Global Phishing Survey: Trends and Domain Name Use in 2H2012

July-December 2012

Unifying the
Global Response
To Cybercrime

An
APWG
Industry
Advisory

Published April 2013

Published 25 April 2013

Authors:

Greg Aaron, Illumintel Inc.
<greg at illumintel.com>
and
Rod Rasmussen, Internet Identity
<rod.rasmussen at internetidentity.com>
with
Research, Analysis Support, and Graphics by
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

Driven by a profit motive, phishers are a creative and efficient lot. By analyzing the phishing that took place in the second half of 2012, we have learned how the phishers perpetrated their attacks, and what defensive measures are and are not working. Some phishers have been breaking into Web hosting providers to great effect, a trend we see in the wider world of cyber-crime.

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 second half of 2012 ("2H2012", 1 July 2012 through 31 December 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. We are grateful to CNNIC and the Anti-phishing Alliance of China (APAC) for sharing their data with us.

Our major findings in this report include:

1. **Phishers are breaking into hosting providers with unprecedented success, using these facilities to launch mass phishing attacks. The number of phishing attacks rose due to this technique, and attacks leveraging these resources represented 47% of all phishing attacks recorded worldwide in the second half of 2012.** *(See pages 5-6.)*
2. **The average and median uptimes of phishing attacks remained lower than the historical average.** *(Pages 7-8)*
3. **Phishers registered more subdomains than regular domain names** *(pages 16-17),* **while the number of domain names registered by phishers has dropped significantly since early 2011** *(pages 11-12).*

Basic Statistics

Millions of phishing URLs were reported in 2H2012, but the number of unique phishing attacks and domain names used to host them was much smaller.[1] The 2H2012 data set yielded the following statistics:

- **There were at least 123,486 unique phishing attacks worldwide.** This is more than the 93,462 attacks we observed in the first half of 2012. The increase is due to an increase in phishing attacks that leveraged shared virtual servers to compromise multiple

[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.

domains at once. (See the section "Shared Virtual Server Hacking" on page 5 for more.) An *attack* is defined as a phishing site that targets a specific brand or entity. A single domain name can host several discrete phishing attacks against different banks, for example.

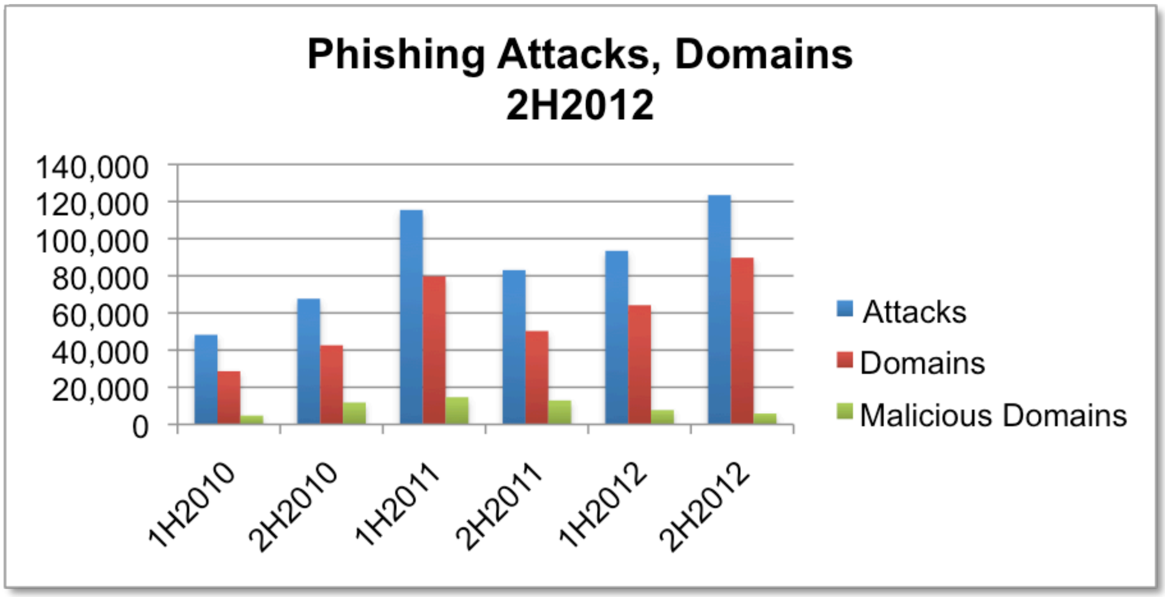
- **The attacks used 89,748 unique domain names.**[2] Again, this is up from the 64,204 domains used in 1H2012, due to shared virtual server hacking. The number of domain names in the world grew from 240 million in May 2012 to 258 million in November 2012.[3]
- In addition**, 2,489 attacks were detected on 1,841 unique IP addresses, rather than on domain names.** (For example: http://79.173.233.18/paypal/.) The number of attacks using IPs has remained steady for three years. None of these phish were reported on IPv6 addresses.
- Of the 89,748 phishing domains, **we identified 5,835 domain names that we believe were registered maliciously, by phishers.** The number of maliciously-registered phishing domains has been in steady decline -- down significantly from 7,712 in 1H2012, 12,895 in 2H2011, and 14,650 in 1H2011. Of those 5,835 domain names, 2,791 (48%) were registered to phish Chinese targets, down from 5,117 in 1H2012 and 7,991 in 2H2011. The other 83,913 domains were almost all hacked or compromised on vulnerable Web hosting.
- **The average uptimes of phishing attacks remained lower than usual. The average uptime in 2H2012 was 26 hours and 13 minutes, compared to the all-time low of 23 hours and 10 minutes recorded in 1H2012.** The median uptime in1H2012 was 10 hours and 19 minutes – almost twice the historically low median of 5 hours and 45 minutes achieved in 1H2012.
- **Phishing occurred in 207 top-level domains (TLDs), but 82% of the malicious domain registrations were in just three TLDs**: .COM, .TK, and .INFO.
- **We counted 611 target institutions, up from 486 in the first half of 2012**. Targets include the users of banks, e-commerce sites, social networking services, ISPs, government tax bureaus, online gaming sites, postal services, and securities companies. PayPal was the most-targeted institution.
- **Only about 1.4% of all domain names that were used for phishing contained a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations.")
- One hundred forty-seven of the 89,748 domain names were internationalized domain names (IDNs), and only two 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

	2H2012	1H2012	2H2011	1H2011	2H2010	1H2010
Phishing domain names	89,748	64,204	50,298	79,753	42,624	28,646
Attacks	123,486	93,462	83,083	115,472	67,677	48,244
TLDs used	207	202	200	200	183	177
IP-based phish (unique IPs)	1,841	1,864	1,681	2,385	2,318	2,018
Maliciously registered domains	5,835	7,712	12,895	14,650	11,769	4,755
IDN domains	147	58	36	33	10	10
Number of targets	611	486	487	520	587	568

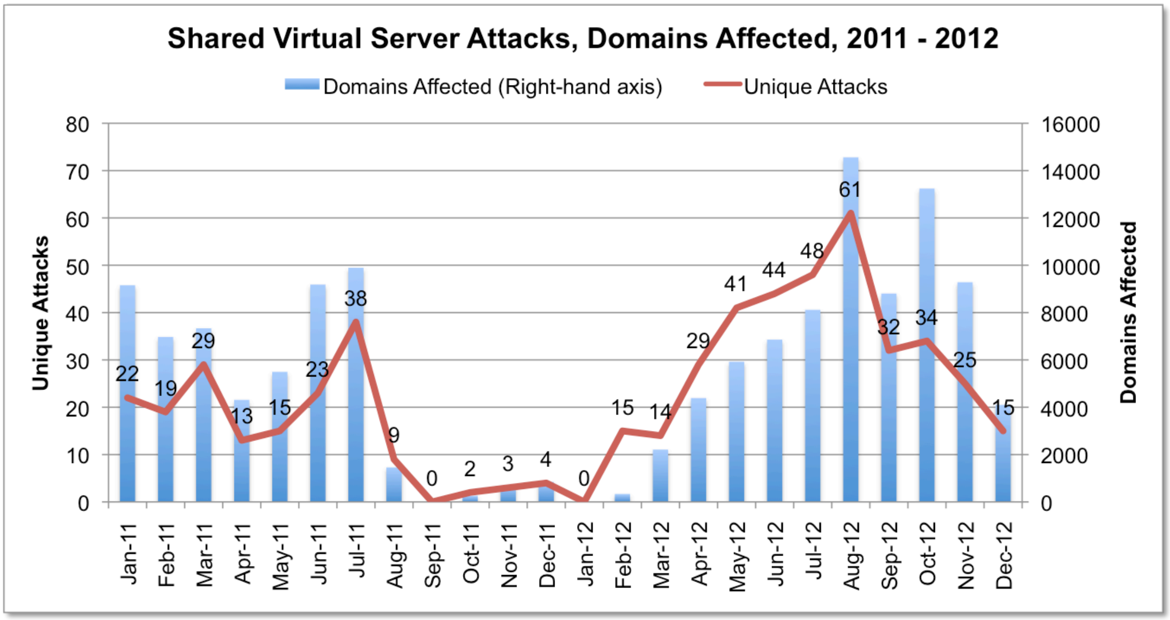


Phishing against targets in China dropped notably. Phishers continued to target PayPal most of all brands, with 39% of all phishing attacks aimed at PayPal users.

