Global Phishing Survey: Trends and Domain Name Use in 1H2014

January-June 2014

APWG

Unifying the
Global Response
To Cybercrime

Published 25 September 2014

An
APWG
Industry
Advisory

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

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 are criminal, but they do make rational decisions about how to go about their work. They're in it for the money, and they work to make their schemes as productive as possible while evading detection. To combat phishing we need to know what the phishers are doing, and how. Where is the phishing taking place? What companies are most vulnerable? Were the slew of new top-level domains a bonanza for phishers? By analyzing the phishing that took place in the first half of 2014, the authors have some answers, and those answers may surprise you.

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 2014 ("1H2014", 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. The authors 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. **Apple became the world's most-phished brand. (Page 7)**
2. **The introduction of new top-level domains did not have an immediate major impact on phishing. (Page 12)**
3. **Chinese phishers were responsible for 85% of the domain names that were registered for phishing. (Page 13)**
4. **Malicious domain and subdomain registrations continue at historically high levels, largely driven by Chinese phishers. (Page 13, Page 19)**
5. **The average uptimes of phishing attacks remain near historic lows, pointing to some success by anti-phishing responders. (Page 8)**
6. **The companies (brands) targeted by phishing targets were diverse, with many new targets, indicating that e-criminals are looking for new opportunities in new places. (Page 6)**
7. **Mass hackings of vulnerable shared hosting providers led to 20% of all phishing attacks. (Page 15)**

Key Statistics

Millions of phishing URLs were reported in 1H2014 but the number of unique phishing attacks and domain names used to host them was much smaller.[1] The 1H2014 data set

[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.

yielded the following statistics:

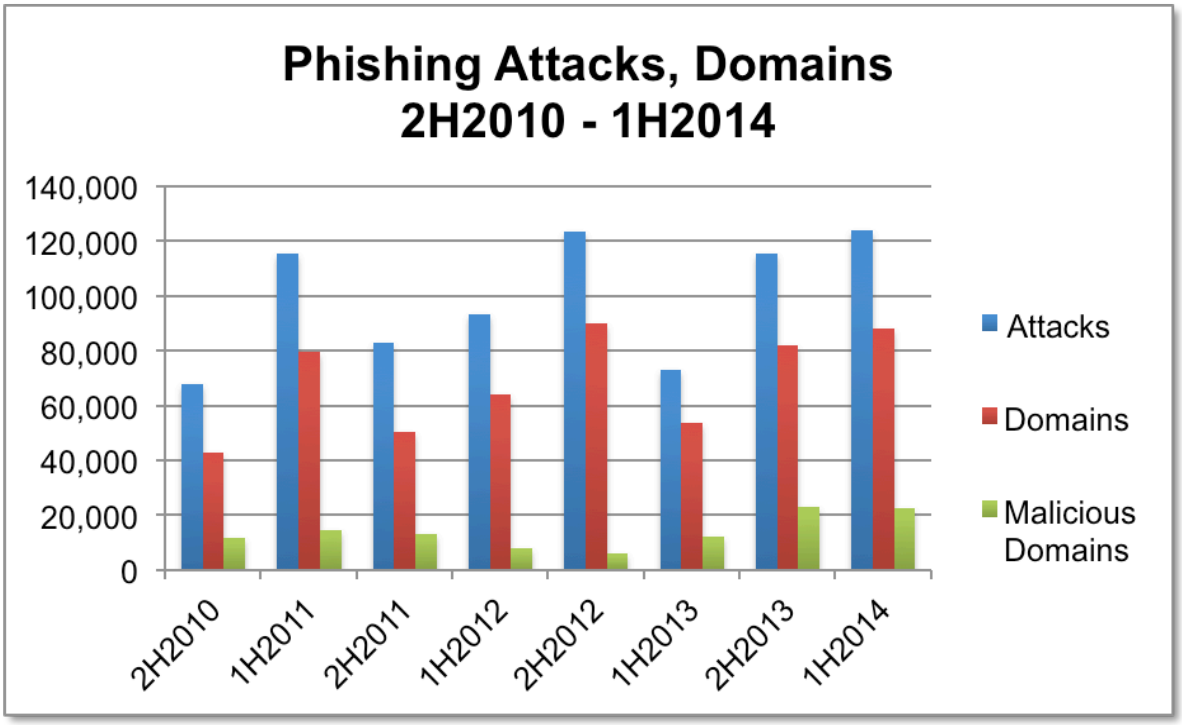
- **There were at least 123,741 unique phishing attacks worldwide**. **This is the most we have seen in a period since the second half of 2009**. Most of the growth in attacks came from increases in attacks against vulnerable hosting (shared virtual servers attacks, page 17) and also increased use of maliciously registered domains and subdomains. 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 87,901 unique domain names.**[2] This is up from the 82,163 domains used in 2H2013. The number of domain names in the world grew from 271.5 million in November 2013 to 279.5 million in April 2014.[3]
- Of the 87,901 phishing domains, **we identified 22,679 domain names that we believe were registered maliciously, by phishers.** This is almost the same number of found in 2H2013. **Most of these registrations were made by Chinese phishers, especially using free domain name registrations in certain TLDs.** The other 59,485 domains were almost all hacked or compromised on vulnerable Web hosting. Please see pages 13-15 for more detail.
- In addition**, 2,891 attacks were detected on 2,317 unique IP addresses, rather than on domain names.** (For example: http://77.101.56.126/FB/) We did not observe phish of any kind on IPv6 addresses.
- **We counted 756 targeted institutions, the highest number we have seen in any of our past studies**.
- **The average phishing attack uptime in 1H2014 was 32 hours and 32 minutes.** The median uptime in 1H2014 was 8 hours and 42 minutes, meaning that half of all phishing attacks stay active for less than 9 hours.
- **Phishing occurred in 227 top-level domains (TLDs), but 90% of the malicious domain registrations (20,565) were in just five TLDs**: .COM, .TK, .PW, .CF. and .NET. A small number of phishing attacks were seen in the new generic top-level domains that began launching in early 2014.
- **Only about 1.7% of all domain names that were used for phishing contained a brand name or variation thereof.** (See "Compromised Domains vs. Malicious Registrations" on page 15.)
- One hundred and twelve of the 87,901 domain names were internationalized domain names (IDNs). We observed one homographic attack.
- The use of URL shorteners for phishing has bounced back a bit, largely due to abuse at a single provider.

[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

	1H2014	2H2013	1H2013	2H2012	1H2012	2H2011
Phishing domain names	87,901	82,163	53,685	89,748	64,204	50,298
Attacks	123,741	115,565	72,758	123,476	93,462	83,083
TLDs used	227	210	194	207	202	200
IP-based phish (unique IPs)	2,317	837	1,626	1,981	1,864	1,681
Maliciously registered domains	22,679	22,679	12,173	5,833	7,712	12,895
IDN domains	112	82	78	147	58	36
Number of targets	756	681	720	611	486	487

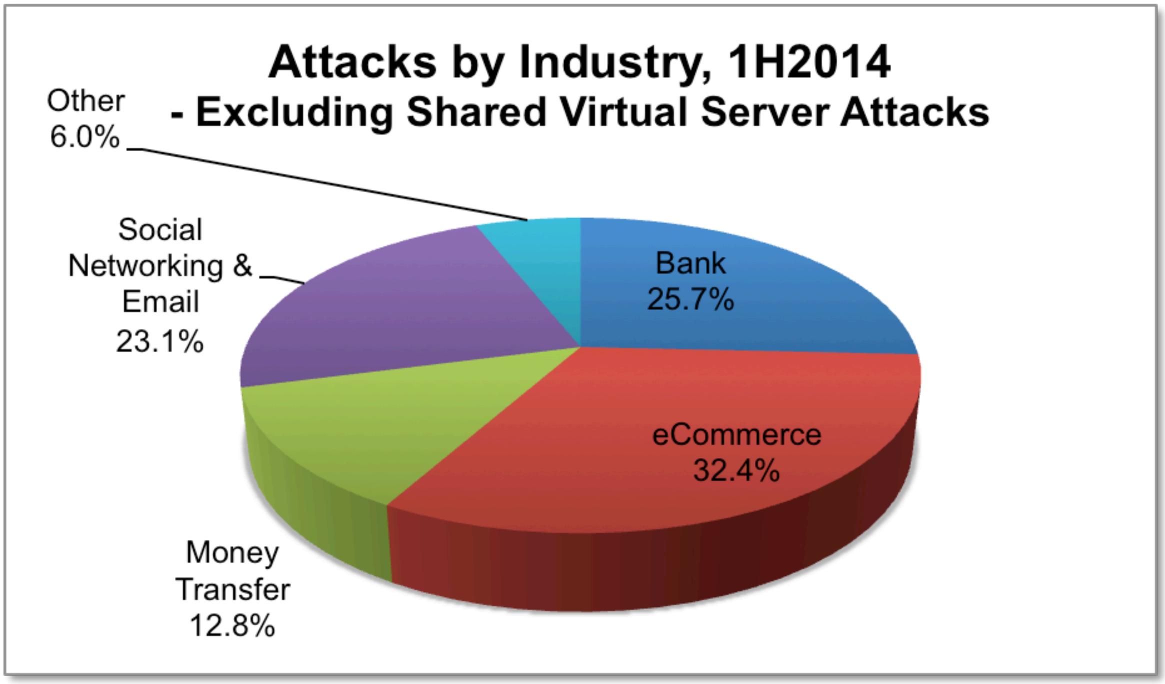


Target Distribution

We counted 756 unique target institutions during the period, up from the 681 found in 2H2013. Of the 756 targets that were phished in 1H2014, almost half of them — 347 to be precise — were not phished in 2H2013. This is amount of "churn" or turnover shows phishers trying out new targets. They are looking for companies that are newly popular, have vulnerable user bases, and/or are not ready to defend themselves against phishing.

It appears that almost any enterprise with an online presence can be a phishing target—if a site takes in personal data, then there may be phishers who want to exploit it. There was a notable variety among the 1H2014 targets, with phishers seeking user credentials to all sorts of Web sites.

