Global Phishing Survey: Trends and Domain Name Use in 1H2012

APWG

Unifying the
Global Response
To Cybercrime

Published October 2012

An
APWG
Industry
Advisory

Published October 23, 2012

Authors:

Rod Rasmussen, Internet Identity
<rod.rasmussen at internetidentity.com>
and
Greg Aaron, Afilias
<gaaron at afilias.info>

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

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

Phishing in the first half of 2012 reminded us that e-crime has no boundaries. Phishers crossed national boundaries to hit targets at home and abroad. Phishers hacked into servers to perpetrate mass attacks across the globe. And phishers took advantage of all kinds of online services, especially if they were lightly defended or convenient.

This report seeks to understand trends and their significance by quantifying the scope of the global phishing problem. Specifically, this new report examines all the phishing attacks detected in the first half of 2012 ("1H2012", January 1, 2012 through June 30, 2012). The data was collected by the Anti-Phishing Working Group, and supplemented with data from several phishing feeds, CNNIC, and private sources. The APWG phishing repository is the Internet's most comprehensive archive of phishing and e-mail fraud activity.

Our major findings in this report include:

1. **The average and median uptimes of phishing attacks dropped to a record low in 1H2012, by far the lowest since we began measuring in January 2008.** *(Page 6)*
2. **The number of phishing attacks rose.** *(Pages 4-5)*
3. **Phishers registered more subdomains than regular domain names** *(page 16)*, **while the number of domain names registered by phishers has dropped by almost half since early 2011** *(pages 12-13)*.
4. **The number of targeted institutions has dropped; phishers continue to target larger or more popular targets.** *(Page 5)*
5. **Phishers attacking Chinese institutions were responsible for two-thirds of all malicious domain name registrations made in the world.** *(Page 12)* **These phishers use both Chinese and non-Chinese registrars, but not .CN domain names.** *(Page 15)*
6. **Domain name owners in South America had their web servers compromised by phishers in growing numbers.** *(Page 11)*

Basic Statistics

Millions of phishing URLs were reported in 1H2012, but the number of unique phishing attacks and domain names used to host them was much smaller.[1] The 21H2012 data set yielded the following statistics:

- **There were at least 93,462 unique phishing attacks worldwide, in 202 top-level domains (TLDs).** This is more than the 83,083 attacks we observed in the second half of 2011**.** The increase is due in part to an increase in phishing attacks that leveraged shared virtual servers to compromise multiple domains at once. An "attack" is

[1] 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. 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.

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 attacks used 64,204 unique domain names.**[2] Again, this is up from the 50,298 domains used in 2H2011. The number of domain names in the world grew from 226.5 million in November 2011 to 240 million in May 2012.[3]
- In addition**, 2,410 attacks were detected on 1,864 unique IP addresses, rather than on domain names.** (For example: http://79.173.233.18/paypal/.) The number of attacks using IPs has remained relatively steady for two years. None of these phish were reported on IPv6 addresses.
- Of the 64,204 phishing domains, **we identified 7,712 that we believe were registered maliciously, by phishers.** This is down significantly from 12,895 in 2H2011 and 14,650 in 1H2011. Of those, 5,117 (66%) were registered to phish Chinese targets, down from 7,991 in 2H2011. The other 56,492 domains were almost all hacked or compromised on vulnerable Web hosting.
- **Phishing is generally distributed by top-level domain market share, but 90% of the malicious domain registrations were in just three TLDs**: .TK, .COM, and .IN.
- **We counted 486 target institutions, virtually the same as the 487 in 2H2011 but far below the 587 attacked in 2H2010**. Targets include the users of banks, e-commerce sites, social networking services, ISPs, government tax bureaus, online gaming sites, postal services, and securities companies.
- **Only about 2% of all domain names that were used for phishing contained a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations.")
- Only 58 of the 64,204 domain names were internationalized domain names (IDNs), and none were homographic attacks.

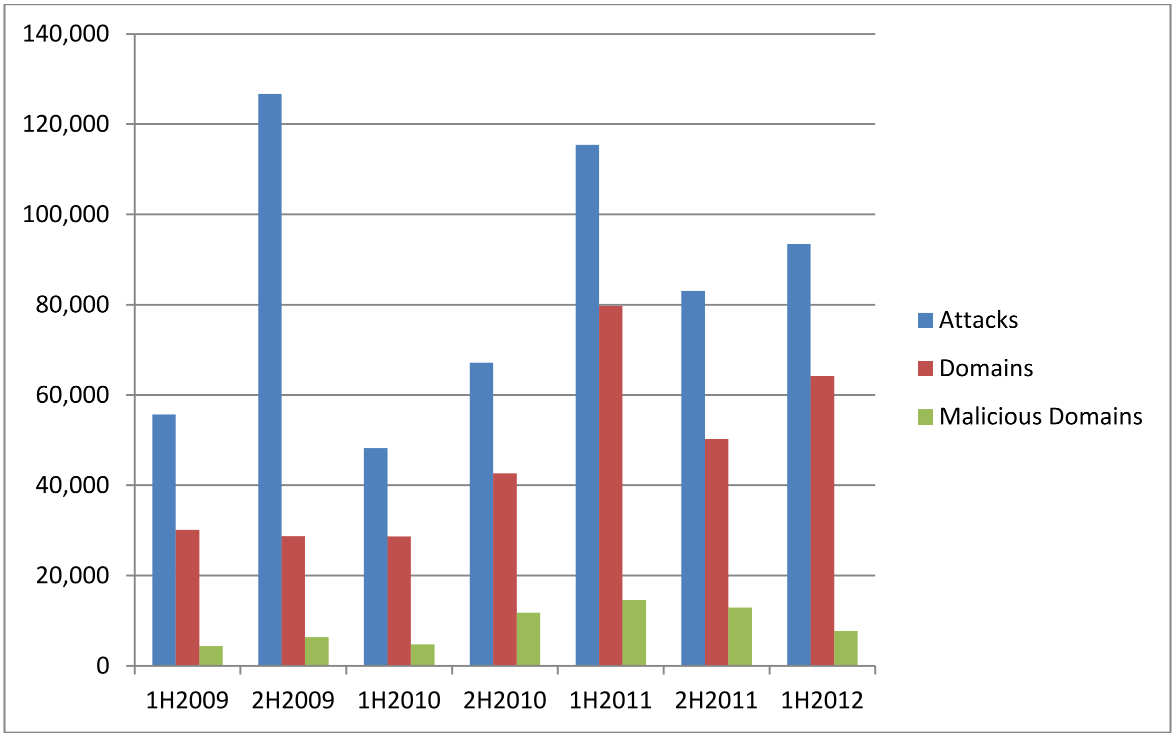
[2] "Domain names" are defined as second-level domain names, plus third-level domain names if the relevant registry offers third-level registrations. An example is the .CN (China) registry, which offers both second-level registrations and third-level registrations (in zones such as com.cn, gov.cn, zj.cn,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

[3] As per our research, including gTLD stats from ICANN.org, and stats provided by the ccTLD registry operators.

Basic Statistics

	1H2012	2H2011	1H2011	2H2010	1H2010
Phishing domain names	64,204	50,298	79,753	42,624	28,646
Attacks	93,462	83,083	115,472	67,677	48,244
TLDs used	202	200	200	183	177
IP-based phish (unique IPs)	1,864	1,681	2,385	2,318	2,018
Maliciously registered domains	7,712	12,895	14,650	11,769	4,755
IDN domains	58	36	33	10	10
Number of targets	486	487	520	587	568

Phishers attacked fewer targets, concentrating on larger, more prominent targets. We believe they did so because there is less money to be made off the smaller targets. It is easier for phishers to sell stolen credentials associated with more popular institutions, and there is a growing emphasis on gaining access to e-mail accounts, which enable phishers to spam from whitelisted services such as Gmail, Hotmail, Yahoo!, and so on.

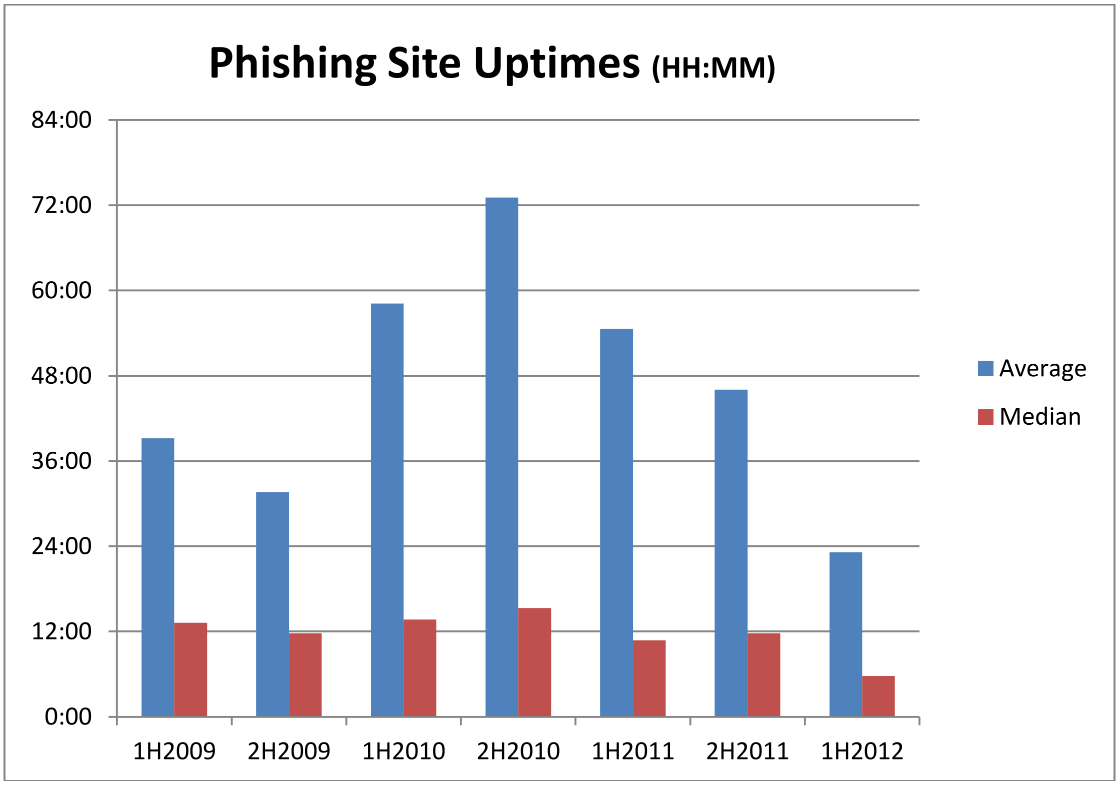


Phishing against targets in China remained prevalent, but not as heavy as in late 2011. Chinese e-commerce site Taobao.com dropped from the most-targeted site to the number two position, with PayPal taking over the number one position again in 1H2012. We are grateful to CNNIC and APAC for sharing their data with us.

