Global Phishing Survey: Trends and Domain Name Use in 2H2014

APWG

Unifying the
Global Response
To Cybercrime

An
APWG
Industry
Advisory

Published 27 May 2015

Authors:

Greg Aaron, Illumintel Inc.
<greg at illumintel.com>

and

Rod Rasmussen, IID
<rod.rasmussen at internetidentity.com>

Table of Contents

OVERVIEW 4
KEY STATISTICS 5
TARGET DISTRIBUTION 7
PHISHING BY UPTIME 9
PREVALENCE OF PHISHING BY TOP-LEVEL DOMAIN (TLD) 11
THE NEW TOP-LEVEL DOMAINS 13
COMPROMISED DOMAINS VS. MALICIOUS REGISTRATIONS 15
REGISTRARS USED FOR MALICIOUS DOMAIN REGISTRATIONS 18
USE OF SUBDOMAIN SERVICES FOR PHISHING 19
USE OF INTERNATIONALIZED DOMAIN NAMES (IDNS) 21
USE OF URL SHORTENERS FOR PHISHING 22
A WORD ABOUT SPEAR-PHISHING 23
APPENDIX: PHISHING STATISTICS AND UPTIMES BY TLD 24
ABOUT THE AUTHORS & ACKNOWLEDGMENTS 38

Overview

The Internet continues to evolve at a dizzying pace – and criminals are often on the leading edge, seeking new ways to steal money and take advantage of the unwary. What are the phishers taking advantage of – new top-level domains? Up-and-coming targets? New international opportunities? By analyzing the phishing that took place in the second half of 2014, we have some answers, and those answers may surprise you.

This report seeks to understand know what the phishers are doing, and how, by quantifying the scope of the global phishing problem. Specifically, this new report examines all the phishing attacks detected in the second half of 2014 ("2H2014", 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. **New companies are constantly being targeted by phishers.** Some phishers are attacking targets where consumers may least expect it. (Page 7)
2. **The ten companies that are targeted most often by phishers are attacked constantly, sometimes more than 1,000 times per month. Together the top ten targets suffered more than three-quarters of all the phishing attacks observed worldwide. (Page 7)**
3. **The number of domain names used for phishing reached an all-time high. (Page 5)**
4. **Phishing in the new top-level domains started slowly. We expect to see phishing levels in them rise as time goes on. (Page 13)**
5. **Chinese phishers were responsible for 85% of the domain names that were registered for phishing. These phishers started using .CN domains more frequently. (Page 15)**
6. **Phishing attacks were not mitigated as quickly. The median uptime of phishing attacks increased to 10 hours 6 minutes — up from 8 hours and 42 minutes in 1H2014.** This means that phishing attacks were not being shut down as efficiently in the critical first hours, when most victims fall prey. (Page 9)

Key Statistics

Millions of phishing URLs were reported in 2H2014 but the number of unique phishing attacks and domain names used to host them was much smaller.[1] The 2H2014 data set yielded the following statistics:

- **There were at least 123,972 unique phishing attacks worldwide**. This was almost exactly the same number as in the first half of 2014, and the most we have seen in a period since the second half of 2009. 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 95,321 unique domain names**.[2] **This is the most we have ever recorded in a half-year period.** The number of domain names in the world grew from 279.5 million in April 2014 to 287.3 million in December 2014.[3]
- Of the 95,321 phishing domains, **we identified 27,253 domain names that we believe were registered maliciously, by phishers. This is an all-time high, and much higher than the 22,629 we identified in 1H2014**. Most of these registrations were made by Chinese phishers. The other 68,303 domains were almost all hacked or compromised on vulnerable Web hosting. Please see pages 15-16 for more detail.
- **Seventy-five percent of the malicious domain registrations were in just five TLDs**: .COM, .TK, .PW, .CF, and .NET.
- In addition, 3,582 attacks were detected on 3,095 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 569 targeted institutions. This is down significantly from the all-time high of 756 we observed in 1H2014.** See page 7 for more.
- **The average uptime in 2H2014 was 29 hours and 51 minutes.** The median uptime in 2H2014 increased to 10 hours 6 minutes, **meaning that half of all phishing attacks stay active for slightly more than 10 hours.** See pages 9-10 for more.
- **Phishing occurred in 272 top-level domains (TLDs).** Fifty-six of them were new top-level domains.
- **Only 1.9 percent 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.)

---

[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.

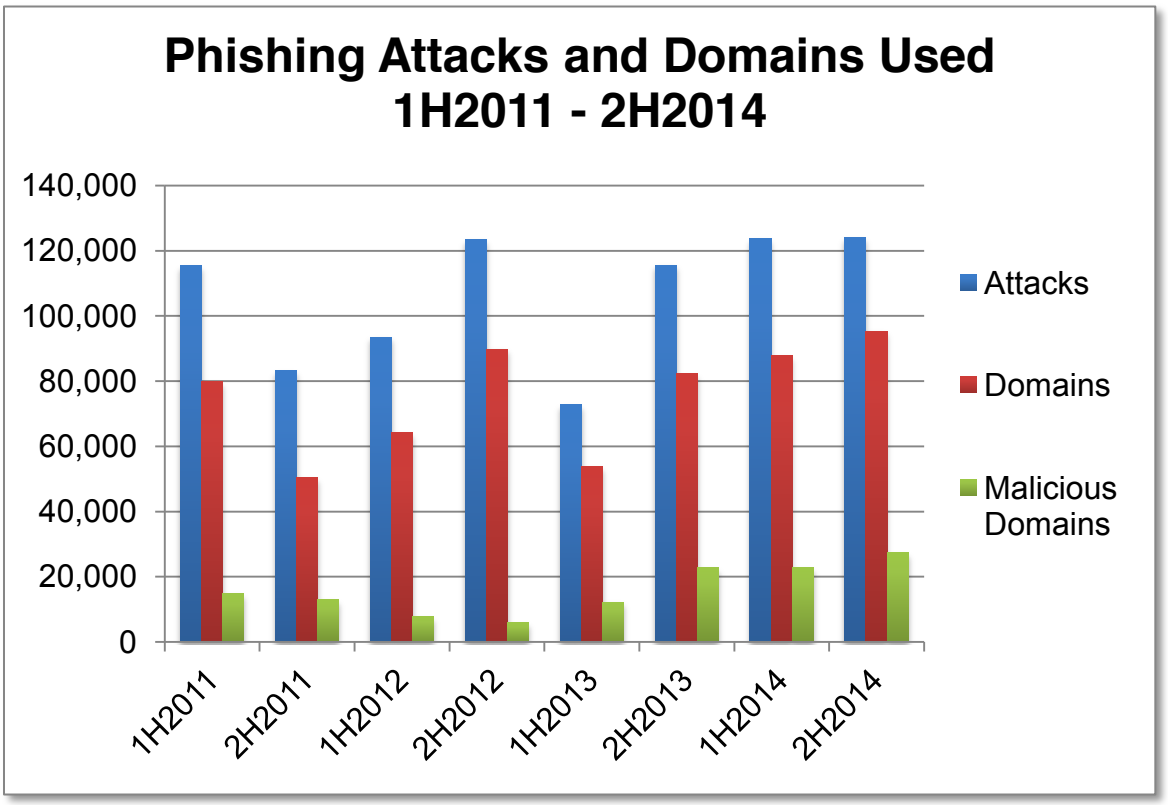
[2] "Domain names" are defined as second-level domain names, plus third-level domain names if the relevant registry offers third-level registrations. An example is the .CN (China) registry, which offers both second-level registrations and third-level registrations (in zones such as com.cn, gov.cn, zj.cn, 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 reports from ICANN.org, new gTLD statistics from ntldstats.com, and numbers provided by the ccTLD registry operators.