Shared Virtual Server Hacking

In a trend we first described in1H2011, a tactic used by phishers drastically affected our statistics in 2H2012. In this attack, a phisher breaks into a web server that hosts a large number of domains – a "shared virtual server" in industry parlance. Once the phisher breaks into such a server, he first uploads one 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 display 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 2H2011, we identified 58,100 phishing attacks that used this mass break-in technique, representing 47% of all phishing attacks recorded worldwide.** We started 2012 with no attacks of this nature, but beginning in February, these attacks started reappearing, peaking in August 2012 with over 14,000 such phishing attacks sitting on 61 different servers. Levels did decline in late 2012, but still remained troublingly high. We identified sets of attacks by analyzing the IP addresses of the machines used, the timing of the attacks, and by the telltale URL paths that the phish shared.


Shared Virtual Server Attacks, Domains Affected, 2011 - 2012

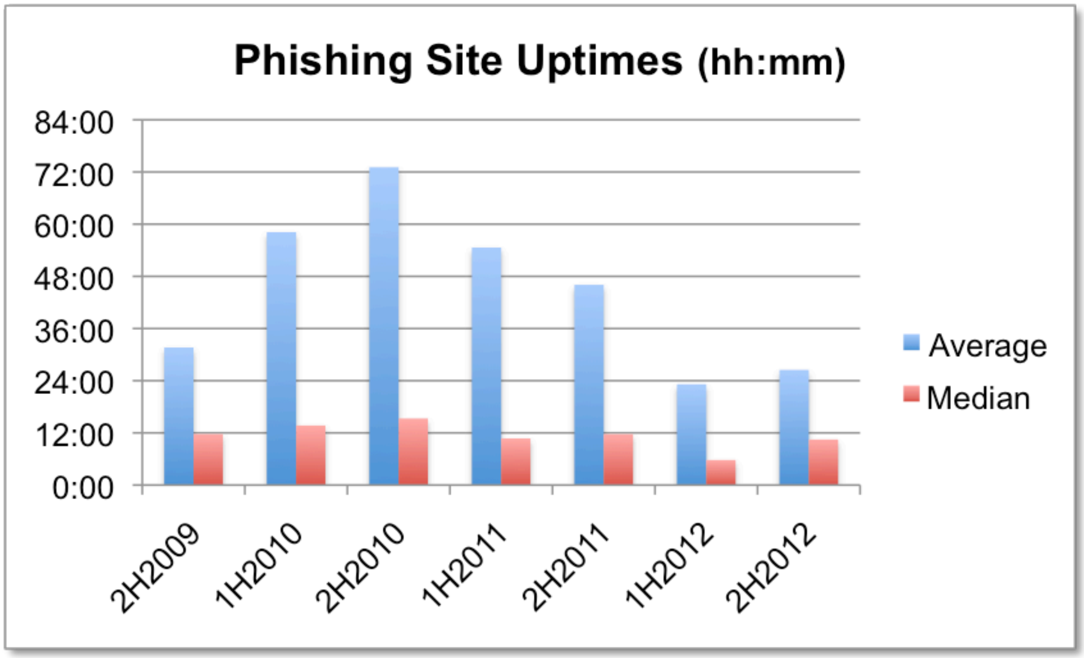
Breaking into such hosting is a high-yield activity, and fits into a larger trend where criminals turn compromised servers at hosting facilities into weapons. Hosting facilities contain large numbers of often powerful servers, and have large "pipes" through which large amounts of traffic can be sent. These setups offer significantly more computing power and bandwidth than scattered home PCs.

In late 2012 into 2013, we have seen increasing use of tools targeting shared hosting environments, and particularly WordPress, cPanel, and Joomla installations. For example, beginning in late 2012 criminals hacked into server farms to perpetrate extended DDoS attacks against American banks. And in April 2013, a perpetrator launched wide-scale brute force attacks against Wordpress installations at hosting providers in order to build a large botnet. Tens of thousands to hundreds of thousands of these shared servers have been cracked by such techniques. Access and use of these boxes is then metered out in the criminal underground for all sorts of activities, including DDoS, malware distribution, and of course, phishing. These attacks highlight the vulnerability of hosting providers and software, exploit weak password management, and provide plenty of reason to worry.

Phishing by Uptime

The average uptimes of phishing attacks remained lower than usual. The average uptime in 2H2012 was 26 hours and 13 minutes, compared to the all-time low of 23 hours and 10 minutes recorded in 1H2012. But the median uptime in1H2012 was 10 hours and 19 minutes – almost twice the historically low median of 5 hours and 45 minutes achieved in 1H2012.

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.

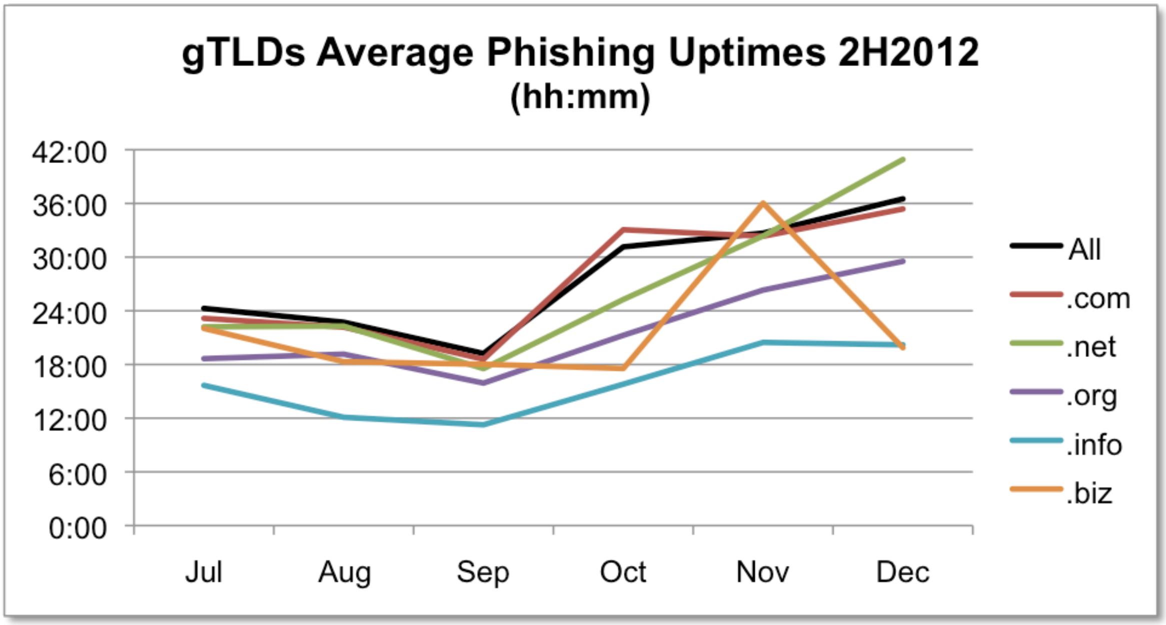


The first day of a phishing attack is the most lucrative for the phisher, so quick takedowns are essential. Long-lived phish can skew the averages since some phishing sites last weeks or even months, so medians are also a useful barometer of overall mitigation efforts. CNNIC did not record the uptimes of the phish it documented, so those phish were not part of our uptime calculations.