Phishing by Uptime

The average uptimes of phishing attacks dropped to a record low in 1H2012, by far the lowest since we began measuring in January 2008. The average uptime in1H2012 was 23 hours and 10 minutes, compared to 46 hours and 3 minutes in 2H2011, and a high of 73 hours in 2H2010. The median uptime in1H2012 was 5 hours and 45 minutes – less than half the median of 11 hours and 43 minutes recorded in 2H2011.

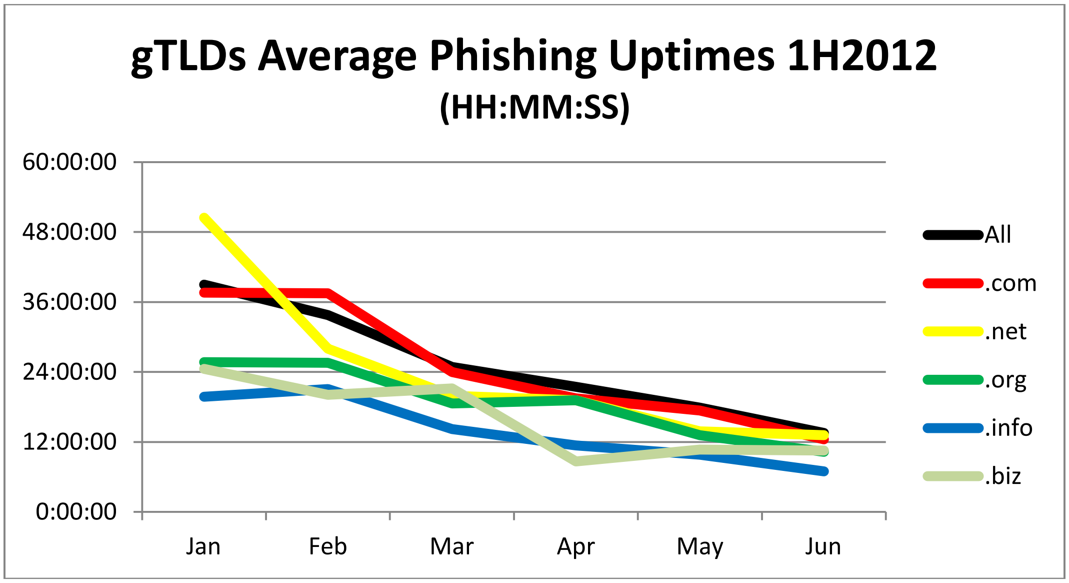
The "uptimes" or "live" times[4] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a measure of the success of mitigation efforts. The longer a phishing attack remains active, the more money the victims and target institutions lose.



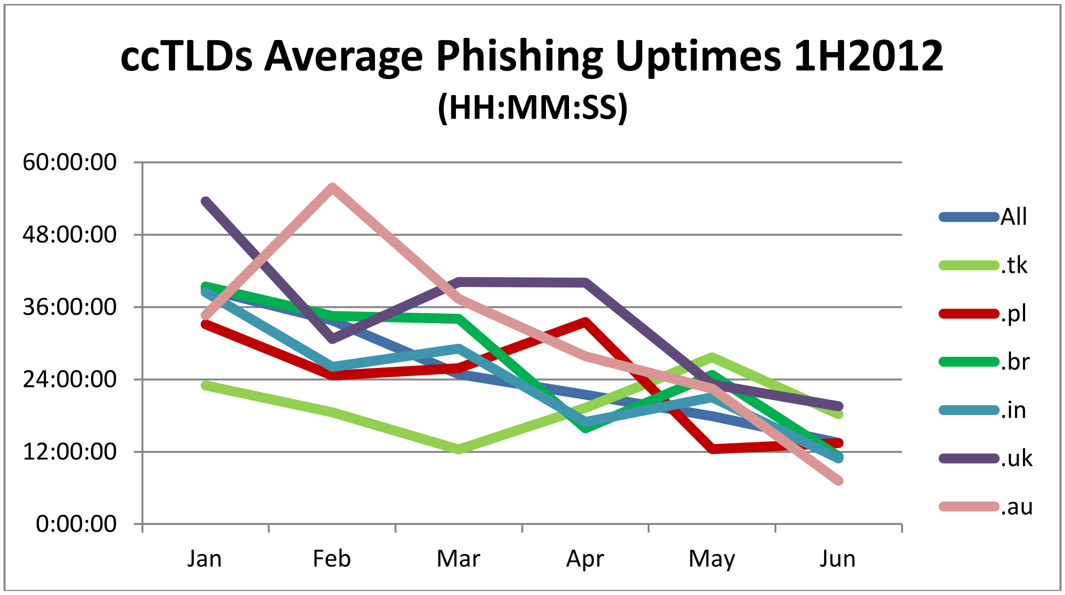
[4] The system used to track the uptimes automatically monitored the phishing sites, and monitoring began as soon as the system became aware of a phish via feeds or honeypots. Each phish was checked several times per hour to confirm its availability, and was not declared "down" until it had stayed down 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.

The first two days of a phishing attack are 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.

In the large generic top-level domains (gTLDs), .INFO, .BIZ, and .ORG had the lowest uptimes, due to notification and takedown programs at those registry operators:



gTLD times fell over the months as virtual server hacking increased through June. The virtual server attacks tended to be mitigated more efficiently – they may have prompted many complaints to the hosting providers affected, and each mitigation effort took down multiple phishing attacks at once. The uptimes at large country-code TLDs (ccTLDs) varied:

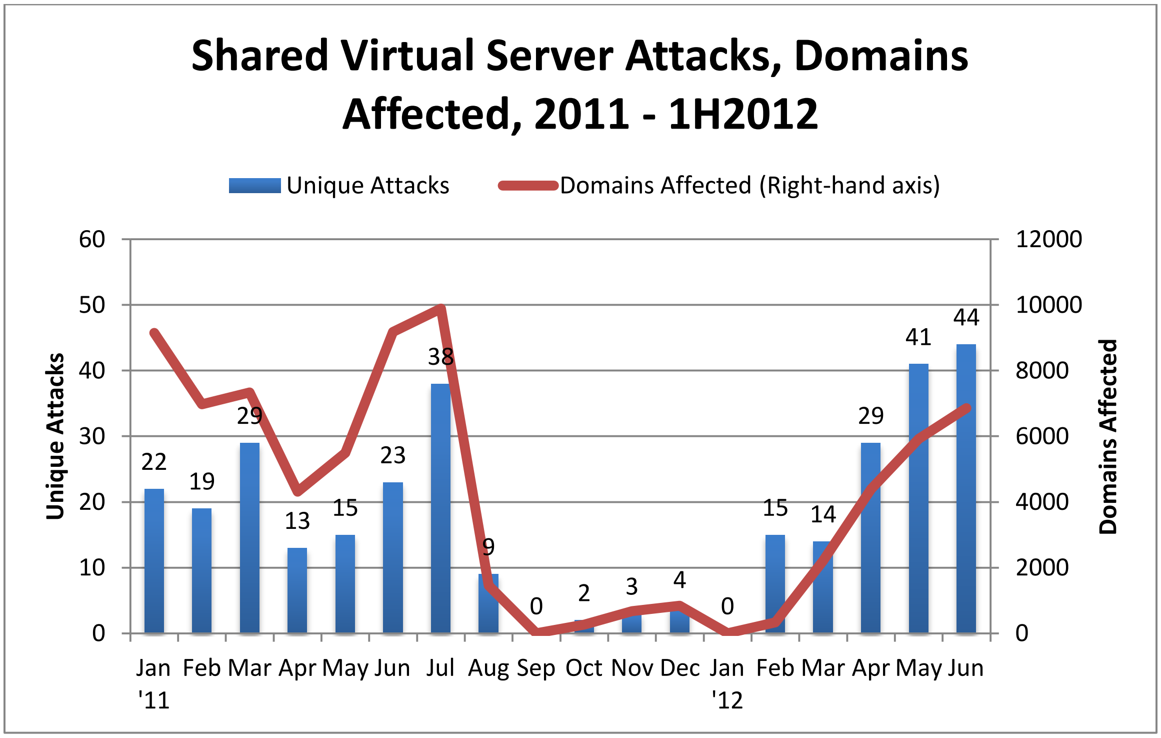


For uptime statistics for every top-level domain, please see the Appendix.

