Global Phishing Survey: Trends and Domain Name Use in 1H2013

APWG

Unifying the
Global Response
To Cybercrime

Published 18 September 2013

An
APWG
Industry
Advisory

Authors:
Rod Rasmussen, Internet Identity
<rod.rasmussen at internetidentity.com>
and
Greg Aaron, Illumintel Inc.
<greg at illumintel.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

Phishers must remain hidden in the shadows, but they also need potential victims to see their work. To combat phishing, we must learn how the phishers create and advertise their bogus sites. These methods change constantly. By analyzing the phishing that took place in the first half of 2013, we have learned how the phishers perpetrated their attacks. The bad guys are trying new tricks and taking advantage of promising new resources. The good guys have won a few battles. And overall, phishing is expanding in places where Internet-using populations are growing.

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 2013 ("1H2013", January 1 to June 30). 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. **Vulnerable hosting providers are inadvertently contributing to phishing. Mass compromises led to 27 percent of all phishing attacks. (See pages 8-9)**
2. **Phishing continues to explode in China, where the expanding middle class is using e-commerce more often. (Pages 12, 14-15)**
3. **The number of phishing targets (brands) is up, indicating that e-criminals are spending time looking for new opportunities. (Page 6)**
4. **Phishers continue to take advantage of inattentive or indifferent domain name registrars, registries, and subdomain resellers**. The number of top-level registries is poised to quintuple over the next two years. **(Pages 9-12, 16-17)**
5. **The average and median uptimes of phishing attacks are climbing. (Pages 6-7)**

Key Statistics

Millions of phishing URLs were reported in 1H2013 but the number of unique phishing attacks and domain names used to host them was much smaller.[1] The 1H2013 data set yielded the following statistics:

[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 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.

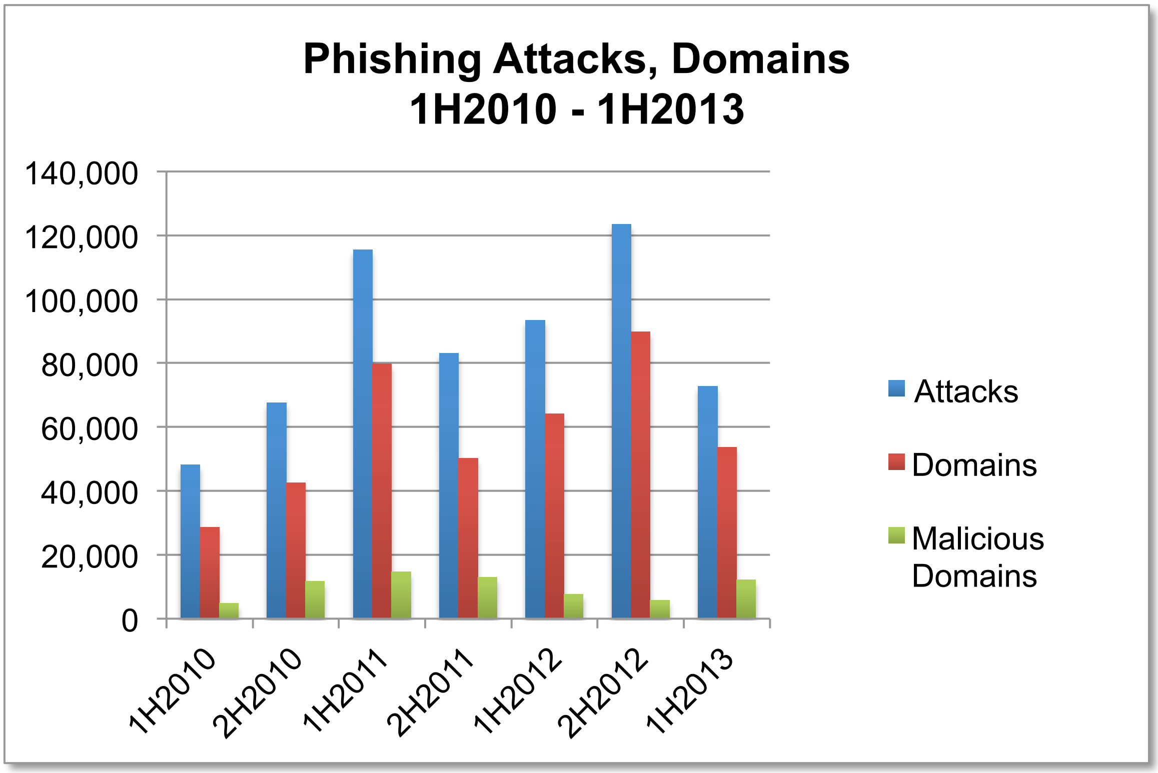
- **There were at least 72,758 unique phishing attacks worldwide**. This is far below the 123,486 attacks recorded in 2H2012. The decrease is due to a decline in phishing attacks that leveraged shared virtual servers to compromise multiple domains at once. (See "Shared Virtual Server Hacking" on page 8.) 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 occurred on 53,685 unique domain names**.[2] Again, this is down from the 89,748 domains used in 2H2012, due to reduced incidents of virtual server hacking. The number of domain names in the world grew from 258 million in November 2012 to 261 million in April 2013.[3]
- In addition**, 1,972 attacks were detected on 1,626 IP addresses, rather than on domain names.** (For example: http://142.234.140.62/pay/jian) The number of attacks using IPs has remained steady for 3.5 years. None of these phish were reported on IPv6 addresses.
- Of the 53,685 phishing domains, **we identified 12,173 domain names that we believe were registered maliciously, by phishers. This is double the 5,835 found in 2H2012. The increase is due to a sudden uptick in domain registrations by Chinese phishers.** The other 41,532 domains were almost all hacked or compromised on vulnerable Web hosting.
- **The average uptimes of phishing attacks are climbing, up from the historic lows seen in early 2012. The average uptime in 1H2013 was 44 hours and 39 minutes, compared to 26 hours and 13 minutes in 2H2012.** The median uptime in 1H2013 was 12 hours and 52 minutes – over twice the historic low median of 5 hours and 45 minutes achieved in 1H2012.
- **Phishing occurred in 195 top-level domains (TLDs), but 82% of the malicious domain registrations were in just three TLDs**: .COM, .TK, and .INFO.
- **We counted 720 target institutions, up significantly from the 611 targeted institutions identified in 2H2012**.
- **Only about 2.3% of all domain names that were used for phishing contained a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations," below.)
- Seventy-eight of the 53,685 domain names were internationalized domain names (IDNs), and three of them were homographic attacks.
- The use of URL shorteners for phishing has plummeted, probably due to better anti-abuse measures at the providers.

[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

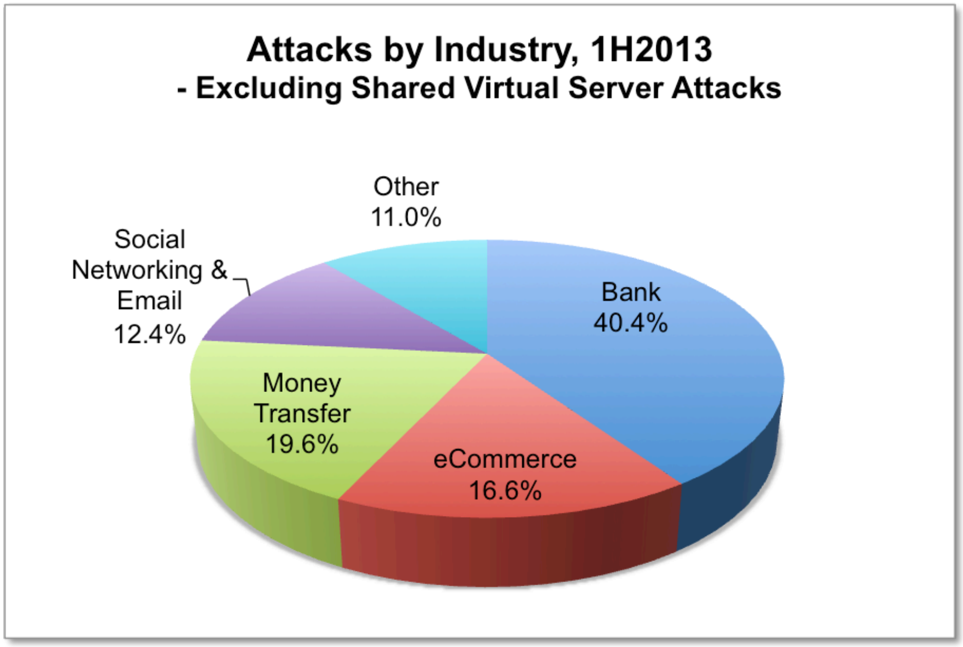
	1H2013	2H2012	1H2012	2H2011	1H2011	2H2010
Phishing domain names	53,685	89,748	64,204	50,298	79,753	42,624
Attacks	72,758	123,476	93,462	83,083	115,472	67,677
TLDs used	194	207	202	200	200	183
IP-based phish (unique IPs)	1,626	1,981	1,864	1,681	2,385	2,318
Maliciously registered domains	12,153	5,833	7,712	12,895	14,650	11,769
IDN domains	78	147	58	36	33	10
Number of targets	720	611	486	487	520	587



Target Distribution

We counted 720 unique target institutions during the period, up significantly from the 611 found in 2H2012. The number of times that the targets were attacked follows a long tail.