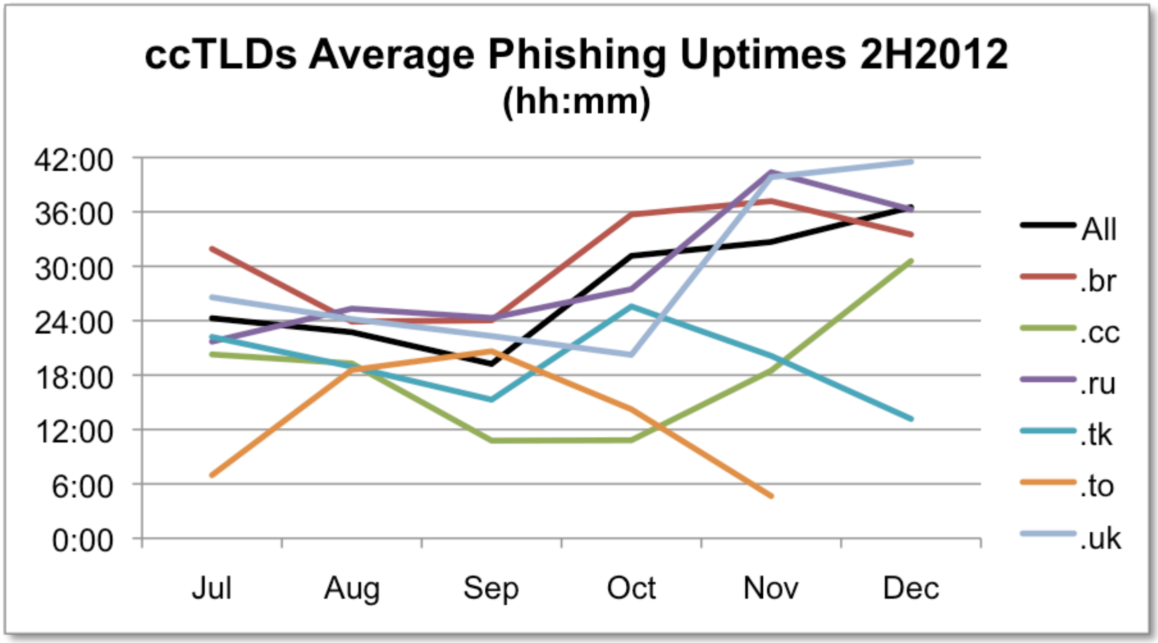
In the large generic top-level domains (gTLDs), phishing times increased over the months as virtual server hacking decreased through December. The virtual server attacks tended to

[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.

be mitigated more efficiently – they prompt many complaints to the hosting providers that are affected, and each mitigation effort took down multiple phishing attacks at once. .INFO, .BIZ, and .ORG had the lowest uptimes, due to notification and takedown programs at those registry operators:



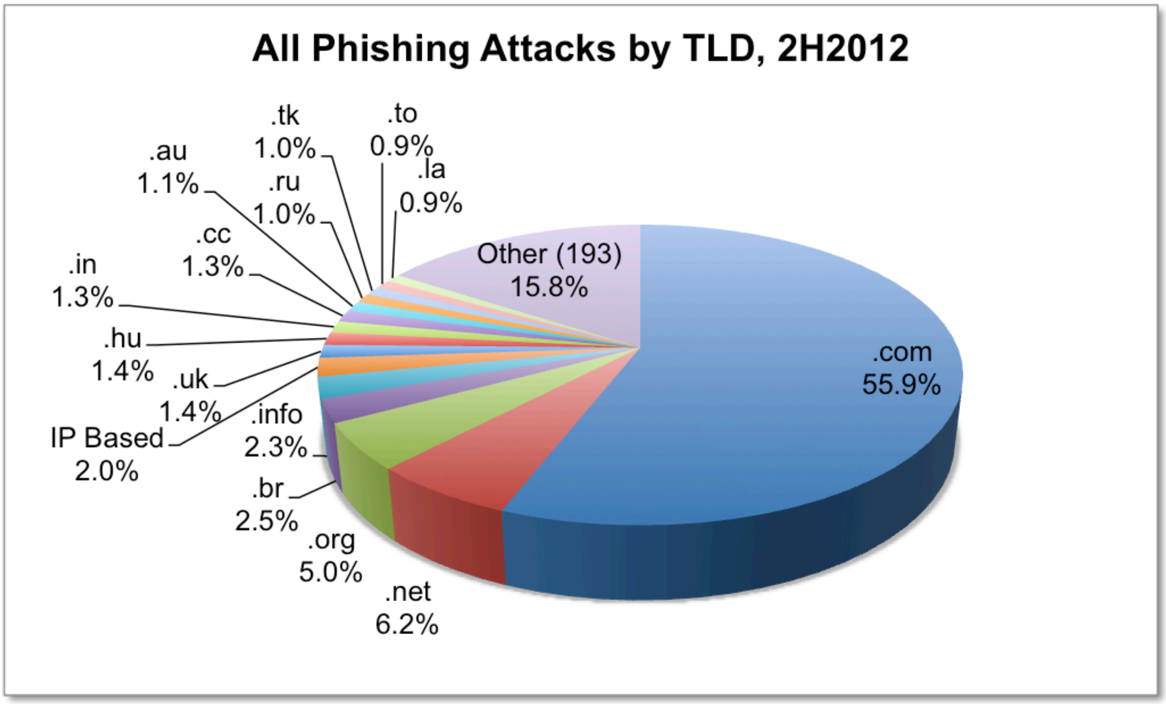
The uptimes at large country-code TLDs (ccTLDs) varied:



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

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. Most phishing takes place on compromised domain names, and so the distribution by TLD roughly parallels TLD market share.



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 domain and attack scores for each TLD.

- **The median domains-per-10,000 score was 4.7**.
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 4.9.** .COM contained 48% of the phishing domains in our data set, and 42% of the domains in the world.

We therefore suggest that domains-per-10,000 scores between 4.7 and 4.9 occupy the

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

middle ground, with scores above 5.0 indicating TLDs with increasingly prevalent phishing.[6] The top TLDs by score are:

Top 10 Phishing TLDs by Domain Score, 2H2012

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

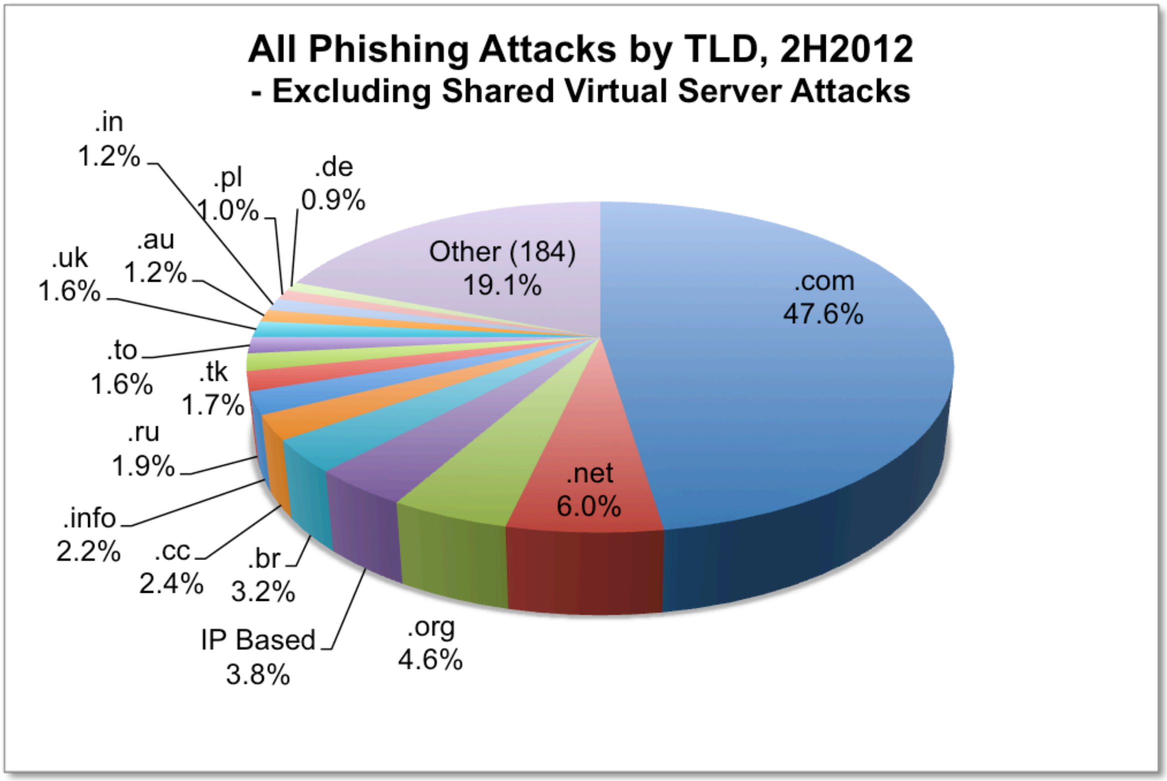
	TLD	TLD Location	# Unique Phishing attacks 2H2012	Unique Domain Names used for phishing 2H2012	Domains in registry, November 2012	Score: Phishing domains per 10,000 domains 2H2012
1	th	Thailand	210	136	63,400	21.5
2	hu	Hungary	1,701	1,192	625,701	19.1
3	cl	Chile	902	731	399,073	18.3
4	pe	Peru	130	93	64,100	14.5
5	ec	Ecuador	41	38	30,500	12.5
6	np	Nepal	42	32	31,710	10.1
7	sg	Singapore	136	120	143,887	8.3
8	br	Brazil	3,129	2,435	3,058,648	8.0
9	in	India	1,638	1,352	1,713,812	7.9
10	ma	Morocco	37	33	43,211	7.6

Domains in South American TLDs continued to experience a rash of server compromises, continuing a trend that began in 1H2012. Thailand's .TH continues to rank highly, as it has for many years, suffering especially from compromised government and university Web servers.

At number eight, compromised .BR domains were used to phish 184 targets, including a wide range of South American banks. India's .IN TLD maintained its position at number nine, used to attack 97 different targets via a mix of compromised and maliciously registered domains.