- One-hundred and three of the 95,321 domain names were internationalized domain names (IDNs). None involved homographic attacks, but some displayed deceptive messages in the translated domains names.

Basic Statistics

	2H2014	1H2014	2H2013	1H2013	2H2012	1H2012
Phishing domain names	**95,321**	87,901	82,163	53,685	89,748	64,204
Attacks	**123,972**	123,741	115,565	72,758	123,476	93,462
TLDs used	**272**	227	210	194	207	202
IP-based phish (unique IPs)	**3,095**	2,317	837	1,626	1,981	1,864
Maliciously registered domains	**27,253**	22,679	22,831	12,173	5,833	7,712
IDN domains	**103**	112	82	78	147	58
Number of targets	**569**	756	681	720	611	486

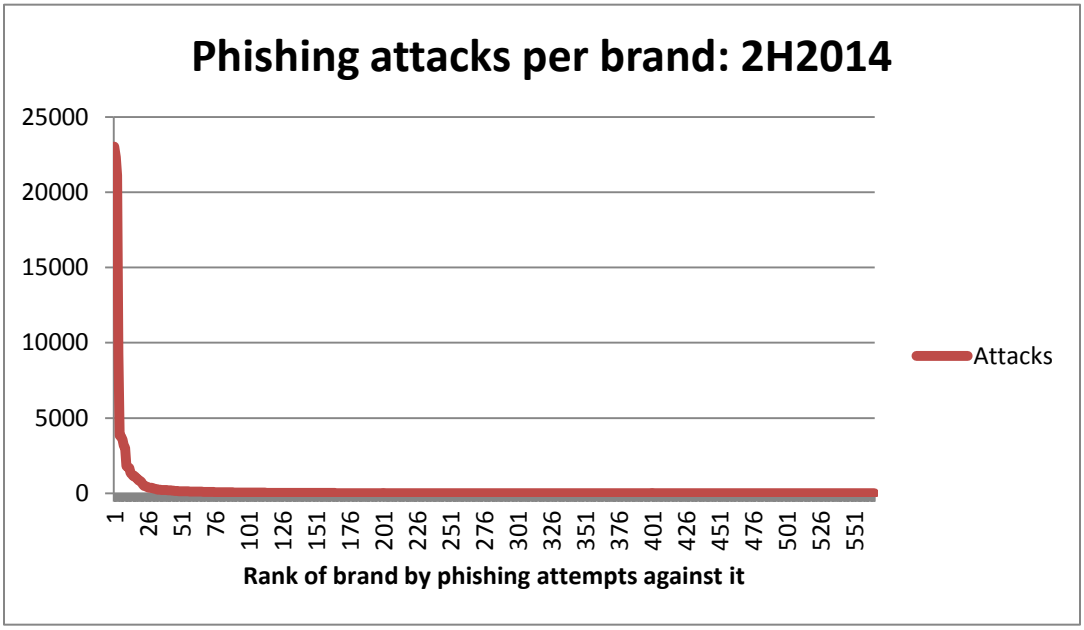


Target Distribution

We counted 569 unique target institutions during the period, down significantly from the 756 we found in 1H2014. Of the 756 targets that were phished in 1H2014, only 289 of them were also phished in 2H2014. In other words, 467 brands were hit in the first part of the year but not the second part of the year.

This amount of "churn" or diversity shows that phishers are always trying new targets. They are looking for companies that have potentially lucrative user bases, are newly popular, and/or are not ready to respond to phishing attacks. If a site takes in personal data, then there may be phishers who want to exploit it.

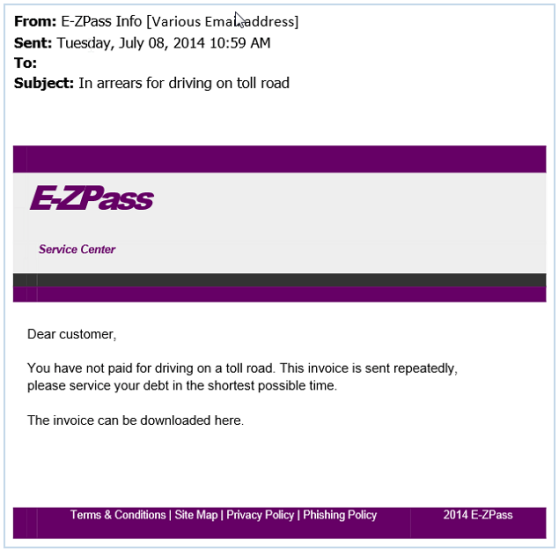
The top 10 targets accounted for over three quarters of all attacks. Phishers continued to attack Apple, PayPal, and Taobao.com heavily. Each of these three e-commerce giants suffered over 20,000 phishing attacks against their respective services and brands. Together, these top three were the targets of nearly 54 percent of the world's phishing attacks. The next seven brands were targeted for a combined 23 percent of all phishing attacks — meaning the top 10 targets accounted for over three quarters of all phishing attacks observed worldwide. The number of times that the targets were attacked follows a long tail. Half of the targets were attacked four or fewer times during the six-month period (up from three times in 1H2014). One hundred and fifty-eight targets were attacked only once each in the period.



The 2H2014 target list featured many banks, including a notable list of banks in Latin America. There were several dozen new targets. Examples of new targets from 2H2014 represent a range of industry sectors:

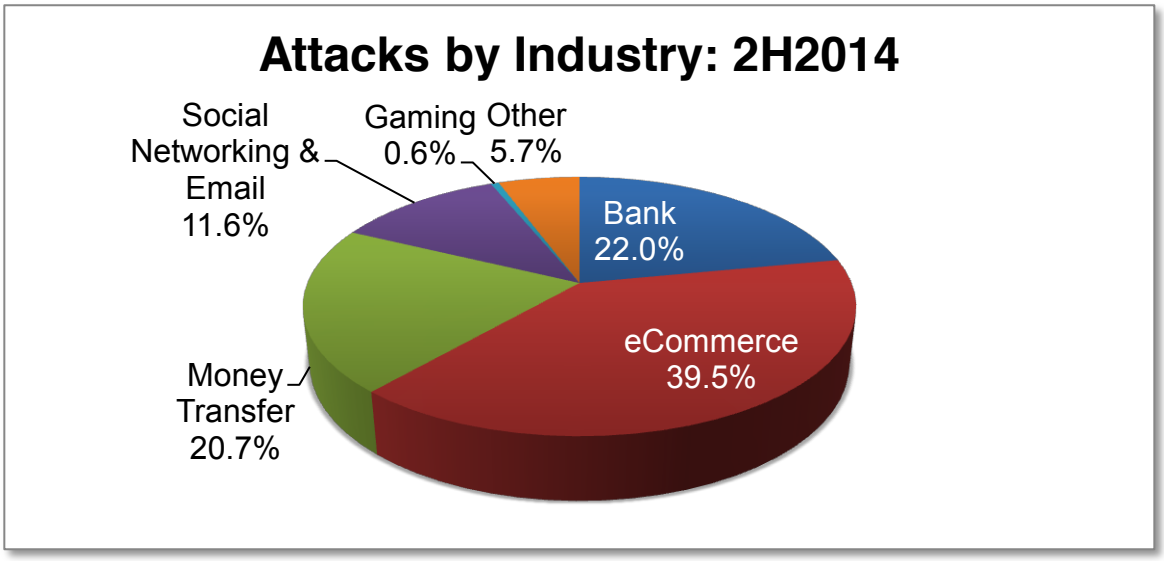
- Endried International, a manufacturer of industrial supplies, specializing in fasteners
- Korean online marketplace Gobizkorea
- Hawaiian Telecom, and Oman Telecommunications Company (Omantel)
- Electricity provider Hydro Quebec, and Italian power utility ENEL
- SulAmérica, the fourth-largest insurance company in Brazil

- Aukro.bg, an online shopping platform serving the Bulgarian market
- Scandinavian payments services provider Nets.EU
- U.S. electronic toll road collection system E-ZPass



A phishing lure e-mail targeting E-ZPass

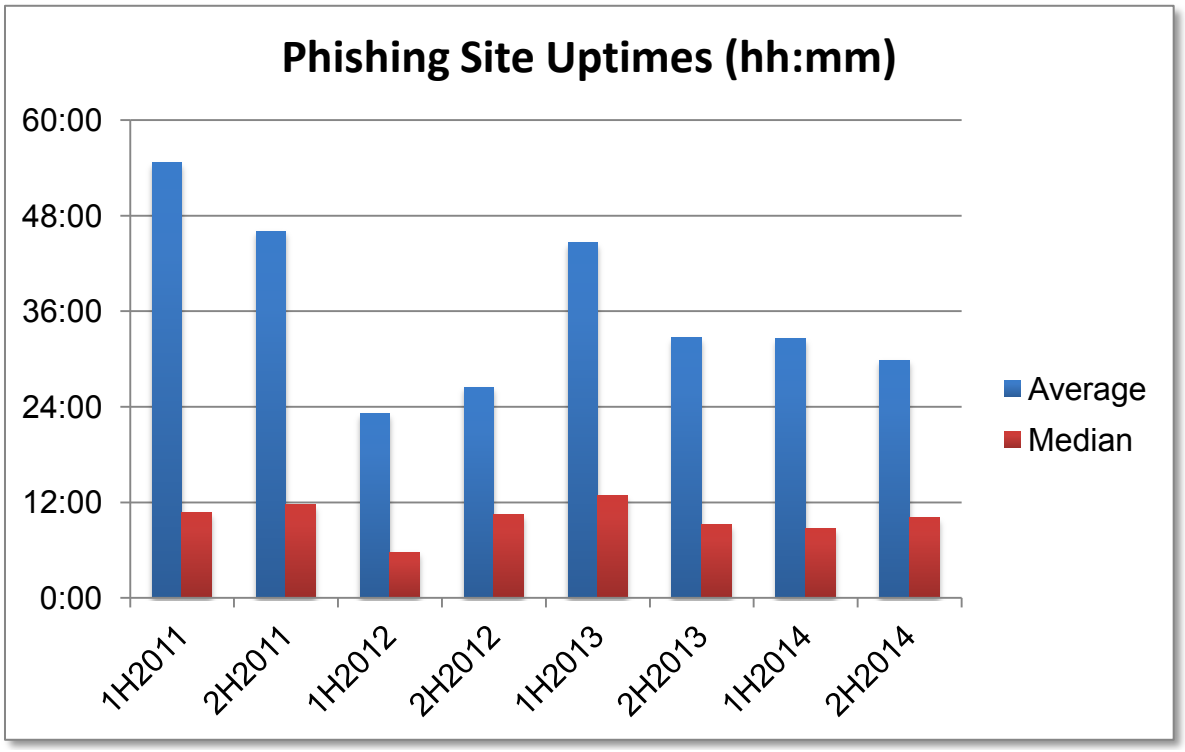
These show criminals seeking the credentials of consumers in places where consumers may least expect it. Phishers target wide-ranging targets for several reasons. One is to perform credit card theft, and hitting new targets may lull consumers into a false sense of security. The phishers can also monetize stolen data through reshipping fraud, a tactic that remains popular. Phishers also steal usernames and passwords from one site in order to try those credential on other sites. Many consumers re-use usernames and passwords, and this poor habit can be costly. If a site is getting phished for the first time, it may have been targeted by a more sophisticated phisher, who had the skill to design a new phishing template.



Phishing by Uptime

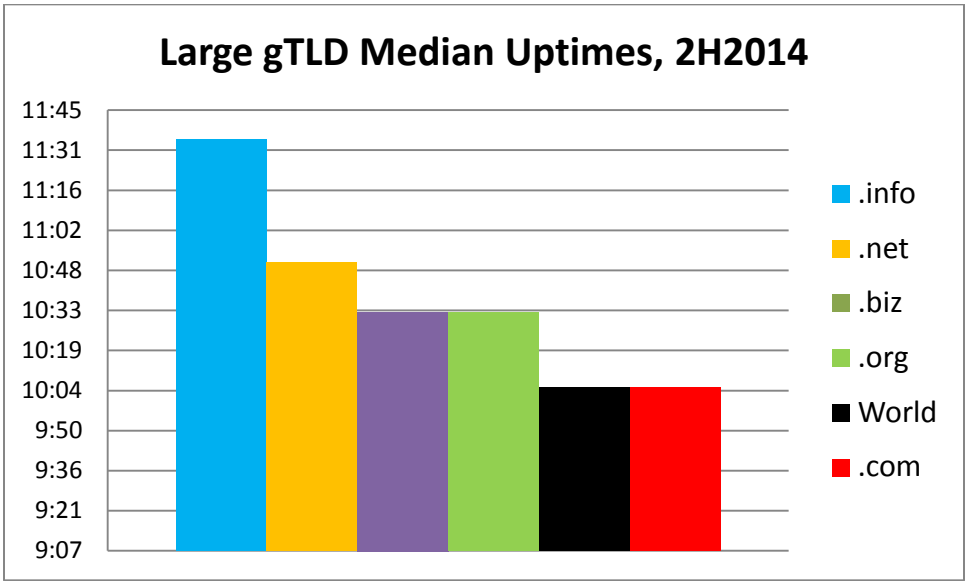
The average uptime for phishing attacks in 2H2014 was 29 hours and 51 minutes — down about 10 percent from 1H2014 which came in at 32 hours and 32 minutes. But the median uptime increased to 10 hours 6 minutes — up from 8 hours and 42 minutes in 1H2014. This means that half of all phishing attacks stay active for slightly more than 10 hours. *For uptime statistics for every top-level domain, please see the Appendix.*

