Global Phishing Survey: Trends and Domain Name Use in 2H2013

APWG

Unifying the
Global Response
To Cybercrime

Published 10 April 2014

An
APWG
Industry
Advisory

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

Table of Contents

Overview

Criminals always look for the latest angles – the best resources to use, the best places to find victims, and the best ways to avoid detection. By analyzing the phishing that took place in the second half of 2013, we've gathered a great deal of information about how phishers perpetrated their attacks.

This report seeks to understand trends and their significance by quantifying the scope of the global phishing problem. Specifically, this new report examines all the phishing attacks detected in the second half of 2013 ("2H2013", July 1 to December 31). 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. **Phishing continues to explode in China, where Chinese phishers are victimizing the growing online population of the country. Chinese phishers were responsible for 85% of the domain names that were registered for phishing. (Pages 11-12, 14-15)**
2. **The average uptimes of phishing attacks declined, and were close to historic lows, pointing to some success by anti-phishing responders. (Page 7)**
3. **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)**
4. **Mass hackings of vulnerable shared hosting providers led to 18% of all phishing attacks. (Page 15)**

Key Statistics

Millions of phishing URLs were reported in 2H2013 but the number of unique phishing attacks and domain names used to host them was much smaller.[1] The 2H2013 data set yielded the following statistics:

- **There were at least 115,565 unique phishing attacks worldwide**. **This is nearly a 60% increase over the 72,758 seen the first half of 2013**, but less than the 123,486 attacks we observed in the second half of 2012. Most of the growth in attacks came from phishing that used 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.

[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.

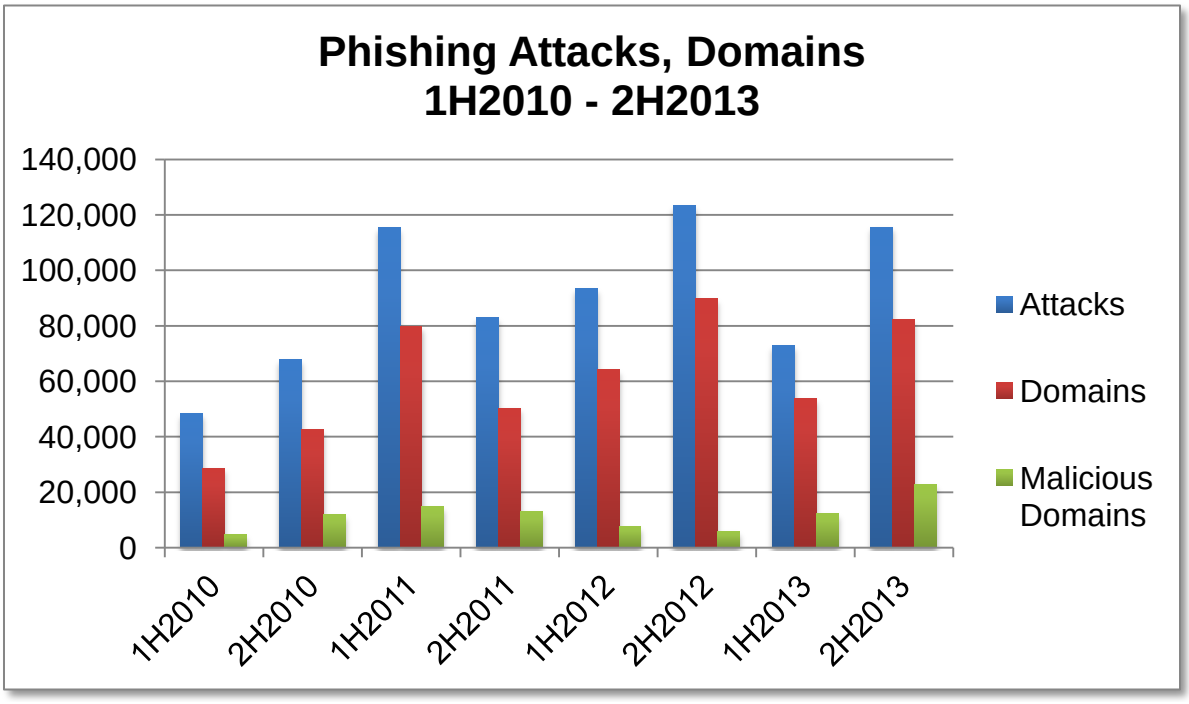
- **The attacks occurred on 82,163 unique domain names.**[2] Again, this is up from the 53,685 domains used in 1H2013. The number of domain names in the world grew from 261 million in April 2013 to 271.5 million in November 2013.[3]
- Of the 82,163 phishing domains, **we identified 22,831 domain names that we believe were registered maliciously, by phishers.** This is significantly higher than the 12,175 we found in 1H2013, and the 5,835 found in 2H2012. **This is the highest number of malicious domain registrations we have ever counted in any of our semiannual surveys, which stretch back seven years to 2007. The increase is due to registrations by Chinese phishers, especially using free domain name registrations in certain TLDs.** The other 59,332 domains were almost all hacked or compromised on vulnerable Web hosting. Please see pages 11-12 for more detail.
- In addition**, 2,394 attacks were detected on 837 unique IP addresses, rather than on domain names.** (For example: http://77.101.56.126/FB/) The number of attacks using IPs has remained steady for four years. None of these phish were found on IPv6 addresses.
- **We counted 681 targeted institutions, down slightly from the 720 targeted institutions identified in 1H2013**.
- **The average uptimes of phishing attacks declined, and were close to historic lows. The average uptime in 2H2013 was 28 hours and 43 minutes.** The median uptime in 2H2013 was 7 hours and 54 minutes, meaning that half of all phishing attacks stay active for less than 8 hours.
- **Phishing occurred in 210 top-level domains (TLDs), but 89% of the malicious domain registrations (20,284) were in just five TLDs**: .COM, .TK, .PW, .INFO, .NET, and .CF.
- **Only about 1.8% of all domain names that were used for phishing contained a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations" on page 11.)
- Eighty-two of the 82,163 domain names were internationalized domain names (IDNs), and none were homographic attacks.
- 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

	2H2013	1H2013	2H2012	1H2012	2H2011	1H2011
Phishing domain names	**82,163**	53,685	89,748	64,204	50,298	79,753
Attacks	**115,565**	72,758	123,476	93,462	83,083	115,472
TLDs used	**210**	194	207	202	200	200
IP-based phish (unique IPs)	**837**	1,626	1,981	1,864	1,681	2,385
Maliciously registered domains	**22,831**	12,173	5,833	7,712	12,895	14,650
IDN domains	**82**	78	147	58	36	33
Number of targets	**681**	720	611	486	487	520



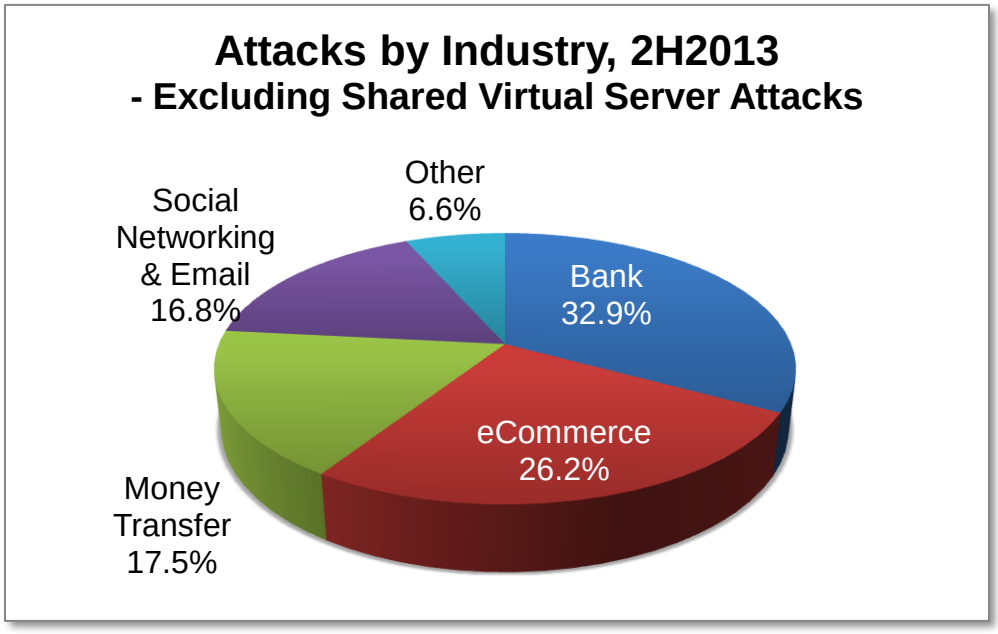
Target Distribution

We counted 681 unique target institutions during the period, down slightly from the 720 found in 2H2012. Of the 681 targets that were phished in 2H2013, almost half of them—324 to be precise—were not phished in 1H2013. This is an unusual amount of "churn" or turnover, and shows phishers trying out new targets. They appear to be 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 2H2013 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 Arab world. The list included diverse sites including AirBNB, Hertz Rent-a-Car, Boise State University, Home Depot, collaboration site Huddle.com, Turkiye Banklar Birligi (the professional bank association of Turkey), Alliance Islamic Bank, Bitcoin-related sites Mt. Gox and Blockchain, jewelry company Tiffany & Co., and the National Bank of Vanuatu.