Attack Methods: Rise of Shared Virtual Server Hacking

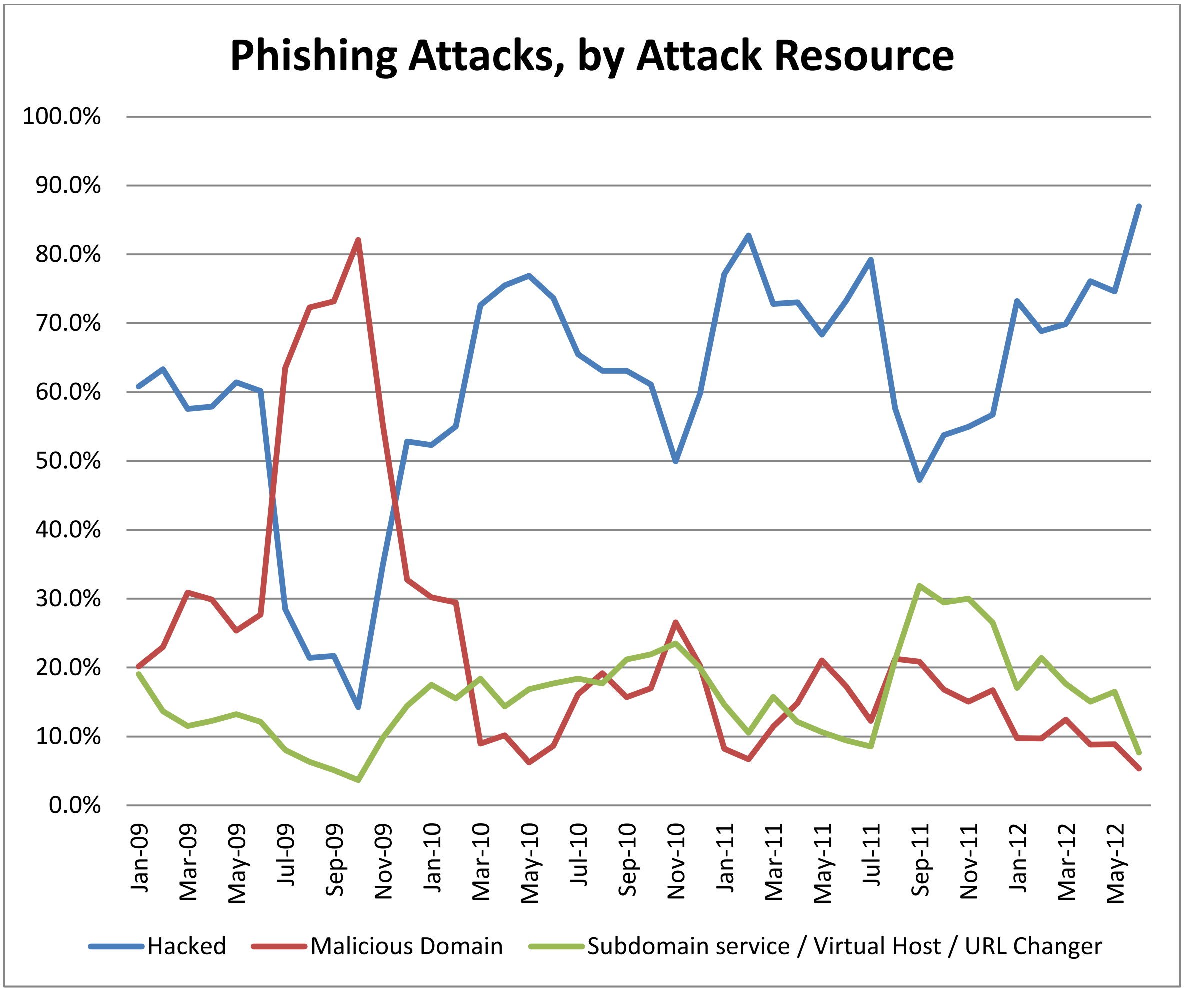
In a trend we first described in1H2011, a tactic used by phishers drastically affected our statistics. In this attack, a phisher breaks into a web server that hosts large numbers of domains – a "shared virtual server" in industry parlance. Once the phisher breaks into such a server, he first uploads a single copy of his phishing content. He then updates the web server configuration to add that content to *every* hostname served by that web server, so that all web sites on that server start displaying the phishing pages via a custom subdirectory.

So instead of hacking sites one at a time, the phisher can infect dozens, hundreds, or even thousands of web sites at a time, depending on the server. In 1H2011, we identified over 40 thousand phishing attacks that used this technique. However, this virtual server hacking dwindled to very low levels after July 2011, with zero attacks of this nature being seen in January 2012. Starting in February however, these attacks started reappearing, and in June there were nearly 7,000 such phishing attacks sitting on 44 different servers.



A Historical Retrospective

Since we have been publishing this survey for several years now, we have enough historical data to provide very interesting context and trends around the use of phishing resources or methods as they ebb and flow over time. In the graph below, we have plotted the percentages of attacks that used hacked domains, versus maliciously registered domains, versus shared virtual hosts and subdomains:



The spike in malicious domain registrations in 2009 was due to the Avalanche phishing gang, which registered large numbers of domains. In general, the trend has been for phishers to use more hacked servers, and fewer resources like domain names that are under the phishers' direct control. There are several factors that may be contributing to these trends: reputation services are blocking domains and subdomains quickly; registrars and registries are more responsive to malicious registrations and have increased their fraud controls; phishers have automated scripts and services that find and exploit large numbers of web servers using known vulnerabilities; and there are more exploitable web services, particularly applications like WordPress or Joomla.

These constant changes are a good illustration of the continually changing landscape the anti-phishing community must deal with. We will continue to track these attacks going forward, and shared web hosting providers should pay particular attention, as it is clear that they are being targeted by at least a segment of the phishing underground.

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 majority of phishing continues to be concentrated in just a few namespaces. Except for .PL subdomains and .TK domains, which were taken advantage of extensively by phishers, phishing attacks were roughly distributed by market share. **The complete tables are presented in the Appendix.**

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"[5] 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.

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 4.0**.
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 3.0.** .COM contained 48% of the phishing domains in our data set, and 44% of the domains in the world.

We therefore suggest that domains-per-10,000 scores between .COM's 3.0 and the median of 4.0 occupy the middle ground, with scores above 4.0 indicating TLDs with increasingly prevalent phishing. [6]

The top TLDs by score are given in the chart below.

[5] Score = (phishing domains / domains in TLD) x 10,000

[6] Notes regarding the statistics:

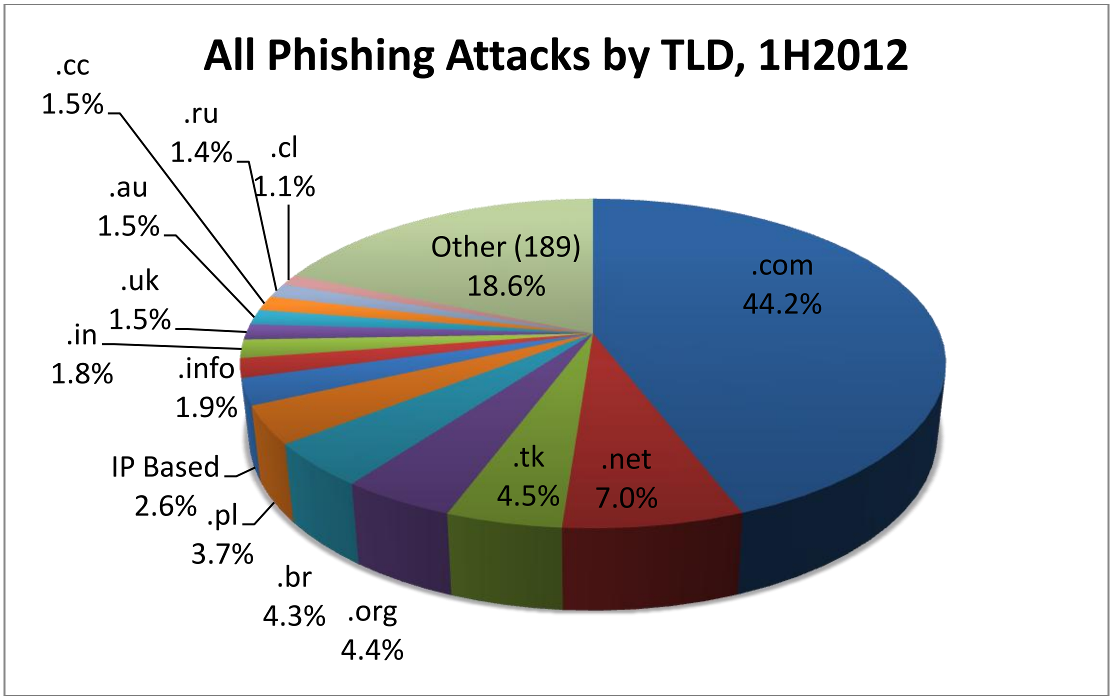
- A small number of phish can increase a small TLD's score significantly, and these push up the study's median score. The larger the TLD, the less a phish influences its score.
- A registry's score can be increased by the action of just one busy phisher, or one vulnerable or inattentive registrar.
-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

Top 10 Phishing TLDs by Domain Score, 1H2012

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

RANK	TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phish per 10,000 domains 2H2011
1	cl	Chile	1,024	831	383,100	21.7
2	pe	Peru	126	115	61,530	18.7
3	id	Indonesia	113	95	78,000	12.2
4	th	Thailand	122	77	69,490	11.1
5	br	Brazil	4,039	3,207	2,959,495	10.8
6	ec	Ecuador	36	31	30,001	10.3
7	ro	Romania	967	533	576,323	9.2
8	za	South Africa	764	644	779,500	8.3
9	in	India	1,690	1,351	1,674,552	8.1
10	uy	Uruguay	35	29	36,908	7.9

South American domains suffered a rash of server compromises. The .CL domains were hacked in unusually high numbers, pushing .CL from a score of 7.2 in 2H2011 to 21.7 in 1H2012. ccTLDs .PL (Peru), .BR (Brazil), .EC (Ecuador), and Uruguay (.UY) also suffered phishing on hacked domains. Thailand's .TH continues to rank highly, as it has for several years, suffering especially from compromised government and university Web servers.