- PayPal was the most-targeted institution (13,498 attacks, or 18.3% of the total), followed by Taobao.com (6,605 attacks, or 9%).
- The top 80 targets were attacked 100 or more times each in the period.
- Half of the targets were attacked one to three times during the period.



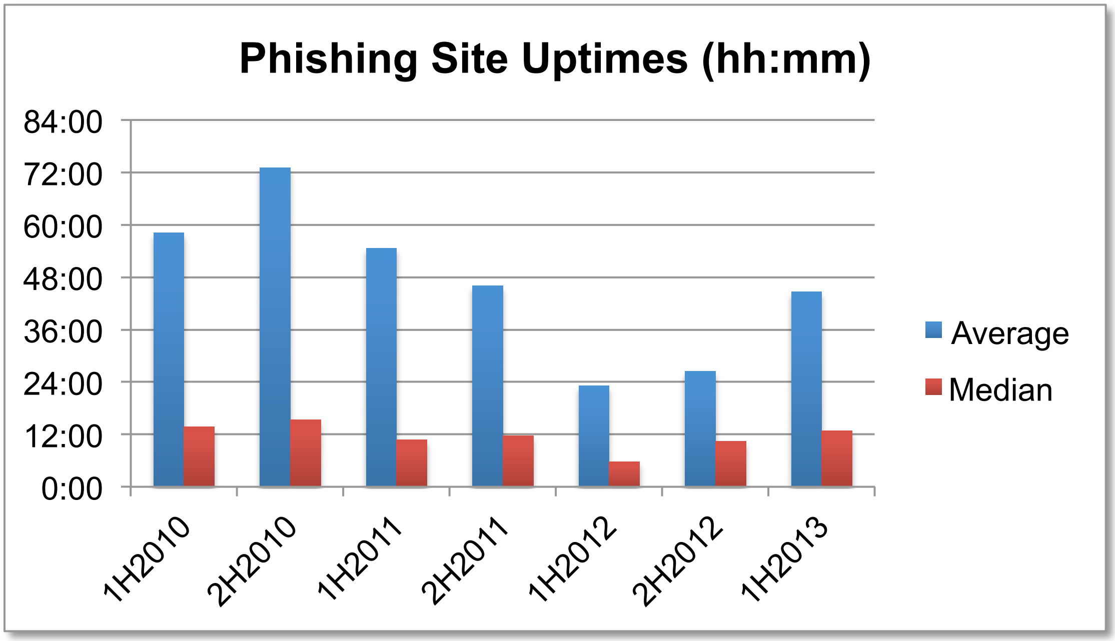
Phishing by Uptime

The average uptimes of phishing attacks are climbing, up from the historic lows seen in early 2012. The average uptime in 1H2013 was 44 hours and 39 minutes, compared to 26 hours and 13 minutes in 2H2012. The median uptime in 1H2013 was 12 hours and 52 minutes – over twice the historic low median of 5 hours and 45 minutes achieved in 1H2012.

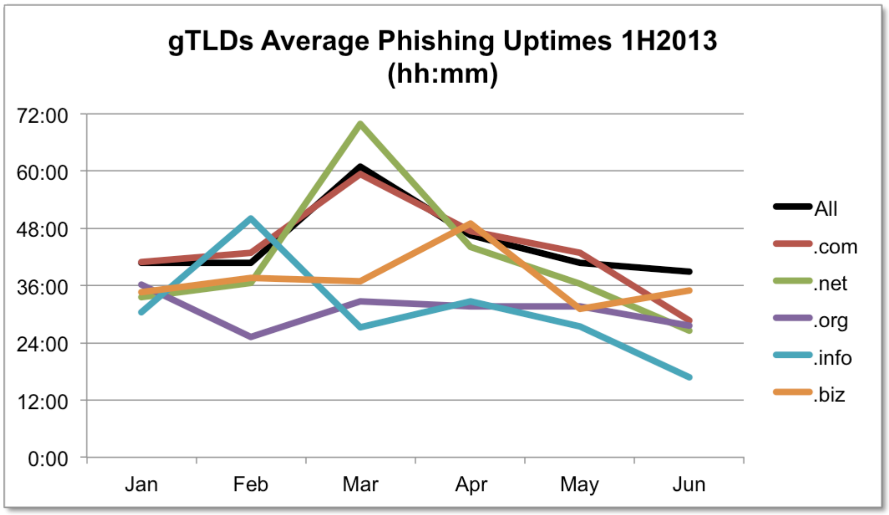
The "uptimes" or "live" times[4] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a measure of the success of mitigation efforts. The first day of a phishing attack is the most lucrative for the phisher, so quick takedowns are essential. Long-lived phish can skew the averages since some phishing sites last weeks or even

[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 percent 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.

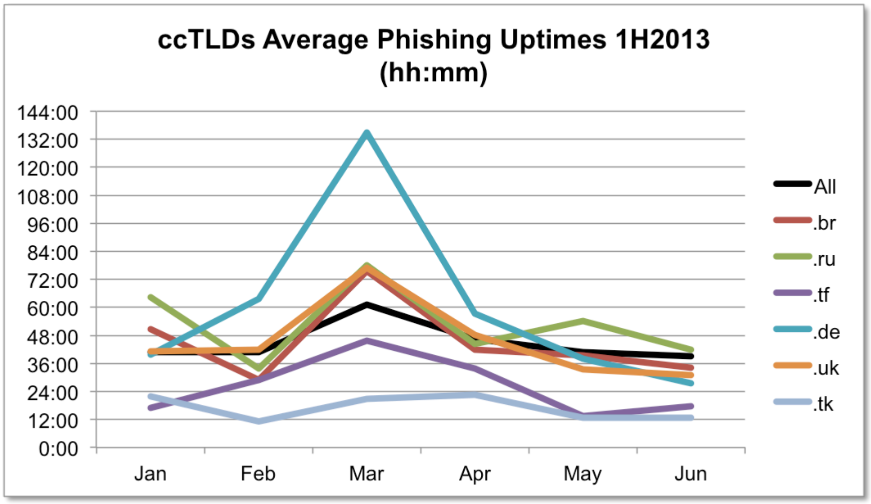
months, so medians are also a useful barometer of overall mitigation efforts. CNNIC did not record the uptimes of the phish it documented, so those phish were not part of our uptime calculations.



In the large generic top-level domains (gTLDs), phishing times increased in March as virtual server hacking decreased, and then decreased in April as virtual server hacking rose. (Virtual server attacks prompt many complaints to the affected hosting providers at one time, revealing the commandeered servers; each mitigation effort takes down multiple phishing attacks at once.) .INFO, .BIZ, and .ORG continue to have below-average uptimes, due to notification and takedown programs at those registry operators:



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

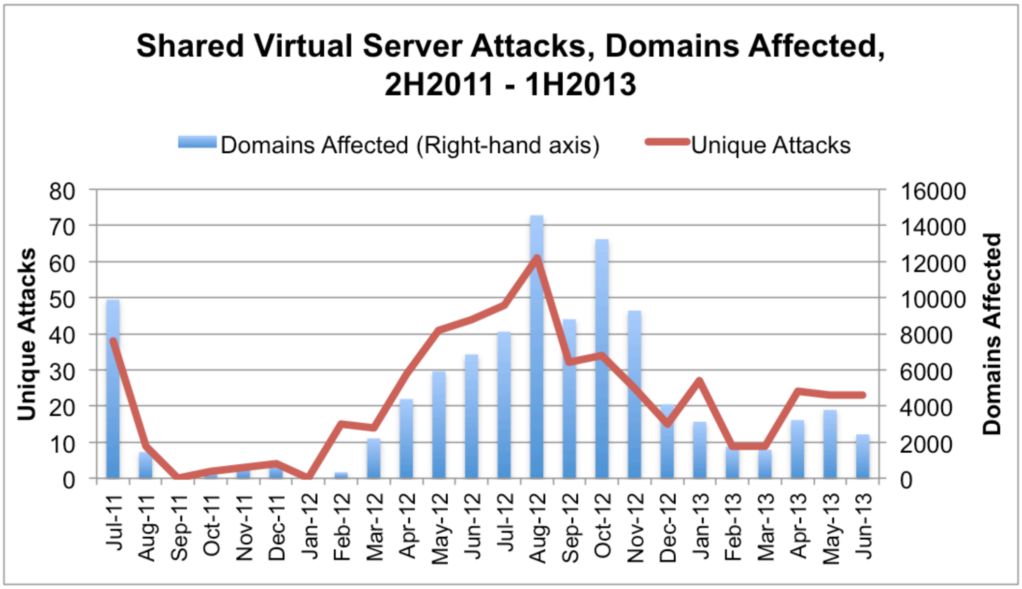


For uptime statistics for every top-level domain, please see the Appendix.