The number of times that the targets were attacked follows a long tail. PayPal was the most-targeted institution (24,580 attacks, or 21% of the total), followed by Taobao.com (19,290 attacks, or 16.7%). Half of the targets were attacked three or fewer times during the six-month period.

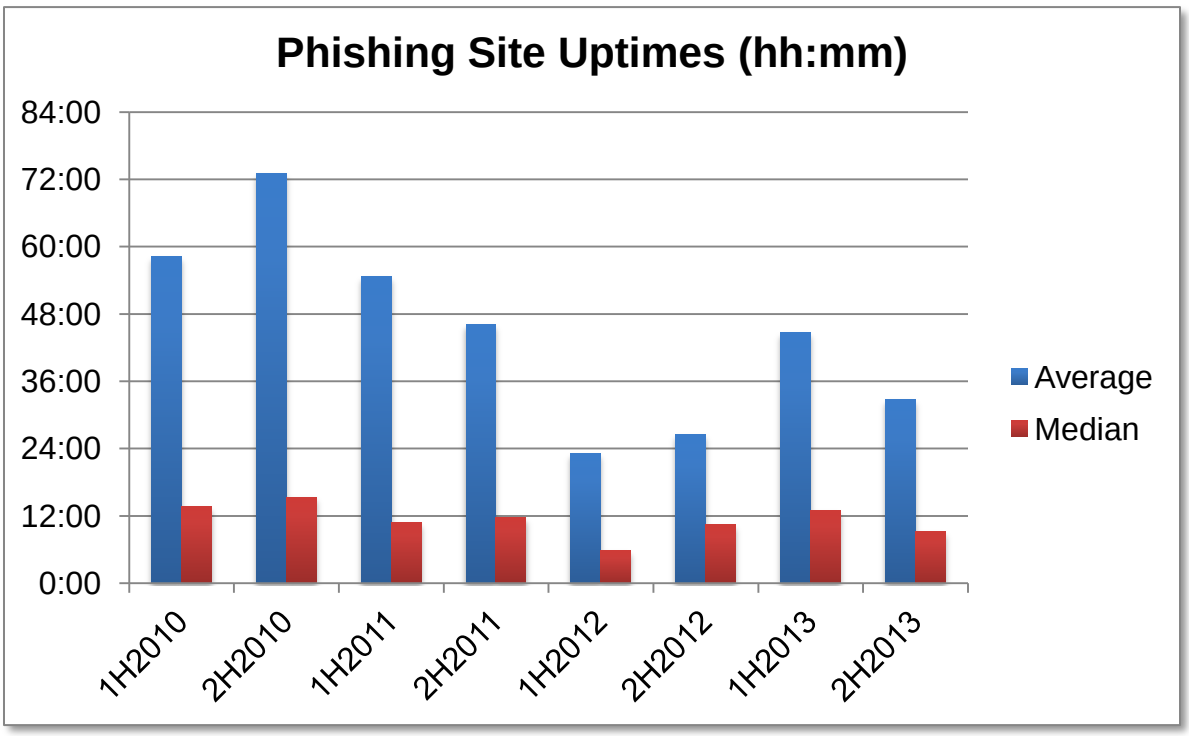
The phishing kits used by less sophisticated phishers tend to contain templates for popular targets. If a site is getting phished for the first time, it may have been targeted by a more sophisticated phisher, who had the skill and motivation to design and execute a new template.



Phishing by Uptime

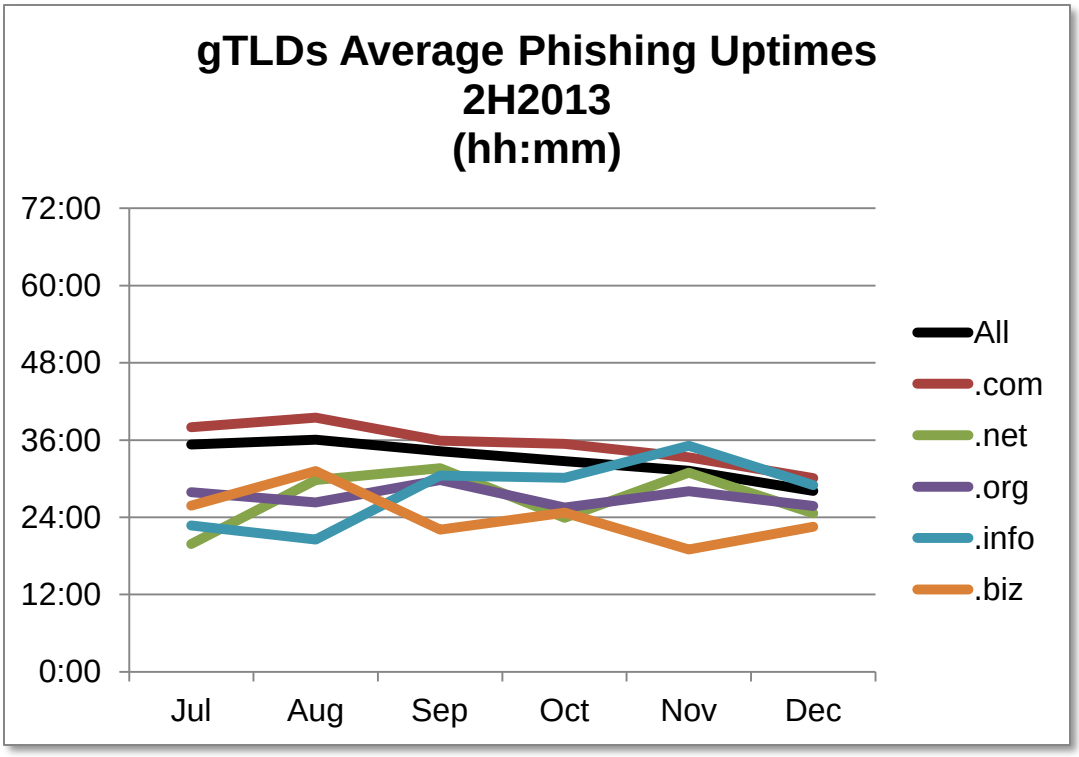
The average uptimes of phishing attacks declined in 2H2013. The average uptime in 2H2013 was 28 hours and 43 minutes. The median uptime in 2H2013 was 7 hours and 54 minutes, meaning that half of all phishing attacks stay active for less than 8 hours.

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 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.