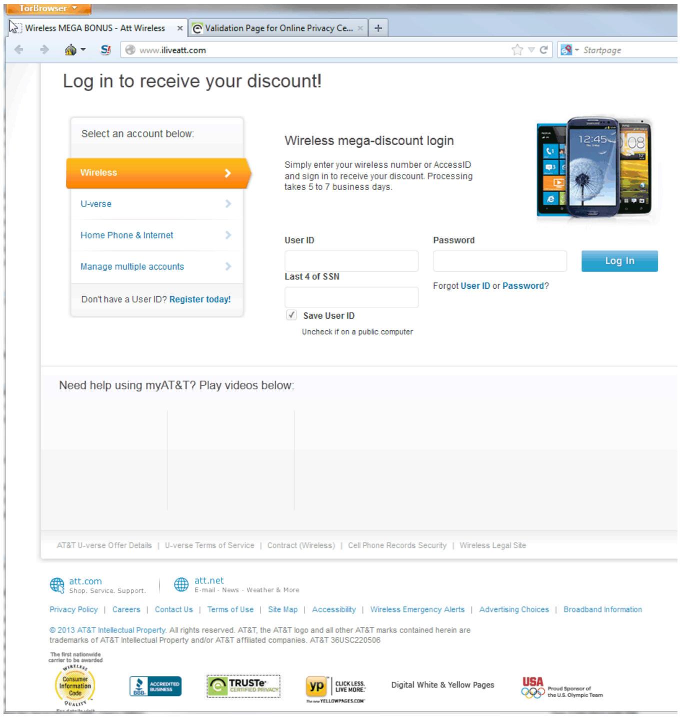
The targets included more large and small banks in Latin America, India, and the Middle East. The list included diverse sites such as real estate brokerage Century21, Bitcoin wallet provider Coinbase, Irish telecom provider Eircom, office space provider Regus, antivirus vendor Norton, cloud storage provider Box, luxury brand Gucci, and FIFA (the international governing body of soccer, which was targeted during the recent World Cup). Such wide distribution of targets could have many causes. Direct credit card theft is always a driver of course, and new targets with less risk exposure in consumers' minds always provide fresh opportunities. This often leads to monetization through reshipment fraud, an age-old tactic that has seen recent resurgence. Stealing access credentials from various online retailers usually leads to similar schemes. Phishers also steal credential from one site to harvest usernames and passwords for attacking other sites. Due to widespread poor consumer habits with password re-use, miscreants can often log into many other services once they obtain a victim's credentials from a single site.



The number of times that the targets were attacked follows a long tail. For the first time, Apple was the world's leading phishing target, with 21,951 attacks (17.7% of all attacks)

Perennial targets PayPal (17,811 attacks, or 14.4%) and Taobao.com (16,418 attacks, or 13.2%) were second and third. Half of the targets were attacked three or fewer times during the six-month period.

The phishing kits used by less sophisticated phishers tend to contain templates for popular targets. If a site is getting phished for the first time, it may have been targeted by a more sophisticated phisher, who had the skill and motivation to design and execute a new template.


TorBrowser
Wireless MEGA BONUS - Att Wireless
Validation Page for Online Privacy Ce...
www.iliveatt.com
Startpage

Log in to receive your discount!

Select an account below:

Don't have a User ID? Register today!

Wireless mega-discount login

Simply enter your wireless number or AccessID and sign in to receive your discount. Processing takes 5 to 7 business days.

User ID

Password

Log In

Last 4 of SSN

Forgot User ID or Password?

☑ Save User ID

Uncheck if on a public computer

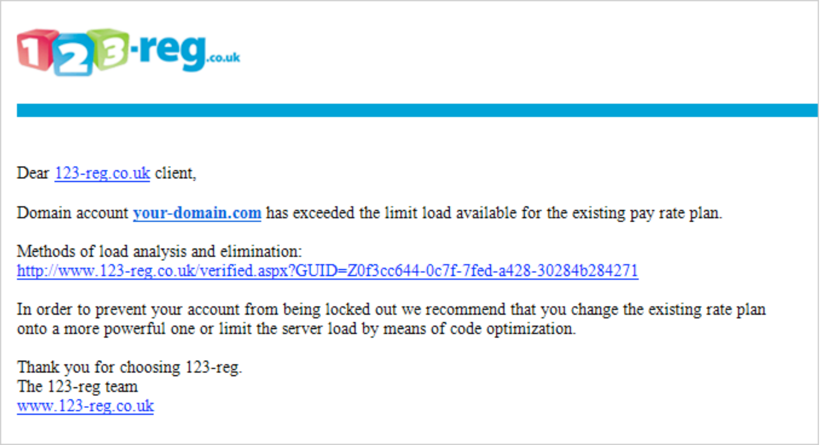
Need help using myAT&T? Play videos below:

AT&T U-verse Offer Details | U-verse Terms of Service | Contract (Wireless) | Cell Phone Records Security | Wireless Legal Site
att.com
Shop. Service. Support.
att.net
E-mail - News - Weather & More
Privacy Policy | Careers | Contact Us | Terms of Use | Site Map | Accessibility | Wireless Emergency Alerts | Advertising Choices | Broadband Information

© 2013 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. AT&T 36USC220506

The first nationwide carrier to be awarded
Wireless Consumer Information Code Quality
ACCREDITED BUSINESS
TRUSTe CERTIFIED PRIVACY
yp CLICK LESS. LIVE MORE.
The new YELLOWPAGES.COM
Digital White & Yellow Pages
USA
Proud Sponsor of the U.S. Olympic Team

Above: "Smishing" is SMS-based phishing. This phish attacked customers of AT&T on March 5, 2014, and was advertised by text messages to consumers' phones.



Dear 123-reg.co.uk client,

Domain account **your-domain.com** has exceeded the limit load available for the existing pay rate plan.

Methods of load analysis and elimination:
http://www.123-reg.co.uk/verified.aspx?GUID=Z0f3cc644-0c7f-7fed-a428-30284b284271

In order to prevent your account from being locked out we recommend that you change the existing rate plan onto a more powerful one or limit the server load by means of code optimization.

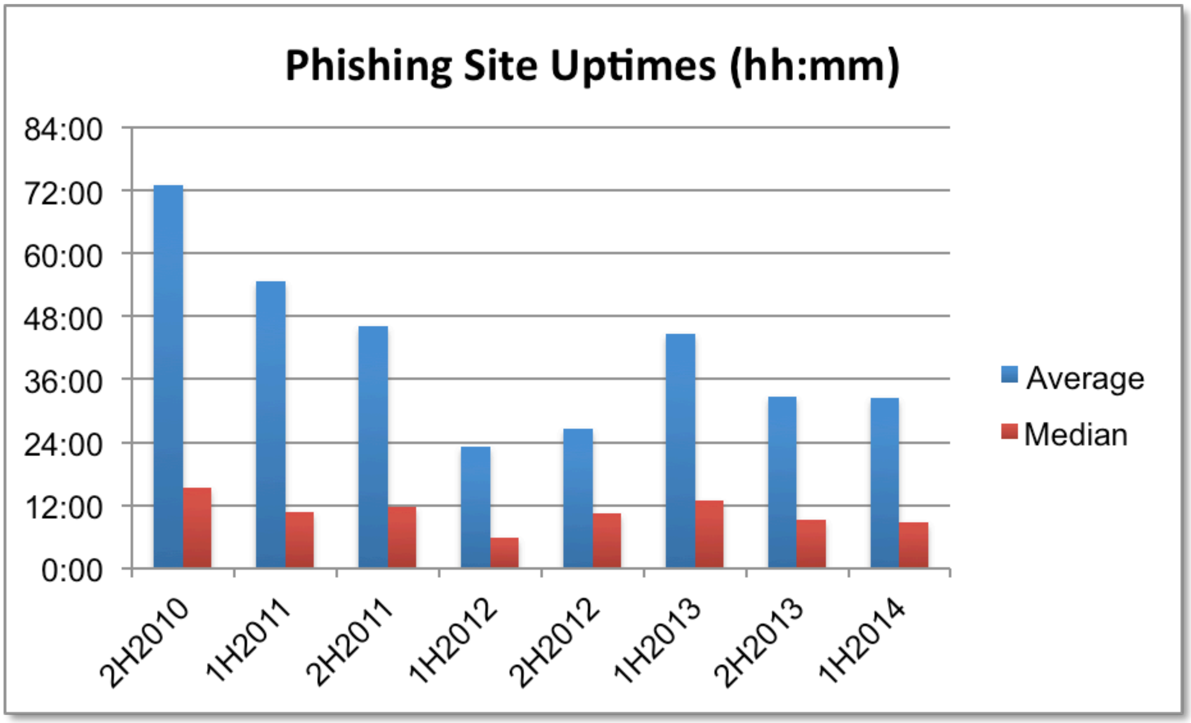
Thank you for choosing 123-reg.
The 123-reg team
www.123-reg.co.uk

Above: a phishing lure e-mail that targeted a domain name registrar/hoster.

Phishing by Uptime

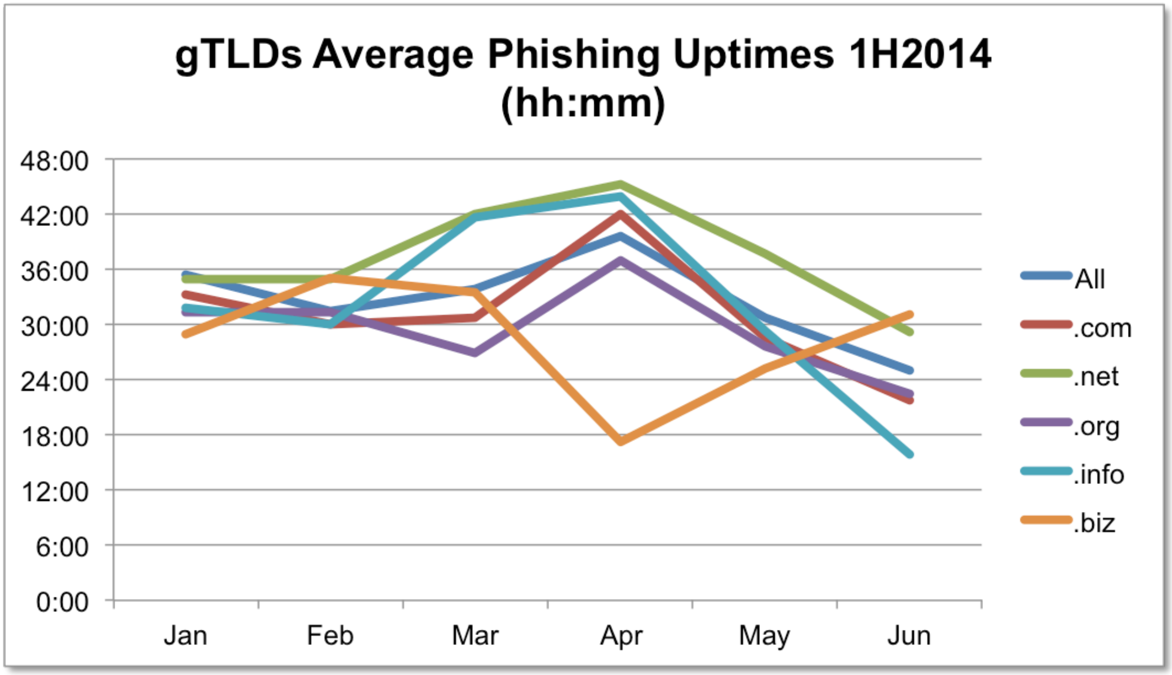
The average uptimes for phishing attacks has remained steady. The average uptime in 1H2014 was 32 hours and 32 minutes. The median uptime in 1H2014 was 8 hours and 42 minutes, meaning that half of all phishing attacks stay active for less than 9 hours.