Shared Virtual Server Hacking

A specific tactic used by phishers continues to heavily impact our statistics. In this attack, a phisher breaks into a web server that hosts a large number of domains – a "shared virtual server." Then he uploads one copy of his phishing content and updates the web server configuration to add that content to *every* hostname served by that server. Then *all* web sites on that server display the phishing pages. Instead of hacking sites one at a time, the phisher often infects hundreds of web sites at a time, depending on the server.

In 1H2013, we identified 115 mass break-ins of this type, resulting in 19,455 phishing attacks. This represents 27% of all phishing attacks recorded worldwide. This is down from 2H2011, when we identified 58,100 virtual server phishing attacks.



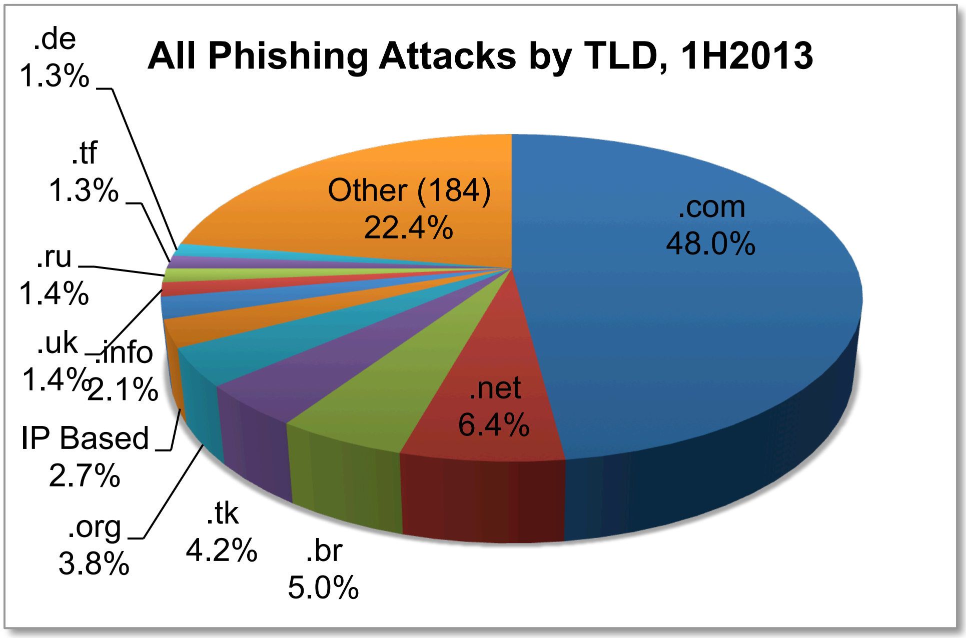
We identified sets of attacks by analyzing the IP addresses of the machines used, the timing of the attacks, and by the telltale URL paths that the phish shared.

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.

We continue to observe increasing use of tools for targeting shared hosting environments, and particularly WordPress, cPanel, and Joomla installations. Automated cracking tools are providing tens of thousands of fresh datacenter servers to the criminal underground via various marketplaces. We see such servers being utilized for all manner of abuse beyond phishing, ranging from underground proxy networks to large-scale DDoS attacks, both of the "Brobot" variety and DNS amplification attacks. This is an area the web hosting community and the security community need to work together on to improve. Margins are thin in the hosting business, there are many layers of resellers, and often times there is limited or even no abuse-handling capability at hosting providers. Thus we have a uniquely difficult challenge to take on as an industry in the next year.

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 phishing-domains-per-10,000 score was 3.1** (versus 4.7 in 2H2012).
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 2.5.** .COM contained 52% of the phishing domains in our data set, and 43% of the domains in the world.

We therefore suggest that domains-per-10,000 scores between 2.5 and 3.1 occupy the middle ground, with scores above 3.1 indicating TLDs with increasingly prevalent phishing.[6] The top TLDs by score are:

Top 10 Phishing TLDs by Domain Score, 1H2013

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

	TLD	TLD Location	# Unique Phishing attacks 1H2013	Unique Domain Names used for phishing 1H2013	Domains in registry, April 2013	Score: Phishing domains per 10,000 domains 1H2013
1	.pw	Palau	115	109	55,000	19.8
2	.np	Nepal	97	64	32,500	19.7
3	.th	Thailand	166	125	65,350	19.1
4	.si	Slovenia	219	196	108,100	18.1
5	.ec	Ecuador	64	48	30,500	15.7

[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.

	TLD	TLD Location	# Unique Phishing attacks 1H2013	Unique Domain Names used for phishing 1H2013	Domains in registry, April 2013	Score: Phishing domains per 10,000 domains 1H2013
6	.pe	Peru	143	107	69,505	15.4
7	.sa	Saudi Arabia	40	33	30,400	10.9
8	.cl	Chile	494	357	418,558	8.5
9	.br	Brazil	3,668	2,669	3,265,768	8.2
10	.ma	Morocco	44	33	43,299	7.6

.PW was an obscure ccTLD that was re-launched for general availability on 25 March 2013. Phishers and spammers decided to test out the new space, and the spike in abuse resulted in some network blocking and blocklistings by reputation services. This highlights the need for any new, generally available TLD to have adequate abuse monitoring in place. The .PW registry operator applied additional anti-abuse measures to combat the problem, and abuse has decreased sharply.

Thailand's .TH continues to rank highly, as it has for many years, suffering especially from compromised government and university Web servers. At number nine, compromised .BR domains were used to phish 171 targets across the globe, including a wide range of South American banks.

Beginning in late 2013 and into 2015, approximately 1,200 new top-level domains will launch, the result of a multi-year planning and application process run by the Internet Corporation for Assigned Names and Numbers (ICANN), which coordinates the top level of the Internet. Some of the new TLDs will be "closed," operated by companies for their own use, and these will offer no opportunity for malicious registrations. Some new TLDs will be for the use of designated communities; their restrictive registration policies may deter criminals. And hundreds of the new TLDs will be "open," offering general registration to a worldwide audience. This last category will offer the most opportunities for criminals.

A number of measures have been put in place in the New TLD program to cut down on abuse and protect brand owners, including new streamlined arbitration procedures, preferential registration periods for trademark owners, and required abuse reporting contacts for registry operators. ICANN-accredited registrars will also start implementing new registrant validation measures aimed at improving the accuracy of WHOIS records and making it harder for criminals to hide behind bogus contact details. But the bottom line is that real vigilance and active monitoring will be required to keep criminals out of any new TLD. We will watch the new TLD introductions carefully to report noteworthy events.

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 53,685 phishing domains, **we identified 12,173 domain names that we believe were registered maliciously by phishers. This is double the 5,835 found in 2H2012. The increase is due to a sudden increase in domain registrations by Chinese phishers.** The other 41,532 domains were almost v call hacked or compromised on vulnerable Web hosting.

Of the 12,173 malicious registrations, at least 8,240 (68%) were registered to phish Chinese targets—services and sites in China that serve a primarily Chinese customer base.[7] Chinese phishers have always preferred to register domains more than other phishers, relying upon hacked domains and compromised Web servers less often than phishers elsewhere. The 1H2013 registrations show Chinese phishers increasingly hungry for resources. The major targets included Taoao.com, the Industrial and Commercial Bank of China (ICBC), CCTV, ZJSTV, and Tencent. The domains were registered at primarily Chinese registrars (see pages 14-15) but also American registrars, and were hosted in China, the US, and elsewhere. The phishers used only 122 .CN domains, preferring the easier availability of other TLDs such as .TK, .COM, .INFO, and even some .US domains.