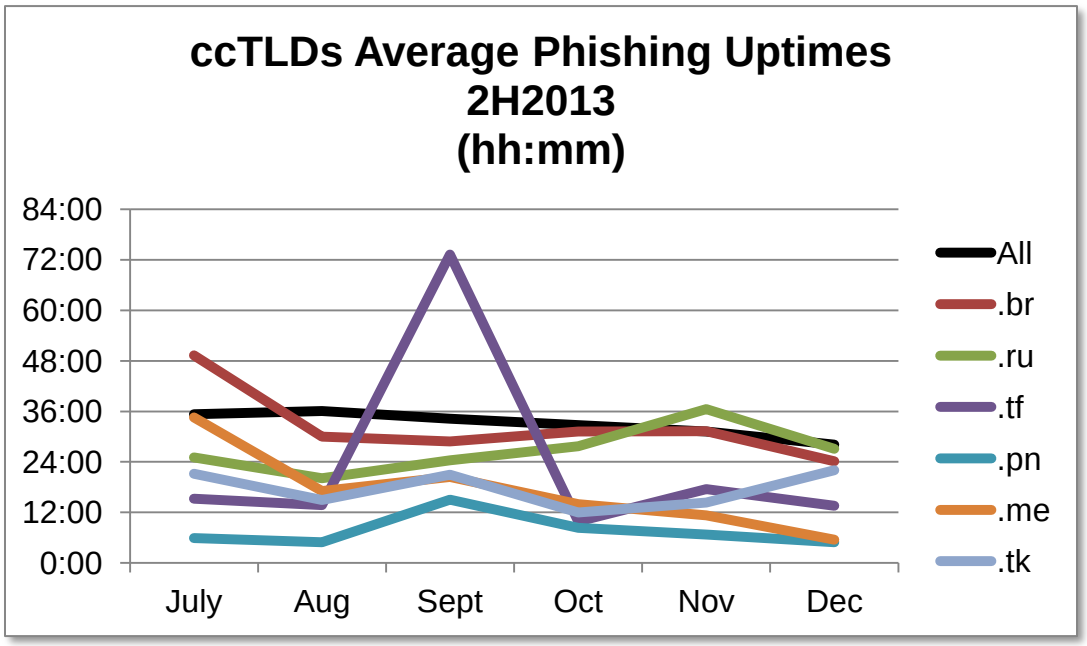


In the large generic top-level domains (gTLDs): the .INFO, .BIZ, and .ORG registry operators have notification and takedown programs; .COM/.NET does not.

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



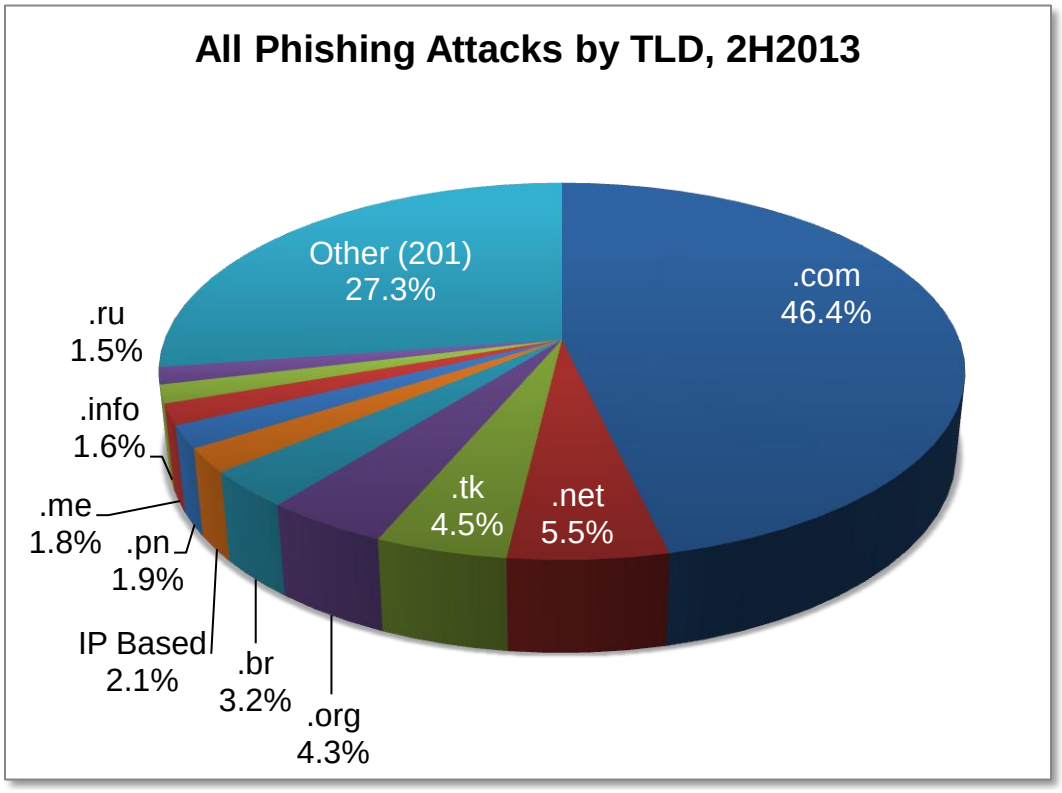
The uptimes at various country-code TLDs (ccTLDs) varied:



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

Prevalence of Phishing by Top-Level Domain (TLD)

We analyzed the phishing domains and attacks to see how they were distributed among the TLDs. The majority of phishing continues to be concentrated in just a few namespaces. Most phishing takes place on compromised domain names, and so the distribution by TLD roughly parallels TLD market share.



To put the numbers in context and measure the prevalence of phishing in a TLD, we use the metrics "Phishing Domains per 10,000" and "Phishing Attacks per 10,000." "Phishing Domains per 10,000"[5] is a ratio of the number of domain names used for phishing in a TLD to the number of registered domain names in that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of phishing relative to others.

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

The complete tables are presented in the Appendix, including the domain and attack scores for each TLD.

- **The median phishing-domains-per-10,000 score was 4.9** (versus 3.1 in 1H2013).
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 3.7.** .COM contained 46% of the phishing domains in our data set, and 42% of the

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

domains in the world.

We therefore suggest that domains-per-10,000 scores between 3.7 and 4.9 occupy the middle ground, with scores above 4.9 indicating TLDs with increasingly prevalent phishing.[6] The top TLDs by score are:

Top 10 Phishing TLDs by Domain Score, 2H2013

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

	TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov 2013	Score: Phishing domains per 10,000 domains 2H2013
1	.np	Nepal	105	88	32,500	27.1
2	.pw	Palau	1,007	924	350,000	26.4
3	.th	Thailand	215	155	64,990	23.8
4	.cl	Chile	1,010	807	443,251	18.2
5	.pe	Peru	112	100	75,116	13.3
6	.gr	Greece	463	407	377,000 *(est.)*	10.8
7	.id	Indonesia	126	104	101,892	10.2
8	.ec	Ecuador	35	31	30,500	10.2
9	.br	Brazil	3,674	3,023	3,322,000	9.1
10	.ma	Morocco	44	33	43,325	7.6

The .NP domains used for phishing all involved compromised domains on hacked web servers. The .PW registry operator applied additional anti-abuse measures to combat malicious registrations in 2H2013, and abuse has decreased sharply since then. Thailand's .TH continues to rank highly, as it has for many years, suffering especially from compromised government and university Web servers.

The .CF, .GA. and .ML registries all suffered a great deal of phishing. Freenom, the operator of those TLDs, declined to provide the number of domains in the three registries, making it impossible to rank them. For more about these TLDs, please see "Compromised Domains versus Malicious Registrations" below.

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 into 2016, the

[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.

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. A number of measures have been put in place in the new gTLD 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 gTLD 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.

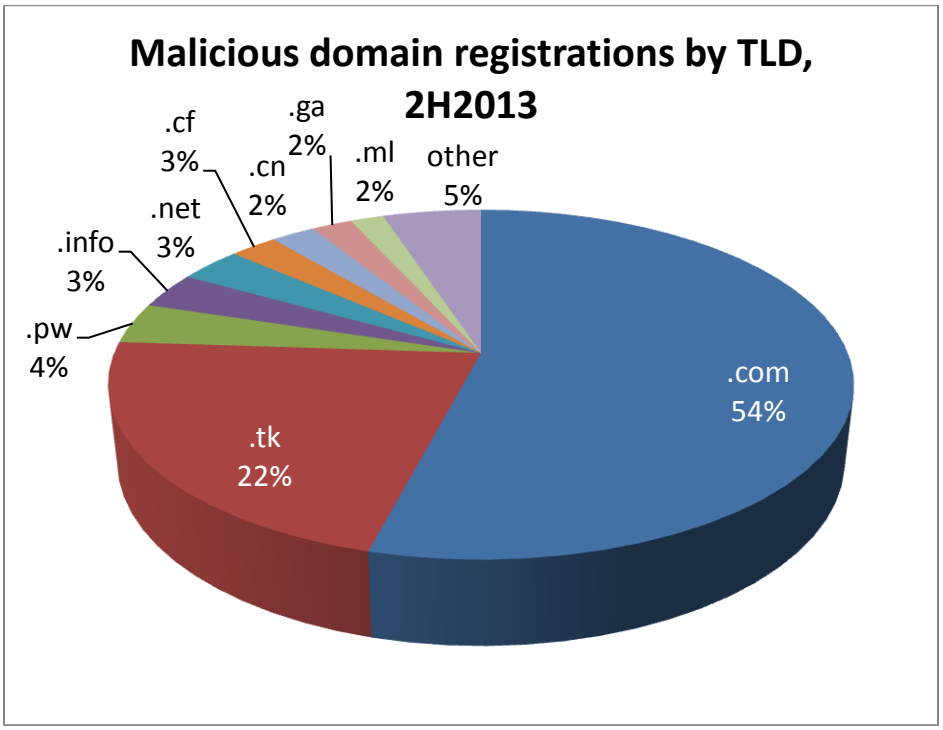
Of the 82,163 domains used for phishing, **we identified 22,831 (27%) that we believe were registered maliciously, by phishers. This was significantly higher than the 12,175 we found in 1H2013, and the 5,835 found in 2H2012. In fact, it is the highest number of malicious domain registrations we have ever counted in any of our semiannual surveys, which stretch back to 2007. The increase is primarily due to registrations by Chinese phishers, who prefer cheap (and free) domain name registrations in certain TLDs.** The other 59,332 domains were almost all hacked or compromised on vulnerable Web hosting.

