dropped precipitously, and completely disappeared during the second half of 2010. Unfortunately, the people behind Avalanche switched to distributing the notorious Zeus Trojan. Zeus is a sophisticated piece of malware that is in the hands of many different e-criminals. The Avalanche gang started incorporating Zeus into its phishing and spamming campaigns in 2009. Zeus is *crimeware*—malware designed specifically to automate identity theft and facilitate unauthorized transactions.

The Avalanche infrastructure is still in existence as of this writing, but its activities are stealthier, focused on malware distribution and control, money mule recruitment, and other underground activities. Recent law enforcement actions and continued takedown efforts by industry do seem to have had an effect on the operation. Avalanche was covered extensively in our previous report covering the first half of 2010, and further information can be found there.

Conclusions

The inclusion of phishing data from CNNIC was a tremendous addition to this report. Clearly there are differences in phishing against Chinese targets, and likely different phishing gangs doing that phishing. We look forward to working with CNNIC and anyone else who may have unique phishing data to contribute to this report in the future. We can all learn from each other to better tackle the phishing problem.

The inclusion of the Chinese data helped drive the numbers of maliciously registered domains we identified up over prior reports, but the majority of phishing still occurs on compromised servers and PCs. As we have occasionally seen the past, changes in TLD registration and security policies do not reduce the amount of phishing in the world, or the targets of that phishing. Rather, it seems to just shift the phishing to other TLDs and services.

The majority of phishing continued to be concentrated in just a few namespaces overall, and the use of subdomain services rose considerably. As we've seen in years past, phishers will gravitate towards certain services they can abuse in bulk, and over 10 percent of phishing was seen on just two services. We will continue to monitor the abuse of URL shortening services and subdomain services by phishers.

The average and median uptimes of phish continued to rise in 2H2010. We are concerned about the rise in phishing uptimes in 2010 over prior years, and will continue to dig into this phenomenon.