[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.

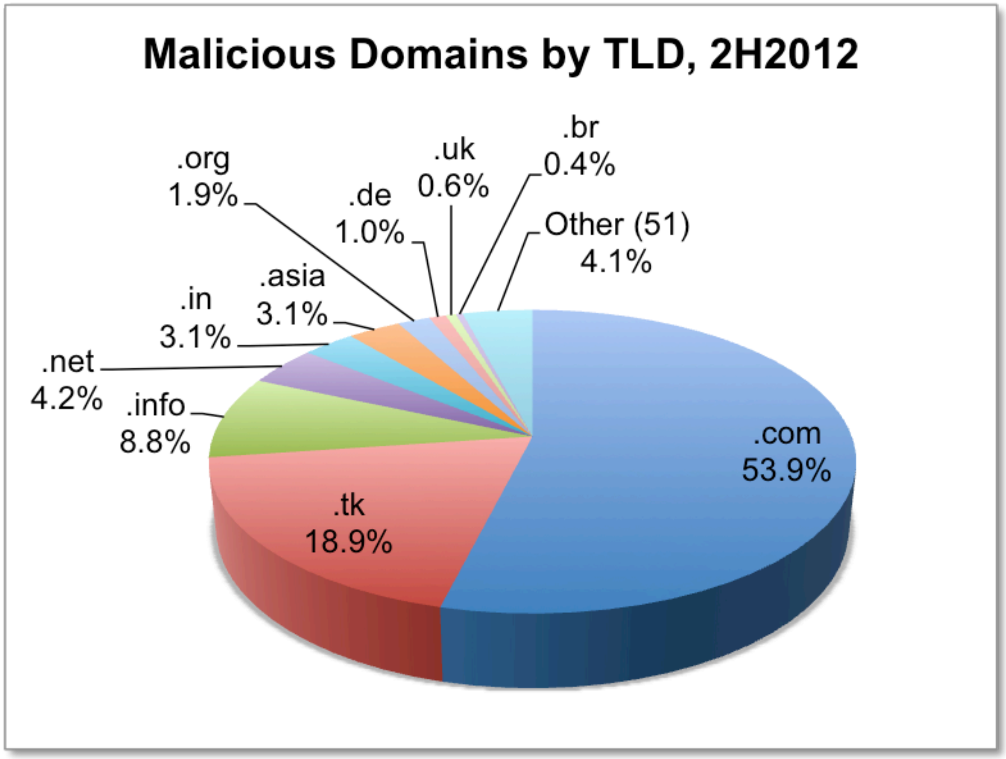


Compromised Domains vs. Malicious Registrations

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 89,748 domains used for phishing, **we identified 5,835 (6.5%) that we believe were registered maliciously, by phishers. This number represents a significant and steady decline over the last two years,** from a high of 14,650 in 1H2011. The other 83,913 domains were almost all hacked or compromised on vulnerable Web hosting.

Of those 5,835 domains, 2,800 (48%) were registered to phish Chinese targets. This is down from 1H2012, when two-thirds of the world's malicious registrations targeted Chinese institutions. However, the stats continue to highlight how Chinese phishers use hacked domains and compromised Web servers less often than phishers elsewhere. Those phsihers tended to registered widely-available gTLD domain names using registrars inside or and outside of China. The ccTLD of China, .CN, had only 16 malicious registrations during the report period.



Almost 82% of the malicious domain registrations were made in just three TLDs: .COM, .TK, and .INFO. The .COM registry has no anti-abuse program. The .INFO TLD has an active abuse response program, but the TLD remains inexpensive compared to others, which attracts registrations by spammers, phishers, and other abusers. In 1H2012, half of the world's malicious registrations were make in the .TK TLD, which offers free domain name registrations. That percentage went down to 19% in 2H2012, as the .TK registry continued a program that gives anti-phishing companies and accredited brand owners the ability to directly suspend .TK domains in the registry. (These partners include Facebook, Internet Identity, and the Anti-Phishing Alliance of China.)

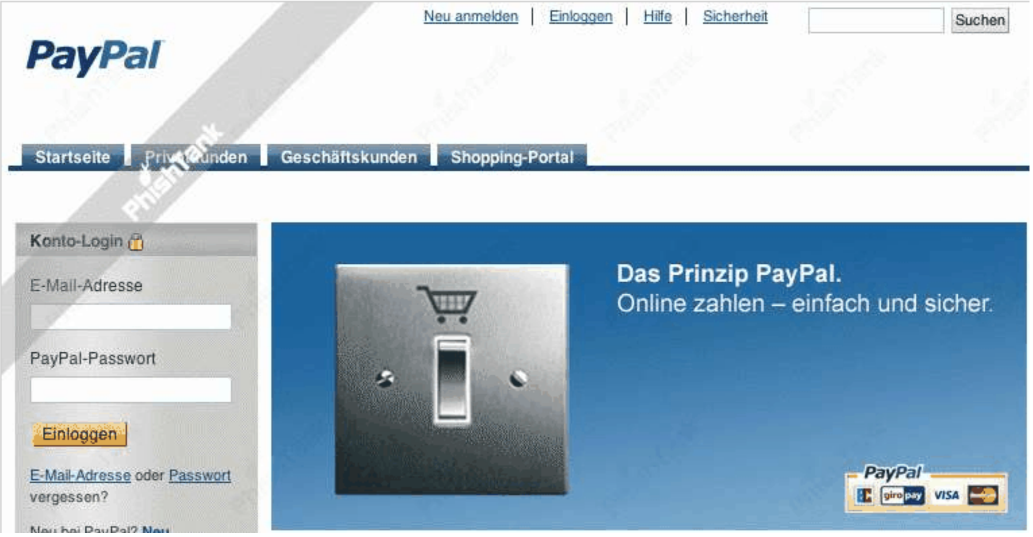
Of the 5,835 maliciously registered domains, just 1,242 contained a relevant brand name or variation thereof—often a misspelling.[7] This is far below the 2,232 we found in 2H2011. **This represents just 1.4% of all domains that were used for phishing, and 21% of all maliciously registered domains recorded in the sampling period.**

So, most maliciously registered domain names 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.**

[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).

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.

Sometimes phishers even use their domain registrations in counter-intuitive ways. This phish was mounted on the maliciously-registered domain name *www-cituibank.net*, but it didn't attack Citibank:



Konto-Login

E-Mail-Adresse

PayPal-Passwort

Einloggen

E-Mail-Adresse oder Passwort vergessen?

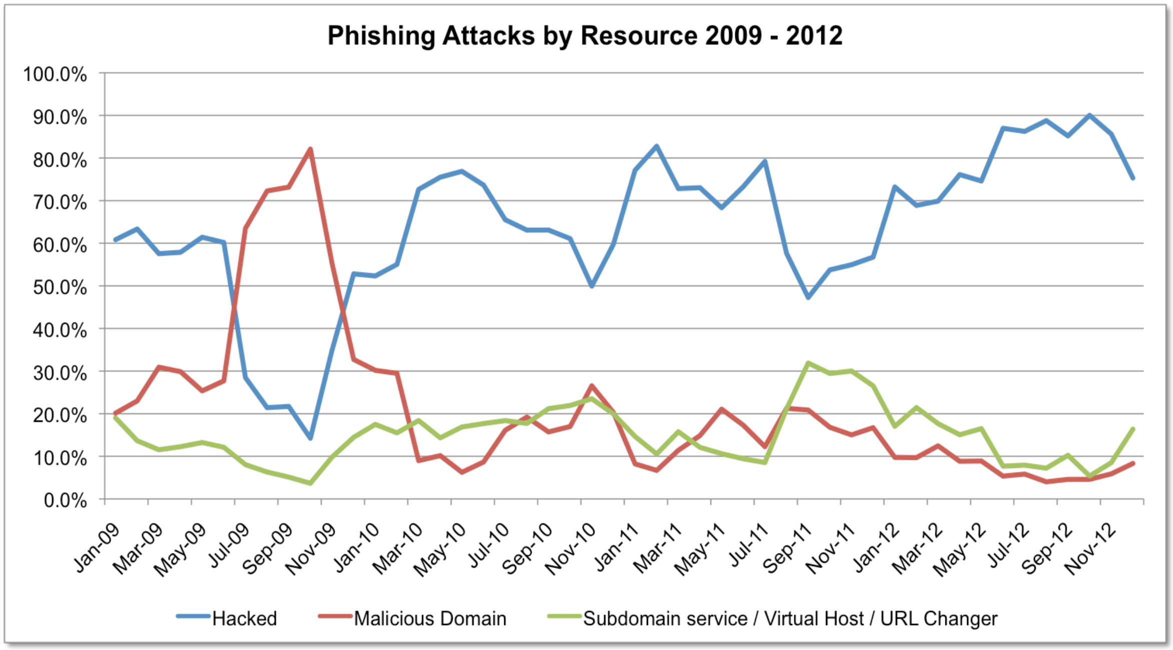
Neu bei PayPal? Neu

Das Prinzip PayPal.
Online zahlen – einfach und sicher.