Of those 22,831 malicious domain registrations, 19,348 (85%) 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, relying upon hacked domains and compromised Web servers less often than phishers elsewhere. The 2H2013 registrations show Chinese phishers increasingly hungry for resources. Their major targets included Taobao.com, the Industrial and Commercial Bank of China (ICBC), CCTV, ZJSTV, and Tencent. The domains were registered in 39 different TLDs, at registrars in China, the US, and Europe, and hosted in China, the US, and elsewhere. The registrations clustered around ten TLDs:

[7] 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.

	TLD	Number of malicious registrations (total)	Number of malicious registrations that targeted Chinese brands
1	.com	12,347	10,822
2	.tk	5,016	4,518
3	.pw	860	819
4	.info	763	575
5	.net	740	424
6	.cf	558	552
7	.cn	519	515
8	.ga	479	461
9	.ml	392	379
10	.asia	152	118

Phishing kits containing templates for a variety of Chinese targets can be purchased in underground fora for RMB1,000 – about US$160. At this rate, just one or two successful phishing attacks can pay for the kit.



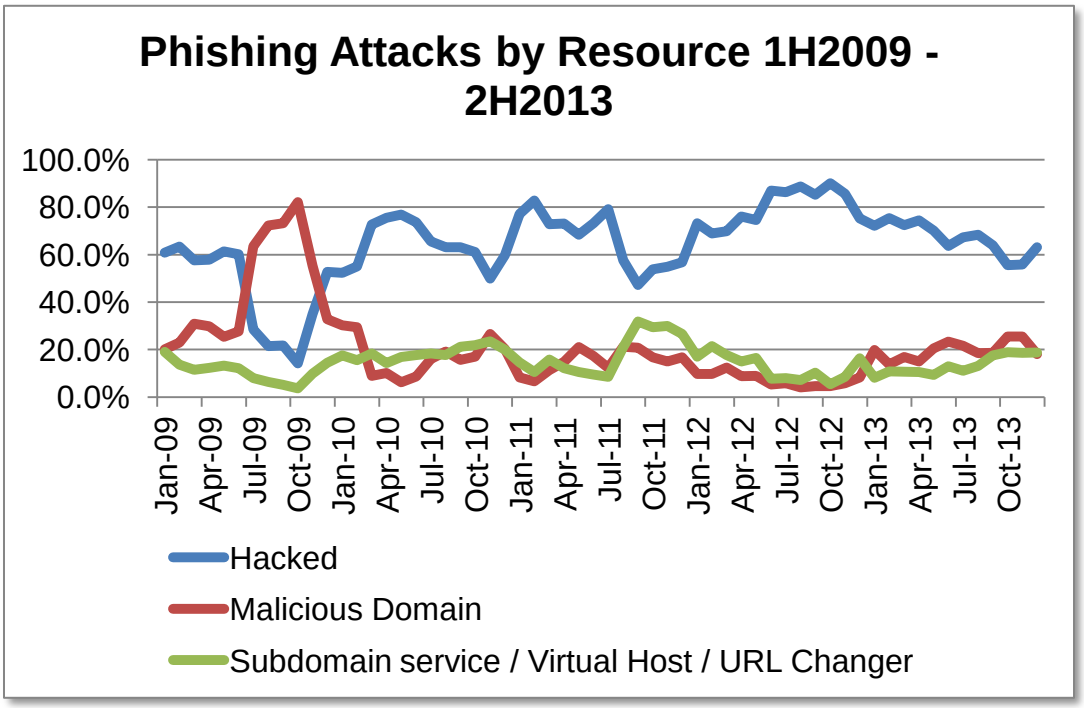
The .TK, .CF, .GA, and .ML registries are all run by Freenom, a Netherlands-based company that offers free domain name registrations. (It then monetizes the traffic to the expired domains.) Freenom has operated .TK under the free model for several years, and added .CF, .GA, and .ML to its program during 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, the mitigation of the malicious registrations lagged in Freenom's new spaces -- .CF, .GA. and .ML all had uptimes that were above the global average and median. Freenom declined to provide us with the number of domains registered in these three TLDs.

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.

Of the 22,831 maliciously registered domains, just 1,541 contained a relevant brand name or reasonable variation thereof—often a misspelling.[8] **This represents 1.8% of all domains that were used for phishing, and just 6.7% 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. 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.



[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).

Registrars Used for Malicious Domain Registrations

Phishers (especially Chinese phishers) registered many more domain names in 2H2013 than in any period we have studied, back to 2007. The increase is troubling, since malicious registrations had been trending downward since 2010, and reducing malicious registrations has been a primary motivation for writing the Global Phishing Surveys.

Where are the phishers registering these domains? We were able to obtain the name of the sponsoring registrar for 92% 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.

Phishers utilized at least 230 registrars in 2H2013. GoDaddy holds roughly half of the gTLD market, but sponsored only 7% 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 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 65% (10,650) of the domains registered maliciously.

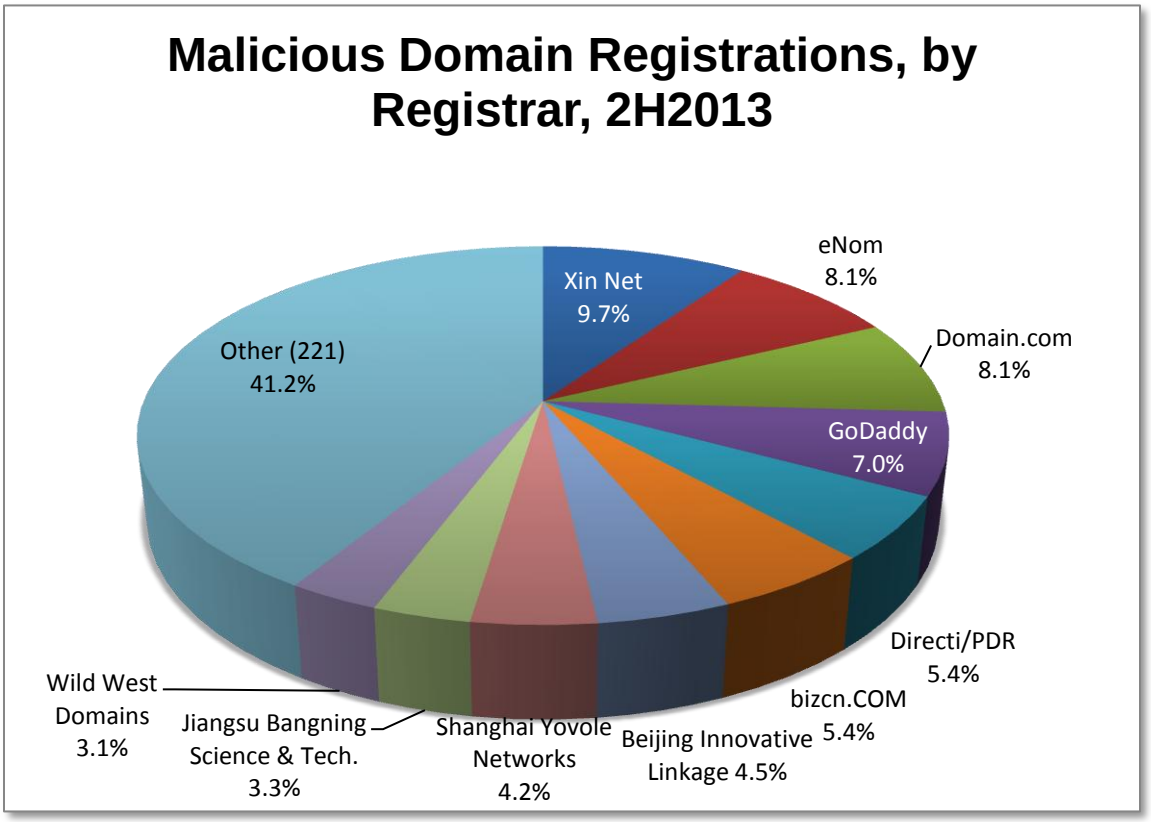
Top Phishing Registrars by Malicious Domain Score 2H2013