Appendix: Phishing Statistics and Uptimes by TLD

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
ac	Ascension Island	0	0	15,098					0	
ad	Andorra	0	0	1,400					0	
ae	United Arab Emirates	15	8	87,000	0.9	1.7	41:02:42	8:26:19	0	0.0
aero	sponsored TLD	5	1	7,055	1.4	7.1	39:25:26	42:54:14	0	0.0
af	Afghanistan	1	1	2,000	5.0	5.0	2:01:41	2:01:41	0	0.0
ag	Antigua and Barbuda	3	3	16,789	1.8	1.8	3:21:22	1:00:54	1	0.6
ai	Anguilla	0	0	2,010					0	
al	Albania	12	10	3,769	26.5	31.8	25:05:24	7:31:39	0	0.0
am	Armenia	19	5	13,637	3.7	13.9	20:53:46	6:11:08	0	0.0
an	Netherlands Antilles	1	1	1,040	9.6	9.6	9:03:30	9:03:31	0	0.0
ao	Angola	1	1	250	40.0	40.0	8:19:26	8:19:26	0	0.0
ar	Argentina	199	148	2,199,507	0.7	0.9	100:16:37	21:08:36	3	0.0
as	American Samoa	0	0						0	
asia	sponsored TLD	21	21	179,685	1.2	1.2	51:38:20	13:07:31	13	0.7
at	Austria	141	97	980,421	1.0	1.4	81:13:19	23:01:17	0	0.0
au	Australia	754	491	1,866,664	2.6	4.0	74:17:10	15:57:07	3	0.0
aw	Aruba	1	1				38:49:02	38:49:02	0	
az	Azerbaijan	7	3	10,372	2.9	6.7	228:42:28	20:18:17	0	0.0
ba	Bosnia and Herzegovina	14	10	11,239	8.9	12.5	97:55:24	10:01:16	0	0.0
bd	Bangladesh	19	15	4,923	30.5	38.6	83:22:41	14:16:43	0	0.0
be	Belgium	238	181	1,081,042	1.7	2.2	72:44:09	17:44:19	9	0.1
bf	Burkina Faso	0	0						0	
bg	Bulgaria	30	19	23,675	8.0	12.7	43:04:14	9:17:34	0	0.0
bh	Bahrain	0	0						0	
biz	generic TLD	303	220	2,109,530	1.0	1.4	67:33:55	9:49:20	30	0.1
bm	Bermuda	0	0	7,194					0	
bn	Brunei Darussalam	1	1	845	11.8	11.8	141:46:55	141:46:56	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
bo	Bolivia	5	4	5,950	6.7	8.4	71:48:53	74:10:59	0	0.0
br	Brazil	2,011	1,030	2,275,031	4.5	8.8	88:20:39	23:07:04	21	0.1
bs	Bahamas	0	0						0	
bt	Bhutan	1	1				11:08:48	11:08:49	0	
bw	Botswana	2	2				53:24:23	53:24:23	0	
by	Belarus	32	15				69:59:01	16:33:50	0	
bz	Belize	18	7	47,639	1.5	3.8	32:22:24	13:19:48	1	0.2
ca	Canada	354	258	1,522,748	1.7	2.3	70:36:46	14:19:13	1	0.0
cat	sponsored TLD	13	7	45,381	1.5	2.9	31:14:26	29:29:20	0	0.0
cc	Cocos (Keeling) Islands	4,963	55	registry declined to provide; estimated 100,000	5.5	496.3	129:13:32	54:00:05	15	1.5
cd	Congo, Democratic Repub.	1	1	5,100	2.0	2.0	24:59:56	24:59:56	1	2.0
cg	Congo	0	0						0	
ch	Switzerland	204	125	1,487,523	0.8	1.4	61:17:52	13:06:11	0	0.0
ci	Côte d'Ivoire	0	0	1,650					0	
cl	Chile	171	128	299,463	4.3	5.7	48:22:35	21:13:23	0	0.0
cm	Cameroon	4	1				9:29:02	9:21:21	0	
cn	China	360	278	5,420,950	0.5	0.7	75:41:46	18:27:28	131	0.2
co	Colombia	86	43	527,428	0.8	1.6	55:39:16	13:21:59	4	0.1
com	generic TLD	28,296	19,311	92,739,962	2.1	3.1	71:21:06	13:36:35	5,617	0.6
coop	sponsored TLD	2	1	7,020	1.4	2.8	20:22:57	20:22:58	0	0.0
cr	Costa Rica	15	8	12,300	6.5	12.2	31:12:41	15:01:35	0	0.0
cu	Cuba	1	1	2,175	4.6	4.6	17:48:00	17:48:00	0	0.0
cx	Christmas Island	22	7	5,100	13.7	43.1	28:07:09	6:09:41	0	0.0
cy	Cyprus	6	5	6,900	7.2	8.7	85:33:13	20:55:36	0	0.0
cz	Czech Republic	222	94	732,305	1.3	3.0	64:33:34	12:49:00	2	0.0
de	Germany	801	588	13,904,646	0.4	0.6	61:58:39	12:42:51	15	0.0
dj	Djibouti	0	0						0	
dk	Denmark	280	170	1,085,200	1.6	2.6	70:12:58	12:49:24	1	0.0
dm	Dominica	1	1				9:18:08	9:18:09	0	
do	Dominican Republic	15	5	15,200	3.3	9.9	33:10:16	3:04:48	0	0.0
dz	Algeria	4	2				17:50:55	13:11:00	0	
ec	Ecuador	31	26	22,729	11.4	13.6	65:16:04	15:09:18	1	0.4