On top of that, Chinese phishers registered at least 450 additional domains to attack targets outside of China, mainly the game sites for Battle.net, Runescape, and World of Warcraft.

Observers outside of China did not detect most of the phish that CNNIC/APAC did inside of China, possibly because they are not parsing Chinese-language emails effectively, or do not have enough Chinese customers to justify setting up in-country honeypots. Whatever the case, the phishing takes advantage of registration, hosting, and payment infrastructures in different countries, and everyone ends up losing--except the phishers.

Almost 82 percent of the 12,173 malicious domain registrations were made in just three TLDs: .COM (6,477), .TK (2,801), and .INFO (655). The .COM registry has no anti-abuse program. The .TK registry offers free domain name registrations. It also gives accredited interveners the ability to directly suspend .TK domains in the registry. (These partners include Facebook, Internet Identity, and the Anti-Phishing Alliance of China.) While this speeds takedowns, it does not prevent phishing from occurring. The .INFO registry operator has an abuse response program, but the TLD remains inexpensive compared to others, a factor which has historically attracted abuse.

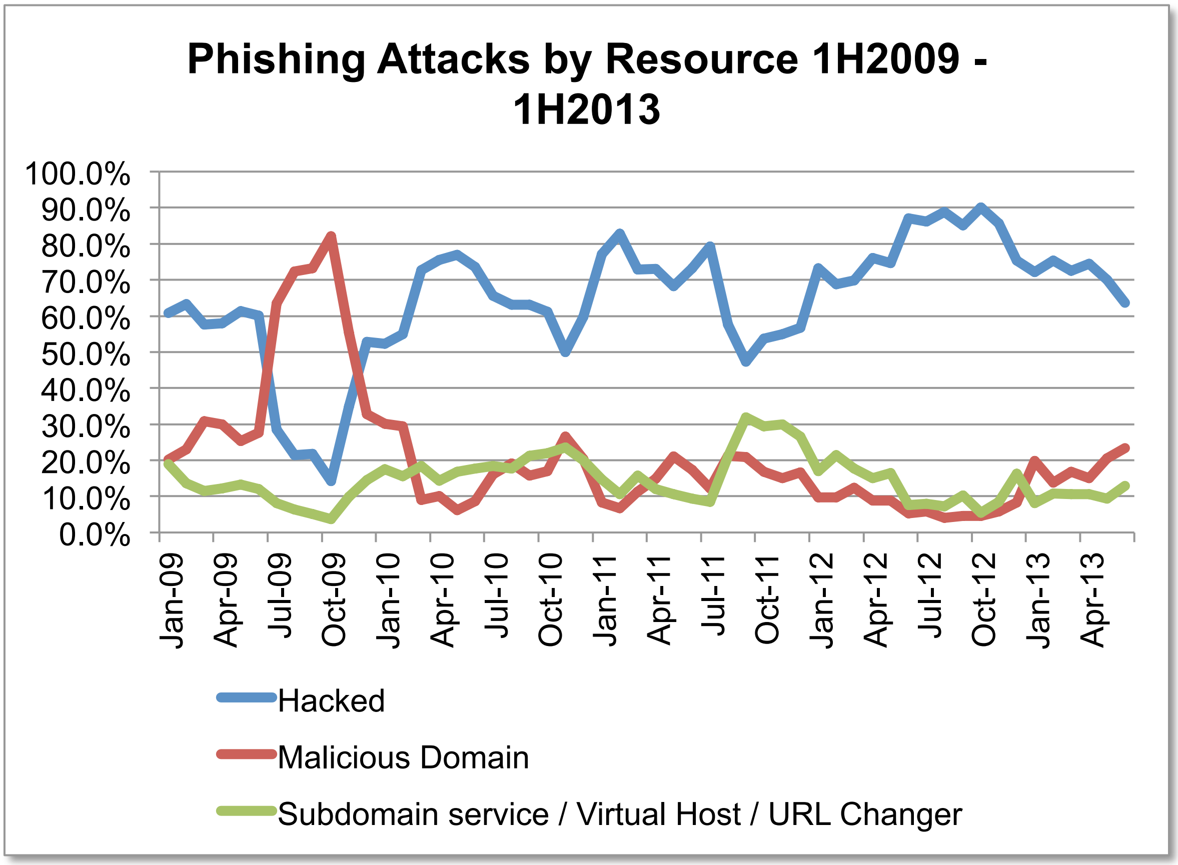
Of the 12,173 maliciously registered domains, just 1,244 contained a relevant brand name or reasonable variation thereof—often a misspelling.[8] This is the same number as we found

[7] These phishing attacks were primarily advertised by e-mail lures written in Chinese. Other factors about these attacks also point to perpetrators in China.

[8] 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).

in 2H2012. **This represents just 2.3 percent of all domains that were used for phishing, and 10 percent of all maliciously registered domains recorded in the sampling period.** The registrations by Chinese phishers often consisted of nonsense strings.

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 their brand 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 often 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. And increasingly, brand owners and legitimate mailers use custom tracking domains and special-offer domains for their marketing campaigns—domains that are very different from the brand owner's "home" or most familiar domain name anyway. Again, this is a factor that phishers can exploit – the domain simply doesn't matter when socially engineering potential victims.



Registrars Used for Malicious Domain Registrations

Phishers (especially Chinese phishers) registered significantly more domain names in 1H2013. Where are the phishers registering these domains? We were able to obtain the name of the sponsoring registrar for 11,514 of the 12,173 (95%) of the gTLD and ccTLD domains that were registered exclusively to support phishing. This research was made possible via WHOIS data captured by DomainTools.com, for which we thank DomainTools. Domains-under-management numbers were compiled by examining ICANN reports and other resources.

Phishers utilized at least 267 registrars in 1H2013—at least 127 more than in 2H2012. The registrar marketplace is diverse. One major player, GoDaddy, holds roughly half of the gTLD market share, but had only 8 percent of the malicious phishing registrations. Some registrars also support reseller programs, through which many of these domains were sold, but the authors were not able to discern reseller identities because it is not available in the WHOIS records.

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 15 registrars below accounted for 66 percent (8,059) of the domains registered maliciously.

Top Phishing Registrars by Malicious Domain Score, 1H2013

All registrars must have more than 25 malicious phishing registrations and 50,000 gTLD domain names under management

Rank	Registrar	Malicious Domains	Domains at registrar, May 2013	Malicious Domains per 10,000
1	Shanghai Yovole Networks Inc. *(China)*	1,235	332,064	37.2
2	Hang Zhou E-Business Services Co. Ltd. *(China)*	177	104,741	16.9
3	Beijing Innovative Linkage Technology Ltd. dba DNS.com.cn *(China)*	607	405,491	15.0
4	Jiangsu Bangning Science & Technology Co. Ltd *(China)*	572	390,053	14.7
5	Web Commerce Communications dba Webnic.cc *(Malaysia)*	160	318,678	5.0