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

Rank	Registrar	Malicious Domains	Domains at registrar, Nov. 2014	Malicious Domains per 10,000
1	Ninhand Networks Co. Ltd. *(China)*	175	37,303	46.9
2	Guangdong Jin Wanbang Technology Investment Co., Ltd. *(China)*	430	207,718	20.7
3	Bizcn.com, Inc. *(China)*	887	475,501	18.7
4	Hangzhou Aiming Network Co.,Ltd *(China)*	466	299,440	15.6
5	Beijing Innovative Linkage Technology Ltd. dba dns.com.cn *(China)*	748	498,143	15.0
6	Xin Net Technology Corp. *(China)*	1,591	1,370,776	11.6
7	Jiangsu Bangning Science & Technology Co. Ltd *(China)*	538	464,285	11.6
8	Shanghai Yovole Networks Inc. *(China)*	700	612,941	11.4
9	35 Technology Co., Ltd *(China)*	464	434516	10.7
10	Domain.com, LLC *(USA)*	1,333	2,251,001	5.9

11	Chengdu West Dimension Digital Technology Co., Ltd. *(China)*	191	350,153	5.5
12	1 API GMBH *(Germany)*	209	383,689	5.4
13	Directi/PDR *(India)*	895	3,932,561	2.3
14	Wild West Domains *(USA)*	506	3,926,702	1.3
15	eNom *(USA)*	1,338	11,576,561	1.2
16	Hichina Zhicheng Technology Ltd. *(China)*	179	1,778,977	1.0

The top nine registrars are located in China. This is 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 515 .CN domains for phishing, almost exclusively through Chinese registrars, a number triple that in 1H2013.

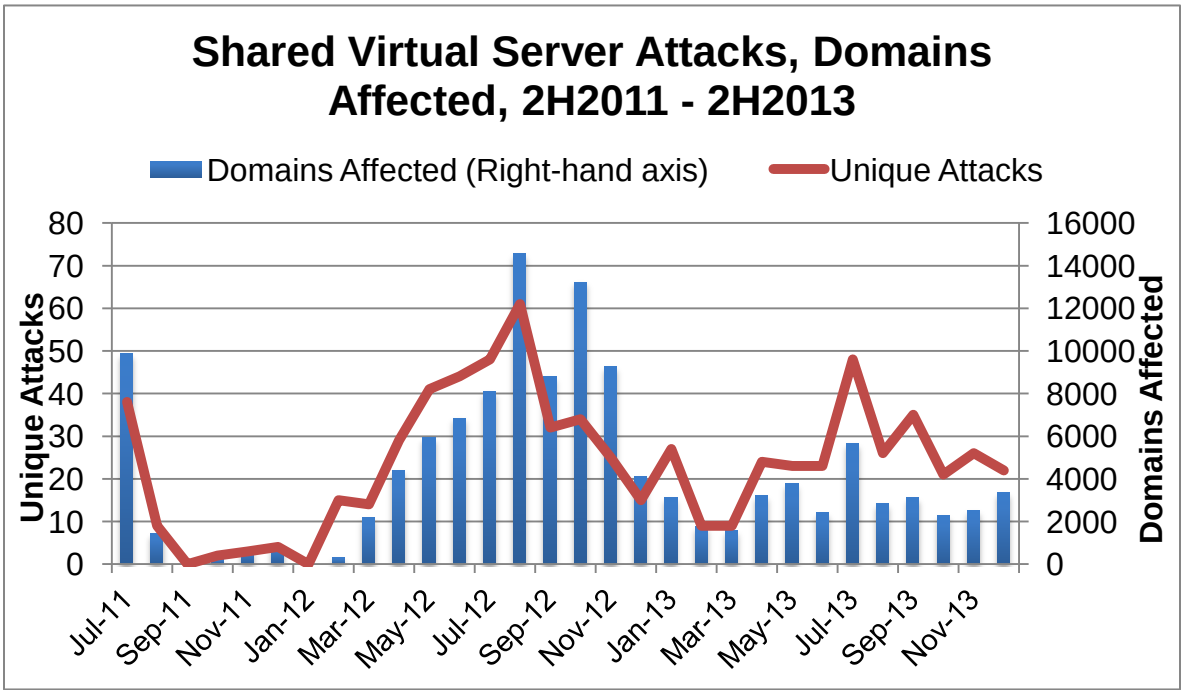


About 28% of the world's malicious registrations were made at the ccTLD registries run by Freenom (.TK, .CF, .GA, and .ML.) Freenom also serves as the registrar for those domains. These large numbers of fraudulent ccTLD domain registrations were excluded from the analysis above. However, they do make 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. 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 2H2013, we identified 178 mass break-ins of this type, resulting in 20,911 phishing attacks. This represents 18% of all phishing attacks recorded worldwide. Though there were more break-ins in 2H2013, they resulted in about the same overall level of attack as 1H2013, when we identified 19,455 virtual server phishing attacks (27% of the total). The 2H2013 attacks apparently targeted servers with smaller numbers of domains hosted on them than in 1H2013.



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 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 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 and need to get serious about it.

Use of Subdomain Services for Phishing

After seeing steady declines for over a year, **we saw the use of subdomain registrations for phishing more than double in 2H2013**. However, because of the large jump in domains registered for phishing in the same period, phishers still registered far fewer subdomains than they registered "regular" domain names. **However, subdomain registrations still represent 15% 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:

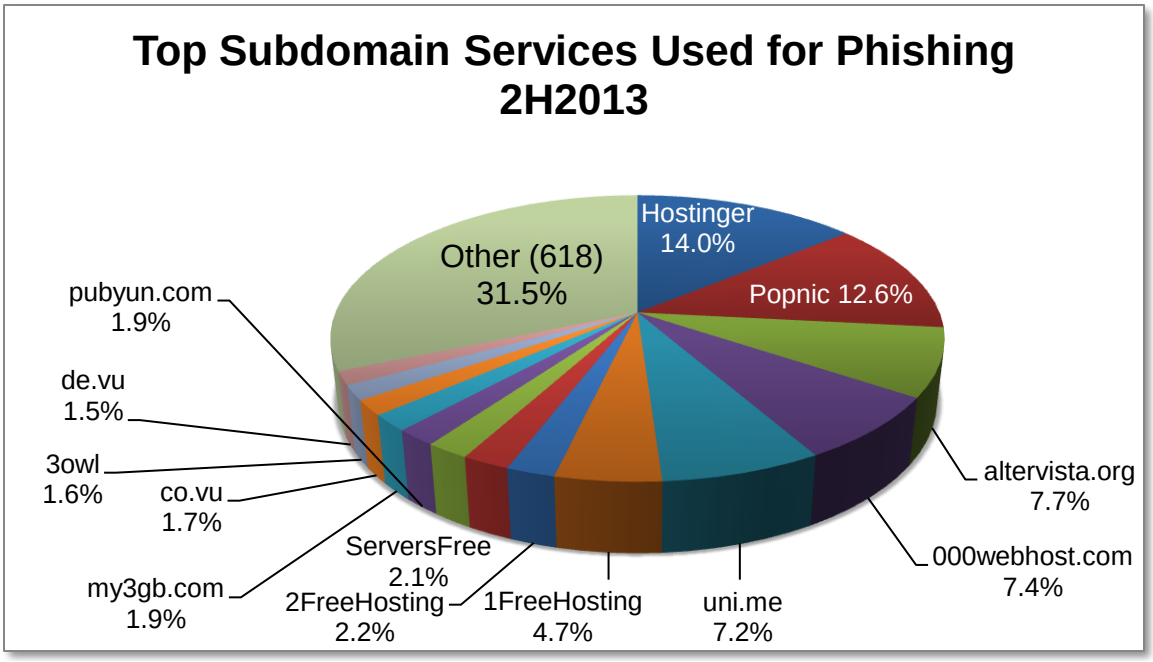
<customer_term>.<service_provider_sld>.TLD

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.[9] While many of these services are responsive to complaints, proactive measures to keep criminals from abusing their services are limited.