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
edu	U.S. higher education	22	15				25:09:31	6:52:21	0	
ee	Estonia	20	14	84,500	1.7	2.4	79:46:15	44:29:49	0	0.0
eg	Egypt	5	1	6,000	1.7	8.3	95:33:47	42:31:04	0	0.0
er	Eritrea	0	0						0	
es	Spain	229	163	1,249,820	1.3	1.8	61:34:01	18:22:22	5	0.0
et	Ethiopia	0	0						0	
eu	European Union	301	220	3,248,347	0.7	0.9	64:06:09	10:26:54	26	0.1
fi	Finland	36	31	245,744	1.3	1.5	129:45:20	21:00:30	0	0.0
fj	Fiji	0	0	4,000					0	
fk	Falkland Islands	0	0						0	
fm	Micronesia, Fed. States	2	2				18:31:19	18:31:20	0	
fo	Faroe Islands	0	0	3,000					0	
fr	France	963	442	1,833,755	2.4	5.3	46:47:21	12:34:11	9	0.0
gd	Grenada	20	3	3,500	8.6	57.1	26:59:30	19:54:57	0	0.0
ge	Georgia	28	22	18,230	12.1	15.4	58:02:04	16:06:04	0	0.0
gg	Guernsey	9	6				64:08:27	12:59:42	0	
gh	Ghana	0	0						0	
gi	Gibraltar	0	0	1,805					0	
gl	Greenland	10	2	4,260	4.7	23.5	6:51:42	3:02:00	0	0.0
gov	U.S. government	0	0	5,000					0	
gp	Guadeloupe	8	8	1,500	53.3	53.3	15:43:23	9:27:04	0	0.0
gr	Greece	138	100	322,000	3.1	4.3	63:02:09	16:13:12	1	0.0
gs	South Georgia & Sandwich Is.	4	2				17:06:46	13:19:49	0	
gt	Guatemala	10	9	8,630	10.4	11.6	84:59:05	76:30:58	0	0.0
gy	Guyana	1	1	1,250	8.0	8.0	10:24:29	10:24:29	0	0.0
hk	Hong Kong	38	30	194,918	1.5	1.9	23:13:24	7:32:34	0	0.0
hm	Heard and McDonald Is.	1	1				1:06:17	1:06:18	0	
hn	Honduras	3	2	4,992	4.0	6.0	9:45:20	6:26:15	0	0.0
hr	Croatia	22	17	81,175	2.1	2.7	88:20:19	20:49:27	0	0.0
ht	Haiti	7	1				78:00:57	65:10:43	0	
hu	Hungary	365	255	542,000	4.7	6.7	66:18:33	17:44:14	0	0.0
id	Indonesia	68	44				64:54:41	12:34:10	4	
ie	Ireland	116	96	151,023	6.4	7.7	50:50:14	28:14:12	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
il	Israel	44	38	195,971	1.9	2.2	58:14:41	11:41:59	1	0.1
im	Isle of Man	7	4	26,000	1.5	2.7	33:08:32	13:07:48	1	0.4
in	India	526	421	791,165	5.3	6.6	60:12:38	15:15:00	251	3.2
info	generic TLD	1,884	1,629	7,251,486	2.2	2.6	67:26:52	14:14:23	1,164	1.6
io	British Indian Ocean Terr.	21	21	3,300	63.6	63.6	135:30:10	135:30:10	10	30.3
IP address		3,051	2,318	n/a					0	
iq	Iraq	0	0						0	
ir	Iran	298	169	175,600	9.6	17.0	50:01:43	15:41:44	9	0.5
is	Iceland	16	15	31,107	4.8	5.1	87:30:29	13:48:23	0	0.0
it	Italy	362	233	2,017,002	1.2	1.8	95:12:05	22:08:45	0	0.0
je	Jersey	0	0						0	
jm	Jamaica	5	5	5,064	9.9	9.9	4:22:11	4:19:32	0	0.0
jo	Jordan	0	0	4,015					0	
jobs	sponsored TLD	0	0	32,787					0	
jp	Japan	165	108	1,185,714	0.9	1.4	54:16:04	12:20:46	0	0.0
ke	Kenya	23	14	14,050	10.0	16.4	50:13:00	14:17:00	0	0.0
kg	Kyrgyzstan	8	6	4,524	13.3	17.7	56:31:10	26:49:40	0	0.0
kh	Cambodia	3	2				125:40:33	78:26:04	0	
ki	Kiribati	0	0						0	
kr	Korea	372	197	1,101,344	1.8	3.4	60:56:24	21:33:45	0	0.0
kw	Kuwait	0	0	2,808					0	
ky	Cayman Islands	0	0	6,760					0	
kz	Kazakhstan	49	28	50,534	5.5	9.7	32:07:14	10:28:38	0	0.0
la	Lao People's Demo. Rep.	61	44				60:45:15	22:49:15	29	
lb	Lebanon	2	2	3,100	6.5	6.5	40:39:55	40:39:56	1	3.2
lc	St. Lucia	42	11	2,188	50.3	192.0	87:37:24	12:13:00	0	0.0
li	Liechtenstein	13	6	62,739	1.0	2.1	229:48:48	27:31:08	0	0.0
lk	Sri Lanka	8	6	7,050	8.5	11.3	199:41:27	67:50:43	0	0.0
ls	Lesotho	1	1				389:18:06	389:18:06	0	