The "uptimes" or "live" times[4] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a metric 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 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.

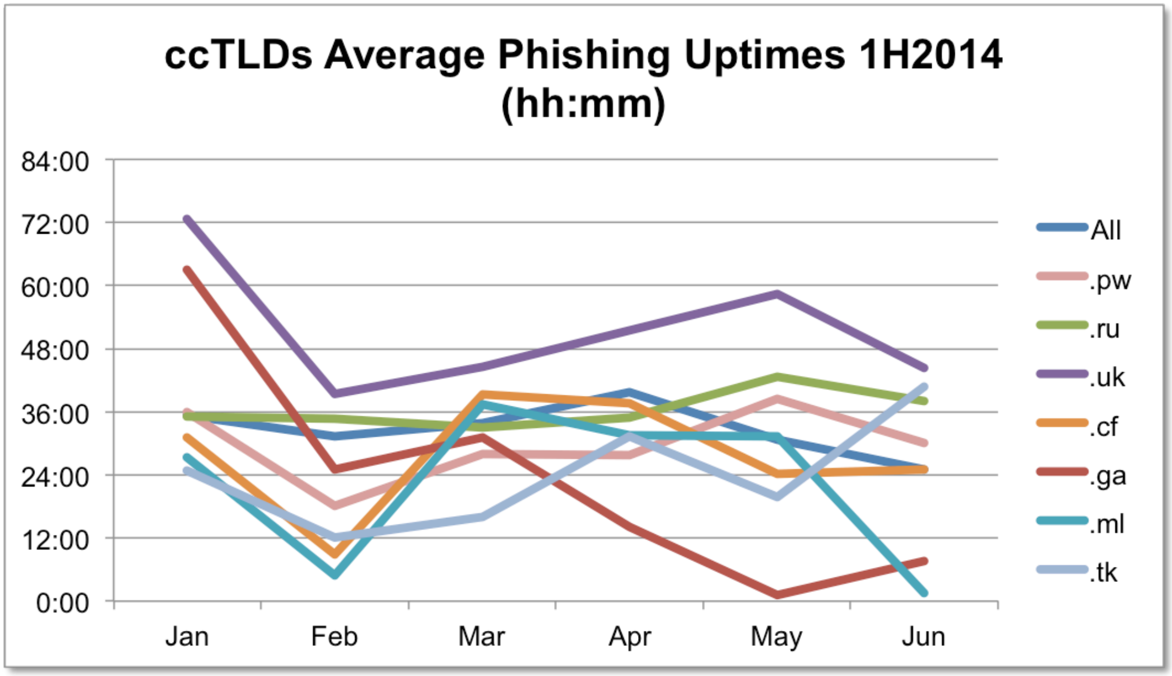


[4] The system used to track the uptimes automatically monitored the phishing sites, and monitoring began as soon as the system became aware of a phish via feeds or honeypots. Each phish was checked several times per hour to confirm its availability, and was not declared "down" until it had stayed down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

In the large generic top-level domains (gTLDs): the .INFO, .BIZ, and .ORG registry operators have notification and takedown programs; .COM/.NET does not.



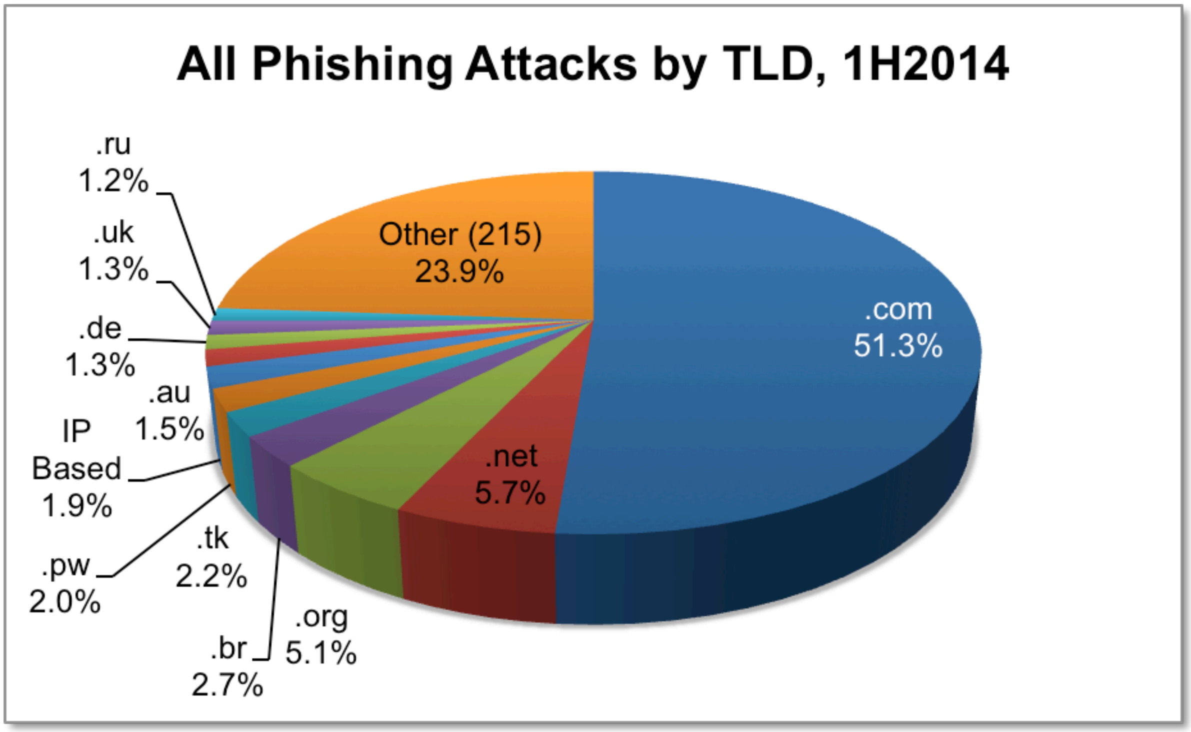
The uptimes at various country-code TLDs (ccTLDs) were less uniform:



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 phishing-domains-per-10,000 score was 4.7** (versus 3.1 in 1H2013).
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 4.1.** .COM contained 54% of the phishing domains in our data set, and 41.8% of the domains in the world.

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

We therefore suggest that domains-per-10,000 scores between 4.1 and 4.7 occupy the middle ground, with scores above 4.7 indicating TLDs with increasingly prevalent phishing.[6] The top TLDs by score are:

Top 10 Phishing TLDs by Domain Score, 1H2014

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

	TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014
1	.cf	Central African Republic	1,327	1,283	40,000	320.8
2	.ml	Mali	556	523	44,000	118.9
3	.pw	Palau	2,484	2,318	190,000	122.0
4	.ga	Gabon	285	270	63,000	42.9
5	.th	Thailand	262	176	64,099	27.5
6	.np	Nepal	105	93	39,000	23.8
7	.ma	Morocco	106	92	43,350	21.2
8	.pk	Pakistan *(est.)*	115	86	42,000	20.5
9	.cl	Chile	1,188	921	455,886	20.2
10	.ke	Kenya	63	53	34,790	15.2

The .CF, .GA, and .ML ccTLD registries were repurposed in 2013 to offer free domains names. They are operated by Freenom, which also operates the free .TK registry.[7] For more about these TLDs, please see “Compromised Domains versus Malicious Registrations” below.

The .PW registry was plagued by Chinese phishers, who registered at least 1,889 domains to phish Taobao.com and other Chinese targets. Thailand’s .TH continues to rank highly, as it has for many years, suffering from compromised government and university Web servers.

[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.

[7] Freenom declined to provide registration numbers for .CF, .ML, and .GA, and so our domains-in-registry numbers are from DomainTools.

The New Top-Level Domains

Beginning in January 2014, the first of the new generic top-level domains (gTLDs) began rolling out. Approximately 1,200 new top-level domains will launch from 2014 through 2016, the result of a multi-year process run by the Internet Corporation for Assigned Names and Numbers (ICANN), which coordinates the top level of the Internet.

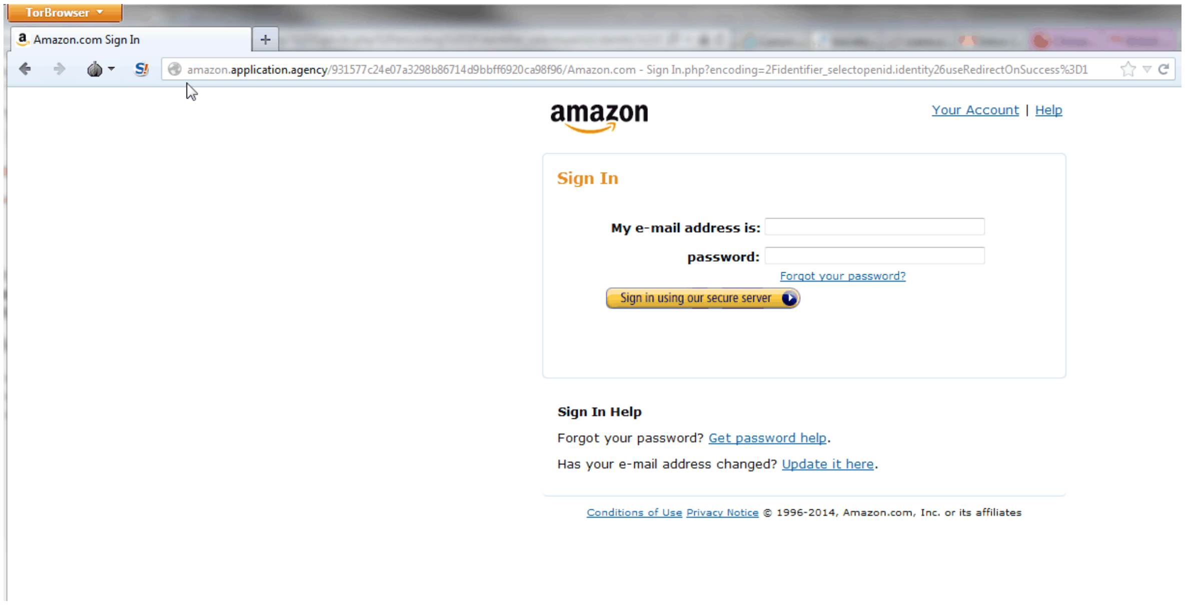
As of this writing, the new gTLD program has not resulted in a bonanza of phishing. A few phishers experimented with new gTLD domain names, perhaps to see if anyone noticed. But most of the new gTLD domains that were used for phishing were actually on compromised web sites. Why haven't phishers taken big advantage of the virgin name space that new gTLDs offer?

First, phishers usually don't register domains that contain brand names. Instead, any domain will do—they fool Web users by placing the brand name in a subdirectory or subdomain in the phishing URL. For more about this phenomenon, see "Compromised Domains vs. Malicious Registrations" below.