There were 17,674 phishing attacks hosted on subdomain services in the second half of 2013, on 17,703 unique subdomains that utilized 795 domain names. This is more than double the 7,134 attacks we recorded in 1H2013, and represented 15% of all 2H2013 phishing attacks. Many of the subdomain attacks were against Chinese targets like Taobao.com, but a majority attacked online services like FaceBook, Yahoo, and PayPal.

We saw a large number of subdomain services being abused by phishers for the first time. **More than 200 subdomain service domains were abused in 2H2013 that we had never seen in prior reports**. 1,272 attacks were hosted on the new service "hyd.me" alone. Clearly, phishers love to "test-drive" new subdomain services.

[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.



The favorite service for phishers to abuse in 2H2013 was Hostinger (back-ended by Maine-Hosting), where at least 2,476 malicious subdomains were spotted, representing 14% of all subdomain phishing. This service runs dozens of domains under its service, and is very prompt at removing abuse. Unfortunately, Hostinger lacks a method to deter phishers from using its service in the first place.

Second on the list was a provider that "popped" onto the list for this period--PopNIC. This service seems to be professionally run, and provides a WHOIS service and an online abuse reporting form. Perhaps a recent marketing campaign has brought awareness of PopNIC's free subdomains to the attention of phishers, and its easy-to-use control panel may be another draw.

PopNIC.com

Top Subdomain Services Used for Phishing, 2H2013

Rank	Attacks	Provider
1	2,476	Hostinger
2	2,237	popnic.com
3	1,361	altervista.org
4	1,301	000webhost.com
5	1,272	uni.me
6	834	1FreeHosting
7	387	2FreeHosting
8	378	ServersFree
9	346	uCoz
10	331	pubyun.com
11	329	my3gb.com
12	302	co.vu
13	290	3owl
14	269	de.vu
15	243	at.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 ă 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 2013 we found only eight true homographic phishing attacks, and none in 2H2013.

Eighty-two IDN domains names were used for phishing in 2H2013, but only eight were malicious registrations, with the others being hacked domains. When phishers do play with IDNs, they usually involve additional words other than brand names, and the non-IDN equivalents are readily available. For example, a phisher registered the non-IDN domain

espace-securite-ebay.com in August 2013, and then registered an IDN variation a few weeks later, perhaps just because he liked the first one:

xn--espace-scurit-ebay-iwbf.com → espace-sécurité-ebay.com

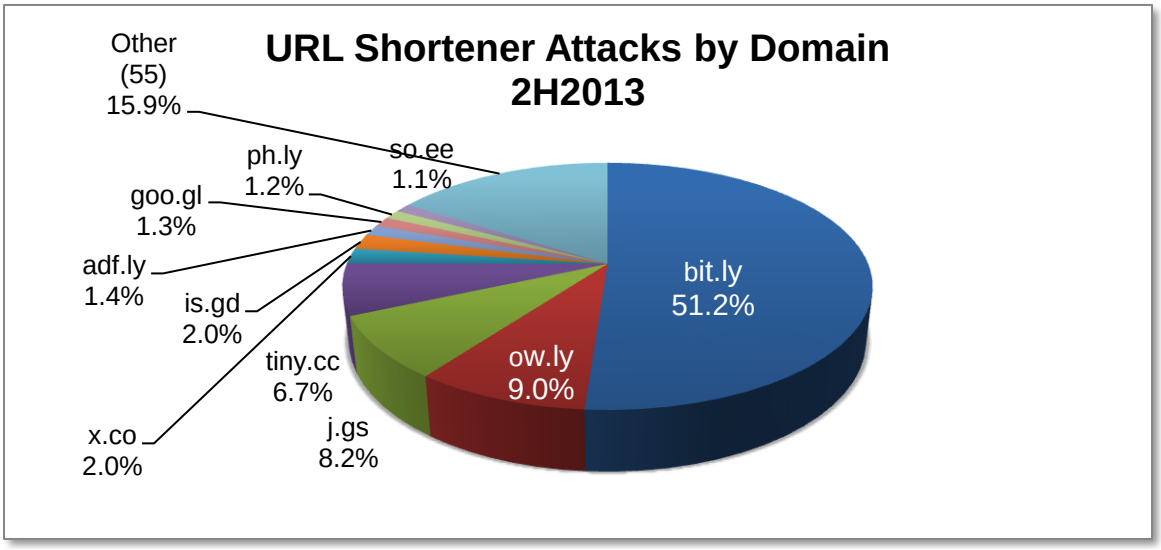
Given that IDNs have been widely available for years, why haven't phishers utilized IDN homographic attacks more often?

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.

Beginning in early 2014, a series of new IDN registries are launching under the auspices of ICANN's new gTLD program. 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. 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. In our last report, such use plummeted to only 270 attacks in 1H2013, sharply down from 785 in 2H2012. Unfortunately, the phishers have come back to using this technique again, with 999 such phishing attacks detected in 2H2013.



In 2H2013, just over half of the 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. This is disappointing, as tinyURL barely made our 1H2013 report at all, after being the most abused system in prior reports. In 2H2013 the phishers likely figured out how to game tinyURL's system better, as the appearance of malicious URLs using tinyURL grew from an average one per day in July 2013 to at least 144 in December 2013.

It has become clear from both their stated policies and actual results that most of the major URL shortener providers have put better screening for malicious forwarding destinations in place, and are making it easier and more efficient to report abuse. 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.

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 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
ac	Ascension Island	4	3	16,200	1.9	2.5	20:44	20:44		
ad	Andorra	1	1	1,500	6.7	6.7	0:20	0:20		
ae	United Arab Emirates	39	22	104,000	2.1	3.8	65:24	13:10		
aero	sponsored TLD	3	3	8,947	3.4	3.4	24:47	24:47		
af	Afghanistan	5	3				24:19	11:56		
ag	Antigua and Barbuda	3	3	19,766	1.5	1.5	22:56	25:15	2	
ai	Anguilla	7	4	3,800	10.5	18.4	13:05	11:54		
al	Albania	8	7	7,800	9.0	10.3	53:04	16:45		
am	Armenia	56	21	22,090	9.5	25.4	15:59	8:55		
an	Netherlands Antilles	16	2	800	25.0	200.0	36:05	42:03		
ao	Angola	1	1	300	33.3	33.3	9:15	9:15		
ar	Argentina	829	658	2,800,000	2.4	3.0	36:29	8:51	7	0.0
arpa	Advanced Research Project Agency									
as	American Samoa	7	2				150:35	12:36		
asia	sponsored TLD	273	222	442,069	5.0	6.2	40:10	8:19	152	3.4
at	Austria	171	141	1,210,450	1.2	1.4	33:24	9:41	3	0.0
au	Australia	1,314	1,056	2,737,931	3.9	4.8	44:34	9:17	6	0.0
aw	Aruba			625						
ax	Åland Islands	1	1				7:31	7:31		
az	Azerbaijan	17	15	20,050	7.5	8.5	70:14	32:32	1	0.5
ba	Bosnia and Herzegovina	27	21	15,292	13.7	17.7	56:44	21:45	1	0.7
bd	Bangladesh	25	25	5,000	50.0	50.0	31:30	13:04		
be	Belgium	314	252	1,429,548	1.8	2.2	47:30	10:20	6	0.0
bf	Burkina Faso									
bg	Bulgaria	20	13	26,000	5.0	7.7	17:27	2:51		
bh	Bahrain									
bi	Burundi	2	2				55:36	82:50		
biz	generic TLD	713	617	2,697,853	2.3	2.6	28:48	6:39	85	0.3