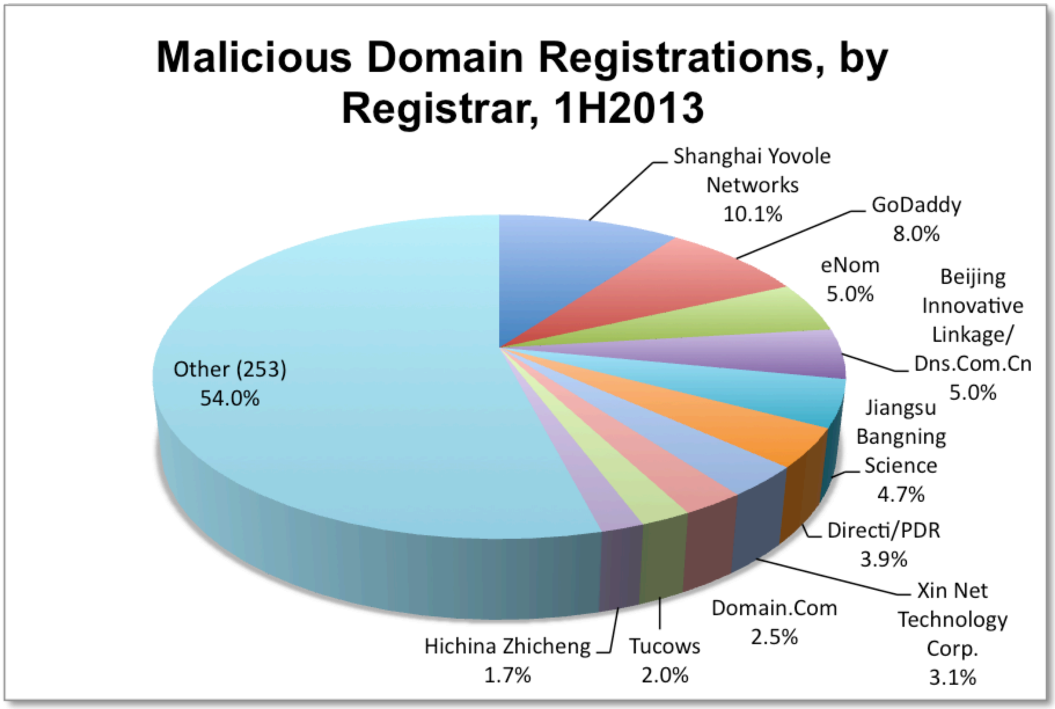
Rank	Registrar	Malicious Domains	Domains at registrar, May 2013	Malicious Domains per 10,000
6	1API GmbH *(Germany)*	113	241,203	4.7
7	Xin Net Technology Corporation *(China)*	382	1,459,147	2.6
8	Bizcn.Com Inc. *(China)*	125	505,802	2.5
9	DotTK	2,801	16,100,000	1.7
10	Domain.com LLC dba Dotster *(USA)*	310	2,036,287	1.5
11	PDR Ltd. dba Publicdomainregistry.com *(India)*	478	3,147,935	1.5
12	Hichina Zhicheng Technology Ltd *(China)*	208	1,669,183	1.2
13	OVH *(France)*	113	1,418,822	0.8
14	Register.com *(USA)*	166	2,627,028	0.6
15	eNom *(USA)*	612	11,751,759	0.5

Just under a quarter of the world's malicious registrations were made at the .TK registry, which also serves as the registrar for those domains and offers domains for free. Due to the large number of domains in the registry, the relative rate of malicious registrations at .TK was 1.7 per 10,000.

Continuing a trend, eight of the top twelve registrars are located in China. This was due to the fact that Chinese phishers tend to register domain names for their phishing, and often used Chinese registrars. Domains registered at the Chinese registrars were often used to phish Chinese targets such as Alibaba, Taobao.com, and CCTV, 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, but the majority took place at registrars within China. Phishers registered 165 .CN domains for phishing, almost exclusively through Chinese registrars, a number up substantially from 2H2012.

One registrar stood far apart from the rest: Shanghai Yovole Networks Inc. (http://www.yovole.com/), which retained its top position on this list. While its score improved considerably from 749 per 10,000 to 37 per 10,000, that appears to be the result of many more domains under management, of which a good portion have been tied to other abusive before. Three other Chinese registrars had scores above 10. Chinese registrars continue having difficulty keeping miscreants from registering gTLD domains via their services. The use of Chinese registrars is disturbing, and the authors recommend that Chinese registrars implement the APWG's "Anti-Phishing Best Practices Recommendations for Registrars."

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 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 yet again in 1H2013. Phishers registered far fewer subdomains than they registered "regular" domain names, because the latter were so popular with Chinese phishers. **However, subdomain registrations still represent 10 percent of all phishing attacks.** We continue to see phishers seeking new providers that they can exploit.

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

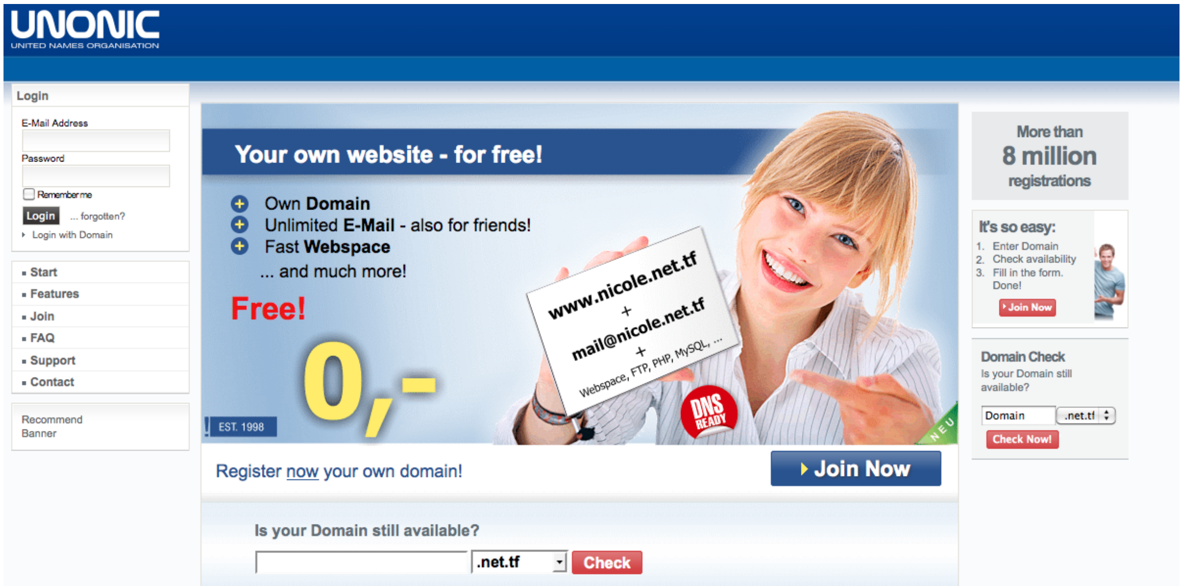
Use of subdomain services continues to be a challenge, because many of the services are free, offer anonymous registration, and only the subdomain providers themselves can effectively mitigate these phish.[9] While many of these services are responsive to complaints, proactive measures to keep criminals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

[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.

There were 7,134 phishing attacks hosted on subdomain services in the first half of 2013, on 6,465 unique subdomains. This was a 14 percent decrease from the 8,294 attacks we recorded in 2H2012, but still represented 10 percent of all 1H2013 phishing attacks. Despite usage of subdomains for phishing growing in proportion to the overall techniques used, the absolute number of subdomains did continue to decline. 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 saw a large new number of subdomain services being abused by phishers. **More than 270 subdomain service domains were abused in 1H2013 that we had never seen in prior reports**. Approximately 1,270 attacks were seen on these "new" domains to the phishing world. Clearly, if you run a subdomain reselling service, it is likely that phishers will "test-drive" your service to launch attacks.

The favorite service for phishers to abuse in 1H2013 was UNONIC, where at least 865 malicious subdomains were spotted. This service has not previously been noticed as a major source of malicious subdomains, showing that phishers will take advantage of any service they find is vulnerable. This German company provides "free" registration services and has many different subdomains that can be registered under the .tf (French Southern and Antarctic Lands) TLD. The service has a very professional website and a "Report Abuse" feature, so it is somewhat surprising that it has abused so heavily in the first half of 2013. This may indicate that may indicate that this service's "up-front" preventative processes aren't deterring phishers.



Second on the list was a provider that has been seen as a highly abused service previously – 3owl.com. This service exemplifies many things that are "broken" on the Internet today, as it is completely unclear where this service is actually based and if the people involved do anything to curtail abuse. The WHOIS record for the domain is "privacy protected" on a GoDaddy domain, and the website does not provide direct contact information. Beyond that, the privacy policy and "About Us" sections of the website are circular links to advertisements, telling the consumer nothing about the actual service. There is a way to report abuse, but it is unclear whether anyone actually pays attention to submissions.

Also of interest is the blogging service run by Google: BlogSpot.com. While there were no particular subdomains abused more heavily than others, the cumulative number of phishing sites discovered under this Google service topped 300 in the first half of 2013. Google has had long-standing problems dealing with abuse reports in a timely manner.