lt	Lithuania	53	44	119,902	3.7	4.4	60:57:26	22:10:34	0	0.0
lu	Luxembourg	7	6	49,500	1.2	1.4	29:37:54	16:09:36	0	0.0
lv	Latvia	48	25	89,200	2.8	5.4	52:41:12	19:18:52	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
ly	Libya	99	15	9,300	16.1	106.5	76:54:35	11:10:55	0	0.0
ma	Morocco	74	34	36,669	9.3	20.2	102:00:26	8:20:08	0	0.0
mc	Monaco	2	2				21:25:40	21:25:41	0	
md	Moldova	17	16	8,700	18.4	19.5	64:13:18	5:42:15	0	0.0
me	Montenegro	139	51	416,307	1.2	3.3	66:30:37	9:53:14	17	0.4
mg	Madagascar	0	0	1,000					0	
mk	Macedonia	10	9	4,322	20.8	23.1	117:57:51	11:26:36	0	0.0
ml	Mali	0	0						0	
mn	Mongolia	55	13	8,809	14.8	62.4	41:13:21	14:07:58	0	0.0
mo	Macao	1	1				130:26:53	130:26:53	0	
mobi	sponsored TLD	26	23	977,074	0.2	0.3	117:21:51	31:45:12	10	0.1
mp	Northern Mariana Islands	7	2				232:58:17	6:28:59	0	
mr	Mauritania	0	0						0	
ms	Montserrat	15	6	10,000	6.0	15.0	53:09:24	17:34:48	0	0.0
mt	Malta	1	1	12,000	0.8	0.8	203:49:36	203:49:37	0	0.0
mu	Mauritius	12	3	7,500	4.0	16.0	69:58:25	58:30:39	0	0.0
museum	sponsored TLD	0	0	463					0	
mx	Mexico	253	114	450,453	2.5	5.6	80:44:57	18:38:14	0	0.0
my	Malaysia	70	55	108,211	5.1	6.5	103:52:39	17:04:52	0	0.0
mz	Mozambique	0	0	1,885					0	
na	Namibia	1	1				8:55:05	8:55:05	1	
name	generic TLD	30	20	235,667	0.8	1.3	176:52:34	15:04:45	4	0.2
nc	New Caledonia	3	1				38:26:57	17:32:13	0	
ne	Niger	1	1				37:04:36	37:04:36	0	
net	generic TLD	4,895	3,185	13,776,690	2.3	3.6	82:01:17	16:51:27	1,258	0.9
nf	Norfolk Island	10	6	2,100	28.6	47.6	74:34:37	8:38:54	0	0.0
ng	Nigeria	4	3	1,350	22.2	29.6	20:47:33	14:04:02	0	0.0
ni	Nicaragua	5	3	5,905	5.1	8.5	170:31:37	103:29:30	0	0.0
nl	Netherlands	658	497	4,162,539	1.2	1.6	56:50:58	14:25:08	39	0.1
no	Norway	105	78	489,952	1.6	2.1	89:03:15	18:52:09	0	0.0
np	Nepal	35	23	22,000	10.5	15.9	91:39:39	14:56:40	0	0.0
nr	Nauru	3	2	450	44.4	66.7	71:46:29	67:38:31	0	0.0
nu	Niue (estimated)	50	22	200,000	1.1	2.5	30:18:02	10:34:31	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
nz	New Zealand	104	81	417,103	1.9	2.5	48:43:20	13:46:32	2	0.0
om	Oman	1	1				9:31:45	9:31:45	0	
org	generic TLD	2,704	1,702	8,678,049	2.0	3.1	71:46:40	13:08:33	254	0.3
pa	Panama	0	0	6,250					0	
pe	Peru	27	19	45,180	4.2	6.0	29:18:19	8:33:47	0	0.0
pf	French Polynesia	0	0	133					0	
ph	Philippines	25	15	registry declined to provide			147:37:24	12:32:33	0	
pk	Pakistan	43	27	registry declined to provide			52:54:17	16:13:32	0	
pl	Poland	672	403	1,927,364	2.1	3.5	70:24:56	16:21:39	2	0.0
pn	Pitcairn	19	3	877	34.2	216.6	90:04:12	15:34:30	0	0.0
pro	sponsored TLD	1	1	94,607	0.1	0.1	10:56:21	10:56:21	0	0.0
ps	Palestinian Territory	9	8	5,430	14.7	16.6	178:03:28	25:43:51	0	0.0
pt	Portugal	94	68	337,721	2.0	2.8	42:22:06	6:44:23	0	0.0
py	Paraguay	6	6	11,200	5.4	5.4	338:02:21	82:48:26	0	0.0
qa	Qatar	1	1						0	
re	Réunion	2	2	6,102	3.3	3.3	57:01:28	57:01:28	0	0.0
rf (.рф)	Russian Federation IDN (.xn--p1ai)	0	0	18,346					0	
ro	Romania	356	191	470,550	4.1	7.6	50:27:00	13:05:19	2	0.0
rs	Serbia	31	26	60,500	4.3	5.1	70:09:20	23:36:53	0	0.0
ru	Russian Fed.	1,103	599	3,046,151	2.0	3.6	86:48:23	18:47:00	10	0.0
rw	Rwanda	1	1				81:48:03	81:48:04	0	
sa	Saudi Arabia	13	10	20,984	4.8	6.2	122:09:41	21:05:28	0	0.0