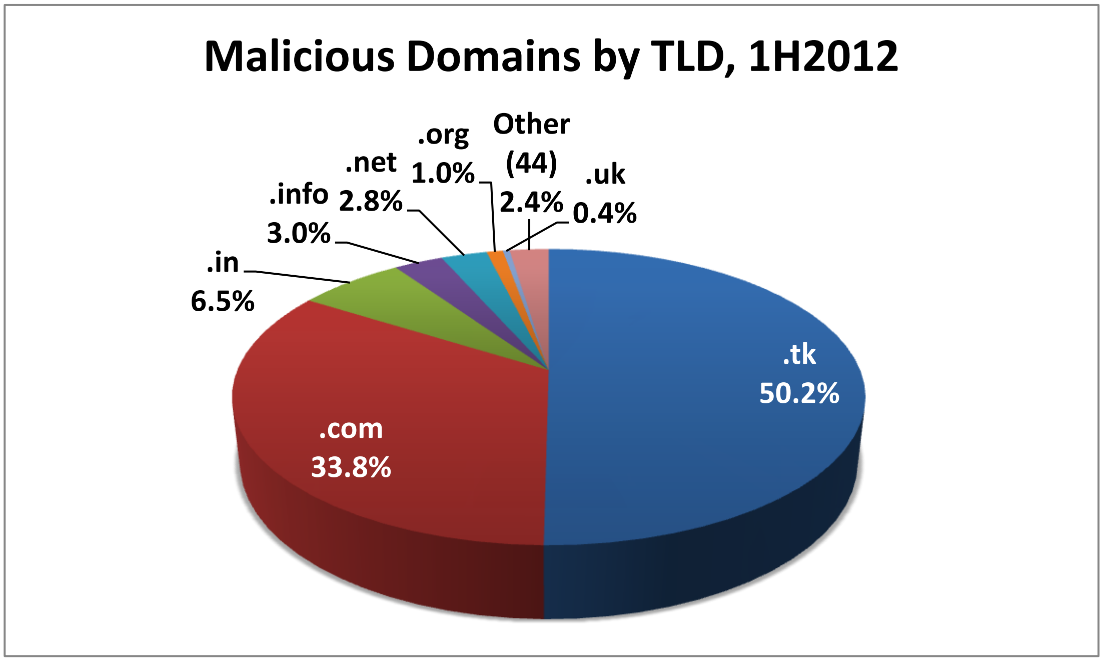
India's .IN TLD dropped from the number two position in 2H2011 to number nine. In 2H2011, more than half of the attacks using .IN domains targeted users of Battle.net, the online gaming site. In 1H2012, .IN domains were used to attack a more even distribution of 91 different targets.

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, 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 64,204 phishing domains, **we identified 7,712 that we believe were registered maliciously, by phishers. This is down significantly** from 12,895 in 2H2011 and 14,650 in 1H2011. The other 56,492 domains were almost all hacked or compromised on vulnerable Web hosting.

Of those 7,712 domains, 5,117 (66%) were registered to phish Chinese targets. This is down from 7,991 such domains in 2H2011. Chinese phishers continue to register domains for phishing, and use hacked domains less often.



Half of the world's malicious registrations were make in the .TK TLD. 90% of the malicious domain registrations were made in just three TLDs: .TK, .COM, and .IN.

.TK domains are offered for free, and the .TK registry offers an API that allows trusted partners to shut down domains that are being used for phishing and other abuses. (These partners include Facebook, Internet Identity, and the Anti-Phishing Alliance of China.) Taobao.com was the target most frequently attacked using .TK domains, another reminder that Chinese phishers prefer to register domains much more than other phishers.

Otherwise, phishers turned to subdomain services, which are more lightly defended than top-level domains, and offer cheaper (often free) registrations.

Of the maliciously registered domains, 1,350 contained a relevant brand name or variation thereof—often a misspelling.[7] This is far below the 2,232 we found in 2H2011. **This represents just 2% of all domains that were used for phishing, and 17% of all maliciously registered domains recorded in the sampling period.**

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 domain name of any meaning, or no meaning at all, 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.

Registrars Used for Malicious Domain Registrations

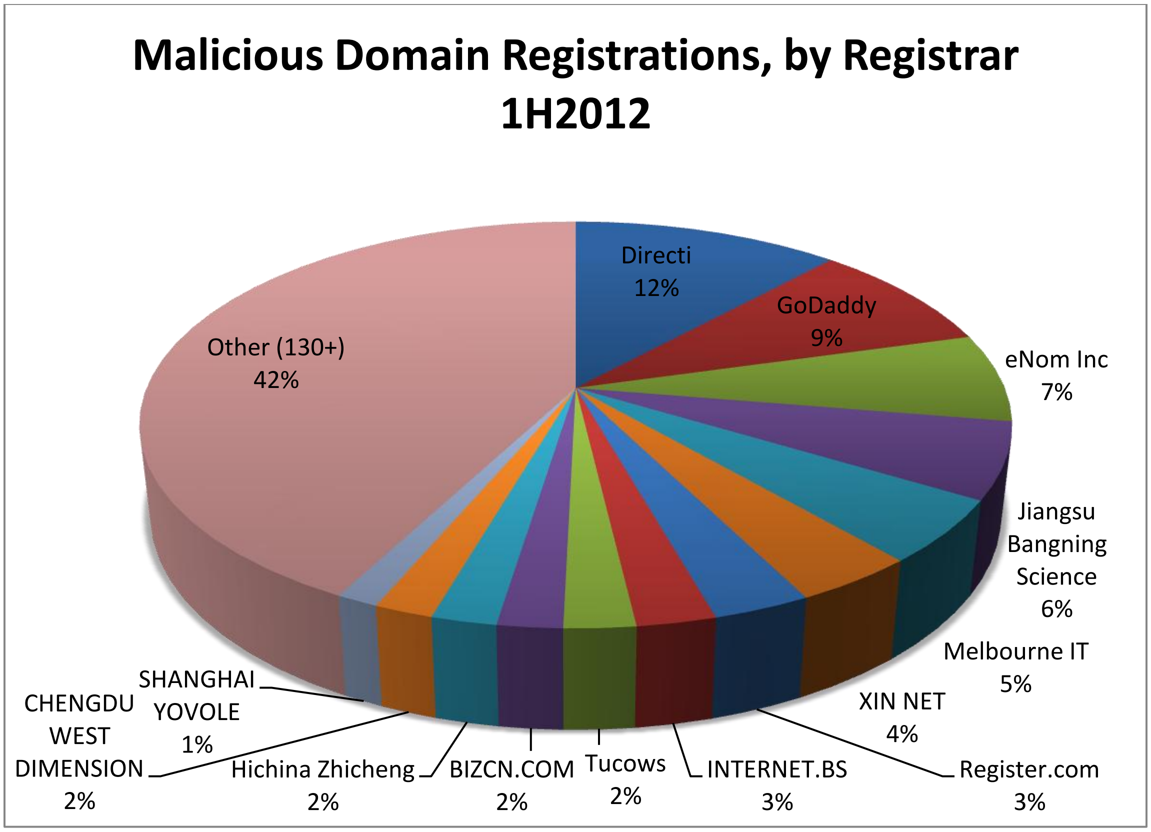
This report continues our analysis of registrars used by phishers to purchase domain names. This is made possible via WHOIS data captured by DomainTools.com, recorded shortly after each domain was created. We thank DomainTools; its data covered 7,354 of the 7,712 (95%) of the gTLD and ccTLD domains that were registered exclusively to support phishing. Phishers utilized a wide variety of registrars to obtain malicious domains in 1H2012, with at least 140 registrars involved.

Just over half of the world's malicious registrations were made in the .TK registry, and .TK is also the registrar of record for those domains, so we have omitted .TK domains from the remainder of our analysis, leaving a set of 3,773 domains to study.

The registrar marketplace is diverse. One major player, GoDaddy, holds roughly half of the gTLD market share. It is notable that phishers used GoDaddy far less often than would be expected given GoDaddy's market share. Then there are about twenty medium-to-large players, and then a long tail of smaller registrars.

As one may expect, some of the largest registrars – Directi, eNom, MelbourneIT, Register.com, and Tucows -- appeared on the chart of most-often-exploited registrars, in part due to their market shares. Some registrars also support reseller programs, through which some of these domains were sold, but we were not able to discern reseller identities. With better data available for this survey round, especially for ccTLD registrations, we were able to identify 140 registrars that had been used for at least one malicious registration.

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



To compare dissimilar registrars with each other, we used the same metric we use for comparing various TLDs – malicious domains per 10,000 domains under management. We use this metric to identify registrars that may be exploited out of proportion to their size. The top 21 registrars below accounted for 79% (2,991) of the domains registered maliciously.

Seven of the top eleven registrars are located in China. Chinese phishers tend to register domain names for their phishing, rather than compromising web servers. Phishers registered only 11 .CN domains for phishing, preferring to purchase inexpensive domains in .TK, .IN, .COM, and .INFO. Domains registered at the Chinese registrars were often used to phish Chinese targets such as Taobao.com, CCTV, and China Construction Bank, but were also used to phish outside targets such as Facebook and PayPal. Chinese phishers also registered at registrars outside the country, in order to attack targets within China. Like other kinds of online services, domain registration knows no national boundaries, and phishers register domains names where they find it convenient.

Top Phishing Registrars by Malicious Domain Score, 2H2011

All registrars with more than 25 malicious phishing registrations and 1,000 gTLD domain names under management

RANK	Registrar	Malicious Domain Names used for phishing 2H2011	gTLD domains at registrar, March 2012[8]	Score: Phish per 10,000 domains 2H2011
1	Shanghai Yovole	63	1,537	40.99
2	Chengdu West Dimension	88	3,177	27.70
3	Jiangsu Bangning Science	287	76,858	3.73
4	Internet.BS	118	89,402	1.32
5	Dynamic Network Services	28	58,555	0.48
6	EuroDNS	35	81,813	0.43
7	BIZCN.COM	97	278,109	0.35
8	Directi	558	1,724,071	0.32
9	XIN NET	184	980,268	0.19
10	Beijing Innovative	30	171,574	0.17
11	Hichina Zhicheng	97	751,285	0.13
12	Domainpeople	41	326,586	0.13
13	Register.com	146	1,911,337	0.08
14	Melbourne IT	237	3,128,559	0.08
15	Name.com	42	567,410	0.07
16	eNom Inc	333	7,830,968	0.04
17	Fastdomain	28	1,271,361	0.02
18	Tucows	106	6,447,422	0.02
19	GoDaddy	418	30,340,427	0.01
20	1 & 1 Internet	29	4,462,657	0.01
21	Network Solutions	26	5,542,203	0.00

Two registrars stood far apart from the rest: Shanghai Yovole Networks Inc. (http://www.yovole.com/) and Chengdu West Dimension Digital Technology (http://west263.com/), small Chinese registrars with very high scores. Chengdu West was by far the registrar with the worst score in our last report, indicating that the issues there haven't been solved. Other domains sponsored by Chengdu West including hundreds of cybersquatting domains containing the brand-names of clothing lines, apparently supporting the sale of counterfeit goods.