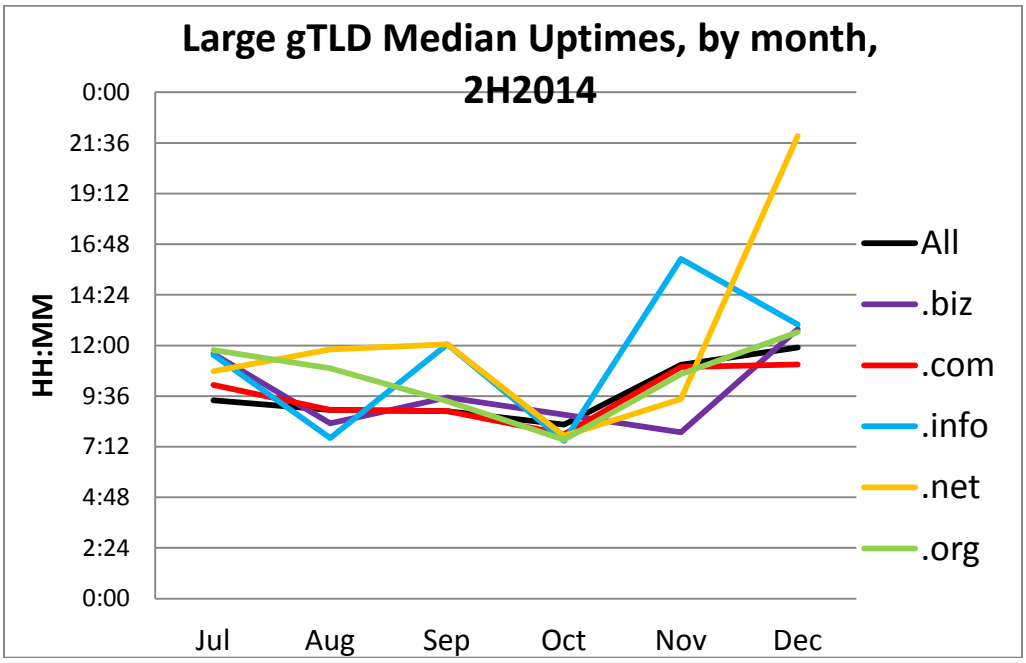
The "uptimes" or "live" times[4] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a metric of the success of mitigation efforts. The first day of a phishing attack is the most lucrative for the phisher, so quick takedowns are essential. Long-lived phish can skew the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



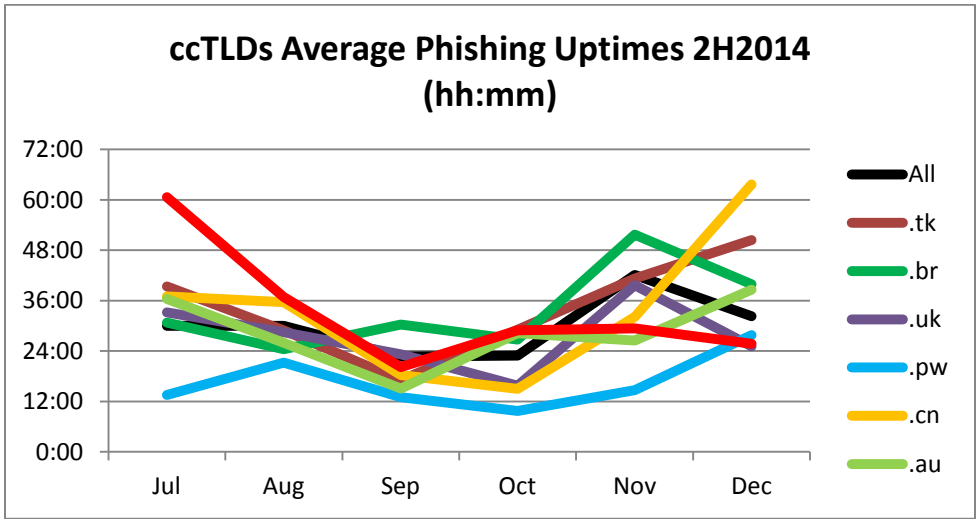
[4] The system used to track the uptimes automatically monitored the phishing sites, and monitoring began as soon as the system became aware of a phish via feeds or honeypots. Each phish was checked several times per hour to confirm its availability, and was not declared "down" until it had stayed down 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 percent of sites "re-activate" after one hour of being down. Also, some phishing sites employ countermeasures that make automated monitoring difficult and less likely to deliver accurate data. 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 anti-phishing notification and takedown programs; the .COM/.NET registry does not. .INFO, .BIZ, and .ORG had lower average times than .COM/.NET. This indicates that .INFO, .BIZ, and .ORG allow fewer phish to remain online for very long times. However, .INFO, .BIZ, and .ORG had *higher median uptimes* than .COM and the world median. .INFO's median uptime was 11:35 — the highest of the five gTLDs, and one-and-a-half hours higher than the world median. This indicates that the .INFO, .BIZ, and .ORG mitigation programs were less effective in the crucial hours after a phishing attack launches – less effective even than in some large TLDs like .COm and .DE that don't perform mitigation at all. This was not the case in past years, and high median uptimes may indicate a problem with emphasis or execution.



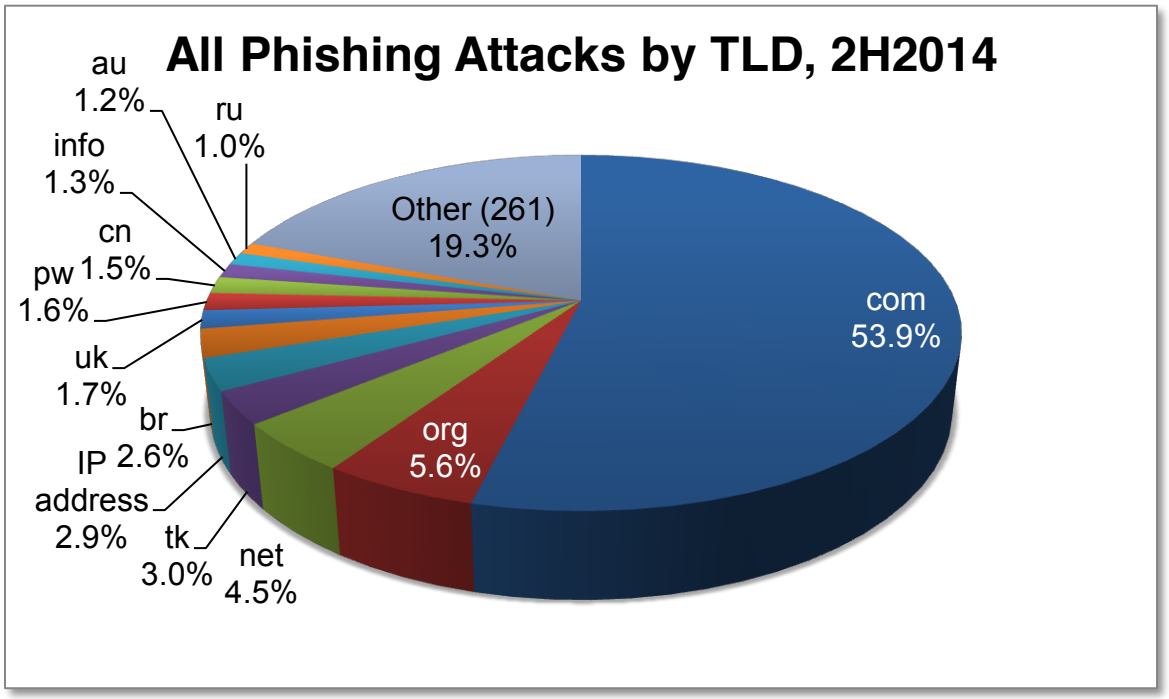


The uptimes at various country-code TLDs (ccTLDs) were less uniform and tend to track with particular campaigns:



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 distribution by TLD has roughly paralleled TLD market share.