Second, most of the new gTLDs have been in their early phases of introduction. Those that have been available for purchase by the general public have usually been priced higher than .COM and other popular legacy TLDs. Phishers and spammers have been able to get cheaper domain names in the legacy TLDs.

This situation will certainly change, though. As autumn 2014 begins, the new gTLD market is becoming more crowded and competitive, and some registries have begun to compete aggressively on price. As prices drop and the new gTLDs gain more adoption, we are seeing an increase in phishing on new gTLD domains, due to both malicious registrations and compromised domains on hacked servers. Anecdotal discussions in the security community also indicate that malware authors and other miscreants are experimenting with registering domains in some of the new gTLD domains for various malicious activities. In future reports we'll compare the new TLDs to the old and see what hot spots develop.

TLD	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	# Total Malicious Domains Registered 1H2014
.agency	1	1	3,951	2.5	2.5	1
.center	1	1	13,939	0.7	0.7	1
.club	3	3	1,819	16.5	16.5	1
.company	1	1	16,614	0.6	0.6	
.email	3	3	25,979	1.2	1.2	1
.gallery	1	1	10,404	1.0	1.0	
.guru	2	2	53,195	0.4	0.4	
.land	2	2	10,831	1.8	1.8	
.photos	1	1	10,274	1.0	1.0	
.tips	1	1	20,991	0.5	0.5	1
.today	1	1	21,890	0.5	0.5	



amazon.application.agency/931577c24e07a3298b86714d9bbff6920ca98f96/Amazon.com - Sign In.php?encoding=2Fidentifier_selectopenid.identity26useRedirectOnSuccess%3D1

Sign In

My e-mail address is:

password:

Forgot your password?

Sign in using our secure server

Sign In Help

Forgot your password? Get password help.

Has your e-mail address changed? Update it here.

Conditions of Use Privacy Notice © 1996-2014, Amazon.com, Inc. or its affiliates

Above: application.agency – a new gTLD domain used to phish Amazon's customers on May 7, 2014.

Compromised Domains vs. Malicious Registrations

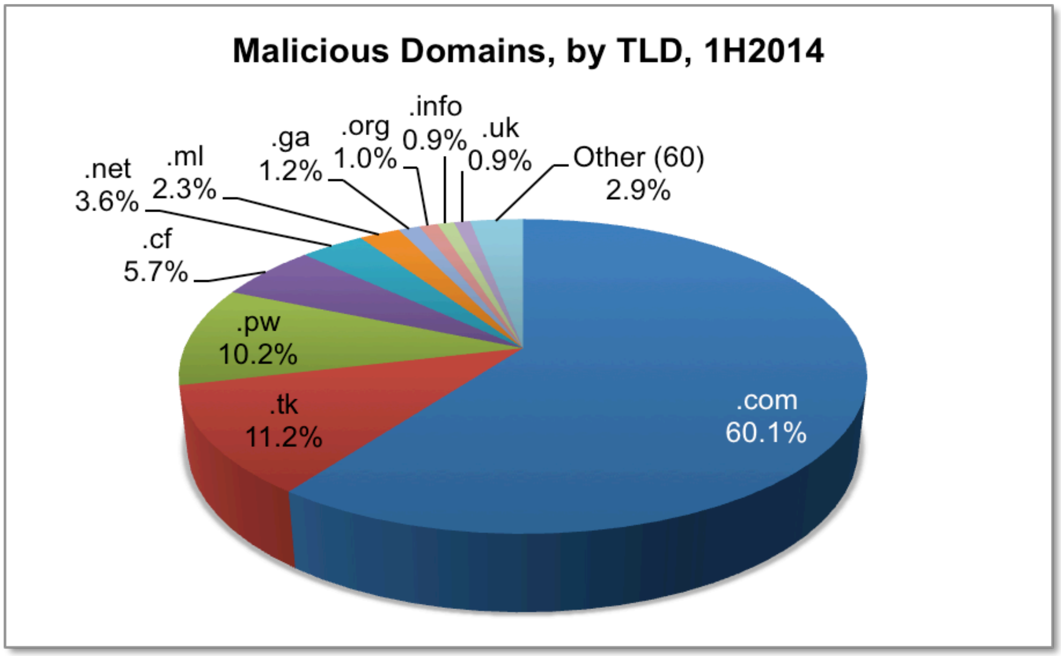
We performed an analysis of how many domain names were registered by phishers, versus phish that appeared on compromised (hacked) domains. These different categories are important because they present different mitigation options for responders, and offer insights into how phishers commit their crimes. 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 it was registered in a batch or in a pattern that indicated common ownership or intent.

Of the 87,901 domains used for phishing, **we identified 22,679 (25.8%) domains that we believe were registered maliciously, by phishers. The number is primarily due to registrations by Chinese phishers, who prefer cheap (and free) domain name registrations in certain TLDs.** The other 65,222 domains were almost all hacked or compromised on vulnerable Web hosting.

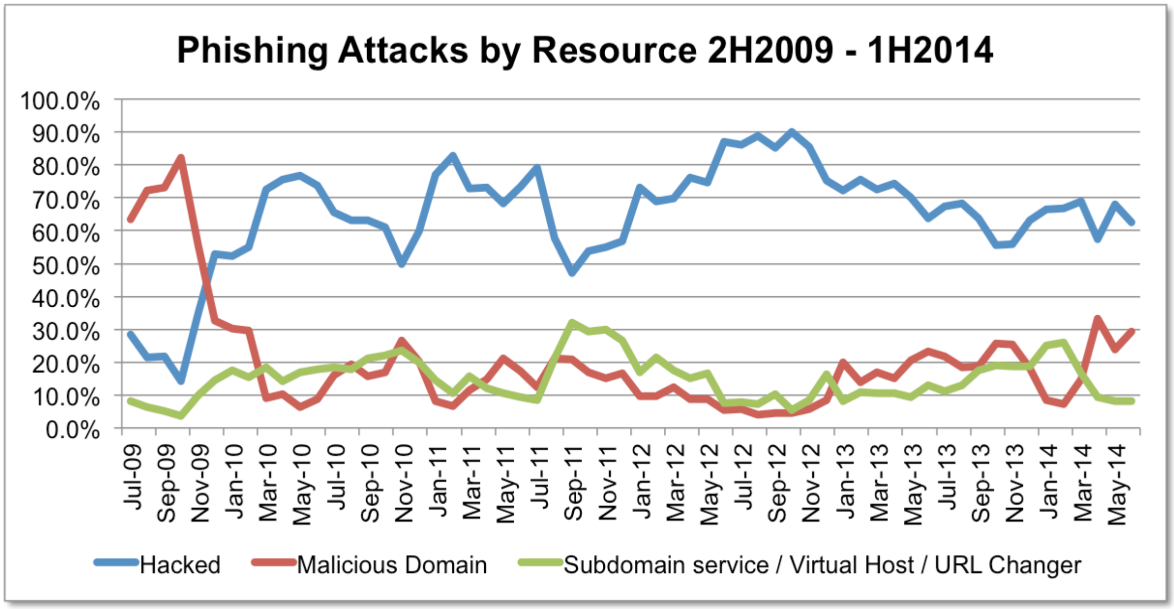
Of those 22,679 malicious domain registrations, 19,356 (85%) were registered to phish Chinese targets—services and sites in China that serve a primarily Chinese customer base.[8] These numbers are almost identical to those observed in 2H2013. Chinese phishers have always preferred to register domains, relying upon hacked domains and compromised

[8] These phishing attacks were advertised via e-mail lures written in Chinese, via SMS messages in Chinese sent to mobile phone customers in China, and via instant message clients popular in China such as Tencent QQ. Many of the domain registrations made by these phishers are made at Chinese registrars. Other factors about these attacks also point to perpetrators in China as well.

Web servers less often than phishers elsewhere. Their major targets included Taobao.com, the Industrial and Commercial Bank of China (ICBC), CCTV, Alibaba, and Tencent.



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, are not seeing instant-messenger and SMS lures, 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.



Twenty percent of the world's malicious registrations were made in the .TK, .CF, .GA, and .ML registries. Freenom, a Netherlands-based company that offers free domain name registrations, runs these registries. (It then monetizes the traffic to the expired domains.) Freenom has operated .TK under the free model for several years, and added .CF, .GA, and .ML to its program during the second half of 2013. Freenom gives accredited interveners access to directly suspend domains in the .TK registry. (These partners include Facebook, Internet Identity, and the Anti-Phishing Alliance of China.) However, Freenom does not offer a similar tool to mitigate phishing on .CF, .ML, and .GA domains. This lack shows -- while .TK domains were mitigated quickly, phish in .CF, .GA. and .ML all had uptimes that were much longer.

Of the 22,679 maliciously registered domains, just 1,498 contained a relevant brand name or reasonable variation thereof—often a misspelling.[9] **This represents 1.7% of all domains that were used for phishing, and just 6.6% of all maliciously registered domains recorded in the sampling period.** Instead, the registrations made by 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.

Some Internet users are so unaware of how to read a URL that phishers even registered deliberately counter-productive domain names. These included hackerstuff.tk, fuckingme.tk, and professionalhacker.pw, all used to phish Facebook users. One phisher used google.ge to phish Facebook instead.

Registrars Used for Malicious Domain Registrations

Phishers (especially Chinese phishers) continued to register malicious domain names at nearly the same high rate as in 2H2013. This high level of fraudulent registrations is concerning, because malicious registrations had been trending downward since 2010, and reducing malicious registrations has been a primary motivation for writing our Global Phishing Survey reports.

Where are the phishers registering these domains? We were able to obtain the name of the sponsoring registrar for 90 percent 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 are grateful. The following analysis looks at generic top-level domain (gTLD) registrations only. ICANN makes public how many gTLD domains each of its registrars sponsors, but ccTLD registration numbers by registrar are not generally available.

[9] Examples of domain names we have counted as containing brand names included: serviceid-apple.com (Apple), batlte.com (Battle.net), 99886taobao.com (taobao.com), and faaccebok.com (Facebook).

Phishers utilized at least 275 registrars in 1H2014, up from 230 in 2H2013. GoDaddy holds roughly half of the gTLD market, but sponsored less than 5% of the malicious gTLD phishing registrations. Some registrars also support reseller programs through which many of these domains were sold, but we were not able to discern reseller identities because it was not consistently available in WHOIS.