A good rule of thumb for identifying a registrar that has a higher level of fraudulent registrations than normal would be more than one per 10,000 domains under management. We made significant headway in obtaining registrar information between our last report and this one, and will continue to study this area and refine our methodologies as we gather more data for future reports.

[8] Source: Webhosting.info

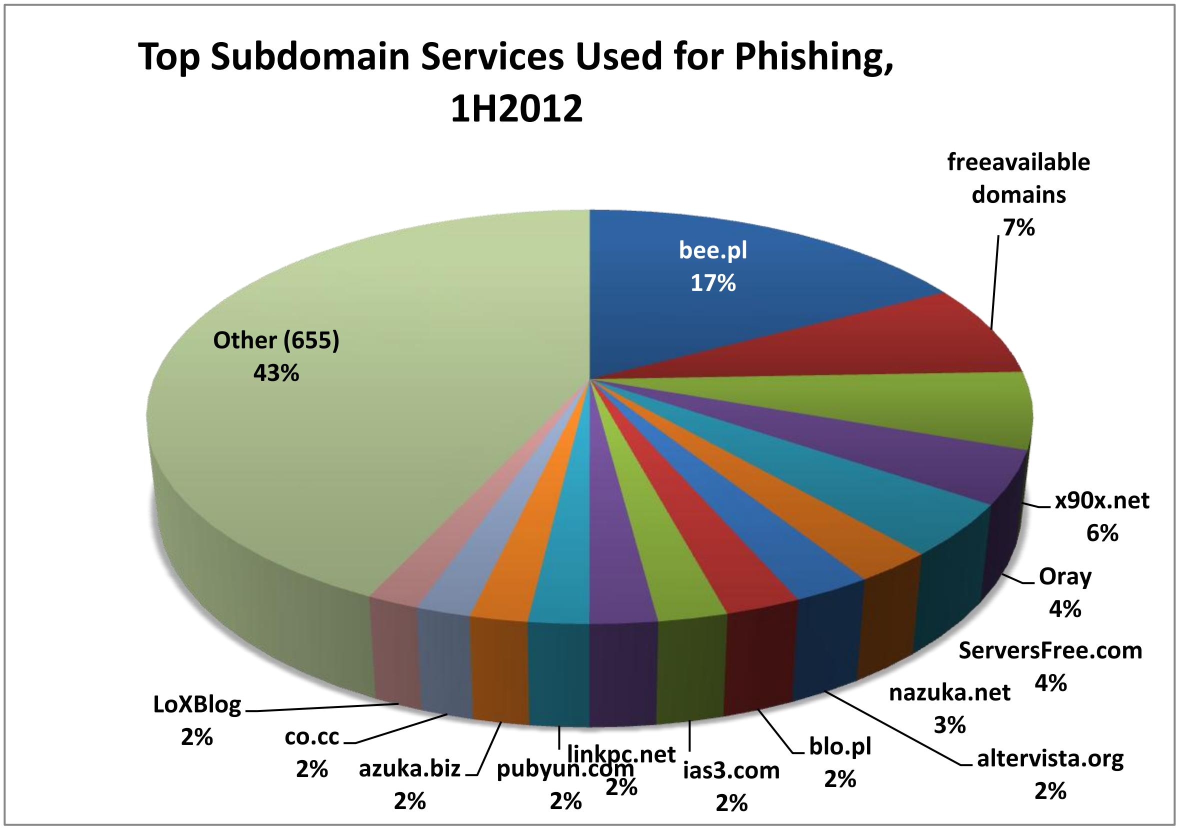
Use of Subdomain Services for Phishing

We continue to see very heavy abuse of subdomain services. **In a continuing trend, phishers registered far more subdomains than they registered "regular" domain names. However, the overall use of subdomain services for phishing fell from 21% to 14% of all attacks. We also see phishers seeking out new providers that they can exploit.**

There were 13,307 phishing attacks hosted on subdomain services in the first half of 2012, using 13,109 unique subdomains. Compare that to the 7,712 "regular" domain names registered by phishers in 1H2012. This was approximately a 20% decrease from the 17,390 attacks we recorded in 2H2011, but still represents 14% of all phishing attacks. This is a far lower rate than the 21% was saw in 2H2011, and could be a sign that at least some subdomain services are starting to prevent, detect, and respond to abuse of their services.

We define "subdomain registration services" as providers that give customers subdomain "hosting accounts" beneath a domain name that the provider owns. These services effectively offer users a "domain name" in their own DNS space for a variety of purposes, and often offer free DNS management. 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

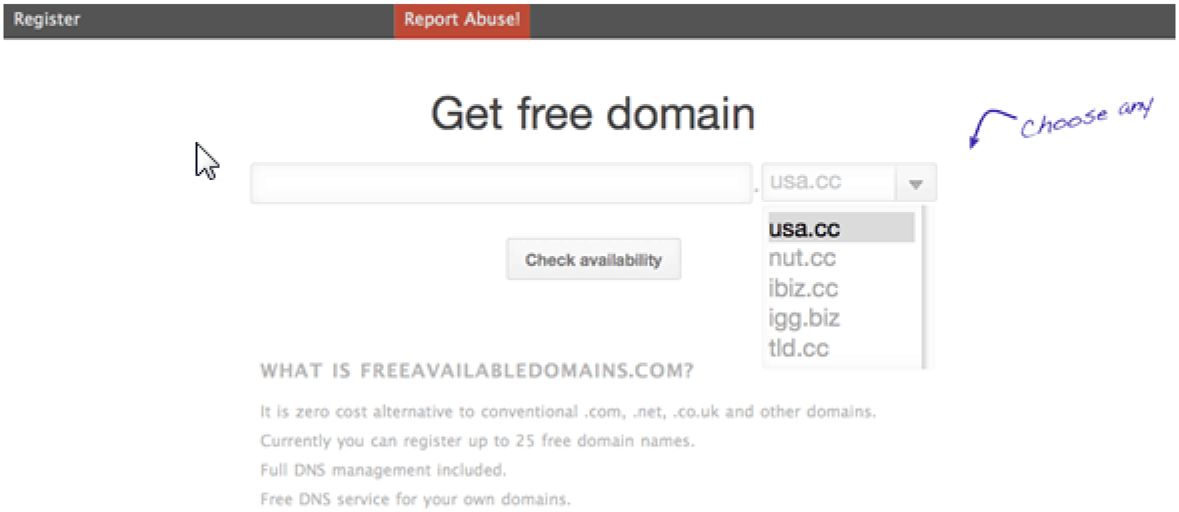


Use of subdomain services continues to be a challenge, because many of the services are free, offer anonymous registration, and only the subdomain providers themselves can effectively mitigate these phish.[9] While many of these services are responsive to complaints, very few take proactive measures to keep criminals from abusing their services in the first place.

The Poland-based bee.pl service (a.k.a. osa.pl) was far-and-away the most abused for phishing in the first half of 2012, just as it was 2H2011. **More than 17% of attacks using subdomain services occurred on subdomains provided by bee.pl**. The good news is that the absolute numbers of phishing sites found under the service fell from 4,500 in 2H2011 to less than 2,300 in 1H2012. We will continue to monitor this provider closely given its continuing issues.

We saw a large new number of subdomain services being abused by phishers. **More than 50 subdomain services were abused in 1H2012 that we had never seen in prior reports.** This clearly indicates that phishers are expanding their reach and constantly looking for new ways to set up their sites.

Second place went to such a provider, freeavailabledomains.com, where nearly 1,000 malicious subdomains were spotted. From the volume, it would appear that this site have some issues to fix. As can be seen in the following screen shot however, this service actually provides a "Report Abuse" option – a growing and welcome trend in the subdomain reseller space.



WHAT IS FREEAVAILABLEDOMAINS.COM?

It is zero cost alternative to conventional .com, .net, .co.uk and other domains.
Currently you can register up to 25 free domain names.
Full DNS management included.
Free DNS service for your own domains.

The home page of freeavailabledomains.com

[9] 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.

Many of the most abused subdomain providers saw huge increases in volume, or had never been abused for phishing before. Eight of the top ten subdomain resellers on our list had never cracked the top 15 before, and several of them were brand-new to our survey.

On the bright side, several services that been significantly abused in the past saw major decreases in phishing registrations. Services with perennial problems like co.cc and cx.cc saw massive decreases in phishing on their domains. Many of the subdomains services we looked at in the past six months are now offering WHOIS services and abuse reporting forms. Given the high levels of abuse they've been experiencing this isn't too surprising, but we certainly encourage other subdomain resellers to adopt similar tactics.

We have identified over 750 subdomain registration providers, which offer services on more than 3,500 domain names. This is a space that is even larger than the current top-level domain space, since each subdomain service is effectively its own "domain registry." The subdomain services have many business models, and are unregulated. It has not been surprising to see criminals move into this space as some TLD registries and registrars have implemented better anti-abuse policies and procedures. As some of the subdomain services that see heavy abuse add security measures of their own, there seems to be a ready supply of similar services cropping up that phishers can turn to.

Top 20 Subdomain Services Used for Phishing, 1H2012

Rank	Total Attacks	Provider
1	2,290	bee.pl (osa.pl)
2	958	freeavailabledomains.com
3	799	x90x.net
4	548	Oray
5	541	ServersFree.com
6	326	nazuka.net
7	324	altervista.org
8	310	blo.pl
9	284	ias3.com
10	275	linkpc.net
11	247	pubyun.com
12	236	azuka.biz
13	225	co.cc
14	214	LoXBlog
15	191	cu.cc
16	190	1FreeHosting
17	154	r.gd
18	154	tripod.com
19	149	3owl.com
20	147	ce.ms

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 in a meaningful fashion**.