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

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

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

- **The median phishing-domains-per-10,000 score was 3.4** (versus 4.7 in 1H2014).
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 4.7. The** .COM TLD contained 58 percent of the phishing domains in our data set, and 41.3 percent of the domains in the world.

We therefore suggest that domains-per-10,000 scores between 3.4 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, 2H2014

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

	TLD	TLD Location	# Unique Phishing attacks 2H2014	Unique Domain Names used for phishing 2H2014	Domains in registry, Dec 2014	Score: Phishing domains per 10,000 domains 2H2014
1	cf	Central African Republic	646	626	81,000	77.3
2	pw	Palau	1,979	1,753	229,639	76.3
3	za	South Africa	433	361	102,381	35.3
4	ga	Gabon	300	285	98,000	29.1
5	ml	Mali	261	245	86,000	28.5
6	th	Thailand	200	146	65,000	22.5
7	pk	Pakistan *(DUM est.)*	124	100	46,000	21.7
8	pe	Peru	165	120	81,222	14.8
9	cl	Chile	764	595	473,069	12.6
10	ve	Venezuela *(est)*	74	59	50,000	11.8

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

[6] Notes regarding the statistics:

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

.CF, .GA and .ML are African ccTLDs that 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 continued to be plagued by Chinese phishers, who registered at least 1,331 domains to attack Taobao.com and a few other Chinese targets. Thailand's .TH has ranked highly for many years; all the phishing there took place on compromised servers, including on 64 government and university domains.

The New Top-Level Domains

Phishing in the new gTLDs started slowly and is rising. We expect to see phishing levels in them rise further, and predict that a small number of these new TLDs will attract significant numbers of malicious registrations.

Beginning in January 2014, the first of the new generic top-level domains (gTLDs) began rolling out. Approximately 1,200 new gTLDs will launch through 2017, 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. 2H2014 was the period in which an appreciable number of these new gTLDs entered general availability and started to gain market share, and therefore the first period in which we can truly begin to analyze phishing in this TLD sector. The complete tables are presented in the Appendix, including the domain and attack scores for each TLD.

As of December 2014, the new gTLDs had less phishing relative to the legacy gTLDs and ccTLDs. This was to be expected, since these TLDs are very young and didn't have a lot of web sites that can be compromised by phishers. As they mature and garner more adoption, the new gTLDs will inevitably see more of their domains compromised for phishing, and phishing levels in the new gTLDs may approach the world average.

From 1 July to 31 December 2014:

- About 295 new gTLDs opened for registration by the public. As of 31 December, 3,684,316 domains had been registered in all new gTLDs.
- Phishing occurred in 56 of those new gTLDs; 239 had no phishing at all.
- A total of 454 new gTLD domain names were used for phishing. Of those, 335 were maliciously registered.
- Twenty-four nTLDs had malicious registrations made in them, often just one or two. Forty-eight had compromised domains used for phishing, often just one or two.
- Almost two-thirds of the phishing in the new gTLDs—288 domains—was concentrated in the .XYZ registry. (Of the 335 maliciously registered domains, 274 were in .XYZ.) This is the first example of malicious registrations clustering in one new gTLD, and we are seeing more examples in early 2015.

As noted above, the median phishing-domains-per-10,000 score for all TLDs in the world was 3.4. Only nine of the 295 new gTLDs had scores above 3.4. It should be noted that

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

during 2H2014, most of the new gTLDs has less than 30,000 domains in them, the threshold at which we usually begin to rank TLDs.

Two important notes:

1. Into 2014, cybercriminals were able to get cheaper domain names in legacy TLDs. But the TLD market is now more crowded and competitive than at any time in history, and some registries are competing aggressively on price. Some new gTLDs are dropping their prices lower than .COM, and that will attract phishing and other kinds of abuse.
2. Tens of thousands of domains in the new gTLDs are being consumed by spammers, and are being blocklisted by providers such as Spamhaus and SURBL. So while relatively few new gTLD domains have been used for phishing, the total number of them being used maliciously is *much* higher.

.XYZ is the largest new gTLD, and had the most phishing. .XYZ garnered attention when its domains were offered for free via a promotion at registrar Network Solutions.[8] However, only 4 of the 288 phishing domains in .XYZ were registered at Network Solutions. That is because the free domains were not offered to all comers – they were only given to existing Network Solutions registrants, to match their existing .COM domains. This mitigated the chance of the free domains getting into the hands of phishers. Instead, most of the .XYZ phishing registrations (298) were made at Xin Net and other Chinese registrars, and were used to attack Chinese targets. A lesson here is that when it comes to abuse, who can obtain domains in a TLD (and in what quantities) may be as important as the (low) price of the domain.

.XYZ had a phishing-per-10,000-domains score of 3.6, which was just slightly above the average of 3.4 for all TLDs, and lower than .COM's score of 4.7. Since most phishing domains in .XYZ were fraudulently registered and most in .COM compromised, .XYZ had a significantly higher incidence of malicious domain registrations per 10,000 coming in at 3.4 versus 1.4 for .COM.