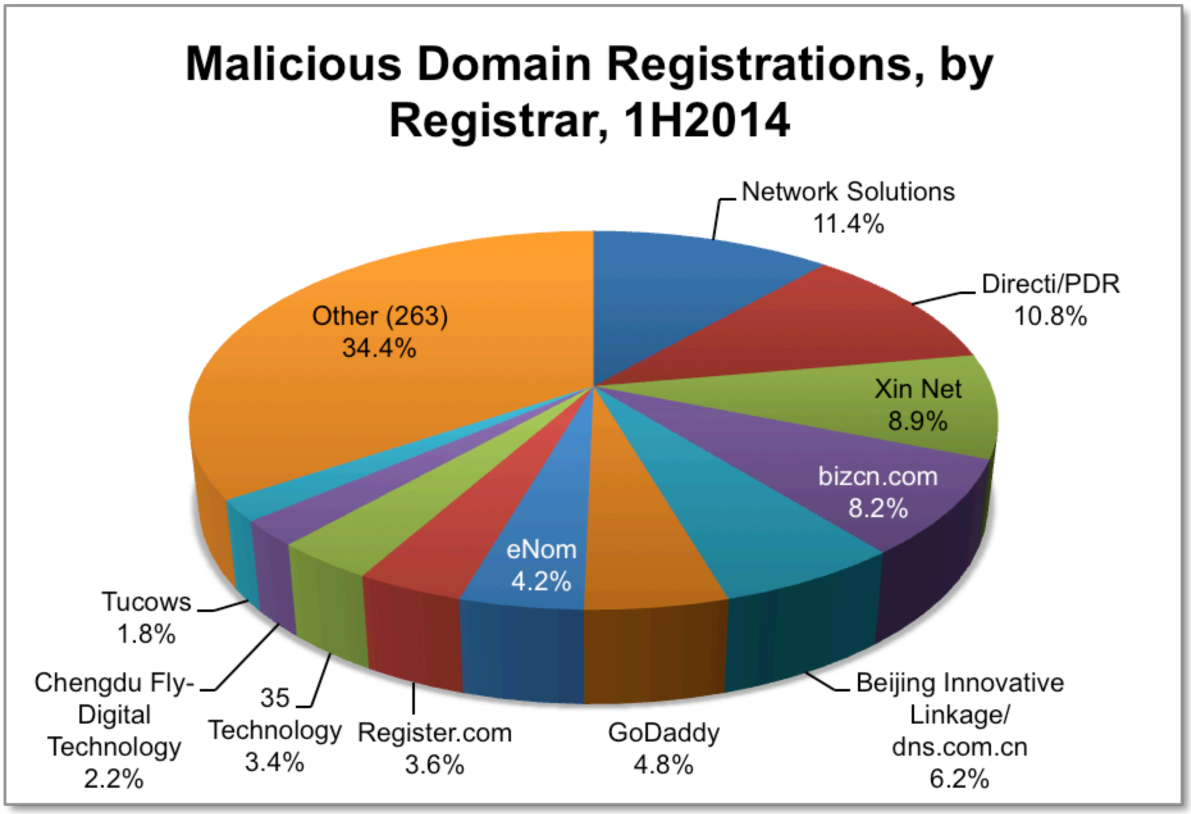
To compare dissimilar registrars with each other, we used the same metric we use for comparing various TLDs – malicious domains per 10,000 domains under management. We use this metric to identify registrars that may be exploited out of proportion to their size. The 15 registrars below accounted for 71 percent (10,645) of the 14,695 maliciously registered phishing domains in the gTLD space.

Top Phishing Registrars by Malicious Domain Score 1H2014

All registrars must have more than 100 malicious phishing registrations and 30,000 gTLD domain names under management

Rank	Registrar	Malicious Domains	gTLD Domains at registrar, April 2014	Malicious Domains per 10,000
1	CHENGDU FLY-DIGITAL TECHNOLOGY CO.	396	59,853	66
2	FOSHAN YIDONG NETWORK CO. LTD	262	106,637	25
3	BIZCN.COM	1,475	605,117	24
4	BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD. DBA DNS.COM.CN	1,123	503,255	22
5	35 TECHNOLOGY CO.	612	486,104	13
6	XIN NET TECHNOLOGY CORPORATION	1583	1,629,895	10
7	ERANET INTERNATIONAL (TodayNIC)	103	110,000	9
8	SHANGHAI MEICHENG TECHNOLOGY INFORMATION DEVELOPMENT CO.	123	216,890	6
9	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	1,795	4,276,163	4
10	SHANGHAI YOVOLE NETWORKS INC.	132	423,183	3
11	NETWORK SOLUTIONS, LLC.	2,064	7,212,702	3
12	CHENGDU WEST DIMENSION DIGITAL TECHNOLOGY CO.	120	419,377	3
13	REGISTER.COM, INC.	648	2,750,202	2
14	REGISTER.IT SPA	131	572,744	2
15	JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD	78	374,189	2

Nine of the top ten registrars are located in China. This is largely due to the fact that Chinese phishers tend to register domain names for their phishing, and use Chinese registrars regularly. 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 occasionally 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 just 110 .CN domains for phishing, almost exclusively through Chinese registrars. This is down from 515 in 2H2013, so may indicate better prevention of such registrations.

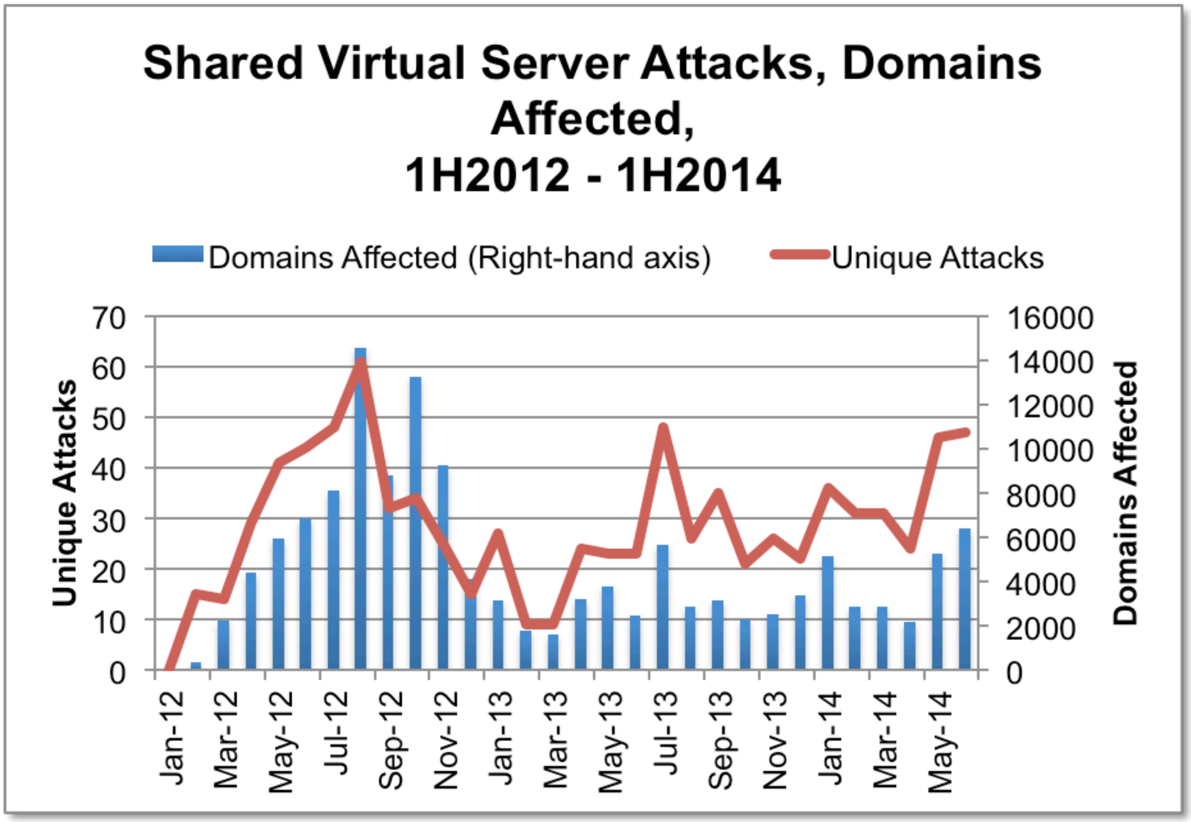


About 19 percent of the world's malicious registrations were made at the ccTLD registries run by Freenom (.TK, .CF, .GA, and .ML.) Freenom also serves as the registrar for those domains. These large numbers of fraudulent ccTLD domain registrations were excluded from the analysis above. However, they do make Freenom the registrar with the largest number of malicious registrations.

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. Alternatively, the phisher can use an automation tool to enumerate all hosted websites on a server, using a known server flaw to quickly add his phishing content to each domain it hosts. 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 1H2014, we identified 215 mass break-ins of this type, resulting in 24,662 phishing attacks. This represents 20% of all phishing attacks recorded worldwide. Versus 2H2013, both break-ins (178 in 2H2013) and attacks (20,911 in 2H2013) were up noticeably. They resulted in about 20 percent of all phishing attacks, versus 18 percent in 2H2013. This trend is interesting and it is unclear whether these attacks are more effective and are thus being run more often to capitalize, or whether the technique is less effective so attackers need to launch more in order to reap the same number of credentials.



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 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 significant use of tools that allow criminals to target shared hosting environments, and particularly WordPress, cPanel, and Joomla installations. These automated cracking tools are providing thousands of fresh datacenter servers to the criminal underground, offered through various marketplaces. We see such servers 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.

Use of Subdomain Services for Phishing

After seeing steady declines over a year ago, **we saw the use of subdomain registrations for phishing continue at a high pace in 1H2014**. The rate remained steady vs. 2H2013 and phishers still registered far fewer subdomains than they registered "regular" domain names. **However, subdomain registrations still represent 14% of all phishing attacks.**

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" -- their own DNS space -- 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

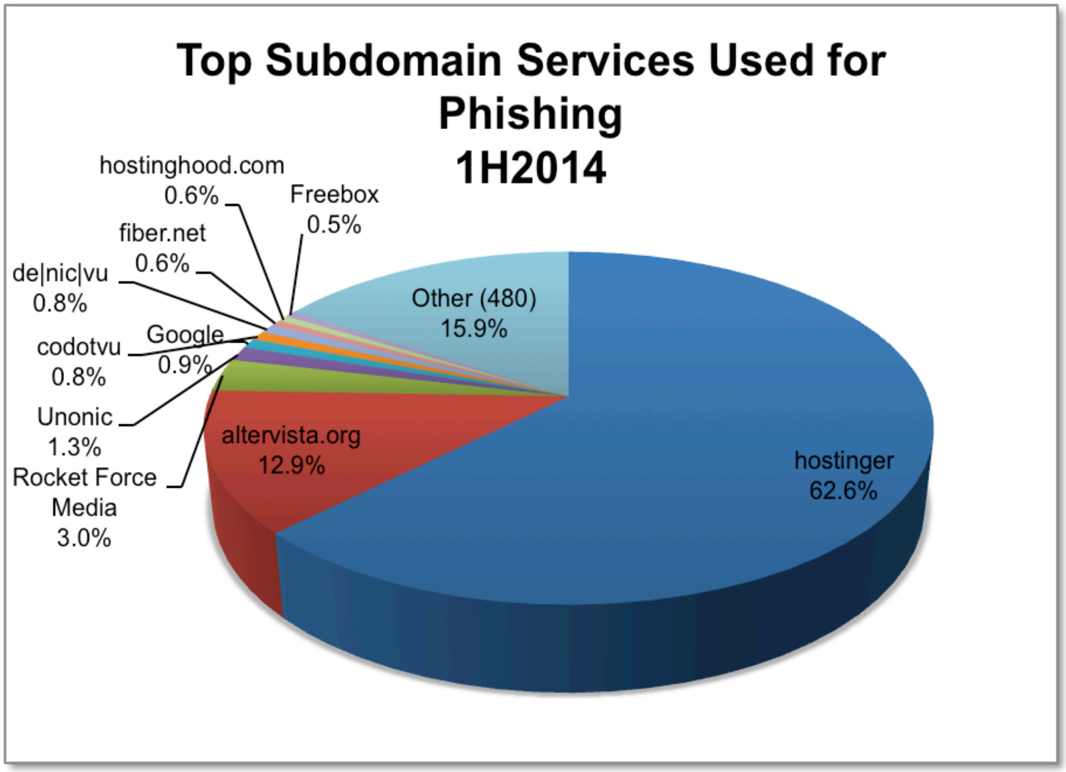
We know of more than 800 subdomain providers. Use of subdomain services continues to be a challenge, because many of the services are free, offer anonymous registration, and only the subdomain providers themselves can effectively mitigate these phish.[10] While many of these services are responsive to complaints, proactive measures to keep criminals from abusing their services are limited.