IDNs are domain names that contain one or more non-ASCII characters. Such domain names can contain letters with diacritical marks such as ǎ and ü, or be composed of characters from non-Latin scripts such as Arabic, Chinese, Cyrillic, or Hindi. Over the past seven 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 38 approved IDN TLDs. While most IDN TLDs are not active, the .рф (.rf) TLD of the Russian Federation contains 830,000 domains, and the Korean TLD .한국 rapidly gained 220,000 registrations.

The IDN homographic 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 wholly) indistinguishable. Since January 2007, we have found only five homographic phishing attacks, and there were no homographic attacks evident in 1H2012. Fifty-eight regular, second-level IDNs were compromised by phishers in 1H2012.

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

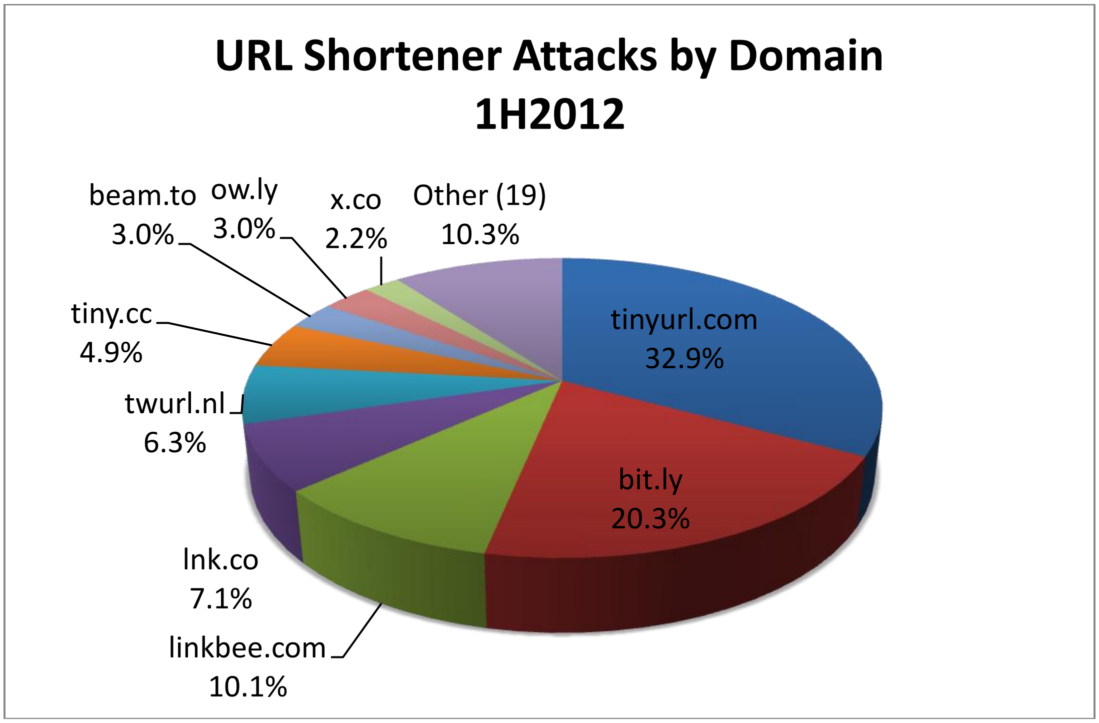
1. Phishers don't *need* to resort to such attacks. As noted elsewhere in this report, the domain name itself usually does not matter to a phisher.
2. By default, some browser manufacturers show the punycode version of the domain name (such as "xn--hotmal-t9a.net") in the address bar, instead of the 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 continue to use "URL shortening" services to obfuscate phishing URLs, but such use involved only 507 attacks in 1H2012, though up from 398 in 2H2011. 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.

Most of the major URL shortener providers have been aggressively screening for malicious forwarding destinations and imposing rules to make it much harder to abuse their systems. In an emerging best practice, many such services provide tools for investigators to quickly determine forwarding destinations for specific URLs, and automated abuse reporting functions. We encourage all URL shortener providers to implement similar tactics. SURBL (http://www.surbl.org) provides free information on abusive use of shortener services, and all subdomain resellers should consider signing up for this feed of malicious URLs in order to mitigate abuse on their services.



We have also seen criminals create their own fake URL shortener services. The domain's home page may look like any other URL shortener service, but the reality is that the criminals are using the domain strictly for their own purposes. We classify such sites used for phishing as malicious domains, and they are not counted under this category.

Conclusions

Phishers continue to shift toward the more economical options in their quest for profits. A wide variety of factors, from changes in top-level-domain registration and security policies to the availability of automated hacking tools, have tended to shift phishing toward compromised sites and vulnerable services. In the first half of 2012, we saw phishers continue to pursue these economically driven techniques, with more hacking of legitimate servers and especially shared web hosting environments.

We also saw phishers continue to concentrate on victims that can be monetized effectively and efficiently. Phishers in China are having some success victimizing Chinese citizens, particularly those who use Taobao.com. Attacks against web mail services rose, ostensibly due to increased demand for compromised account credentials to facilitate spamming. And in general, phishers concentrated on a smaller number of targets, perhaps because it was not economical to reach users of smaller institutions, or because user credentials at certain targets command a better price.