[image source: Phishtank]

A Historical Retrospective

Our historical data points out very interesting trends around the use of phishing resources or methods as they ebb and flow over time. 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. In fact, malicious domain registrations remained under 10% of all phishing domains for the last three quarters of 2012 – quite a change from the "good old days"! 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 and Joomla.

The last point is particularly important in early 2013, as the scale of these problems has been increasing exponentially. In late 2012 into 2013, we have seen the rise of automated tools and attacking botnets that are targeting shared hosting environments, and particularly WordPress, cPanel, and Joomla installations. These attacks take a variety of forms from brute-force logins to exploiting known vulnerabilities. Reports show that 10's if not 100's of thousands of these shared servers have been cracked by such techniques. Access and use of these boxes is then metered out in the criminal underground for all sorts of activities, including DDoS, malware distribution, and of course, phishing.

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 large and growing a segment of the phishing underground as well as DDoS services that are impacting their business significantly. Network and server hygiene are critical factors for web hosters to enforce diligently.

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.

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, 2H2012

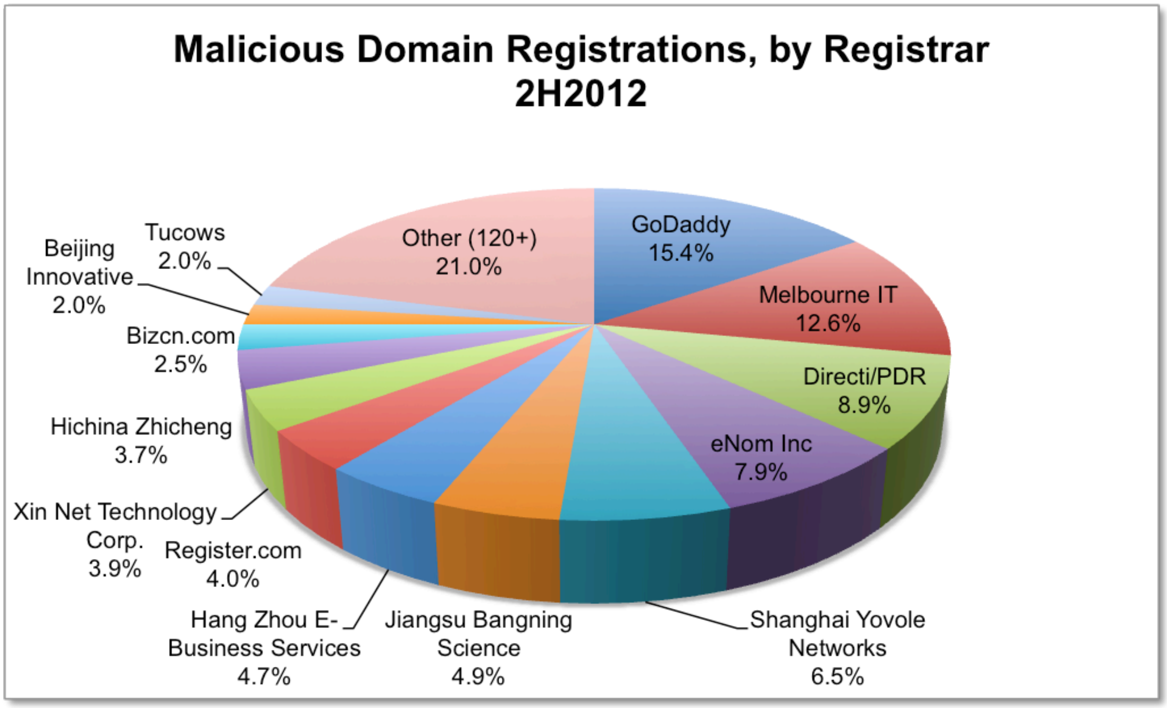
All registrars with more than 25 malicious phishing registrations and 1,000 gTLD domain names under management

Rank	Registrar	Malicious Domain Names used for Phishing 2H2012	Domains at Registrar, March 2013	Score: Phish per 10,000 Domains 2H2012
1	Shanghai Yovole Networks	294	3,924	749.24
2	Chengdu West Dimension	35	3,881	90.18
3	Hang Zhou E-Business Services	214	28,473	75.16
4	Jiangsu Bangning Science	224	69,651	32.16
5	Internet.bs	60	71,571	8.38
6	Beijing Innovative	93	153,930	6.04
7	1API	60	106,738	5.62
8	Bizcn.com	113	247,665	4.56
9	DirectI/PDR	404	1,567,875	2.58
10	Hichina Zhicheng	169	669,145	2.53
11	Melbourne IT	573	2,782,884	2.06
12	Xin Net Technology Corp.	176	876,949	2.01
13	Register.com	180	1,804,145	1.00
14	Name.com	40	521,476	0.77
15	Fast Domain	70	1,195,093	0.59
16	eNom Inc	358	6,965,073	0.51

17	OVH	38	848,597	0.45
18	GoDaddy	700	28,041,724	0.25
19	Tucows	92	5,892,672	0.16
20	1 & 1 Internet AG	44	4,184,238	0.11

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.



Use of Subdomain Services for Phishing

We continue to see abuse of subdomain services, but this tactic declined significantly in 2H2012. **However, phishers again registered far more subdomains than they registered "regular" domain names. The overall use of subdomain services for phishing fell from 14% to 8% of all attacks. We continue to see phishers seeking new providers that they can exploit.**

There were 8,294 phishing attacks hosted on subdomain services in the second half of 2012, using 7,798 unique subdomains. Compare that to the 6,465 attacks using 5,835 "regular" domain names registered by phishers in 2H2012. This was approximately a 40% decrease from the 13,307 attacks we recorded in 1H2012, but still represents 8% of all phishing attacks. This is a far lower rate than the 14% we saw in 1H2012, and continues a positive trend in this space. While the continued rise in hacked sites explains a big chunk of the overall number shift, the absolute number of subdomains did decline significantly. We believe that this can be in part explained by more subdomain services putting tools in place to prevent, detect, and respond to abuse of their services.

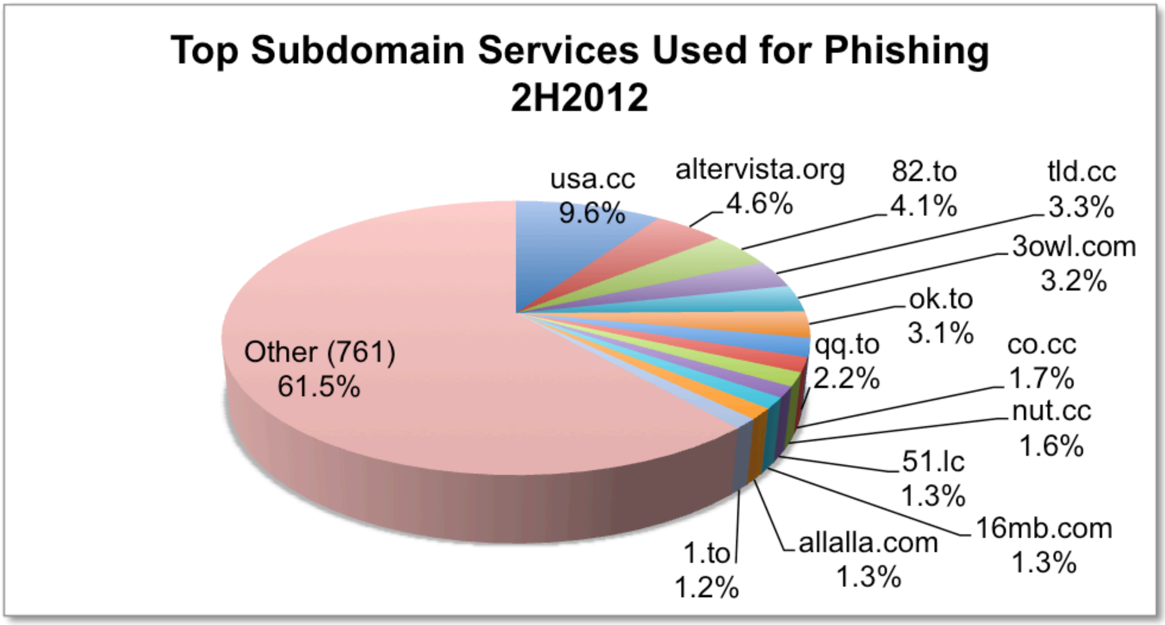
We define "subdomain registration services" as providers that give customers subdomain "hosting accounts" beneath a domain name that the provider owns. These services effectively offer users a "domain name" in their own DNS space for a variety of purposes, and often offer free DNS management. Thus a 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.[8] While many of these services are responsive to complaints, proactive measures to keep criminals from abusing their services are limited.