Use of subdomain services for phishing remained high in 1H2014, but did decline a bit from our last report, from 17,674 (15% of all attacks) to 16,986 (14% of all attacks). The number of domains used for malicious subdomains was down quite a bit, from 795 to 678, but one domain (altervista.org) alone saw 2,194 malicious subdomains created under it in 1H2014. Many of the subdomain attacks were against Chinese targets like Taobao.com, but a vast majority attacked online services like Facebook, Google, Yahoo, Hotmail, and PayPal.

As in the 2H2013 report, in 1H2014 we saw a large number of subdomain services being abused by phishers for the first time. **200 subdomain service domains were abused in 1H2014 that we had never seen in prior reports.** Clearly, phishers still like to "test-drive" new subdomain services. This may be to get around anti-abuse features of more experienced subdomain resellers or to avoid the poor reputation some of the "burned" domains that have been previously abused may have in general.

Hostinger (back-ended by Maine-Hosting) continues to be the favorite service for phishers to abuse in where at least 10,640 malicious subdomains were spotted, representing a whapping 63 percet of all subdomain phishing. This service runs dozens of domains under its service, and is very prompt at removing abuse. Unfortunately, Hostinger still appears to lack a reliable method to deter phishers from using its service in the first place. This total is nearly quadrupled from 2,376 in 2H2013, and clearly demonstrates a need for better tactics to curtail such large-scale abuse. The only other company with a sizable share of malicious subdomains is industry veteran AlterVista, coming in with 2,194 malicious subdomains, or 13 percent of the world total.

[10] 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.



Some notable drops from the list of most-abused subdomain resellers include POPNIC, , and 000webhost.com who each had over 1,000 subdomains in 2H2013, but disappeared from the top 20 entirely in 1H2014.

Top Subdomain Services Used for Phishing, 1H2014

Rank	Attacks	Provider
1	10,640	Hostinger
2	2,194	altervista.org
3	513	Rocket Force Media
4	222	Unonic
5	154	Google
6	144	codotvu
7	133	de|nic|vu

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 eight 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 June 2014 we have found only nine true homographic phishing attacks.

One hundred and twelve IDN domains names were used for phishing in 1H2014, but only three were malicious registrations, with the others being hacked domains. Of those three, only one was a homographic attack, using an accented "i":

xn--nterbank-b2a.com → ínterbank.com

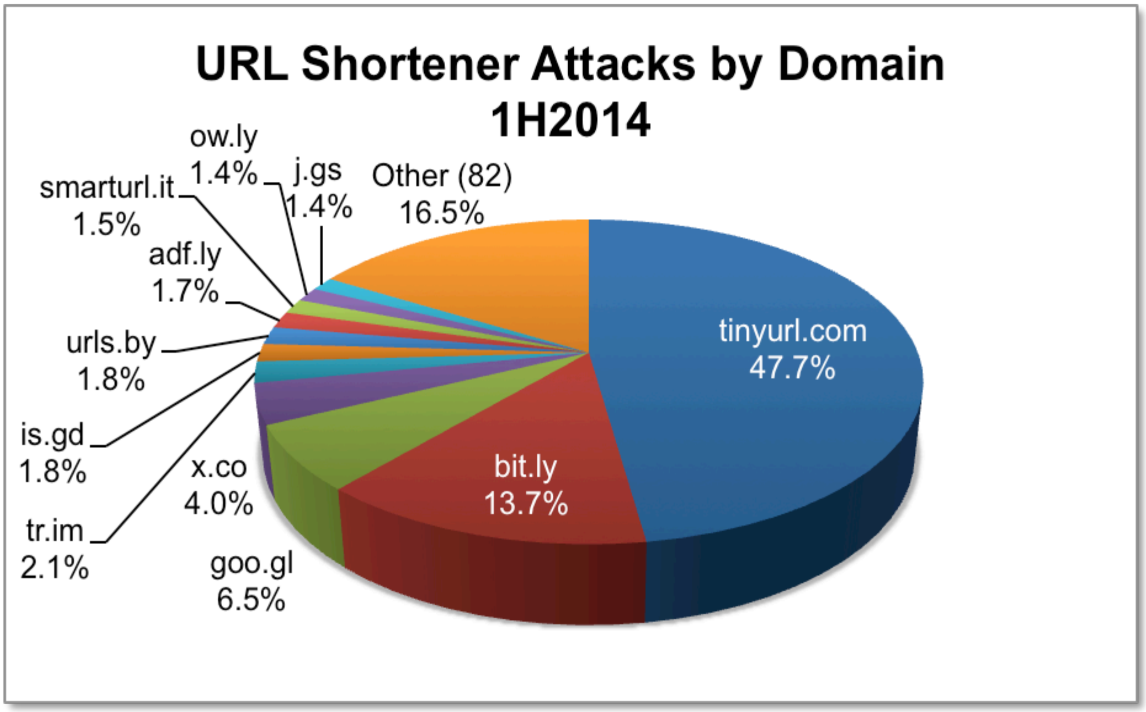
Given that IDNs have been widely available for years, why haven't phishers utilized IDN homographic attacks more often?

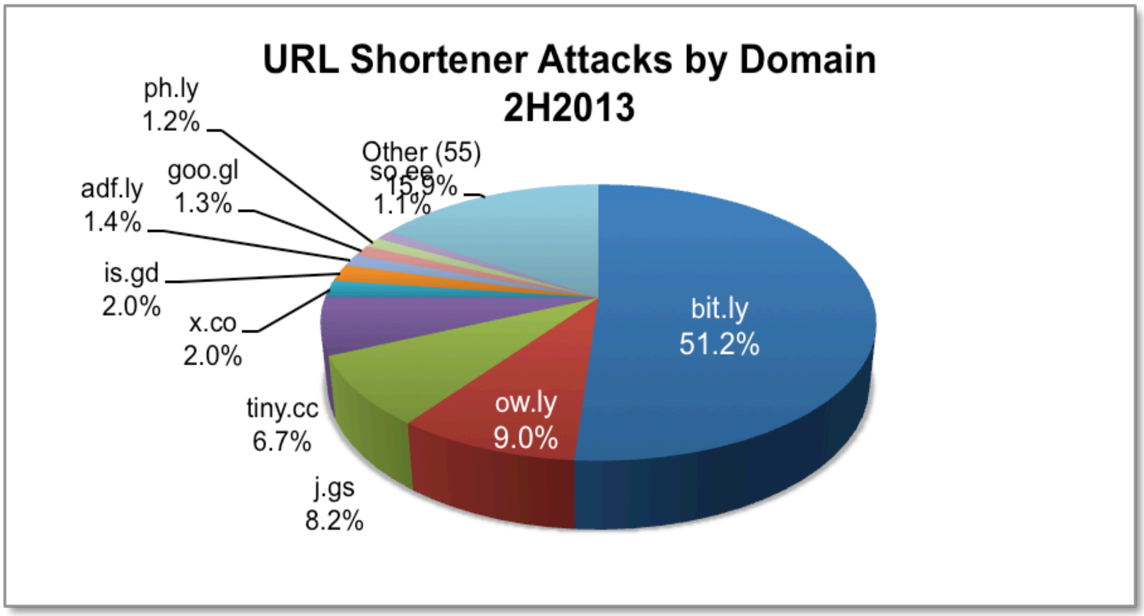
1. Phishers don't *need* to resort to such attacks. As noted elsewhere in this report, the domain name itself usually does not matter to a phisher.
2. By default, some browser manufacturers show the punycode version of the domain name (such as "xn--hotmal-t9a.net") in the address bar, instead of the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

Use of URL Shorteners for Phishing

Phishers continue to their recent resurgence in using "URL shortening" services to obfuscate phishing URLs. Users of those services can obtain a very short URL to put in their limited-space posts or Tweets, which automatically redirects the visitor to a much longer "hidden" URL. Phishers increased their use of this technique again in 1H2014, with such attacks rising sharply from 999 in 2H2013 to 1696 in 1H2014. This still only represents 1.4% of all phishing attacks, but prior work in this space had nearly eliminated such attacks. This continued increase may be pointing to newly exploited flaws in the shortening services' defenses, or perhaps, lowered diligence.

1H2014 saw almost half of all URL shortener phish occurring on the very popular tinyURL service with 809 attacks. Bit.ly, another large provider in the space moved from first to second place in the same period, with 233 attacks, down from 512 in 2H2013. The only other service with significant share of attacks was owl.ly, another popular service.





Most of the major URL shortener providers have put screening mechanisms for malicious forwarding destinations in place, and have made it easier and more efficient to report abuse than in years past. In an emerging best practice, many shortener 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. The continued increase in shortener-based phish shows that one can never let their guard down, continually adjusting to phishers' latest tactics.

Blocklist provider 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 still being seen in conjunction with malware exploit kit sites, pharma spam, and other abusive behavior, and while outside the scope of this report shows that this problem is not truly "solved" at this point.

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 against specialized or small targets, like students at a particular university.
- Spies involved in corporate and government espionage.
- Hacktivists who seek publicity for their causes.