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
bm	Bermuda	1	1	8,100	1.2	1.2	25:46	25:46		
bn	Brunei Darussalam			1,150						
bo	Bolivia	12	11	8,500	12.9	14.1	9:42	4:40		
br	Brazil	3,674	3,023	3,322,000	9.1	11.1	33:16	9:43	29	0.1
bs	Bahamas			2,400						
bt	Bhutan	44	37	1,100	336.4	400.0	27:28	5:16		
bw	Botswana	3	3				9:56	10:18		
by	Belarus	272	180				36:33	8:40		
bz	Belize	28	20	44,845	4.5	6.2	60:15	9:37	1	
ca	Canada	671	527	2,195,000	2.4	3.1	54:17	9:51	3	0.0
cat	sponsored TLD	21	17	70,476	2.4	3.0	22:31	7:04		
cc	Cocos (Keeling) Islands (estimated)	380	186	750,000	2.5	5.1	13:50	5:23	126	1.7
cd	Congo, Democratic Repub. (estimated)	8	4	5,200	7.7	15.4	11:01	10:49		
cf	Central African Republic	594	558	*(operator declined)*			30:44	11:30	558	
cg	Congo									
ch	Switzerland	209	172	1,827,020	0.9	1.1	31:53	7:44	1	0.0
ci	Côte d'Ivoire	1	1	2,500	4.0	4.0	48:15	48:15		
cl	Chile	1,010	807	443,251	18.2	22.8	38:52	10:40	3	0.1
cm	Cameroon *(estimated)*	13	11	12,500	8.8	10.4	44:52	7:38	3	2.4
cn	China	938	799	9,609,571	0.8	1.0	33:33	10:52	519	0.5
co	Colombia	406	274	1,576,833	1.7	2.6	15:12	5:35	23	0.1
com	generic TLD	53,592	42,086	114,076,050	3.7	4.7	35:18	9:19	12,347	1.1
coop	sponsored TLD	1	1	7,718	1.3	1.3	31:25	31:25		
cr	Costa Rica	10	8	15,161	5.3	6.6	41:54	9:03		
cu	Cuba			2,351						
cv	Cape Verde			900						
cx	Christmas Island	35	12	5,520	21.7	63.4	31:07	7:53		
cy	Cyprus	13	10	12,500	8.0	10.4	19:24	12:15		
cz	Czech Republic	295	201	1,091,320	1.8	2.7	37:45	10:08		
de	Germany	1,078	855	15,629,804	0.5	0.7	27:15	8:16	81	0.1
dj	Djibouti	1	1				4:40	4:40		
dk	Denmark	183	128	1,253,528	1.0	1.5	35:09	10:29	1	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
dm	Dominica			14,000						
do	Dominican Republic	18	18				19:30	0:26		
dz	Algeria	3	2	5,256	3.8	5.7	10:58	12:15		
ec	Ecuador	35	31	30,500	10.2	11.5	37:58	9:13		
edu	U.S. higher education	35	16	7,590	21.1	46.1	60:55	16:31		
ee	Estonia	92	13	72,325	1.8	12.7	15:46	7:49	1	0.1
eg	Egypt *(estimated)*	11	8	6,000	13.3	18.3	25:47	16:08		
er	Eritrea			120						
es	Spain	1,125	349	1,698,696	2.1	6.6	30:52	10:56	4	0.0
et	Ethiopia	2	2	1,200	16.7	16.7	30:31	33:58		
eu	European Union	456	386	3,700,750	1.0	1.2	30:49	9:00	29	0.1
fi	Finland	67	56	337,448	1.7	2.0	46:33	12:11		
fj	Fiji	7	2	4,000	5.0	17.5	11:21	8:37		
fk	Falkland Islands			110						
fm	Micronesia, Fed. States	9	7				25:08	4:20		
fo	Faroe Islands	4	3				231:01	234:53	1	
fr	France	894	653	2,702,620	2.4	3.3	48:28	11:20	146	0.5
ga	Gabon	526	479	*(operator declined)*			29:09	13:19	479	
gd	Grenada	11	3	4,400	6.8	25.0	9:20	10:37		
ge	Georgia	37	30	20,500	14.6	18.0	34:52	10:46		
gg	Guernsey	108	8				6:24	3:11		
gh	Ghana	2	1				15:58	23:44		
gi	Gibraltar			2,061						
gl	Greenland	68	2	5,500	3.6	123.6	6:37	2:08		
gm	Gambia	1	1				3:43	3:43		
gov	U.S. government			5,000						
gp	Guadeloupe	29	17	1,500	113.3	193.3	34:50	11:30		
gr	Greece *(estimated)*	463	407	377,000	10.8	12.3	36:11	6:19	3	0.1
gs	South Georgia & Sandwich Islands	37	10				16:08	4:13	1	
gt	Guatemala	11	10	13,256	7.5	8.3	15:11	14:15		
gy	Guyana	13	3				7:14	8:49		
hk	Hong Kong	57	41	252,155	1.6	2.3	29:04	14:23	4	0.2

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
hm	Heard and McDonald Is.									
hn	Honduras	2	2				102:34	149:35		
hr	Croatia	185	178	81,517	21.8	22.7	29:36	14:50		
ht	Haiti	428	5	2,200	22.7	1,945.5	16:19	11:17		
hu	Hungary	198	150	636,000	2.4	3.1	38:24	13:57		
id	Indonesia	126	104	101,892	10.2	12.4	48:10	10:06	1	0.1
ie	Ireland	113	80	183,990	4.3	6.1	23:21	6:58		
il	Israel	83	70	228,500	3.1	3.6	51:19	10:05	1	0.0
im	Isle of Man	43	12				44:57	7:07		
in	India	915	749	1,345,819	5.6	6.8	49:04	9:20	46	0.3
info	generic TLD	1,800	1,541	5,931,947	2.6	3.0	28:20	9:12	763	1.3
int	sponsored TLD									
io	British Indian Ocean Terr.	5	5				16:10	15:08		
IP address	(no domain name used)	2,394								
iq	Iraq			450						
ir	Iran	419	336	459,623	7.3	9.1	33:05	9:51	2	0.0
is	Iceland	21	19	45,800	4.1	4.6	67:36	8:00		
it	Italy	618	491	2,500,000	2.0	2.5	39:37	11:39	3	0.0
je	Jersey	2	2				15:53	23:00		
jm	Jamaica	2	2	6,300	3.2	3.2	0:17	0:17		
jo	Jordan	3	3	4,360	6.9	6.9	51:45	60:09		
jobs	sponsored TLD			44,443						
jp	Japan	149	108	1,353,969	0.8	1.1	62:41	13:11	1	0.0
ke	Kenya	52	37	29,109	12.7	17.9	35:12	16:18		
kg	Kyrgyzstan	6	4	5,300	7.5	11.3	9:30	2:32		
kh	Cambodia	8	6				10:23	9:33		
ki	Kiribati									
kn	Saint Kitts And Nevis									
kr	Korea	298	180	1,048,000	1.7	2.8	47:19	11:47		
kw	Kuwait	1	1				3:15	3:15		
ky	Cayman Islands	3	3				1:00	1:07		
kz	Kazakhstan	83	64	100,360	6.4	8.3	47:10	14:52	2	0.2
la	Lao People's Demo. Rep. *(domains estimated)*	7	5	9,000	5.6	7.8	31:58	4:00		

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
lb	Lebanon	1	1	3,700	2.7	2.7	18:16	18:16		
lc	St. Lucia	15	12	3,950	30.4	38.0	12:19	10:36	1	
li	Liechtenstein	18	6	64,500	0.9	2.8	158:20	9:30		
lk	Sri Lanka	22	16				44:04	28:51		
lr	Liberia	4	2				23:49	25:20		
ls	Lesotho	11	7				44:40	11:01		
lt	Lithuania	125	51	160,600	3.2	7.8	22:35	10:43		
lu	Luxembourg	16	11	77,900	1.4	2.1	19:27	6:22		
lv	Latvia	70	44	111,000	4.0	6.3	18:00	9:09		
ly	Libya	106	5	13,950	3.6	76.0	21:54	4:45		
ma	Morocco	44	33	43,325	7.6	10.2	33:51	11:08		
mc	Monaco			2,400						
md	Moldova	34	32	23,400	13.7	14.5	28:16	10:07	1	0.4
me	Montenegro	2,077	120	723,511	1.7	28.7	12:40	4:26	9	0.1
mg	Madagascar									
mk	Macedonia	23	23				38:36	6:05		
ml	Mali	419	392	*(operator declined)*			30:05	8:33	392	
mn	Mongolia	19	14	15,106	9.3	12.6	27:01	17:21	1	
mo	Macao									
mobi	sponsored TLD	40	37	1,200,531	0.3	0.3	35:49	9:47	4	0.0
mp	Northern Mariana Islands	1	1				91:50	91:50		
mr	Mauritania	1	1				1:50	1:50		
ms	Montserrat	23	8	9,500	8.4	24.2	90:16	54:24	1	1.1
mt	Malta *(estimated)*	6	6	6,250	9.6	9.6	26:17	26:17		
mu	Mauritius	480	6	8,000	7.5	600.0	27:25	13:27		
museum	sponsored TLD			431						
mv	Maldives	1	1				5:56	5:56		
mx	Mexico	486	335	687,155	4.9	7.1	24:38	7:02		
my	Malaysia	172	127	182,162	7.0	9.4	33:13	10:15	1	0.1
mz	Mozambique	8	4	4,000	10.0	20.0	21:15	9:15		
na	Namibia									
name	generic TLD	36	30	208,831	1.4	1.7	23:11	11:13	2	0.1
nc	New Caledonia	3	3				0:41	0:41		