sc	Seychelles	0	0	4,847					0	
sd	Sudan	0	0						0	
se	Sweden	213	156	1,032,555	1.5	2.1	60:43:08	16:53:36	3	0.0
sg	Singapore	63	37	121,004	3.1	5.2	93:43:11	25:30:05	0	0.0
sh	Saint Helena	1	1				81:38:08	81:38:08	1	
si	Slovenia	34	29	88,350	3.3	3.8	36:20:40	14:40:54	0	0.0
sk	Slovakia	71	27	227,664	1.2	3.1	32:23:50	9:17:30	1	0.0
sl	Sierra Leone	0	0	750					0	
sm	San Marino	0	0	1,910					0	
sn	Senegal	2	2	2,700	7.4	7.4	4:16:11	4:16:12	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
st	Sao Tome and Principe	2	2				44:38:17	44:38:18	0	
su	Soviet Union	53	24	88,925	2.7	6.0	54:33:34	20:25:17	0	0.0
sv	El Salvador	2	2	4,725	4.2	4.2	84:36:20	84:36:20	0	0.0
sy	Syria	0	0						0	
sz	Swaziland	0	0	1,030					0	
tc	Turks and Caicos	16	9	10,200	8.8	15.7	46:55:36	15:23:45	0	0.0
tel	generic TLD	0	0	255,130					0	
tf	French Southern Territories	14	5	1,550	32.3	90.3	78:12:59	23:46:59	0	0.0
tg	Togo	0	0						0	
th	Thailand	125	65	51,438	12.6	24.3	74:12:22	17:49:47	0	0.0
tj	Tajikistan	1	1	18,600	0.5	0.5	4:59:16	4:59:16	0	0.0
tk	Tokelau (estimated)	2,536	2,429	4,030,709	6.0	6.3	77:27:53	21:54:16	2,429	6.0
tl	Timor-Leste	21	11	1,797	61.2	116.9	104:57:50	25:05:00	0	0.0
tm	Turkmenistan	1	1	3,777	2.6	2.6	112:38:16	112:38:16	0	0.0
tn	Tunisia	0	0	8,000					0	
to	Tonga	201	64	13,300	48.1	151.1	100:08:37	8:58:08	31	23.3
tp	Portuguese Timor	6	3				14:19:01	14:10:46	0	
tr	Turkey	47	38	230,500	1.6	2.0	53:43:03	12:12:07	1	0.0
travel	sponsored TLD	1	1	42,483	0.2	0.2	10:50:14	10:50:15	0	0.0
tt	Trinidad and Tobago	13	6	2,200	27.3	59.1	200:46:42	27:41:37	0	0.0
tv	Tuvalu (estimated)	75	40	163,074	2.5	4.6	57:46:38	17:16:19	0	
tw	Taiwan	177	126	468,712	2.7	3.8	65:32:47	12:02:05	4	0.1
tz	Tanzania	1	1	3,500	2.9	2.9	5:01:56	5:01:57	0	0.0
ua	Ukraine	250	155	517,405	3.0	4.8	63:42:29	17:04:06	1	0.0
ug	Uganda	9	6	3,258	18.4	27.6	232:12:52	57:18:49	0	0.0
uk	United Kingdom	1,677	1,046	8,880,507	1.2	1.9	64:09:20	14:41:26	57	0.1
us	United States	495	398	1,663,065	2.4	3.0	90:07:48	18:00:38	255	1.5
uy	Uruguay	13	9	27,925	3.2	4.7	158:32:23	18:56:15	0	0.0
uz	Uzbekistan	1	1	10,757	0.9	0.9	108:05:24	108:05:24	0	0.0
vc	St. Vincent and Grenadines	5	3	6,302	4.8	7.9	23:06:35	23:06:36	0	0.0
ve	Venezuela	32	26	150,000	1.7	2.1	34:35:38	16:24:45	1	0.1
vg	British Virgin Islands	20	7	8,350	8.4	24.0	84:45:35	17:31:09	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2010	Unique Domain Names used for phishing 2H2010	Domains in registry Oct 2010	Score: Phish per 10,000 domains 2H2010	Score: Attacks per 10,000 domains 2H2010	Average Uptime 2H2010 hh:mm:ss	Median Uptime 2H2010 hh:mm:ss	# Total Malicious Domains Registered 2H2010	Malicious registrations score/10,000 domains in registry
vi	Virgin Islands	2	2	1,100	18.2	18.2	8:05:27	8:05:28	0	0.0
vn	Vietnam	141	78	170,245	4.6	8.3	45:49:12	22:09:58	1	0.1
vu	Vanuatu	2	2				9:09:03	9:09:04	0	
ws	Samoa	117	27	544,500	0.5	2.1	123:11:04	13:29:46	1	0.0
ye	Yemen	0	0						0	
yu	Yugoslavia (TLD deprecated March 2010)	0	0	0					0	
za	South Africa	242	181	600,359	3.0	4.0	70:11:50	15:48:21	4	0.1
zm	Zambia	0	0						0	
zw	Zimbabwe	1	1	10,855	0.9	0.9	0:23:21	0:23:21	0	0.0
	TOTALS	**67,677**	**42,624**	**205,615,855**					**11,769**	