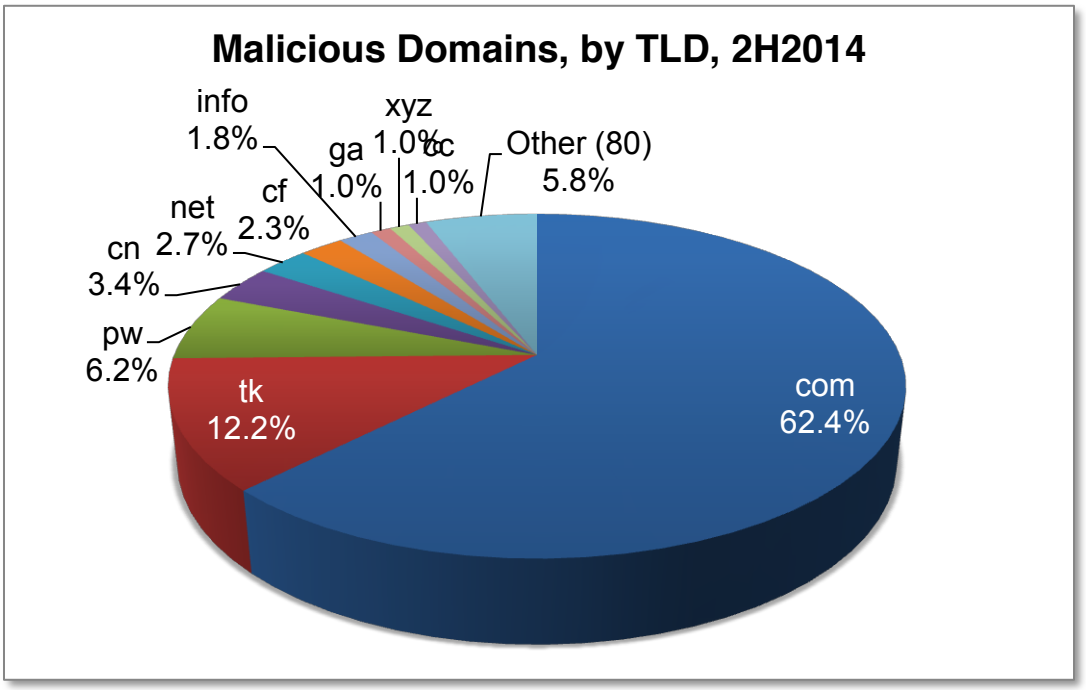
Above: http://paypal.com-secure-my-account.link/startprocess.php – a domain in the new .LINK gTLD, used to phish PayPal on 20 August 2014. Screenshot: PhishTank.

[8] See http://domainincite.com/16771-xyz-launch-inflated-by-massive-netsol-giveaway and http://domainincite.com/18348-netsols-free-xyz-bundle-renews-at-57

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 95,321 domains used for phishing, **we identified 27,253 (28.6%) 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 68,068 domains were almost all hacked or compromised on vulnerable Web hosting.



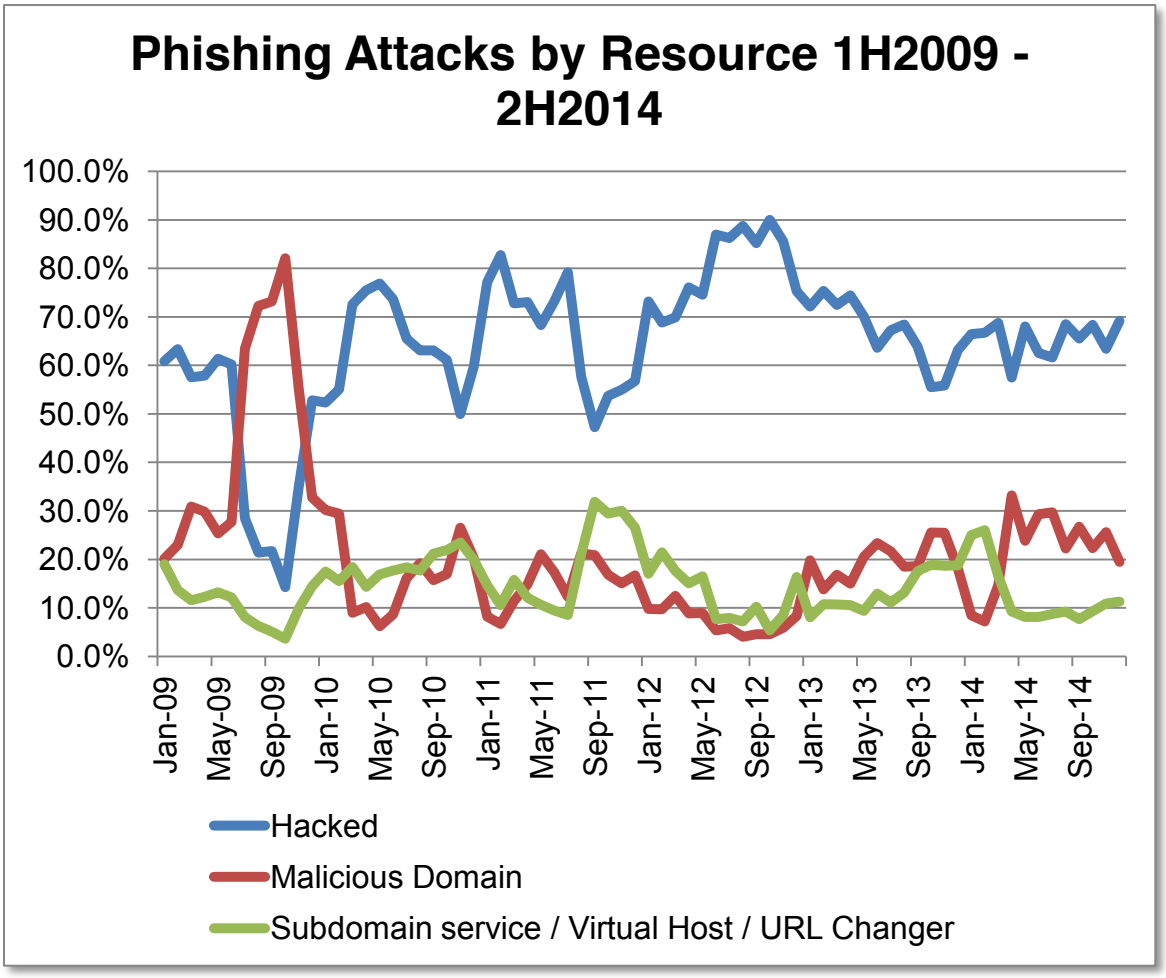
Seventy-five percent of the malicious domain registrations were in just five TLDs: .COM, .TK, .PW, .CF, and .NET.

Of the 27,253 malicious domain registrations, 22,603 (84%) were registered to phish Chinese targets — services and sites in China that serve a primarily Chinese customer base.[9] Chinese phishers have always preferred to register domains, relying upon hacked domains and compromised Web servers less often than phishers elsewhere. Their major targets were Taobao.com, the Industrial and Commercial Bank of China (ICBC), the Bank of China (BOC), and Alipay.

[9] 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.

For the first time in the several years since China changed its domain name registration policies, we saw phishers registering .CN domains in large numbers – 940 .CN domains in 2H2014. Before, Chinese phishers avoided .CN in favor of TLDs such as .COM and .TK, and they registered just 291 .CN domains in 1H2014.

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.



Once again, a large percentage (16.5%) of the world's malicious registrations were made in the .TK, .CF, .GA, and .ML registries. They are 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, until recently, Freenom did not offer a similar tool to mitigate phishing on .CF, .ML, and .GA domains, and times for those TLDs were much longer than .TK in 1H2014. Freenom

then extended the program to its other TLDs, and the change showed up clearly – mitigation times in .CF, .GA, and .ML dropped significantly between the first half of 2014 and the second. Further, far fewer malicious phishing domains were registered in those new registries in 2H2014 versus 1H2014 – dropping from 2,702 to 1,156.