Appendix: Phishing Statistics and Uptimes by TLD

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
ac	Ascension Island	1	1	16,200	0.6	0.6	63:09	63:09		
ad	Andorra			1,500						
ae	United Arab Emirates	54	28	114,000	2.5	4.7	52:40	08:37		
aero	sponsored TLD	2	2	8,221	2.4	2.4	20:26	20:26		
af	Afghanistan	6	5				17:27	06:35		
ag	Antigua and Barbuda	1	1	19,936	0.5	0.5	02:17	02:17		
agency	generic TLD	1	1	452	22.1	22.1			1	22.1
ai	Anguilla	26	4	3,800	10.5	68.4	48:22	13:42		
al	Albania	11	10	8,000	12.5	13.8	16:31	22:44		
am	Armenia	63	24	22,486	10.7	28.0	33:24	09:45	1	0.4
an	Netherlands Antilles	1	1	800	12.5	12.5	1086:27	1086:27		
ao	Angola	1	1	300	33.3	33.3	12:02	12:02		
ar	Argentina	913	690	2,800,000	2.5	3.3	42:50	09:40	5	0.0
arpa	Advanced Research Project Agency									
as	American Samoa	6	4	12,000	3.3	5.0	78:34	30:25	1	0.8
asia	sponsored TLD	96	70	351,982	2.0	2.7	34:54	09:07	33	0.9
at	Austria	147	117	1,230,577	1.0	1.2	44:04	16:06	2	0.0
au	Australia	1,801	1,446	2,828,193	5.1	6.4	23:07	06:59	8	0.0
aw	Aruba			650						

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
ax	Åland Islands									
az	Azerbaijan	16	13	21,801	6.0	7.3	24:02	17:12		
ba	Bosnia and Herzegovina	77	76	15,374	49.4	50.1	05:17	00:42	1	0.7
bb	Barbados	3	3	1,400	21.4	21.4	26:51	06:30		
bd	Bangladesh	50	48	5,000	96.0	100.0	16:06	07:44	1	2.0
be	Belgium	299	246	1,451,183	1.7	2.1	32:31	09:07	4	0.0
bf	Burkina Faso									
bg	Bulgaria	19	14	26,000	5.4	7.3	09:02	03:44		
bh	Bahrain									
bi	Burundi	2	2				02:23	02:23		
biz	generic TLD	525	446	2,756,014	1.6	1.9	29:11	08:20	28	0.1
bm	Bermuda	2	2	8,100	2.5	2.5	03:10	03:10		
bn	Brunei Darussalam	1	1	1,150	8.7	8.7	00:11	00:11		
bo	Bolivia	10	9	8,500	10.6	11.8	10:11	04:31		
br	Brazil	3,368	2,744	3,322,262	8.3	10.1	54:52	16:09	15	0.0
bs	Bahamas	1	1	2,500	4.0	4.0	01:12	01:12		
bt	Bhutan	4	4	1,100	36.4	36.4	05:53	05:34		
bw	Botswana	2	1				372:46	372:46		
by	Belarus	188	117	82,000	14.3	22.9	45:48	06:57		
bz	Belize	18	11	45,445	2.4	4.0	16:17	08:28	3	0.7
ca	Canada	723	635	2,223,978	2.9	3.3	32:00	07:41	6	0.0
cat	sponsored TLD	24	19	74,846	2.5	3.2	17:01	07:29	1	0.1
cc	Cocos (Keeling) Islands	288	96	375,000	2.6	7.7	31:59	08:28	26	0.7
cd	Congo, Democratic Repub.	3	2	5,200	3.8	5.8	104:52	04:07		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
center	generic TLD	1	1	13,939	0.7				1	0.7
cf	Central African Republic *(est.)*	1,327	1,283	30,000	427.7	442.3	30:01	13:44	1,282	427.3
cg	Congo									
ch	Switzerland	262	215	1,869,839	1.1	1.4	32:11	10:41	4	0.0
ci	Côte d'Ivoire	11	9	2,500	36.0	44.0	07:11	03:40		
cl	Chile	1,188	921	455,886	20.2	26.1	31:37	06:53	3	0.1
club	generic TLD	3	3				15:20	21:24	1	
cm	Cameroon *(estimated)*	12	6	12,500	4.8	9.6	77:14	33:20		
cn	China	704	523	10,666,626	0.5	0.7	30:58	10:16	90	0.1
co	Colombia	496	314	1,718,516	1.8	2.9	26:30	08:46	41	0.2
com	generic TLD	63,206	47,554	116,856,602	4.1	5.4	30:16	08:21	13,623	1.2
company	generic TLD	1	1	16,614	0.6	0.6	06:10	06:10		
coop	sponsored TLD	8	7	7,877	8.9	10.2	23:37	18:41		
cr	Costa Rica	5	5	15,454	3.2	3.2	05:47	05:44		
cu	Cuba	4	2	4,768	4.2	8.4	04:58	02:22		
cv	Cape Verde	1	1	900	11.1	11.1	05:26	05:26		
cx	Christmas Island	33	5	5,525	9.0	59.7	23:37	06:39		
cy	Cyprus	5	4	12,500	3.2	4.0	12:34	08:49		
cz	Czech Republic	272	168	1,132,206	1.5	2.4	41:25	12:28	1	0.0
de	Germany	1,562	1,319	15,708,809	0.8	1.0	27:43	20:24	29	0.0
dj	Djibouti	3	3	5,300	5.7	5.7	35:28	30:59		
dk	Denmark	149	123	1,260,991	1.0	1.2	25:47	07:07		
dm	Dominica *(estimated)*			14,000						
do	Dominican Republic	21	12	14,300	8.4	14.7	21:09	05:34		
dz	Algeria	1	1	5,200	1.9	1.9	13:41	13:41		
ec	Ecuador *(estimated)*	32	27	30,500	8.9	10.5	56:19	18:41		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
edu	U.S. higher education	33	25	7,590	32.9	43.5	25:07	11:02		
ee	Estonia	183	19	75,044	2.5	24.4	20:53	03:39		
eg	Egypt	9	6	6,000	10.0	15.0	12:47	05:37		
email	generic TLD	3	3	25,979	1.2	1.2	25:38	02:34	1	0.4
er	Eritrea			150						
es	Spain	1,446	337	1,727,169	2.0	8.4	27:18	04:15	2	0.0
et	Ethiopia	2	2	1,200	16.7	16.7	02:27	02:27		
eu	European Union	547	444	3,800,500	1.2	1.4	48:43	10:01	99	0.3
fi	Finland	47	43	343,783	1.3	1.4	19:01	04:46	1	0.0
fj	Fiji	5	3	4,000	7.5	12.5	13:16	08:04		
fk	Falkland Islands									
fm	Micronesia, Fed. States	7	6	15,100	4.0	4.6	34:07	18:00		
fo	Faroe Islands	2	1				07:19	07:19		
fr	France	958	603	2,773,791	2.2	3.5	53:21	10:14	49	0.2
ga	Gabon	285	270	63,000	42.9	45.2	37:08	12:18	270	42.9
gallery	generic TLD	1	1	10,404	1.0	1.0	12:36	12:36		
gd	Grenada	42	3	4,400	6.8	95.5	16:26	01:14		
ge	Georgia *(estimated)*	45	35	21,000	16.7	21.4	25:53	09:44	2	1.0
gg	Guernsey	7	4	3,900	10.3	17.9	18:15	14:12		
gh	Ghana	3	2	2,600	7.7	11.5	24:42	29:15		
gi	Gibraltar			2,156						
gl	Greenland	112	2	5,500	3.6	203.6	14:53	01:47		
gm	Gambia	5	3				24:40	27:40		
gov	U.S. government			5,000		0.0				
gp	Guadeloupe	9	7	1,500	46.7	60.0	17:02	13:54		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
gr	Greece *(estimated)*	294	257	340,000	7.6	8.6	28:07	09:00	1	0.0
gs	South Georgia & Sandwich Is.	43	6	6,000	10.0	71.7	13:39	05:03		
gt	Guatemala	10	8	14,908	5.4	6.7	48:30	13:41		
guru	generic TLD	2	2	53,195	0.4	0.4	02:16	02:16		
gy	Guyana	11	4				07:46	02:51		
hk	Hong Kong	97	58	260,659	2.2	3.7	72:51	09:38		
hm	Heard and McDonald Is.									
hn	Honduras	3	3				31:42	18:41		
hr	Croatia	89	76	83,447	9.1	10.7	31:35	07:42		
ht	Haiti	24	3	2,200	13.6	109.1	35:55	06:56		
hu	Hungary	232	189	645,879	2.9	3.6	47:09	20:36		
id	Indonesia	230	160	106,179	15.1	21.7	37:45	08:48		
ie	Ireland	88	72	187,800	3.8	4.7	28:41	11:17		
il	Israel	140	107	227,500	4.7	6.2	46:44	11:28		
im	Isle of Man *(estimated)*	63	16	21,250	7.5	29.6	16:50	03:59	1	0.5
in	India	1,211	989	1,528,910	6.5	7.9	29:05	10:04	64	0.4
info	generic TLD	1,408	1,216	5,774,272	2.1	2.4	30:12	09:32	212	0.4
int	sponsored TLD	1	1				50:33	50:33		
io	British Indian Ocean Terr.	7	7	60,100	1.2	1.2	08:03	04:56		
IP address	(no domain name used)	2,891					40:09	11:12		
iq	Iraq			450						
ir	Iran	516	340	500,470	6.8	10.3	23:42	05:03	1	0.0
is	Iceland	24	16	47,500	3.4	5.1	46:42	26:14		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
it	Italy	748	540	2,669,428	2.0	2.8	40:54	09:48	9	0.0
je	Jersey									
jm	Jamaica	1	1	6,500	1.5	1.5	22:04	22:04		
jo	Jordan			4,340						
jobs	sponsored TLD			44,983						
jp	Japan	85	61	1,370,274	0.4	0.6	63:17	16:12		
ke	Kenya	63	53	34,790	15.2	18.1	33:33	08:19		
kg	Kyrgyzstan	19	14	5,300	26.4	35.8	32:46	17:42		
kh	Cambodia	17	10	2,500	40.0	68.0	09:48	08:32		
ki	Kiribati	1	1				39:34	39:34		
kn	Saint Kitts And Nevis									
kr	Korea	145	96	1,095,133	0.9	1.3	75:12	30:59		
kw	Kuwait	1	1	3,800	2.6	2.6	00:30	00:30		
ky	Cayman Islands									
kz	Kazakhstan	147	107	109,605	9.8	13.4	46:43	14:29		
la	Lao People's Demo. Rep. *(estimated)*	17	13	29,000	4.5	5.9	22:39	07:22		
land	generic TLD	2	2	10,831	1.8	1.8	02:50	02:50		
lb	Lebanon	2	1	3,700	2.7	5.4	08:49	08:49		
lc	St. Lucia	3	3	3,972	7.6	7.6	43:30	08:22		
li	Liechtenstein	7	7	64,855	1.1	1.1	43:45	29:40		
lk	Sri Lanka	31	23	16,200	14.2	19.1	52:43	15:55		
lr	Liberia									
ls	Lesotho	4	4				05:21	05:08		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
lt	Lithuania	167	38	164,200	2.3	10.2	34:07	04:46	1	0.1
lu	Luxembourg	26	19	79,800	2.4	3.3	45:02	05:27	1	0.1
lv	Latvia	60	45	111,000	4.1	5.4	42:07	09:48		
ly	Libya	292	9	14,048	6.4	207.9	19:40	04:13		
ma	Morocco	106	92	43,350	21.2	24.5	14:02	00:41	1	0.2
mc	Monaco	1	1	2,300	4.3	4.3	00:30	00:30		
md	Moldova	30	21	24,006	8.7	12.5	31:00	14:18		
me	Montenegro	977	172	761,325	2.3	12.8	31:29	05:48	14	0.2
mg	Madagascar	5	3				40:34	11:22		
mk	Macedonia	32	26	22,500	11.6	14.2	62:05	09:49		
ml	Mali	556	523	34,000	153.8	163.5	31:38	22:05	520	152.9
mn	Mongolia	35	20	16,205	12.3	21.6	38:26	13:45		
mo	Macao	2	2				40:59	40:59		
mobi	sponsored TLD	63	58	1,133,324	0.5	0.6	24:27	07:17	6	0.1
mp	Northern Mariana Islands	1	1				04:52	04:52		
mr	Mauritania									
ms	Montserrat	3	2	8,000	2.5	3.8	115:52	125:34		
mt	Malta *(estimated)*	3	2	6,250	3.2	4.8	22:43	22:43		
mu	Mauritius	99	2	8,000	2.5	123.8	43:12	19:22		
museum	sponsored TLD			431						
mv	Maldives									
mx	Mexico	421	329	711,793	4.6	5.9	42:19	09:23	4	0.1
my	Malaysia	335	231	211,154	10.9	15.9	67:20	14:04	1	0.0
mz	Mozambique	3	3	4,000	7.5	7.5	05:44	03:50		
na	Namibia	1	1				03:04	03:04		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
name	generic TLD	56	33	202,233	1.6	2.8	15:36	05:18	6	0.3
nc	New Caledonia	2	2				48:00	48:00		
ne	Niger	1	1				31:22	31:22		
net	generic TLD	7,059	4,517	15,699,728	2.9	4.5	31:54	07:40	815	0.5
nf	Norfolk Island	26	16	1,417	112.9	183.5	27:30	05:21	1	7.1
ng	Nigeria	43	42	18,000	23.3	23.9	18:26	14:11		
ni	Nicaragua	1	1	6,650	1.5	1.5	20:49	20:49		
nl	Netherlands	742	590	5,460,852	1.1	1.4	33:07	05:52	8	0.0
no	Norway	149	116	625,000	1.9	2.4	38:33	11:38		
np	Nepal	105	93	39,000	23.8	26.9	25:45	02:30		
nr	Nauru			500						
nu	Niue *(estimated)*	39	22	209,000	1.1	1.9	21:43	08:01		
nz	New Zealand	195	157	551,826	2.8	3.5	32:26	10:29		
om	Oman	2	2				02:43	02:43		
org	generic TLD	6,271	3,354	10,446,179	3.2	6.0	28:50	08:45	236	0.2
pa	Panama	1	1				01:15	01:15		
pe	Peru	116	85	78,922	10.8	14.7	35:51	08:07		
pf	French Polynesia	1	1				16:21	16:21		
pg	Papua New Guinea									
ph	Philippines *(estimated)*	352	26	42,300	6.1	83.2	17:47	03:40		
photos	generic TLD	1	1	10,274	1.0	1.0	02:42	02:42		
pk	Pakistan *(estimated)*	115	86	42,000	20.5	27.4	64:41	16:43		
pl	Poland	1,204	710	2,489,623	2.9	4.8	36:44	06:53	7	0.0
pm	Saint Pierre & Miquelon	16	3	5,300	5.7	30.2	17:31	04:36		
pn	Pitcairn	29	12				12:31	04:15		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
post	sponsored TLD			19						
pro	sponsored TLD	32	30	130,664	2.3	2.4	20:20	13:12	1	0.1
ps	Palestinian Territory	11	11	6,600	16.7	16.7	34:40	13:05	1	1.5
pt	Portugal	132	112	240,000	4.7	5.5	34:01	12:44		
pw	Palau	2,484	2,318	190,000	122.0	130.7	30:23	16:00	2,312	121.7
py	Paraguay	10	8	15,000	5.3	6.7	39:32	09:02		
qa	Qatar	5	3				126:39	09:56		
re	Réunion	2	2	22,418	0.9	0.9	01:09	01:09		
ro	Romania	515	407	645,000	6.3	8.0	46:36	11:04		
rs	Serbia	44	34	82,950	4.1	5.3	31:57	04:55		
ru	Russian Fed.	1,449	1,086	4,899,000	2.2	3.0	36:11	09:31	13	0.0
rw	Rwanda									
sa	Saudi Arabia	33	25	28,000	8.9	11.8	64:22	12:36		
sc	Seychelles	1	1	6,217	1.6	1.6				
sd	Sudan	3	3				75:42	102:42		
se	Sweden	136	111	1,324,000	0.8	1.0	34:29	08:56	1	0.0
sg	Singapore	120	99	160,012	6.2	7.5	35:20	09:39		
sh	Saint Helena	4	3				84:39	84:39		
si	Slovenia	80	54	112,180	4.8	7.1	22:44	06:47	1	0.1
sk	Slovakia	111	72	312,160	2.3	3.6	51:41	05:53		
sl	Sierra Leone									
sm	San Marino			1,950						
sn	Senegal	4	4	3,500	11.4	11.4	17:38	13:54		
so	Somalia	3	2				01:34	01:34		