Appendix: Phishing Statistics and Uptimes by TLD

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
ac	Ascension Island	1	1	16,000	0.6	0.6	7:51:23	7:51:23	0	0.0
ad	Andorra	1	1	1,450	6.9	6.9	239:36:55	239:36:55	0	0.0
ae	United Arab Emirates	29	21	94,000	2.2	3.1	54:09:35	6:52:32	0	0.0
aero	sponsored TLD	3	3	7,980	3.8	3.8	23:16:24	12:08:09	0	0.0
af	Afghanistan	2	2				2:20:27	2:20:27	0	
ag	Antigua and Barbuda	2	2	19,524	1.0	1.0	7:48:58	7:48:59	0	0.0
ai	Anguilla	11	2	3,300	6.1	33.3	3:58:06	3:58:07	0	0.0
al	Albania	5	5	7,500	6.7	6.7	5:31:40	2:04:07	0	0.0
am	Armenia	21	8	19,900	4.0	10.6	15:43:52	2:12:25	0	0.0
an	Netherlands Antilles	0	0	900					0	
ao	Angola	0	0	250					0	
ar	Argentina	499	412	2,437,500	1.7	2.0	29:20:22	8:53:26	2	0.0
arpa	Advanced Research Project Agency	0	0						0	
as	American Samoa	4	4				8:26:20	8:23:46	0	
asia	sponsored TLD	18	14	197,864	0.7	0.9	24:01:18	5:19:42	0	0.0
at	Austria	94	67	1,133,707	0.6	0.8	49:50:36	18:37:30	0	0.0
au	Australia	1,383	1,101	1,731,128	6.4	8.0	24:58:02	5:03:41	2	0.0
aw	Aruba	0	0	600					0	
az	Azerbaijan	5	5	13,831	3.6	3.6	16:58:06	12:49:55	0	0.0
ba	Bosnia and Herzegovina	17	15	13,500	11.1	12.6	18:55:19	11:02:36	0	0.0
bd	Bangladesh	12	9	4,950	18.2	24.2	13:34:28	10:13:22	0	0.0
be	Belgium	536	479	1,292,600	3.7	4.1	13:11:39	1:32:22	12	0.1
bf	Burkina Faso	1	1				29:11:44	29:11:45	0	
bg	Bulgaria	19	13	24,400	5.3	7.8	22:05:54	5:43:00	0	0.0
bh	Bahrain	1	1				1:03:33	1:03:34	0	
biz	generic TLD	877	313	2,296,289	1.4	3.8	14:40:24	3:28:11	5	0.0
bm	Bermuda	3	2	7,900	2.5	3.8	5:29:11	7:43:09	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
bn	Brunei Darussalam	1	1	1,150	8.7	8.7	4:29:35	4:29:35	0	0.0
bo	Bolivia	22	18	8,200	22.0	26.8	10:40:43	6:13:23	0	0.0
br	Brazil	4,039	3,207	2,959,495	10.8	13.6	22:02:59	6:18:34	24	0.1
bs	Bahamas	0	0	2,300					0	
bt	Bhutan	6	6				22:32:13	3:08:00	0	
bw	Botswana	0	0						0	
by	Belarus	43	25				43:26:03	13:50:50	0	
bz	Belize	9	7	48,066	1.5	1.9	57:42:53	4:57:19	2	0.4
ca	Canada	632	521	1,926,000	2.7	3.3	28:42:33	5:32:05	5	0.0
cat	sponsored TLD	16	14	53,817	2.6	3.0	18:47:28	17:21:16	0	0.0
cc	Cocos (Keeling) Islands *(estimated)*	1,373	75	900,000	0.8	15.3	16:44:43	7:53:53	3	0.0
cd	Congo, Democratic Repub.	3	2	5,200	3.8	5.8	10:27:29	8:17:57	0	0.0
cg	Congo	1	1				18:49:05	18:49:06	0	
ch	Switzerland	348	308	1,700,985	1.8	2.0	18:44:25	2:03:46	0	0.0
ci	Côte d'Ivoire	3	2	2,100	9.5	14.3	361:45:33	314:40:56	0	0.0
cl	Chile	1,024	831	383,100	21.7	26.7	30:10:45	8:44:08	1	0.0
cm	Cameroon	20	11	12,000	9.2	16.7	25:29:19	16:51:22	0	0.0
cn	China	156	120	3,502,064	0.3	0.4	24:05:44	12:55:60	11	0.0
co	Colombia	354	269	1,250,856	2.2	2.8	15:50:11	8:11:03	11	0.1
com	generic TLD	41,265	31,228	105,601,144	3.0	3.9	23:04:36	5:25:59	2,588	0.2
coop	sponsored TLD	2	2	14,729	1.4	1.4	9:47:00	9:47:00	0	0.0
cr	Costa Rica	26	24	14,200	16.9	18.3	10:46:10	0:37:32	0	0.0
cu	Cuba	1	1	2,250	4.4	4.4	50:44:57	50:44:58	0	0.0
cx	Christmas Island	18	9	5,225	17.2	34.4	43:21:32	17:53:51	0	0.0
cy	Cyprus	6	6	9,950	6.0	6.0	23:31:58	8:50:04	0	0.0
cz	Czech Republic	170	107	948,871	1.1	1.8	39:41:14	13:54:32	0	0.0
de	Germany	849	573	15,069,393	0.4	0.6	32:35:26	12:36:49	6	0.0
dj	Djibouti	0	0						0	
dk	Denmark	263	209	1,185,409	1.8	2.2	31:40:57	11:29:15	0	0.0
dm	Dominica	1	1	14,500	0.7	0.7	0:30:18	0:30:18	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
do	Dominican Republic	13	12				21:06:58	4:05:23	0	
dz	Algeria	2	2	4,366	4.6	4.6	118:06:17	118:06:18	0	0.0
ec	Ecuador	36	31	30,001	10.3	12.0	24:26:59	8:42:35	0	0.0
edu	U.S. higher education	36	31	7,588	40.9	47.4	36:08:56	10:16:40	0	0.0
ee	Estonia	28	21	65,635	3.2	4.3	31:21:34	19:38:18	0	0.0
eg	Egypt	10	8	6,000	13.3	16.7	60:31:57	7:37:09	0	0.0
er	Eritrea	0	0						0	
es	Spain	381	288	1,548,844	1.9	2.5	29:40:55	12:10:00	2	0.0
et	Ethiopia	1	1	1,000	10.0	10.0	88:18:20	88:18:20	0	0.0
eu	European Union	347	276	3,592,000	0.8	1.0	20:22:28	7:30:20	7	0.0
fi	Finland	26	23	290,801	0.8	0.9	43:34:52	10:06:39	0	0.0
fj	Fiji	0	0	4,000					0	
fk	Falkland Islands	0	0	100					0	
fm	Micronesia, Fed. States	7	6				9:09:21	3:01:51	0	
fo	Faroe Islands	2	2				1:47:29	1:47:29	0	
fr	France	703	502	2,339,564	2.1	3.0	31:15:25	13:08:43	2	0.0
gd	Grenada	156	2	4,300	4.7	362.8	16:05:25	12:43:28	0	0.0
ge	Georgia	289	277	18,400	150.5	157.1	3:55:44	0:59:35	0	0.0
gg	Guernsey	45	5				35:25:41	33:05:06	0	
gh	Ghana	2	2				21:01:55	21:01:56	0	
gi	Gibraltar	0	0	1,896					0	
gl	Greenland	22	5	4,600	10.9	47.8	18:47:58	3:48:19	0	0.0
gov	U.S. government	3	3	5,000	6.0	6.0	23:44:24	4:53:26	0	0.0
gp	Guadeloupe	20	15	1,475	101.7	135.6	20:14:43	8:01:45	1	6.8
gr	Greece *(estimated)*	267	212	450,000	4.7	5.9	23:16:18	7:58:39	0	0.0
gs	South Georgia & Sandwich Is.	2	2	8,160	2.5	2.5	0:10:00	0:10:00	1	1.2
gt	Guatemala	12	9	10,820	8.3	11.1	17:21:35	4:55:05	0	0.0
gy	Guyana	2	2	2,050	9.8	9.8	38:58:14	38:58:15	0	0.0
hk	Hong Kong	31	23	233,562	1.0	1.3	23:51:38	10:14:51	0	0.0
hm	Heard and McDonald Is.	3	1				19:44:16	19:44:16	0	
hn	Honduras	6	6	6,256	9.6	9.6	10:40:44	6:11:28	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
hr	Croatia	40	35	79,224	4.4	5.0	20:04:22	11:20:28	0	0.0
ht	Haiti	4	3				26:24:15	25:55:04	0	
hu	Hungary	176	126	620,111	2.0	2.8	63:27:19	18:35:39	0	0.0
id	Indonesia	113	95	78,000	12.2	14.5	20:32:33	6:45:08	0	0.0
ie	Ireland	77	55	179,731	3.1	4.3	30:11:30	12:35:53	0	0.0
il	Israel	89	65	230,100	2.8	3.9	48:37:04	14:32:19	1	0.0
im	Isle of Man	19	8				18:57:46	8:41:03	2	
in	India	1,690	1,351	1,674,552	8.1	10.1	23:27:07	7:57:25	474	2.8
info	generic TLD	1,764	1,514	8,153,167	1.9	2.2	12:32:24	4:01:44	231	0.3
int	sponsored TLD	2	1						0	
io	British Indian Ocean Terr.	0	0						0	
IP address	(no domain name used)	2,410							0	
iq	Iraq	0	0						0	
ir	Iran	276	138	267,226	5.2	10.3	15:59:50	3:46:09	0	0.0
is	Iceland	20	17	38,900	4.4	5.1	189:38:15	75:28:39	1	0.3
it	Italy	454	339	2,403,000	1.4	1.9	47:52:27	15:26:47	1	0.0
je	Jersey	11	5				16:39:44	8:59:43	0	
jm	Jamaica	1	1	6,400	1.6	1.6	156:53:45	156:53:46	0	0.0
jo	Jordan	2	1	4,200	2.4	4.8	8:32:48	8:32:49	0	0.0
jobs	sponsored TLD	0	0	41,700					0	
jp	Japan	183	110	1,291,433	0.9	1.4	58:29:11	27:14:11	1	0.0
ke	Kenya	16	15	22,000	6.8	7.3	29:28:49	17:26:20	0	0.0
kg	Kyrgyzstan	62	4	5,300	7.5	117.0	4:07:23	0:21:15	0	0.0
kh	Cambodia	4	2	1,550	12.9	25.8	3:30:13	3:28:15	0	0.0
ki	Kiribati	0	0						0	
kr	Korea	550	357	1,095,127	3.3	5.0	25:00:27	11:20:10	1	0.0
kw	Kuwait	3	3	3,181	9.4	9.4	0:10:00	0:10:00	0	0.0
ky	Cayman Islands	1	1				1:03:39	1:03:40	0	
kz	Kazakhstan	57	44	73,050	6.0	7.8	47:41:20	21:56:30	1	0.1
la	Lao People's Demo. Rep. *(domains estimated)*	45	10	9,500	10.5	47.4	27:02:04	9:37:09	1	1.1