Top 20 Subdomain Services Used for Phishing, 1H2013

Rank	Attacks	Domain	Provider
1	833	net.tf	UNONIC.COM
2	347	3owl.com	3owl.com
3	290	usa.cc	freeavailabledomains.com
4	240	nazuka.net	nazuka.net
5	226	altervista.org	altervista.org
6	193	my3gb.com	my3gb.com
7	155	kmdns.net	kmdns.net
8	137	3eeweb.com	3eeweb.com
9	92	p.ht	Hostinger
10	89	cixx6.com	cixx6.com
11	81	wink.ws	wink.ws
12	66	instantfreesite.com	instantfreesite.com
13	62	5gbfree.com	5gbfree.com
14	62	chickenkiller.com	chickenkiller.com
15	55	fav.cc	fav.cc
16	55	ias3.com	ias3.com
17	50	co.vu	co.vu
18	48	oicp.net	Oray
19	46	hol.es	Hostinger
20	45	vicp.cc	Oray

We know of over 800 subdomain registration providers, which offer services on more than 3,800 domain names. 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.

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.

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. From January 2007 to December 2012 we found only five homographic phishing attacks.

In spring 2013, there were three homographic attacks:

xn--paypl-uqa.com → paypàl.com
xn--tunes-4sa.eu → îtunes.eu
xn--tunes-bta.fr → ïtunes.fr

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.

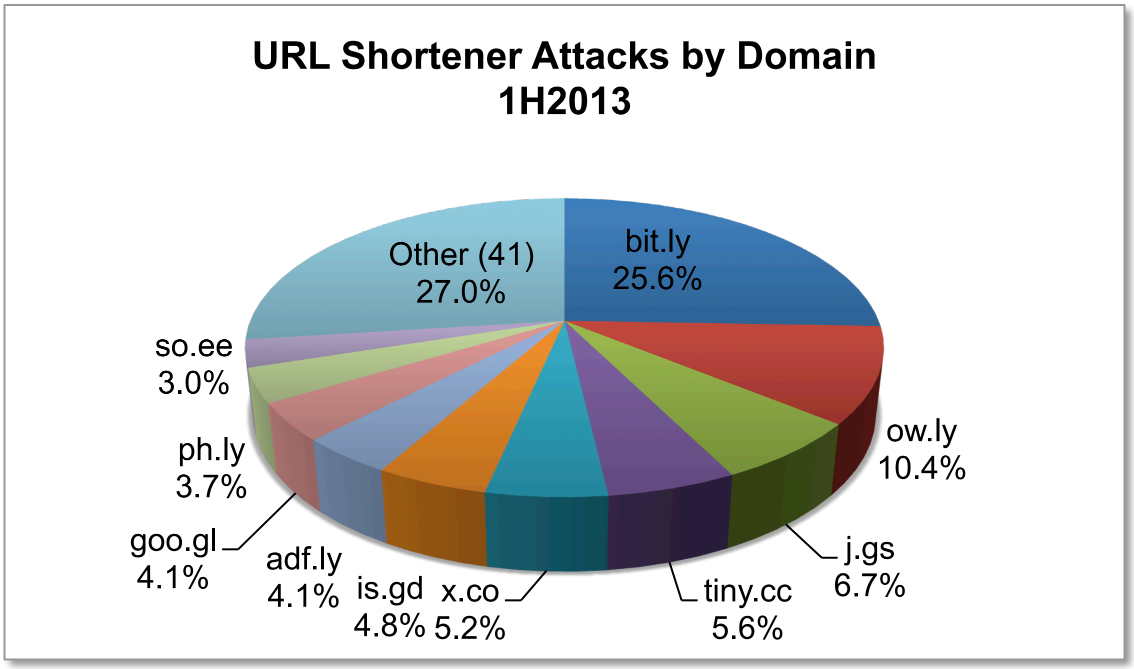
In late 2013 and beyond, new IDN registries will be awarded to a wider range of operators, and so we will continue to monitor for interesting trends.

Use of URL Shorteners for Phishing

Phishers continue to use "URL shortening" services to obfuscate phishing URLs, but such use plummeted to only 270 attacks in 1H2013, sharply down from 785 in 2H2012. 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.

This may be evidence that most of the major URL shortener providers have put better screening for malicious forwarding destinations and are making it easier and more efficient to report abuse. 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 and continue to improve them.

SURBL (http://www.surbl.org) provides free information on abusive use of shortener services, and all URL shortener services should consider signing up for this feed of malicious URLs in order to mitigate abuse on their services. Large numbers of shortened URLs are being seen in conjunction with malware exploit kit sites, and while outside the scope of this report gives us pause that this problem is truly "solved" at this point.



In our previous report, over 65 percent of malicious shortened URLs used for phishing were found at a single provider – tinyURL.com. This is an extremely popular service, but had limited support and no reporting tool available on its website. Apparently they either must have listened to someone, as they barely made this report at all. Hopefully this is a permanent fix and will prove beneficial to both their company and the entire community. During 1H2013, what little abuse there is of shorteners is spread fairly widely, with the industry dominating bit.ly having about a quarter of the abusive phishing redirectors.

A Word About Spear-Phishing

This report measures attacks that targeted the general public. It does not attempt to quantify spear-phishing, which are attacks directed at a few specific individuals. Because they involve a very small number of e-mail lures, and sometimes target company-internal systems, spear-phishing attempts are generally not reported and it is unknown how many take place.

Spear-phishing continues to be an important tool for:

- Criminals who are perpetrating financial crimes. For example, targeted university employees have given up passwords that allowed phishers to redirect payroll deposits.
- Spies involved in corporate and government espionage. In February 2013, security company Mandiant documented spear-phishing by Chinese military hackers.
- Hacktivists who seek publicity for their causes. On August 27 2013, members of the pro-Assad Syrian Electronic Army used crude but effective spear-phishing attacks to obtain the login credentials of a domain name reseller. The SEA then used that access to redirect the domains of The New York Times, among others.

Appendix: Phishing Statistics and Uptimes by TLD

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
ac	Ascension Island	2	2	16100	1.2	1.2	2:49	2:49		
ad	Andorra			1500						
ae	United Arab Emirates	42	23	102,000	2.3	4.1	245:15	56:38	2	0.2
aero	sponsored TLD	2	2	8,586	2.3	2.3	8:10	8:10		
af	Afghanistan									
ag	Antigua and Barbuda	1	1	19,598	0.5	0.5	185:27	185:27		
ai	Anguilla	2	2	3,900	5.1	5.1	16:11	16:11		
al	Albania	1	1	7,500	1.3	1.3	0:18	0:18		
am	Armenia	57	9	22,327	4.0	25.5	17:30	2:15	1	0.4
an	Netherlands Antilles			800						
ao	Angola			300						
ar	Argentina	493	425	2,900,000	1.5	1.7	38:33	14:52	6	0.0
arpa	Advanced Research Project Agency									
as	American Samoa									
asia	sponsored TLD	361	240	474,322	5.1	7.6	31:52	7:58	171	3.6
at	Austria	74	60	1,201,000	0.5	0.6	59:32	16:47		
au	Australia	865	767	2,639,461	2.9	3.3	49:59	12:18	17	0.1
aw	Aruba	3	1	625	16.0	48.0	145:23	139:37		
ax	Åland Islands									
az	Azerbaijan	5	4	17,950	2.2	2.8	40:19	5:32		
ba	Bosnia and Herzegovina	20	12	14,589	8.2	13.7	33:11	22:54	1	0.7
bd	Bangladesh	23	15	5,000	30.0	46.0	35:27	22:21		
be	Belgium	200	157	1,368,637	1.1	1.5	54:50	14:50	11	0.1
bf	Burkina Faso	1	1				12:50	12:50		
bg	Bulgaria	9	7	25,000	2.8	3.6	13:30	4:21		
bh	Bahrain			4,450						
biz	generic TLD	436	324	2,400,109	1.3	1.8	37:15	18:12	52	0.2