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
sr	Suriname	3	3	2,400	12.5	12.5	20:45	15:02		
st	Sao Tome and Principe	9	6	9,000	6.7	10.0	124:22	07:58		
su	Soviet Union	99	77	119,500	6.4	8.3	23:57	06:39	1	0.1
sv	El Salvador	20	9	7,800	11.5	25.6	31:09	14:30		
sx	Sint Maarten	5	4	5,400	7.4	9.3	19:51	19:51		
sy	Syria									
sz	Swaziland	2	2	1,000	20.0	20.0	32:31	32:31		
tc	Turks and Caicos	3	3				11:51	02:57		
tel	generic TLD			145,968						
tf	French Southern Territories	244	11	3,500	31.4	697.1	11:20	05:06		
tg	Togo	4	2				15:53	16:23		
th	Thailand	262	176	64,099	27.5	40.9	29:11	11:25		
tips	generic TLD	1	1	20,991	0.5	0.5			1	0.5
tj	Tajikistan	1	1	6,200	1.6	1.6	15:09	15:09		
tk	Tokelau	2,652	2,533	23,900,000	1.1	1.1	21:36	05:34	2,533	1.1
tl	Timor-Leste	13	5	2,843	17.6	45.7	32:09	10:21		
tm	Turkmenistan	4	2				23:32	14:23		
tn	Tunisia	13	10	21,900	4.6	5.9	52:25	08:08	2	0.9
to	Tonga	49	13	15,600	8.3	31.4	42:05	15:09		
today	generic TLD	1	1	21,890	0.5	0.5	02:58	02:58		
tp	Portuguese Timor									
tr	Turkey	405	305	351,777	8.7	11.5	48:42	11:54		
travel	sponsored TLD	1	1	19,625	0.5	0.5	54:36	54:36		
tt	Trinidad and Tobago	1	1	2,500	4.0	4.0				

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
tv	Tuvalu	110	89	599,000	1.5	1.8	40:53	07:34	1	0.0
tw	Taiwan	245	172	779,229	2.2	3.1	28:30	11:19		
tz	Tanzania	2	2	6,250	3.2	3.2	29:00	29:00		
ua	Ukraine	471	337	684,364	4.9	6.9	37:29	09:42	1	0.0
ug	Uganda	17	13	3,200	40.6	53.1	31:20	09:39		
uk	United Kingdom	1,560	1,303	10,578,800	1.2	1.5	45:17	09:03	206	0.2
us	United States	508	385	1,754,000	2.2	2.9	27:38	07:13	52	0.3
uy	Uruguay	82	68	69,970	9.7	11.7	72:01	03:40		
uz	Uzbekistan	17	13	17,940	7.2	9.5	42:06	08:54		
vc	St. Vincent and Grenadines	52	5	9,244	5.4	56.3	08:57	04:15	1	1.1
ve	Venezuela *(estimated)*	226	174	125,000	13.9	18.1	27:03	10:44	1	0.1
vg	British Virgin Islands	8	4	8,500	4.7	9.4	36:54	14:39		
vi	Virgin Islands			1,700						
vn	Vietnam	281	206	485,155	4.2	5.8	37:15	12:00		
vu	Vanuatu	292	12				18:38	03:06		
wf	Wallis and Futuna									
ws	Samoa *(estimated)*	212	37	300,000	1.2	7.1	47:20	06:53	6	0.2
xn--3e0b707	.한국 (KR IDN)			59,035						
xn--90a3ac	.СРБ (Serbia IDN)			3,390						
xn--fzc2c9e2c	.ලංකා (Sri Lanka IDN)			10						
xn--mgberp4a5d4a	السعودية (Saudi Arabia IDN)			1,800						

TLD	TLD Location	# Unique Phishing attacks 1H2014	Unique Domain Names used for phishing 1H2014	Domains in registry, April 2014	Score: Phishing domains per 10,000 domains 1H2014	Score: Attacks per 10,000 domains 1H2014	Average Uptime 1H2014 hh:mm	Median Uptime 1H2014 hh:mm	# Total Malicious Domains Registered 1H2014	Malicious registrations score/10,000 domains in registry
xn--o3cw4h	.ไทย (.TH IDN)			16,560						
xn--p1ai	.рф (.RF, Russian Federation IDN)	6	6	825,000	0.1	0.1	12:30	11:23		
xn--xkc2al3hye2a	.□□□□□□ (Sri Lanka IDN)									
xxx	sponsored TLD	8	8	109,412	0.7	0.7	54:00	61:51		
ye	Yemen	2	1	900	11.1	22.2	08:16	08:16		
yt	France									
yu	Yugoslavia (TLD deprecated March 2010)									
za	South Africa	434	351	925,731	3.8	4.7	34:35	09:02	1	0.0
zm	Zambia	3	3				01:48	01:48		
zw	Zimbabwe	2	2	1,100	18.2	18.2	11:47	11:47		
	TOTALS	**123,741**	**87,901**	**279,619,938**					**22,679**	**792.9**

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, Bob Hong, and last but not least Xiaodong Lee at CNNIC for the contribution of APAC phishing data for this report. The authors thank DomainTools for its 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 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 piracy cases. Greg serves as the APWG's Senior Research Fellow, and as Co-Chair of the APWG'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. Greg has advised governments, ccTLD operators, and ICANN regarding registry policies and operations, and he oversaw the launches and operations 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. Rod is co-chair of the Anti-Phishing Working Group's (APWG) Internet Policy Committee and has regularly represented the organization in various forums. Rod is a member of ICANN's Security and Stability Advisory Committee (SSAC) and ICANN's Expert Working Group on gTLD Directory Services. He 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 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.

#