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
ne	Niger	5	2				8:39	7:38		
net	generic TLD	6,340	4,232	15,563,189	2.7	4.1	27:26	7:46	740	0.5
nf	Norfolk Island	14	2	1,417	14.1	98.8	12:49	3:08		
ng	Nigeria	26	20				50:33	14:27		
ni	Nicaragua	4	4	6,650	6.0	6.0	13:08	6:14		
nl	Netherlands	664	523	5,378,109	1.0	1.2	39:04	11:49	7	0.0
no	Norway	143	123	604,756	2.0	2.4	52:14	6:58		
np	Nepal	105	88	32,500	27.1	32.3	47:37	5:03		
nr	Nauru			450						
nu	Niue *(domains estimated)*	60	29				26:50	13:49	1	
nz	New Zealand	123	98	540,506	1.8	2.3	31:17	9:35		
om	Oman	2	2				0:15	0:15	1	
org	generic TLD	4,931	2,870	10,367,948	2.8	4.8	27:50	11:34	147	0.1
pa	Panama	4	4				11:32	13:36		
pe	Peru	112	100	75,116	13.3	14.9	44:52	8:17		
pf	French Polynesia	1	1				9:11	9:11		
pg	Papua New Guinea	1	1				2:55	2:55		
ph	Philippines *(declines to issue registration #)*	195	28				21:32	10:38		
pk	Pakistan *(declines to issue registration #)*	207	124				25:32	5:02		
pl	Poland	1,237	794	2,489,121	3.2	5.0	39:34	11:56	9	0.0
pm	Saint Pierre and Miquelon	1	1				0:29	0:29		
pn	Pitcairn	2,242	15				9:26	4:51	3	
post	sponsored TLD			19						
pro	sponsored TLD	27	26	141,132	1.8	1.9	35:30	12:02		
ps	Palestinian Territory	19	19	6,923	27.4	27.4	91:54	10:41		
pt	Portugal	197	141	239,200	5.9	8.2	39:37	13:12		
pw	Palau	1,007	924	350,000	26.4	28.8	24:52	10:55	860	24.6
py	Paraguay	37	33	15,000	22.0	24.7	79:46	8:02	1	0.7
qa	Qatar	1	1				115:51	115:51		
re	Réunion	3	3	22,418	1.3	1.3	44:19	55:18		
ro	Romania	518	413	646,707	6.4	8.0	41:59	9:20	3	
rs	Serbia	45	37	82,700	4.5	5.4	20:01	11:39	1	0.1

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
ru	Russian Fed.	1,694	1,274	4,910,000	2.6	3.5	27:19	6:05	17	0.0
rw	Rwanda	4	3				49:05	47:39		
sa	Saudi Arabia	19	16	30,500	5.2	6.2	76:45	11:26		
sc	Seychelles	3	3	5,024	6.0	6.0	14:38	16:36	1	
sd	Sudan	6	6				14:09	20:38		
se	Sweden	280	231	1,341,000	1.7	2.1	49:56	11:48	1	0.0
sg	Singapore	121	103	154,824	6.7	7.8	22:23	11:34		
sh	Saint Helena	2	2	3,000	6.7	6.7	18:53	26:20	1	3.3
si	Slovenia	92	44	111,900	3.9	8.2	22:16	13:24		
sk	Slovakia	89	60	3,091,189	0.2	0.3	43:54	9:35	3	0.0
sl	Sierra Leone	2	2				31:39	31:39		
sm	San Marino			1,950						
sn	Senegal	4	2	3,500	5.7	11.4	61:27	52:24		
so	Somalia	3	3				7:38	11:16	1	
sr	Suriname									
st	Sao Tome and Principe	6	5				8:05	8:22	1	
su	Soviet Union	118	87	125,300	6.9	9.4	24:01	7:20		
sv	El Salvador	7	6	6,500	9.2	10.8	27:39	21:34		
sy	Syria	1	1				98:03	98:03		
sz	Swaziland									
tc	Turks and Caicos	8	7				5:36	4:08	1	
tel	generic TLD			188,212						
tf	French Southern Territories	252	14	1,500	93.3	1,680.0	17:00	8:40	1	6.7
tg	Togo									
th	Thailand	215	155	64,990	23.8	33.1	31:23	9:48	1	0.2
tj	Tajikistan	3	2	6,200	3.2	4.8	18:22	19:05		
tk	Tokelau	5,251	5,016	20,109,953	2.5	2.6	18:40	5:45	5,016	2.5
tl	Timor-Leste	9	3	2,840	10.6	31.7	13:58	14:31		
tm	Turkmenistan	7	2				7:58	11:51		
tn	Tunisia	34	24	19,500	12.3	17.4	96:57	7:40		
to	Tonga *(estimated)*	39	20	15,500	12.9	25.2	65:48	28:23		
tp	Portuguese Timor									
tr	Turkey	272	203	337,633	6.0	8.1	49:00	14:40		
travel	sponsored TLD	8	6	20,180	3.0	4.0	95:13	18:35		

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
tt	Trinidad and Tobago			2,500						
tv	Tuvalu *(domains est.)*	95	80	175,000	4.6	5.4	26:45	7:20	1	0.1
tw	Taiwan	136	99	766,241	1.3	1.8	88:53	12:24	3	0.0
tz	Tanzania	13	12	6,250	19.2	20.8	35:55	18:34		
ua	Ukraine	411	271	685,318	4.0	6.0	41:26	9:13	3	0.0
ug	Uganda	5	5	3,200	15.6	15.6	12:40	6:33		
uk	United Kingdom	1,612	1,433	10,548,454	1.4	1.5	39:10	9:37	100	0.1
us	United States	420	338	1,795,000	1.9	2.3	33:27	8:25	46	0.3
uy	Uruguay	50	42	68,381	6.1	7.3	51:11	11:50		
uz	Uzbekistan	20	17	17,275	9.8	11.6	26:09	9:10	1	0.6
vc	St. Vincent and Grenadines	281	8	9,051	8.8	310.5	19:57	10:59	1	1.1
ve	Venezuela *(estimated)*	196	150	215,000	7.0	9.1	37:58	11:54		
vg	British Virgin Islands	1	1	8,600	1.2	1.2				
vi	Virgin Islands			17,500						
vn	Vietnam	201	143	434,174	3.3	4.6	39:09	12:56		
vu	Vanuatu	913	9				43:06	14:08		
wf	Wallis and Futuna									
ws	Samoa *(estimated)*	156	36	400,000	0.9	3.9	15:13	8:39	1	0.0
xn--3e0b707	.한국 (KR IDN)			59,500						
xn--90a3ac	.СРБ (Serbia IDN)			3,609						
xn--fzc2c9e2c	.ලංකා (Sri Lanka IDN)			10						
xn--mgberp4a5d4a	.السعودية (Saudi Arabia IDN)			1,800						
xn--o3cw4h	.ไทย (.TH IDN)			16,500						
xn--p1ai	.рф (.RF, Russian Federation IDN)	2	2	810,000	0.0	0.0	43:00	63:00		
xn--xkc2al3hye2a	.இலங்கை (Sri Lanka IDN)			20						
xxx	sponsored TLD	8	5	122,189	0.4	0.7	21:07	5:09		
ye	Yemen			900						
yt	France									

TLD	TLD Location	# Unique Phishing attacks 2H2013	Unique Domain Names used for phishing 2H2013	Domains in registry, Nov. 2013	Score: Phishing domains per 10,000 domains 2H2013	Score: Attacks per 10,000 domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious registrations score/10,000 domains in registry
yu	Yugoslavia (TLD deprecated March 2010)									
za	South Africa	515	472	905,000	5.2	5.7	43:58	9:01	1	0.0
zm	Zambia	7	4				17:44	18:54		
zw	Zimbabwe	8	7	1,100	63.6	72.7	206:22	7:03		
	TOTALS	**115,565**	**82,163**	**274,663,715**					**22,831**	

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 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 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. 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 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.

#