About the Authors & Acknowledgments

The authors wish to thank the following for their support: Peter Cassidy, Foy Shiver, Dave Jevans, and Laura Mather of the APWG; Aaron Routt and Heidi Harris of Internet Identity; and Ram Mohan and Bruce Reeser of Afilias. The authors thank Liming Wang and Wang Wei at CNNIC for the contribution of APAC phishing data for this report. The authors also thank the members of the security industry, the domain name industry, and the law enforcement community who have contributed to anti-phishing programs and research.

Greg Aaron is Director of Key Account Management and Domain Security at Afilias (www.afilias.info). Greg oversees .INFO operations and Afilias' security programs, including domain name abuse policy and practices, and also provides anti-abuse services to the .ORG registry. Greg is an authority on the use of domain names for e-crime, and works with registrars, registries, law enforcement, and researchers regarding phishing, malware, spam, and child pornography cases. In 2010, Greg accepted an OTA Excellence in Online Trust Award for Afilias' anti-abuse programs. He was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG), and served on ICANN's Fast-Flux Working Group. Greg also serves on the Steering Committee of the Anti-Phishing Working Group (APWG). Greg has advised governments, ccTLD operators, and ICANN regarding registry policies and operations, and he oversaw the launches of the .MOBI, .IN, and .ME TLDs. He also has significant experience with Sunrises and Internationalized Domain Names (IDNs). Greg is a magna cum laude graduate of the University of Pennsylvania.

Rod Rasmussen is President and CTO of Internet Identity (www.internetidentity.com), and has served as its technical leader since he co-founded the company in 2001. He is widely recognized as a leading expert on the abuse of the domain name system by phishing criminals. Rasmussen is co-chair of the Anti-Phishing Working Group's (APWG) Internet Policy Committee (IPC), and serves as the APWG's Industry Liaison to various groups around the world, including ICANN, the international oversight body for domain names. He served on ICANN's Fast-Flux Working Group, its Registration Abuse Policy Working Group (RAPWG), and is co-chairing a special ICANN working group looking into provision of zone file access for new gTLDs. He is also a member of the Steering Committee for the Authentication and Online Trust Alliance (AOTA), and an active member of the Digital PhishNet, a collaboration between industry and law enforcement. Prior to starting Internet Identity, Rasmussen held product management roles for LanQuest, a network equipment testing company, and networking product manufacturer Global Village. Rasmussen earned an MBA from the Haas School of Business at the University of California, Berkeley and holds two bachelor's degrees, in Economics and Computer Science, from the University of Rochester.

#