Of the 27,253 maliciously registered domains, just 1,846 contained a relevant brand name or reasonable variation thereof — often a misspelling.[10] **This represents 1.9% of all domains that were used for phishing, and just 6.8% of all maliciously registered domains recorded in the sampling period.** More often than not, the registrations made by phishers often consisted of nonsense strings.

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.

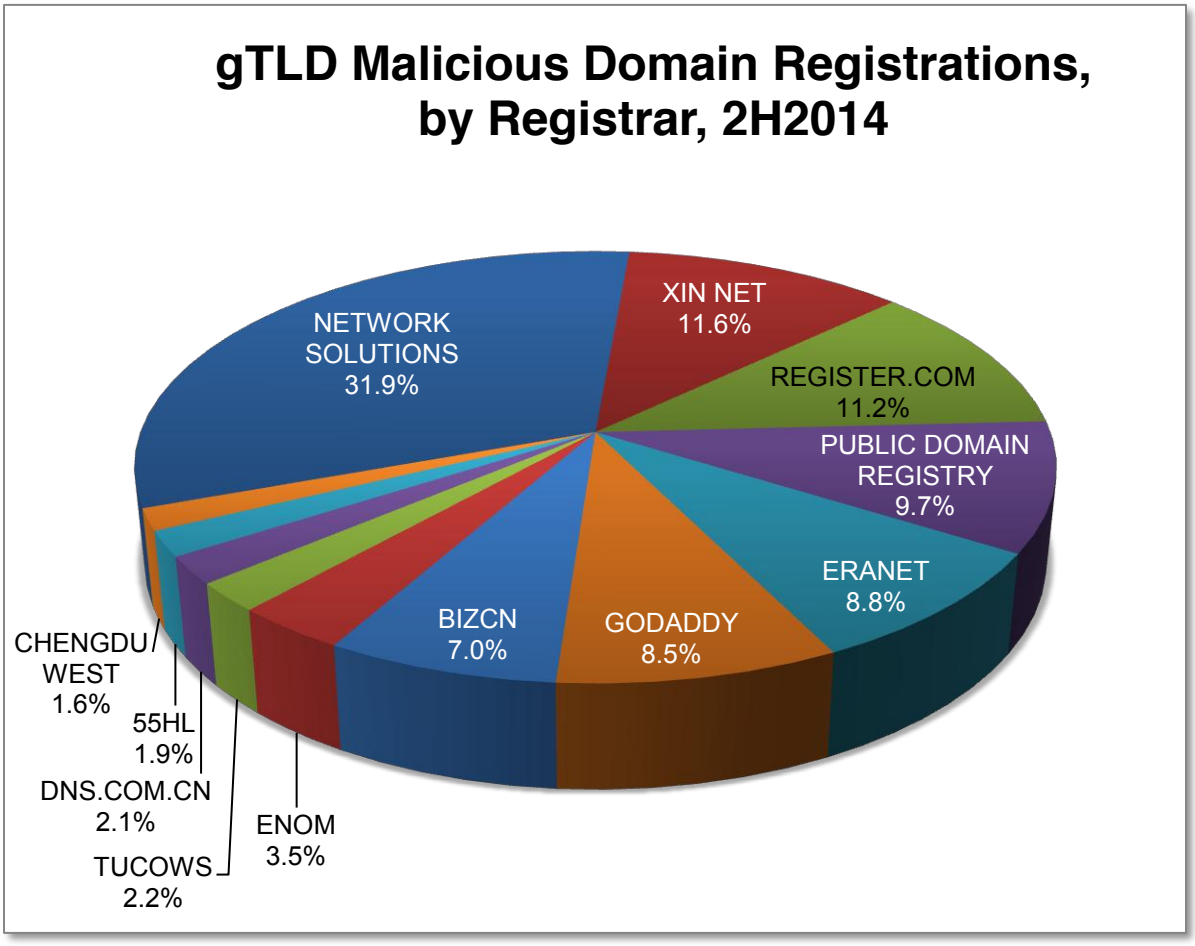
So, most maliciously registered domain names offered nothing to confuse a potential victim. Placing brand names or variations thereof in the domain name itself is not a favored tactic, since brand owners are proactively scanning Internet zone files for their brand names. As we have observed in the past, **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.**

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.

[10] Examples of domain names we counted as containing brand names included: appleuke.com (Apple), paypcil.co (PayPal), qaz89taobao.com (taobao.com), and facebooork.com (Facebook).

Registrars Used for Malicious Domain Registrations

Phishers (especially Chinese phishers) continued to register malicious domain names at an even higher rate than in 1H2014. Where are the phishers registering these domains? 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.



Most malicious registrations were made by Chinese phishers. The above chart shows them making about a third of those registrations at Chinese registrars (EraNet, XinNet, BixCN, Chengdu West), and about half at registrars in the USA (Network Solutions, GoDaddy, Register.com, eNom).

About 16.5 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 second largest number of malicious registrations behind Network Solutions.