We saw a large new number of subdomain services being abused by phishers. **More than 30 subdomain services were abused in 2H2012 that we had never seen in prior reports**. Approximately 2,000 attacks were seen on these "new" services to the phishing world. Clearly, if you run a subdomain reselling service, it is likely that phishers will find you and try to create subdomains on your service to launch attacks.

[8] 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.



The favorite service for phishers to abuse in 2H2012 was freeavailabledomains.com, where almost 1,400 malicious subdomains were spotted. This was up from around 1,000 in 1H2012, and put them at the top of our list. This service actually provides a prominent "Report Abuse" option – a continuing and welcome trend in the subdomain reseller space. This increase may indicate that the "up-front" preventative processes aren't deterring phishers from abusing this service. Second on the list was a previously unseen provider – 1004web.com out of Korea. Offering several subdomains in the .to (Tonga) ccTLD and others, this service came under heavy abuse in 2H2012 with over 1000 phishing attacks on subdomains created on its main domains. There were a few other newcomers to the top of our list of providers as well, but for this period, most of the rest of the next most heavily abused services were hold-overs from prior years.

The Poland-based bee.pl service (a.k.a. osa.pl) was the big success story for this report. After leading the category in our last report, and a perennial top "offender", we did not spot a single phish on a bee.pl subdomain in 2H2012. Unfortunately, it looks like they are revamping their service at the time of the writing of this report, with an "under construction" type page greeting visitors. It would be unfortunate if abuse issues were responsible for their cessation of subdomain services, since other services have learned how to operate in that environment. Along that vein, even more subdomains services we looked at in the past six months are now offering WHOIS services and abuse reporting forms or contact information on their websites. We encourage other subdomain resellers to adopt similar tactics – they work!

We have identified nearly 800 subdomain registration providers, which offer services on more than 3,600 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, 2H2012

Rank	Reseller	Attacks
1	freeavailabledomains.com	1,386
2	1004web.com	1,025
3	000webhost.com	412
4	altervista.org	381
5	3owl.com	269
6	1FreeHosting	158
7	CyDots	144
8	DynDNS	137
9	likedns.cn	134
10	CO.CC, Inc.	120
11	uCoz	113
12	HomeNIC.com	110
13	main-hosting.com	107
14	alpennic.com	105
15	nazuka.net	101
16	pubyun.com	100
17	5gbfree.com	96
18	ias3.com	90
19	blogspot.com	89
20	tripod.com	84

Use of Internationalized Domain Names (IDNs)

Data continues to show that the unique characteristics of Internationalized Domain Names (IDNs) are not being used to facilitate phishing in any 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; there are now more than 38 approved IDN TLDs, with many more to come in late 2013 and beyond. While most IDN TLDs are not active, the .рф (.rf) TLD of the Russian Federation contains 780,000 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, thereby allowing the phisher to spoof a brand name. Since January 2007, we have found only five homographic phishing attacks, and none since 2011.

In July 2012, there were two interesting attacks. They were not homographic attacks, but were malicious IDN registrations. The phish were on these URLs:

http://xn--konfliktlsung-paypal-cbc.de/security-payment-gateway.com/index.html
and
http://xn--konfliktlsung-paypal-cbc.info/security-payment-gateway.com/

The string "xn--konfliktlsung-paypal-cbc" is rendered in IDN-enabled browsers and applications as "konfliktlösung-paypal-cbc". The word "konfliktlösung" is German for "conflict resolution." The savvy phisher responsible experimented with the German character to make his domains more authentic-looking to German readers.

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

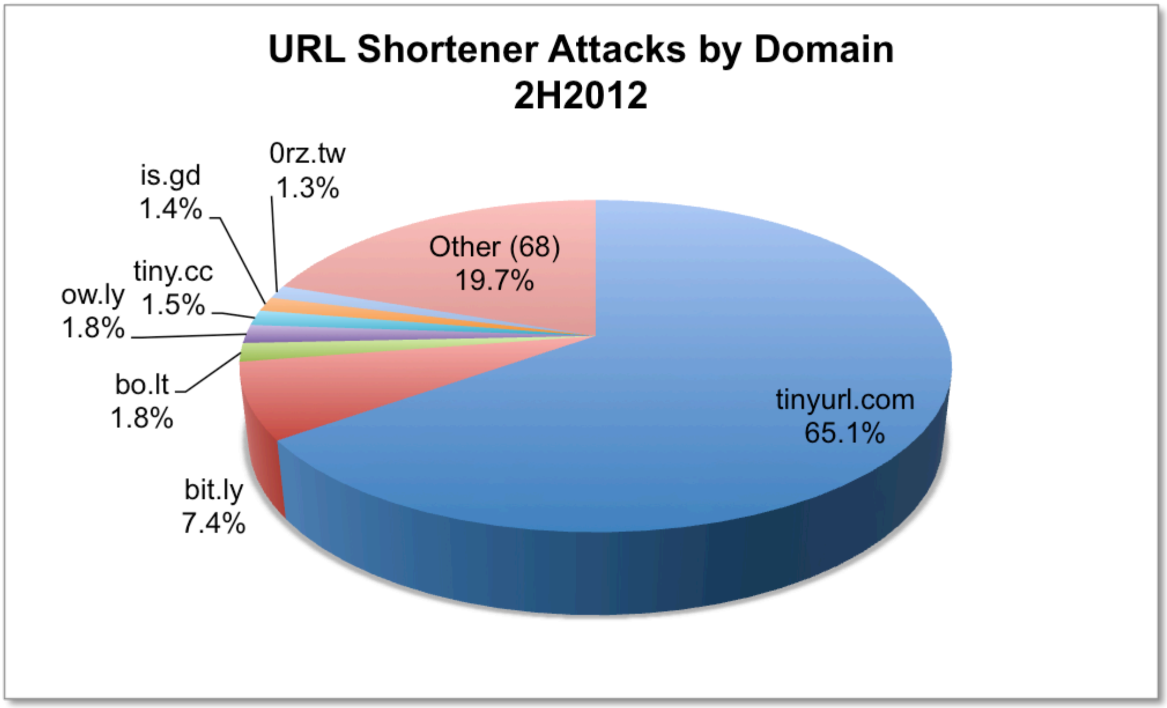
1. Phishers don't *need* to resort to such attacks. As noted elsewhere in this report, the domain name itself usually does not matter to a phisher.
2. By default, some browser manufacturers show the punycode version of the domain name (such as "xn--hotmal-t9a.net") in the address bar, instead of the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

To date, the new IDN TLD registries have been 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. In late 2013 and beyond, new IDN registries will be awarded to a wider range of operators, and so we will continue to monitor for interesting trends.

Use of URL Shorteners for Phishing

Phishers continue to use "URL shortening" services to obfuscate phishing URLs, but such use involved only 785 attacks in 2H2012, though up over 50% from 507 in 1H2012. 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.



Other than a very small number of shortened URLs found at a wide variety of services, the strong majority (over 65%) of malicious shortened URLs used for phishing were found at a single provider – tinyURL.com. This is an extremely popular service, but has limited support and no reporting tool available on its website for abuse issues as of this writing. We encourage the team running this service to take note of this report and implement stronger measures to curb abuse on its service in the future.

Appendix: Phishing Statistics and Uptimes by TLD

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
ac	Ascension Island	1	1	16,100	0.6	0.6				
ad	Andorra	7	6	1,500	40.0	46.7	36:24	24:17		
ae	United Arab Emirates	89	31	100,500	3.1	8.9	32:48	13:30		
aero	sponsored TLD	3	3	8,221	3.6	3.6	10:57	10:57		
af	Afghanistan	7	7				58:09	58:09		
ag	Antigua and Barbuda	1	1	19,762	0.5	0.5				
ai	Anguilla	5	1	3,800	2.6	13.2	16:13	6:21		
al	Albania	9	9	7,500	12.0	12.0	40:55	49:21		
am	Armenia	55	22	20,802	10.6	26.4	10:35	3:50		
an	Netherlands Antilles	1	1	800	12.5	12.5				
ao	Angola	3	3	250	120.0	120.0				
ar	Argentina	913	824	2,500,007	3.3	3.7	25:18	12:49	5	0.0
arpa	Advanced Research Project Agency	1	1				1:54	1:54		
as	American Samoa	7	4				116:29	62:18		
asia	sponsored TLD	340	230	328,383	7.0	10.4	16:00	5:38	179	0.0
at	Austria	93	65	7,588,000	0.1	0.1	32:51	16:16	2	0.0
au	Australia	1,371	1,196	2,551,745	4.7	5.4	27:04	11:52	1	0.0
aw	Aruba	2	1	625	16.0	32.0	39:53	39:53		
ax	Åland Islands	2	2				102:03	102:03		
az	Azerbaijan	21	19	16,129	11.8	13.0	20:11	8:36		
ba	Bosnia and Herzegovina	17	15	14,280	10.5	11.9	21:36	3:15		
bd	Bangladesh	30	23	5,000	46.0	60.0	29:16	7:22		
be	Belgium	289	252	1,338,219	1.9	2.2	26:18	11:39	2	0.0
bf	Burkina Faso	5	1				24:31	33:04		
bg	Bulgaria	25	23	25,000	9.2	10.0	33:07	5:43		
bh	Bahrain	1	1	4,450	2.2	2.2	31:51	31:51		
biz	generic TLD	938	633	2,341,414	2.7	4.0	21:22	9:04	18	0.0