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
bm	Bermuda			8,100						
bn	Brunei Darussalam	1	1	1,150	8.7	8.7	538:29	538:29		
bo	Bolivia	8	5	8,350	6.0	9.6	24:15	9:16		
br	Brazil	3,668	2,669	3,265,768	8.2	11.2	45:21	15:31	114	0.3
bs	Bahamas			2,320						
bt	Bhutan	11	9	1,090	82.6	100.9	29:52	16:08		
bw	Botswana									
by	Belarus	50	37				67:27	17:42	3	
bz	Belize	5	5	44,703	1.1	1.1	18:16	18:47	1	0.2
ca	Canada	500	407	2,042,762	2.0	2.4	53:38	15:42	10	0.0
cat	sponsored TLD	13	11	65,543	1.7	2.0	245:31	30:03	1	0.2
cc	Cocos (Keeling) Islands *(estimated)*	573	70	800,000	0.9	7.2	45:51	6:02	16	0.2
cd	Congo, Democratic Repub. *(estimated)*	3	3	5,200	5.8	5.8	103:18	66:57		
cf	Central African Republic									
cg	Congo									
ch	Switzerland	114	85	1,774,262	0.5	0.6	72:45	17:16	2	0.0
ci	Côte d'Ivoire			2,500						
cl	Chile	494	357	418,558	8.5	11.8	51:23	16:29	8	0.2
cm	Cameroon *(estimated)*	9	6	12,500	4.8	7.2	21:51	0:00		
cn	China	491	387	7,544,052	0.5	0.7	29:53	10:56	165	0.2
co	Colombia	311	263	1,386,328	1.9	2.2	24:53	12:56	26	0.2
com	generic TLD	34,867	27,684	111,163,489	2.5	3.1	43:26	12:27	6,479	0.6
coop	sponsored TLD	2	2	9,983	2.0	2.0	30:18	30:18		
cr	Costa Rica	8	7	14,800	4.7	5.4	8:02	5:35		
cu	Cuba			2,370						
cv	Cape Verde			900						
cx	Christmas Island	15	6	5,250	11.4	28.6	5:42	2:40		
cy	Cyprus	1	1	12,500	0.8	0.8				
cz	Czech Republic	111	73	1,048,161	0.7	1.1	67:08	12:33		
de	Germany	914	771	15,397,225	0.5	0.6	56:03	15:57	121	0.1
dj	Djibouti									
dk	Denmark	172	113	1,242,409	0.9	1.4	63:01	19:08	2	0.0

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
dm	Dominica			14,500						
do	Dominican Republic	21	13				22:19	19:05	1	
dz	Algeria	1	1	4,665	2.1	2.1	34:06	34:06		
ec	Ecuador	64	48	30,500	15.7	21.0	28:31	13:31	1	0.3
edu	U.S. higher education	13	7	7,590	9.2	17.1	31:49	13:35		
ee	Estonia	33	21	69,750	3.0	4.7	34:00	22:04		
eg	Egypt	2	2	6,000	3.3	3.3				
er	Eritrea			120						
es	Spain	305	202	1,648,082	1.2	1.9	44:56	7:53	6	0.0
et	Ethiopia	1	1	1,200	8.3	8.3				
eu	European Union	325	275	3,723,077	0.7	0.9	35:49	12:08	53	0.1
fi	Finland	35	22	316,422	0.7	1.1	203:58	78:45		
fj	Fiji	5	2	4,000	5.0	12.5				
fk	Falkland Islands			105						
fm	Micronesia, Fed. States	10	9				26:05	7:55		
fo	Faroe Islands									
fr	France	451	325	2,601,215	1.2	1.7	61:35	18:13	31	0.1
gd	Grenada	17	3	4,400	6.8	38.6	19:45	8:38		
ge	Georgia	61	41	20,300	20.2	30.0	101:25	89:04	6	3.0
gg	Guernsey	30	4							
gh	Ghana	5	2				32:38	20:38		
gi	Gibraltar			2,033						
gl	Greenland	13	2	5,500	3.6	23.6	32:01	1:07		
gm	Gambia									
gov	U.S. government	1	1	5,000	2.0	2.0	21:59	21:59		
gp	Guadeloupe	10	8	1,475	54.2	67.8	10:08	7:29		
gr	Greece *(estimated)*	203	162	377,000	4.3	5.4	58:48	13:04	6	0.2
gs	South Georgia & Sandwich Is.	24	5	8,160	6.1	29.4	25:06	9:42	1	1.2
gt	Guatemala	14	11	11,900	9.2	11.8	58:24	9:04	1	0.8
gy	Guyana	7	1	2,300	4.3	30.4				
hk	Hong Kong	34	17	245,151	0.7	1.4	125:01	26:47	4	0.2
hm	Heard and McDonald Is.									
hn	Honduras	3	1	6,300	1.6	4.8	40:54	26:55	1	1.6
hr	Croatia	30	29	79,094	3.7	3.8	27:31	12:26		

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
ht	Haiti	94	3	2,200	13.6	427.3	23:45	0:00		
hu	Hungary	190	143	631,189	2.3	3.0	72:56	18:29	4	0.1
id	Indonesia	98	72	109,000	6.6	9.0	30:10	9:16	1	0.1
ie	Ireland	88	64	183,550	3.5	4.8	84:19	19:10	1	0.1
il	Israel	55	44	237,155	1.9	2.3	55:16	14:26	1	0.0
im	Isle of Man	13	9				28:36	20:57	1	
in	India	686	564	1,283,554	4.4	5.3	39:11	12:30	75	0.6
info	generic TLD	1,561	1,308	6,774,502	1.9	2.3	30:00	11:17	655	1.0
int	sponsored TLD									
io	British Indian Ocean Terr.	3	2							
IP address	(no domain name used)	1,972								
iq	Iraq			450						
ir	Iran	188	150	393,689	3.8	4.8	21:22	9:36	11	0.3
is	Iceland	13	12	42,500	2.8	3.1	42:25	13:10		
it	Italy	383	307	2,500,000	1.2	1.5	73:39	20:53	8	0.0
je	Jersey									
jm	Jamaica	2	1	6,400	1.6	3.1				
jo	Jordan	2	1	4,341	2.3	4.6	34:14	34:14		
jobs	sponsored TLD	0	0	44,057						
jp	Japan	111	89	1,334,594	0.7	0.8	55:07	15:10	3	0.0
ke	Kenya	60	48	25,345	18.9	23.7	42:47	20:45	6	2.4
kg	Kyrgyzstan	1	1	5,300	1.9	1.9				
kh	Cambodia	7	7	1,600	43.8	43.8	10:26	11:37		
ki	Kiribati									
kn	Saint Kitts And Nevis	4	4				51:26	15:02		
kr	Korea	260	147	1,173,900	1.3	2.2	59:13	16:47	4	0.0
kw	Kuwait	1	1	3,350	3.0	3.0	10:43	10:43		
ky	Cayman Islands	1	1				3:39	3:39		
kz	Kazakhstan	67	55	88,608	6.2	7.6	20:59	15:02	1	0.1
la	Lao People's Demo. Rep. *(domains estimated)*	8	6	9,000	6.7	8.9	52:18	7:44		
lb	Lebanon	2	1	3,500	2.9	5.7	11:20	11:20		
lc	St. Lucia	11	9	3,784	23.8	29.1	30:26	1:09		
li	Liechtenstein	2	1	69,500	0.1	0.3	26:45	26:45		

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
lk	Sri Lanka	11	10	8,500	11.8	12.9	199:56	30:48		
ls	Lesotho									
lt	Lithuania	32	31	156,500	2.0	2.0	37:25	19:20	3	0.2
lu	Luxembourg	10	8	74,500	1.1	1.3	83:56	59:44		
lv	Latvia	45	33	105,500	3.1	4.3	27:05	11:37	2	0.2
ly	Libya	126	11	13,574	8.1	92.8	30:03	9:45	2	1.5
ma	Morocco	44	33	43,299	7.6	10.2	118:38	15:37	3	0.7
mc	Monaco	1	1	2,370	4.2	4.2	65:13	65:13		
md	Moldova	14	12	22,736	5.3	6.2	70:26	20:48		
me	Montenegro	246	90	678,096	1.3	3.6	32:14	7:43	11	0.2
mg	Madagascar	1	1							
mk	Macedonia	22	18	2,266	79.4	97.1	40:49	7:54		
ml	Mali	1	1				37:53	37:53		
mn	Mongolia	17	13	14,551	8.9	11.7	27:00	9:40		
mo	Macao	8	5	305	163.9	262.3	910:50	1313:49		
mobi	sponsored TLD	60	44	1,078,020	0.4	0.6	25:22	10:02	5	0.0
mp	Northern Mariana Islands									
mr	Mauritania	1	1				7:55	7:55		
ms	Montserrat	113	11	9,800	11.2	115.3	27:35	17:32		
mt	Malta *(estimated)*	1	1	6,250	1.6	1.6	149:59	149:59		
mu	Mauritius	74	4	7,500	5.3	98.7	19:12	2:03		
museum	sponsored TLD			435						
mv	Maldives	1	1				166:27	166:27		
mx	Mexico	321	254	669,414	3.8	4.8	71:13	15:55	26	0.4
my	Malaysia	153	112	202,869	5.5	7.5	38:49	12:57	5	0.2
mz	Mozambique	0	0	4,000						
na	Namibia	1	1							
name	generic TLD	52	40	214,831	1.9	2.4	22:41	6:36	9	0.4
nc	New Caledonia	2	1				43:21	43:21		
ne	Niger									
net	generic TLD	4,640	3,228	15,449,095	2.1	3.0	40:39	11:04	560	0.4
nf	Norfolk Island	12	3	1,600	18.8	75.0	40:25	3:06		
ng	Nigeria	12	12	12,500	9.6	9.6	35:00	20:33	2	1.6
ni	Nicaragua	0	0	6,600						