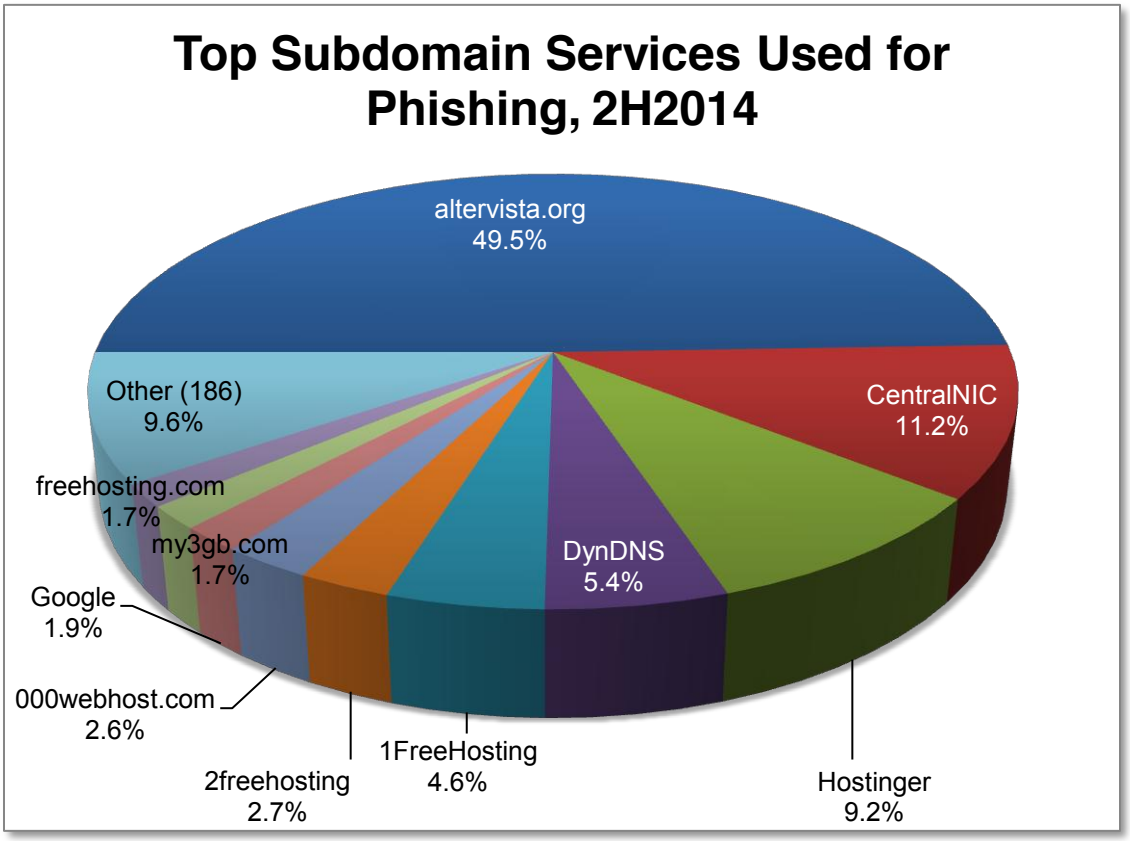
Use of Subdomain Services for Phishing

We saw the use of subdomain registrations for phishing decline sharply in 2H2014. However, subdomain registrations still represent 6% of all phishing attacks.

"Subdomain registration services" are providers that give customers subdomain "hosting accounts" beneath a domain name that the provider owns. These services are effectively domain registries of their own, and 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.[11] Some are responsive to complaints, but many lack proactive measures to keep criminals from abusing their services.



[11] 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.

Use of subdomain services for phishing remained high, but fell from 16,986 (14% of all attacks) in 1H2014 to 7,941 (6% of all attacks) in 2H2014. The number of domains used for malicious subdomains actually increased at the same time from 678 to 733, meaning that the damage was spread across more providers. There was one domain (altervista.org) alone that saw 2,838 malicious subdomains created under it in 2H2014, up from 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.

Nearly 100 subdomain service domains were abused for the first time in 2H2014, providers 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.

The perennially abused subdomain provider altervista.org was the most abused provider in this category. CentralNIC, a big player in the subdomain registry space, was second with 642 attacks. Hostinger (back-ended by Maine-Hosting) continues to be a favorite service for phishers to abuse, with at least 530 domains abused in 2H2014. Happily, this is substantially down from 1H2014 where at least 10,640 malicious subdomains were identified at Hostinger, which was a whopping 63% of all subdomain phishing in 1H2014.

Some notable drops from the list of most-abused subdomain resellers include Rocket List Media and Unonic who each had hundreds of subomains in 1H2014, but had a grand total of just 18 subdomains abused between them in 2H2014.

Top Subdomain Services Used for Phishing, 2H2014

Rank	Attacks	Provider
1	2,838	altervista.org
2	642	CentralNIC
3	530	Hostinger
4	307	DynDNS
5	265	1FreeHosting
6	156	2freehosting
7	151	000webhost.com
8	107	Google

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 found only nine true homographic phishing attacks.

One hundred and three IDN domain names were used for phishing in 2H2014. None were homographic attacks.

Seven of the 103 IDNs were malicious registrations. Of those seven, several were used to display the domain names in Chinese characters. The domain strings themselves were misleading, but did not attempt to exactly copy domain names owned by the targets:

xn--czr93rq40bruk5heszb.com → **工商**银行首页.com = "ICBC Home"

xn--fiq61ierjpnernlcik.cc → **淘宝服**务中心.cc = "Taobao service center"

xn--fiq704ac9c6psbvidn8a.cc → **淘宝申**请中心.cc = "Taobao application center"

xn--kbtj978epvfdrd2y0a1ehe59a.xyz → **淘宝退款官方网站**.xyz = "Taobao official refund website"

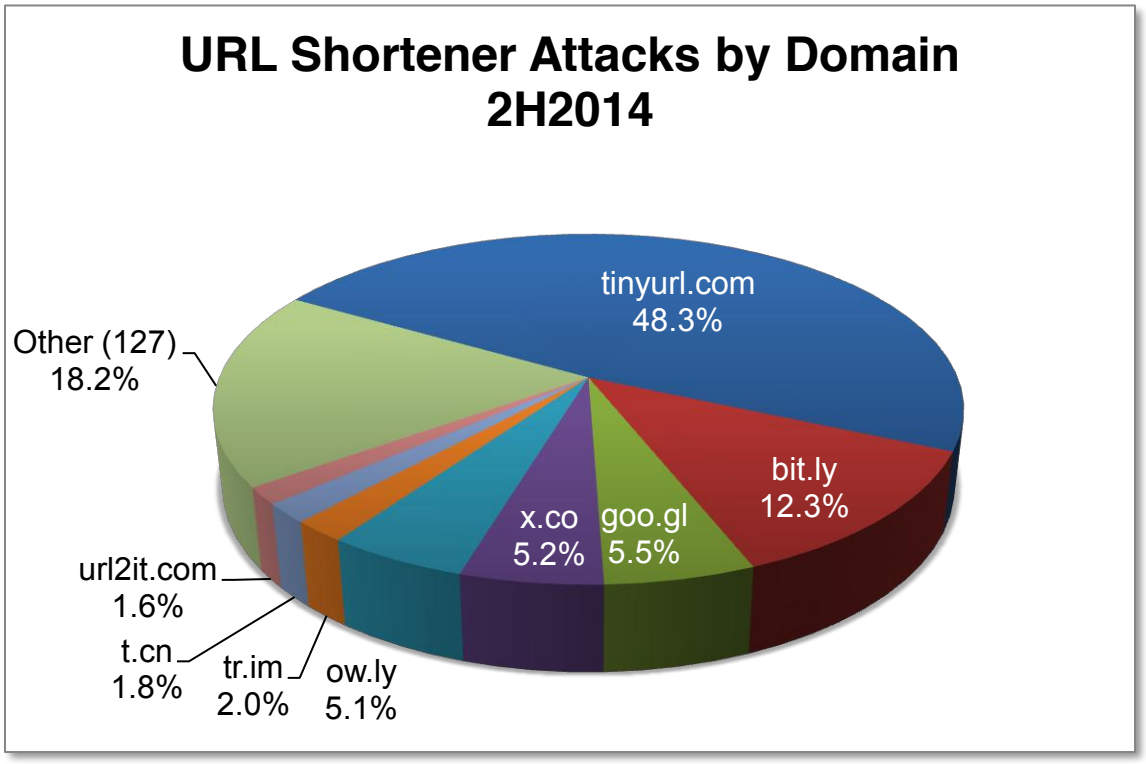
Given that IDNs have been widely available for years, why haven't phishers utilized IDN homographic attacks more often?

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 usually can't see homographic attacks.

Use of URL Shorteners for Phishing

Phishers their use of "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 2H2014, with such attacks nearly doubling from 1,696 in 1H2014 to 3,072 in 2H2014. This still only represents 2.5 percent 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.

2H2014 saw almost half of all URL shortener phish occurring on the very popular tinyURL service with 1,489 attacks, up from 809 attacks in 1H2014. Bit.ly, another large provider in the space stayed in second place in the same period, with 378 attacks, up from 233 in 1H2014. The only other services with significant shares of attacks were goo.gl and owl.ly, tow very popular services.



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 shortner-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.