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
bm	Bermuda			8,050						
bn	Brunei Darussalam			1,150						
bo	Bolivia	32	25	8,350	29.9	38.3	7:24	5:31		
br	Brazil	3,129	2,435	3,058,648	8.0	10.2	30:19	14:35	25	0.0
bs	Bahamas			2,320						
bt	Bhutan	5	5	1,000	50.0	50.0	33:44	27:32		
bw	Botswana	1	1							
by	Belarus	59	35				85:30	21:55		
bz	Belize	17	15	46,836	3.2	3.6	44:42	21:46	1	0.0
ca	Canada	795	611	2,000,500	3.1	4.0	32:41	11:43	3	0.0
cat	sponsored TLD	20	16	59,970	2.7	3.3	13:26	7:19		
cc	Cocos (Keeling) Islands (estimated)	1,626	73	850,000	0.9	19.1	16:50	9:06	5	0.0
cd	Congo, Democratic Repub. (estimated)	6	5	5,200	9.6	11.5	13:49	5:41		
cf	Central African Republic	1	1				4:34	4:34		
cg	Congo									
ch	Switzerland	319	286	1,746,794	1.6	1.8	36:25	14:14	1	0.0
ci	Côte d'Ivoire	1	1	2,400	4.2	4.2	2:57	2:57		
cl	Chile	902	731	399,073	18.3	22.6	40:40	16:16	2	0.0
cm	Cameroon	11	4	12,500	3.2	8.8	10:29	8:12	1	0.0
cn	China	424	261	6,368,633	0.4	0.7	36:41	12:22	16	0.0
co	Colombia	288	234	1,325,000	1.8	2.2	20:55	9:34	12	0.0
com	generic TLD	69,078	53,265	108,205,473	4.9	6.4	25:53	9:35	3,145	0.0
coop	sponsored TLD	3	3	14,938	2.0	2.0	62:55	79:54		
cr	Costa Rica	14	12	14,600	8.2	9.6	5:36	3:18		
cu	Cuba	1	1	2,340	4.3	4.3	48:26	48:26		
cv	Cape Verde	1	1				0:46	0:46		
cx	Christmas Island	28	11	5,225	21.1	53.6	21:07	5:42	1	0.0
cy	Cyprus	8	5	12,000	4.2	6.7	57:35	20:22		
cz	Czech Republic	135	97	1,004,655	1.0	1.3	24:56	15:02		
de	Germany	653	465	15,261,697	0.3	0.4	31:11	15:00	56	0.0
dj	Djibouti	2	2				0:10	0:10		
dk	Denmark	177	142	1,211,407	1.2	1.5	32:22	18:50		

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
dm	Dominica	1	1	14,500	0.7	0.7	8:47	8:47		
do	Dominican Republic	14	13				7:37	5:45		
dz	Algeria			4,469						
ec	Ecuador	41	38	30,500	12.5	13.4	27:34	12:51		
edu	U.S. higher education	27	21	7,590	27.7	35.6	34:38	12:33		
ee	Estonia	15	13	67,720	1.9	2.2	23:05	17:35		
eg	Egypt	2	2	6,000	3.3	3.3	39:51	39:51		
er	Eritrea									
es	Spain	473	392	1,612,649	2.4	2.9	25:24	13:11		
et	Ethiopia	2	1	1,100	9.1	18.2	47:33	47:33		
eu	European Union	443	354	3,690,729	1.0	1.2	29:02	14:00	23	0.0
fi	Finland	178	167	308,267	5.4	5.8	16:55	6:12		
fj	Fiji	1	1	4,000	2.5	2.5				
fk	Falkland Islands	2	1	100	100.0	200.0	33:02	33:02		
fm	Micronesia, Fed. States	13	12				13:09	5:03		
fo	Faroe Islands									
fr	France	684	505	2,509,913	2.0	2.7	29:38	14:08	9	0.0
gd	Grenada	19	6	4,450	13.5	42.7	16:35	7:01		
ge	Georgia	47	36	20,300	17.7	23.2	38:08	16:17		
gg	Guernsey	10	4				15:36	2:26		
gh	Ghana	5	3				13:37	6:00		
gi	Gibraltar			1,932						
gl	Greenland	8	1	5,100	2.0	15.7	16:15	2:42		
gm	Gambia	1	1				38:58	38:58		
gov	U.S. government	1	1	5,000	2.0	2.0	10:56	10:56		
gp	Guadeloupe	18	10	1,475	67.8	122.0	4:18	2:05		
gr	Greece *(estimated)*	319	269	377,000	7.1	8.5	27:58	12:18		
gs	South Georgia & Sandwich Is.	10	5	8,160	6.1	12.3	4:57	2:03		
gt	Guatemala	18	13	11,600	11.2	15.5	46:30	3:21		
gy	Guyana	3	3	2,150	14.0	14.0	15:13	15:13		
hk	Hong Kong	47	36	239,740	1.5	2.0	22:29	8:51	2	0.0
hm	Heard and McDonald Is.	111	3				8:04	4:21		
hn	Honduras	2	2	6,275	3.2	3.2	78:14	78:14		
hr	Croatia	32	26	78,832	3.3	4.1	29:24	17:06		

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
ht	Haiti	8	3				12:42	7:23		
hu	Hungary	1,701	1,192	625,701	19.1	27.2	37:01	10:52	2	0.0
id	Indonesia	154	112	333,000	3.4	4.6	26:53	11:10	1	0.0
ie	Ireland	97	88	180,500	4.9	5.4	29:18	9:46		
il	Israel	85	76	235,148	3.2	3.6	35:33	13:18		
im	Isle of Man	9	8				17:02	12:17	1	0.0
in	India	1,638	1,352	1,713,812	7.9	9.6	28:22	12:03	180	0.0
info	generic TLD	2,779	2,280	7,531,934	3.0	3.7	15:29	7:52	516	0.0
int	sponsored TLD									
io	British Indian Ocean Terr.	1	1				1:31	1:31		
IP address	(no domain name used)	2,489								
iq	Iraq									
ir	Iran	228	166	306,830	5.4	7.4	25:54	12:56	1	0.0
is	Iceland	11	10	40,000	2.5	2.8	22:16	18:24		
it	Italy	517	404	2,500,000	1.6	2.1	36:03	16:28	7	0.0
je	Jersey	1	1				9:47	9:47		
jm	Jamaica			6,400						
jo	Jordan	5	5	4,200	11.9	11.9				
jobs	sponsored TLD			41,959						
jp	Japan	104	75	1,315,399	0.6	0.8	32:19	14:52		
ke	Kenya	76	68	24,750	27.5	30.7	13:09	4:52	1	0.0
kg	Kyrgyzstan	6	6	5,300	11.3	11.3	21:28	21:30		
kh	Cambodia	10	5	1,600	31.3	62.5	11:59	11:55		
ki	Kiribati									
kr	Korea	521	307	1,152,431	2.7	4.5	27:32	12:16		
kw	Kuwait	2	2	3,275	6.1	6.1	4:38	4:38		
ky	Cayman Islands									
kz	Kazakhstan	78	60	82,765	7.2	9.4	37:53	20:31	1	0.0
la	Lao People's Demo. Rep. *(domains estimated)*	1,062	11	9,000	12.2	1180.0	21:03	9:56	1	0.0
lb	Lebanon	2	2	3,490	5.7	5.7	52:51	52:51		
lc	St. Lucia	126	11	3,248	33.9	387.9	14:58	9:37		
li	Liechtenstein	23	13	70,000	1.9	3.3	21:47	13:38		
lk	Sri Lanka	47	37	8,490	43.6	55.4	35:28	9:14		