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
nl	Netherlands	443	375	5,243,494	0.7	0.8	35:19	10:46	31	0.1
no	Norway	80	56	581,386	1.0	1.4	71:29	20:33		
np	Nepal	97	64	32,500	19.7	29.8	95:37	21:45		
nr	Nauru	1	1	450	22.2	22.2				
nu	Niue *(domains estimated)*	59	24	100,000	2.4	5.9	56:37	0:34	2	0.2
nz	New Zealand	102	86	530,479	1.6	1.9	35:23	10:40	1	0.0
om	Oman	2	2				22:23	22:23	1	
org	generic TLD	2,743	2,032	10,258,953	2.0	2.7	31:09	12:03	226	0.2
pa	Panama	2	2	7,200	2.8	2.8	6:03	6:03		
pe	Peru	143	107	69,505	15.4	20.6	29:41	19:22	2	0.3
pf	French Polynesia	2	1							
ph	Philippines *(operator declines to provide DUM)*	28	20				42:33	17:37		
pk	Pakistan *(operator declines to provide DUM)*	238	176				35:38	13:47	2	1.1
pl	Poland	720	507	2,440,637	2.1	3.0	50:10	14:58	18	0.1
pn	Pitcairn	65	6				3:26	4:11		
post	sponsored TLD			8						
pro	sponsored TLD	33	24	156,639	1.5	2.1	24:37	8:32	3	0.2
ps	Palestinian Territory	5	5	7,150	7.0	7.0	30:48	21:46		
pt	Portugal	114	86	236,950	3.6	4.8	66:53	19:01	6	0.3
pw	Palau	115	109	55,000	19.8	20.9	31:13	12:41	94	17.1
py	Paraguay	19	18	14,520	12.4	13.1	17:28	11:22	2	1.4
qa	Qatar	1	1	15,008	0.7	0.7				
re	Réunion	3	3	20,826	1.4	1.4	11:00	13:25	2	1.0
ro	Romania	341	259	641,700	4.0	5.3	60:02	11:18	4	0.1
rs	Serbia	59	45	77,133	5.8	7.6	47:41	16:52	3	0.4
ru	Russian Fed.	1,011	772	4,510,050	1.7	2.2	52:53	13:22	78	0.2
rw	Rwanda									
sa	Saudi Arabia	40	33	30,400	10.9	13.2	30:25	20:00		
sc	Seychelles	1	1	4,915	2.0	2.0	16:11	16:11	1	2.0
sd	Sudan	10	9				5:06	7:01		
se	Sweden	167	127	1,281,322	1.0	1.3	73:38	16:37	1	0.0
sg	Singapore	83	52	148,001	3.5	5.6	114:58	18:52	3	0.2

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
sh	Saint Helena	3	1	3,000	3.3	10.0	134:39	136:37	1	3.3
si	Slovenia	219	196	108,100	18.1	20.3	47:20	6:27		
sk	Slovakia	67	41	292,572	1.4	2.3	86:23	14:35		
sl	Sierra Leone									
sm	San Marino	0	0	1,905						
sn	Senegal	1	1	3,500	2.9	2.9	45:29	45:29		
so	Somalia	9	5				190:01	140:25	4	
sr	Suriname	1	1							
st	Sao Tome and Principe	2	2				3:39	3:39		
su	Soviet Union	73	31	120,100	2.6	6.1	33:47	9:09	2	0.2
sv	El Salvador	10	9	6,500	13.8	15.4	62:21	18:45		
sy	Syria									
sz	Swaziland									
tc	Turks and Caicos	8	3				5:09	5:09		
tel	generic TLD	0	0	211,979						
tf	French Southern Territories	949	14	1,550	90.3	6122.6	38:31	22:38	1	6.5
tg	Togo									
th	Thailand	166	125	65,350	19.1	25.4	27:43	13:21	2	0.3
tj	Tajikistan	2	2	6,200	3.2	3.2	29:34	29:34		
tk	Tokelau	3,077	2,802	16,100,000	1.7	1.9	17:38	7:19	2,801	1.7
tl	Timor-Leste	3	3				2:54	2:43		
tm	Turkmenistan	43	4	3,780	10.6	113.8	31:33	21:16	1	2.6
tn	Tunisia	15	12	16,950	7.1	8.8	115:56	42:16		
to	Tonga	24	13	15,500	8.4	15.5	60:49	36:43		
tp	Portuguese Timor									
tr	Turkey	193	153	333,508	4.6	5.8	43:58	17:39	3	0.1
travel	sponsored TLD	0	0	20,671						
tt	Trinidad and Tobago			2,525						
tv	Tuvalu *(estimated)*	69	55	175,000	3.1	3.9	27:24	13:45	1	0.1
tw	Taiwan	85	64	630,550	1.0	1.3	77:46	25:05	4	0.1
tz	Tanzania	10	8	6,220	12.9	16.1	66:32	23:15		
ua	Ukraine	289	246	700,013	3.5	4.1	30:37	12:06	10	0.1
ug	Uganda	23	11	3,200	34.4	71.9	65:22	31:16	1	3.1
uk	United Kingdom	1,018	870	10,420,705	0.8	1.0	45:13	13:50	61	0.1

TLD	TLD Location	Unique Phishing Attacks 1H2013	Unique Domain Names used for Phishing 1H2013	Domains in Registry, April 2013	Score: Phishing Domains per 10,000 Domains 1H2013	Score: Attacks per 10,000 Domains 1H2013	Average Uptime 1H2013 hh:mm	Median Uptime 1H2013 hh:mm	Total Malicious Domains Registered 1H2013	Malicious Registrations score/10,000 domains in registry
us	United States	335	260	1,795,000	1.4	1.9	37:33	8:59	67	0.4
uy	Uruguay	16	16	74,605	2.1	2.1	31:21	16:37	1	0.1
uz	Uzbekistan	5	4	16,387	2.4	3.1	17:49	0:58		
vc	St. Vincent and Grenadines	9	5	8,692	5.8	10.4	25:01	9:13		
ve	Venezuela	102	67	215,000	3.1	4.7	54:26	13:00	4	0.2
vg	British Virgin Islands	5	2	8,600	2.3	5.8	0:17	0:05		
vi	Virgin Islands			17,500						
vn	Vietnam	117	85	386,803	2.2	3.0	45:04	9:59		
vu	Vanuatu	88	5				39:42	12:51		
wf	Wallis and Futuna	1	1				24:10	24:10		
ws	Samoa *(estimated)*	131	39	450,000	0.9	2.9	23:35	4:51	4	0.1
xn--3e0b707	.한국 (KR IDN)	0	0	91,300						
xn--90a3ac	.СРБ (Serbia IDN)	0	0	5,175						
xn--fzc2c9e2c	.□□□□ (Sri Lanka IDN)	0	0	150						
xn--mgberp4a5d4a	)Saudi Arabia IDN(السعودية.	0	0	1,850						
xn--o3cw4h	.ไทย (.TH IDN)	0	0	1,000						
xn--p1ai	.рф (.RF, Russian Federation IDN)	4	3	788,675	0.0	0.1	13:54	7:52		
xn--xkc2al3hye2a	.□□□□□□ (Sri Lanka IDN)			86						
xxx	sponsored TLD	3	3	108,337	0.3	0.3	99:21	99:21		
ye	Yemen			900						
yt	France									
za	South Africa	287	243	859,000	2.8	3.3	37:18	11:37	8	0.1
zm	Zambia	2	2				7:17	7:17		
zw	Zimbabwe	7	5	1,050	47.6	66.7	9:51	5:04		
	TOTALS	**72,758**	**53,685**	**260,987,759**					**12,175**	

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 Internet companies and top-level domain registry operators. 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. Greg serves a Co-Chair of the Anti-Phishing Working Group's Internet Policy Committee. 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). He was previously the Director of Key Account Management and Domain Security at Afilias. 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) and ICANN's Expert Working Group on gTLD Directory Services. 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 Digital PhishNet, a collaboration between industry and law enforcement, 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. 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.

#