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
lb	Lebanon	2	2	3,500	5.7	5.7	0:28:59	0:28:59	0	0.0
lc	St. Lucia	31	23	3,115	73.8	99.5	8:06:24	3:31:07	0	0.0
li	Liechtenstein	10	8	68,500	1.2	1.5	20:11:52	6:14:52	0	0.0
lk	Sri Lanka	11	8	8,490	9.4	13.0	14:49:00	6:54:11	0	0.0
ls	Lesotho	0	0						0	
lt	Lithuania	44	35	145,550	2.4	3.0	32:43:32	14:34:48	0	0.0
lu	Luxembourg	6	5	68,549	0.7	0.9	10:49:33	3:33:21	0	0.0
lv	Latvia	35	28	100,060	2.8	3.5	57:46:36	25:47:17	0	0.0
ly	Libya	133	10	12,400	8.1	107.3	24:09:25	9:24:32	0	0.0
ma	Morocco	22	17	42,354	4.0	5.2	21:32:01	10:39:05	0	0.0
mc	Monaco	1	1				0:27:16	0:27:17	0	
md	Moldova	12	9	20,697	4.3	5.8	18:46:03	16:24:53	0	0.0
me	Montenegro	168	117	637,940	1.8	2.6	27:30:46	4:39:13	4	0.1
mg	Madagascar	2	2				19:11:20	19:11:21	0	
mk	Macedonia	15	10				47:27:52	14:28:35	0	
ml	Mali	0	0						0	
mn	Mongolia	214	197	12,967	151.9	165.0	6:08:53	0:15:05	0	0.0
mo	Macao	0	0	300					0	
mobi	sponsored TLD	25	23	1,047,487	0.2	0.2	14:50:31	6:40:15	1	0.0
mp	Northern Mariana Islands	5	4				11:10:55	15:35:37	0	
mr	Mauritania	0	0						0	
ms	Montserrat	271	13	9,800	13.3	276.5	33:15:37	14:36:20	5	5.1
mt	Malta	2	2	6,200	3.2	3.2	1:23:04	1:23:04	0	0.0
mu	Mauritius	12	8	7,500	10.7	16.0	20:38:27	9:48:49	0	0.0
museum	sponsored TLD	0	0	440					0	
mv	Maldives	1	1						0	
mw	Malawi	1	1						0	
mx	Mexico	328	248	568,577	4.4	5.8	31:28:35	11:35:45	1	0.0
my	Malaysia	155	121	194,365	6.2	8.0	27:25:57	12:02:27	0	0.0
mz	Mozambique	0	0	1,885					0	
na	Namibia	1	1	220	45.5	45.5	126:37:37	126:37:38	0	0.0
name	generic TLD	19	18	230,572	0.8	0.8	8:13:40	3:00:13	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
nc	New Caledonia	0	0						0	
ne	Niger	0	0	140					0	
net	generic TLD	6,518	3,515	15,097,524	2.3	4.3	22:26:22	5:19:49	208	0.1
nf	Norfolk Island	3	2	1,600	12.5	18.8	48:58:58	54:17:14	0	0.0
ng	Nigeria	26	22	35,000	6.3	7.4	19:19:05	4:09:45	0	0.0
ni	Nicaragua	10	7	6,400	10.9	15.6	10:07:54	3:59:02	0	0.0
nl	Netherlands	936	776	4,956,736	1.6	1.9	21:09:11	6:02:27	1	0.0
no	Norway	89	67	558,004	1.2	1.6	47:35:42	18:28:04	0	0.0
np	Nepal	67	55	29,280	18.8	22.9	33:47:18	11:24:17	0	0.0
nr	Nauru	1	1				0:40:41	0:40:42	0	
nu	Niue *(domains estimated)*	136	39	100,000	3.9	13.6	26:44:36	9:22:42	1	0.1
nz	New Zealand	110	93	485,358	1.9	2.3	34:03:28	11:01:09	1	0.0
om	Oman	0	0						0	
org	generic TLD	4,147	2,870	9,957,774	2.9	4.2	18:17:27	5:58:01	78	0.1
pa	Panama	3	3	7,112	4.2	4.2	16:07:12	14:33:48	0	0.0
pe	Peru	126	115	61,530	18.7	20.5	16:24:47	3:15:38	0	0.0
pf	French Polynesia	0	0						0	
pg	Papua New Guinea	1	1						0	
ph	Philippines *(domains estimated)*	46	35				23:34:05	4:35:12	1	
pk	Pakistan (domains estimated)	58	51	18,000	28.3	32.2	17:05:05	4:16:48	1	0.6
pl	Poland	3,453	565	2,311,649	2.4	14.9	24:21:38	11:53:54	2	0.0
pn	Pitcairn	4	3				29:39:08	36:20:56	0	
post	sponsored TLD	0	0	0					0	
pro	sponsored TLD	13	12	154,664	0.8	0.8	23:18:41	16:14:02	0	0.0
ps	Palestinian Territory	12	9	7,660	11.7	15.7	47:02:52	8:04:40	0	0.0
pt	Portugal	74	57	235,091	2.4	3.1	35:52:02	8:08:15	0	0.0
py	Paraguay	41	39	14,500	26.9	28.3	2:38:26	1:06:30	0	0.0
qa	Qatar	2	2	13,866	1.4	1.4	7:57:11	7:57:11	1	0.7
re	Réunion	7	6	16,510	3.6	4.2	24:17:10	8:32:16	0	0.0
ro	Romania	967	533	576,323	9.2	16.8	21:59:25	5:31:48	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
rs	Serbia	89	54	74,000	7.3	12.0	64:41:43	18:56:25	0	0.0
ru	Russian Fed.	1,304	829	3,860,995	2.1	3.4	39:31:53	13:02:11	8	0.0
rw	Rwanda	2	2				1:44:02	1:44:03	0	
sa	Saudi Arabia	11	9	28,458	3.2	3.9	13:33:24	12:10:46	0	0.0
sc	Seychelles	2	2	4,778	4.2	4.2	6:58:45	6:58:45	0	0.0
sd	Sudan	6	6				0:49:23	0:45:05	0	
se	Sweden	216	156	1,210,031	1.3	1.8	42:11:58	18:53:13	0	0.0
sg	Singapore	89	66	140,107	4.7	6.4	55:29:05	17:18:39	0	0.0
sh	Saint Helena	1	1	2,999	3.3	3.3	14:10:36	14:10:37	0	0.0
si	Slovenia	61	55	103,202	5.3	5.9	49:52:26	15:08:51	0	0.0
sk	Slovakia	66	34	274,360	1.2	2.4	17:47:19	9:42:18	0	0.0
sl	Sierra Leone	0	0						0	
sm	San Marino	0	0	1,900					0	
sn	Senegal	1	1	3,500	2.9	2.9	66:42:35	66:42:36	0	0.0
so	Somalia	24	4						1	
st	Sao Tome and Principe	6	4				6:11:54	5:03:01	0	
su	Soviet Union	37	24	104,544	2.3	3.5	32:42:01	11:44:31	0	0.0
sv	El Salvador	9	5	5,400	9.3	16.7	18:44:26	14:24:46	0	0.0
sy	Syria	2	2				18:47:45	18:47:45	0	
sz	Swaziland	0	0						0	
tc	Turks and Caicos	39	13				10:52:51	7:46:43	0	
tel	generic TLD	0	0	264,241					0	
tf	French Southern Territories	62	7	1,550	45.2	400.0	12:39:35	8:06:47	0	0.0
tg	Togo	2	2				24:22:37	24:22:38	0	
th	Thailand	122	77	69,490	11.1	17.6	29:16:33	13:18:19	0	0.0
tj	Tajikistan	1	1	18,800	0.5	0.5	0:23:14	0:23:15	0	0.0
tk	Tokelau	4,197	3,939	8,994,000	4.4	4.7	19:20:38	10:49:40	3,939	4.4
tl	Timor-Leste	11	7				12:44:02	10:15:51	0	
tm	Turkmenistan	3	1	3,775	2.6	7.9	11:22:39	6:15:07	0	0.0
tn	Tunisia	6	6	14,860	4.0	4.0	6:16:17	0:26:53	0	0.0
to	Tonga	71	16	15,000	10.7	47.3	17:38:53	8:03:27	1	0.7

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
tp	Portuguese Timor	0	0						0	
tr	Turkey	170	138	302,008	4.6	5.6	30:33:06	10:58:56	2	0.1
travel	sponsored TLD	4	4	24,120	1.7	1.7	39:52:25	11:43:25	0	0.0
tt	Trinidad and Tobago	2	1	2,500	4.0	8.0	17:03:07	17:03:07	0	0.0
tv	Tuvalu (*domains estimated)*	133	106	200,000	5.3	6.7	28:19:07	10:30:25	4	0.2
tw	Taiwan	176	123	508,089	2.4	3.5	26:42:05	9:38:24	4	0.1
tz	Tanzania	5	4	5,200	7.7	9.6	53:47:35	29:23:53	0	0.0
ua	Ukraine	253	185	619,517	3.0	4.1	28:54:29	14:48:42	2	0.0
ug	Uganda	5	3	3,200	9.4	15.6	32:58:35	27:18:32	0	0.0
uk	United Kingdom	1,433	1,190	10,131,000	1.2	1.4	33:54:15	10:42:50	28	0.0
us	United States	626	303	1,784,000	1.7	3.5	15:14:37	2:54:22	20	0.1
uy	Uruguay	35	29	36,908	7.9	9.5	53:12:33	6:18:15	0	0.0
uz	Uzbekistan	10	7	14,703	4.8	6.8	25:48:26	10:22:36	0	0.0
vc	St. Vincent and Grenadines	4	4	8,196	4.9	4.9	8:10:17	8:10:18	0	0.0
ve	Venezuela	61	44	213,000	2.1	2.9	38:51:03	15:35:49	0	0.0
vg	British Virgin Islands	1	1	8,300	1.2	1.2	0:36:19	0:36:19	0	0.0
vi	Virgin Islands	0	0	17,000					0	
vn	Vietnam	136	105	300,343	3.5	4.5	44:14:26	15:22:23	1	0.0
vu	Vanuatu	16	5				23:33:33	7:46:20	0	
ws	Samoa	69	44	543,500	0.8	1.3	16:34:01	5:23:45	3	0.1
xn--3e0b707	.한국 (KR IDN)	0	0	220,250					0	
xn--90a3ac	.СРБ (Serbia IDN)	0	0	3,600					0	
xn--fzc2c9e2c	.ලංකා ලංකා (Sri Lanka IDN)	0	0	150					0	
xn--mgberp4a5d4a	.السعودية (Saudi Arabia IDN)	0	0	1,800					0	

TLD	TLD Location	# Unique Phishing attacks 1H2012	Unique Domain Names used for phishing 1H2012	Domains in registry, May 2012	Score: Phishing domains per 10,000 domains 1H2012	Score: Attacks per 10,000 domains 1H2012	Average Uptime 1H2012 hh:mm:ss	Median Uptime 1H2012 hh:mm:ss	# Malicious Domains Registered 1H2012	Malicious registrations score/10,000 domains in registry
xn--o3cw4h	.ไทย (.TH IDN)	0	0	1,000					0	
xn--p1ai	.рф (Russian Federation IDN)	1	1	830,689	0.0	0.0			0	0.0
xn--xkc2al3hye2a	.இலங்கை (Sri Lanka IDN)	0	0	80					0	
xxx	sponsored TLD	0	0	136,632					0	
ye	Yemen	0	0	800					0	
yu	Yugoslavia *(TLD deprecated March 2010)*	0	0	0					0	
za	South Africa	763	644	779,500	8.3	9.8	21:57:53	5:08:33	2	0.0
zm	Zambia	3	3				24:13:19	25:57:05	0	
zw	Zimbabwe	24	21				4:19:08	4:05:16	0	
	TOTALS	**93,462**	**64,204**	**240,418,900**					**7,719**	

About the Authors & Acknowledgments

The authors wish to thank the following for their support: Peter Cassidy and Foy Shiver of the APWG; Aaron Routt of Internet Identity; and Ashish Luthra 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 thank DomainTools for their contribution of WHOIS data to help identify trends in malicious registrations. 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 President of Illumintel Inc., which provides advising and security services to top-level domain registry operators and other Internet companies. 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. He is a member of ICANN's Security and Stability Advisory Committee (SSAC), and was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG). Greg also serves a Co-Chair of the Anti-Phishing Working Group's Internet Policy Committee. He was previously the Director of Key Account Management and Domain Security at Afilias (www.afilias.info), and Greg continues to contribute to Afilias' security programs, including anti-abuse services for the .ORG registry. In 2010, Greg accepted an OTA Excellence in Online Trust Award for Afilias' anti-abuse programs. 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 criminals. Rasmussen is co-chair of the Anti-Phishing Working Group's (APWG) Internet Policy Committee and serves as the APWG's Industry Liaison, representing and speaking on behalf of the organization at events around the world. In this role, he works closely with ICANN, the international oversight body for domain names, and is a member of ICANN's Security and Stability Advisory Committee (SSAC). Rasmussen is a member of the Online Trust Alliance's (OTA) Steering Committee and was recently appointed to the FCC's Communications Security, Reliability and Interoperability Council (FCC CSRIC). He is also an active member of the Digital PhishNet, a collaboration between industry and law enforcement, and is an active participant in the Messaging Anti-Abuse Working Group (MAAWG), and is IID's FIRST representative (Forum of Incident Response and Security Teams). He also is a regular participant in DNS-OARC meetings, the worldwide organization for major DNS operators, registries and interested parties, and in ICANN's series of DNS Security, Stability, and Resiliency Symposiums. Rasmussen earned an MBA from the Haas School of Business at UC-Berkeley and holds two bachelor's degrees, in Economics and Computer Science, from the University of Rochester.

#