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
ls	Lesotho									
lt	Lithuania	43	26	152,050	1.7	2.8	36:22	10:56		
lu	Luxembourg	18	11	71,500	1.5	2.5	29:36	11:21		
lv	Latvia	32	26	100,100	2.6	3.2	29:25	19:28		
ly	Libya	104	16	13,100	12.2	79.4	21:31	7:04	1	0.0
ma	Morocco	37	33	43,211	7.6	8.6	20:59	10:09	1	0.0
mc	Monaco									
md	Moldova	7	7	21,671	3.2	3.2	41:39	42:41		
me	Montenegro	272	164	661,218	2.5	4.1	23:01	10:11	6	0.0
mg	Madagascar	1	1				117:40	117:40		
mk	Macedonia	25	22				27:52	12:39		
ml	Mali	2	2				24:10	24:10		
mn	Mongolia	73	68	13,890	49.0	52.6	24:25	13:42	1	0.0
mo	Macao			300						
mobi	sponsored TLD	130	119	1,037,426	1.1	1.3	6:15	2:11	1	0.0
mp	Northern Mariana Islands	1	1				2:05	2:05		
mr	Mauritania									
ms	Montserrat	147	12	9,800	12.2	150.0	18:30	13:20		
mt	Malta	5	5	6,250	8.0	8.0	31:37	26:05		
mu	Mauritius	12	6	7,500	8.0	16.0	9:11	5:06	1	0.0
museum	sponsored TLD			435						
mx	Mexico	398	306	616,458	5.0	6.5	29:10	10:39	25	0.0
my	Malaysia	139	117	205,300	5.7	6.8	23:39	7:27		
mz	Mozambique			2,000						
na	Namibia	2	2				2:34	2:34		
name	generic TLD	31	27	218,779	1.2	1.4	24:47	13:07	1	0.0
nc	New Caledonia	1	1				40:48	40:48		
ne	Niger									
net	generic TLD	7,667	5,450	15,264,923	3.6	5.0	24:40	8:19	247	0.0
nf	Norfolk Island	6	5	1,600	31.3	37.5	22:15	17:38		
ng	Nigeria	11	9	12,500	7.2	8.8	65:03	38:36		
ni	Nicaragua	4	3	6,600	4.5	6.1	23:40	27:09		
nl	Netherlands	935	863	5,116,759	1.7	1.8	27:53	12:05	11	0.0
no	Norway	87	70	563,972	1.2	1.5	26:31	12:02		

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
np	Nepal	42	32	31,710	10.1	13.2	34:51	11:11		
nr	Nauru	1	1				2:04	2:04		
nu	Niue *(domains estimated)*	78	23	100,000	2.3	7.8	11:50	8:11		
nz	New Zealand	153	132	512,922	2.6	3.0	19:18	7:53		
om	Oman									
org	generic TLD	6,134	4,569	10,095,346	4.5	6.1	20:37	8:55	111	0.0
pa	Panama	8	8	7,125	11.2	11.2	27:53	27:53		
pe	Peru	130	93	64,100	14.5	20.3	23:26	11:10		
pf	French Polynesia									
ph	Philippines *(domains estimated)*	37	29				37:18	12:15		
pk	Pakistan *(domains estimated)*	355	228	18,000	126.7	197.2	36:16	9:12	1	0.0
pl	Poland	718	500	2,392,601	2.1	3.0	29:55	11:55	1	0.0
pn	Pitcairn	4	3				3:25	2:55		
post	sponsored TLD			6						
pro	sponsored TLD	47	31	150,571	2.1	3.1	43:41	10:32	6	0.0
ps	Palestinian Territory	13	9	7860	11.5	16.5	39:58	13:36	1	0.0
pt	Portugal	132	102	235,699	4.3	5.6	30:11	16:01		
py	Paraguay	14	10	13,900	7.2	10.1	17:03	10:47		
qa	Qatar	1	1	14,610	0.7	0.7	5:03	5:03		
re	Réunion	11	11	18,841	5.8	5.8	101:46	46:59	2	0.0
ro	Romania	388	286	609,000	4.7	6.4	30:59	13:36	1	0.0
rs	Serbia	61	50	74,519	6.7	8.2	46:21	12:27	1	0.0
ru	Russian Fed.	1,296	909	4,260,000	2.1	3.0	28:40	13:22	20	0.0
rw	Rwanda									
sa	Saudi Arabia	19	16	29,380	5.4	6.5	42:58	18:06	1	0.0
sc	Seychelles	1	1	6,138	1.6	1.6				
sd	Sudan	8	8				42:24	18:04		
se	Sweden	150	116	1,262,000	0.9	1.2	41:33	14:45		
sg	Singapore	136	120	143,887	8.3	9.5	21:28	13:22		
sh	Saint Helena	2	1	3,000	3.3	6.7	6:37	6:37		
si	Slovenia	53	31	105,300	2.9	5.0	39:36	18:50		
sk	Slovakia	48	30	285,222	1.1	1.7	31:40	8:12		
sl	Sierra Leone									
sm	San Marino	1	1	1,905	5.2	5.2	3:46	3:46		

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
sn	Senegal	1	1	3,500	2.9	2.9	4:59	4:59		
so	Somalia	3	3				10:26	10:26	1	0.0
sr	Suriname	4	4				11:19	5:12		
st	Sao Tome and Principe	3	3				21:45	18:37		
su	Soviet Union	31	20	110,440	1.8	2.8	21:05	19:22		
sv	El Salvador	8	8	5,550	14.4	14.4	14:42	14:42		
sy	Syria	2	1							
sz	Swaziland	4	2				22:21	14:42		
tc	Turks and Caicos	45	18				14:10	9:14		
tel	generic TLD			224,455						
tf	French Southern Territories	162	14	1,550	90.3	1045.2	12:06	7:50		
tg	Togo	1	1				326:37	326:37		
th	Thailand	210	136	63,400	21.5	33.1	29:17	11:53		
tj	Tajikistan	3	1	6,200	1.6	4.8	19:54	24:53		
tk	Tokelau	1,191	1,101	12,118,000	0.9	1.0	19:31	9:46	1,101	0.0
tl	Timor-Leste	7	5				94:40	12:04		
tm	Turkmenistan			3,775						
tn	Tunisia	14	7	15,652	4.5	8.9	58:16	20:39		
to	Tonga	1,072	28	15,100	18.5	709.9	15:02	9:40		
tp	Portuguese Timor									
tr	Turkey	215	164	315,650	5.2	6.8	32:13	13:38		
travel	sponsored TLD	5	4	23,676	1.7	2.1	22:07	12:56		
tt	Trinidad and Tobago	1	1	2,525	4.0	4.0	50:05	50:05		
tv	Tuvalu *(domains est.)*	149	112	175,000	6.4	8.5	42:45	13:03		
tw	Taiwan	100	66	519,500	1.3	1.9	24:28	15:14	5	0.0
tz	Tanzania	10	8	5,600	14.3	17.9	49:51	14:21		
ua	Ukraine	419	335	689,077	4.9	6.1	30:02	12:40		
ug	Uganda	11	10	3,200	31.3	34.4	114:16	15:09		
uk	United Kingdom	1,744	1,451	10,278,800	1.4	1.7	27:54	12:42	35	0.0
us	United States	435	319	1,754,000	1.8	2.5	16:58	6:57	25	0.0
uy	Uruguay	81	39	74,446	5.2	10.9	47:10	31:00		
uz	Uzbekistan	10	8	15,550	5.1	6.4	7:06	5:08		
vc	St. Vincent and Grenadines	13	5	8,470	5.9	15.3	14:35	12:49	1	0.0
ve	Venezuela	75	57	215,000	2.7	3.5	42:54	13:42		

TLD	TLD Location	Unique Phishing Attacks 2H2012	Unique Domain Names used for Phishing 2H2012	Domains in Registry, November 2012	Score: Phishing Domains per 10,000 Domains 2H2012	Score: Attacks per 10,000 Domains 2H2012	Average Uptime 2H2012 hh:mm	Median Uptime 2H2012 hh:mm	Total Malicious Domains Registered 2H2012	Malicious Registrations score/10,000 domains in registry
vg	British Virgin Islands	1	1	8,600	1.2	1.2	1:29	1:29		
vi	Virgin Islands			17,000						
vn	Vietnam	162	121	349,459	3.5	4.6	35:06	18:28		
vu	Vanuatu	39	8				12:29	6:43		
ws	Samoa	72	52	500,000	1.0	1.4	15:55	5:03	4	0.0
xn--3e0b707	.한국 (KR IDN)			91,700						
xn--90a3ac	.СРБ (Serbia IDN)			6,600						
xn--fzc2c9e2c	.□□□□ (Sri Lanka IDN)			150						
xn--mgberp4a5d4a	)Saudi Arabia IDN(السعودية.			1,850						
xn--o3cw4h	.ไทย (.TH IDN)			1,000						
xn--p1ai	.рф (.RF, Russian Federation IDN)	4	3	785,000	0.0	0.1	44:25	44:23		
xn--xkc2al3hye2a	.□□□□□□ (Sri Lanka IDN)			85						
xxx	sponsored TLD			142,953						
ye	Yemen			800						
yt	France	1	1				95:25	95:25	1	0.0
yu	Yugoslavia (TLD deprecated March 2010)			0						
za	South Africa	592	523	819,500	6.4	7.2	30:05	9:41		
zm	Zambia	7	7				11:03	9:44		
zw	Zimbabwe	39	24	1,000	240.0	390.0	29:45	10:30		
	TOTALS	**123,476**	**89,748**	**257,704,826**					**5,833**	

About the Authors & Acknowledgments

The authors wish to thank the following for their support: Peter Cassidy and Foy Shiver of the APWG, and Aaron Routt of Internet Identity. The authors thank Liming Wang, Wang Wei, and Hu Anlei 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). 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 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.

#