Global Phishing Survey: Trends and Domain Name Use in 2H2011

Period July - December 2011

APWG

Unifying the Global Response To Cybercrime

An APWG Industry

Published April 2012

Published April 26, 2012

Authors:

Greg Aaron, Afilias
<gaaron at afilias.info>
and
Rod Rasmussen, Internet Identity
<rod.rasmussen at internetidentity.com>

Research, Analysis Support, and Graphics:
Aaron Routt, Internet Identity

Table of Contents

Disclaimer: *PLEASE NOTE: The APWG and its cooperating investigators, researchers, and service providers have provided this study as a public service, based upon aggregated professional experience and personal opinion. We offer no warranty as to the completeness, accuracy, or pertinence of these data and recommendations with respect to any particular company's operations, or with respect to any particular form of criminal attack. This report contains the research and opinions of the authors. Please see the APWG web site – apwg.org – for more information.*

Overview

Phishers are always refining their methods, to take advantage of new opportunities and circumvent defenses. In the second half of 2011 we discovered several such shifts, with significant implications for phishing targets, service providers, and anti-phishing responders. We hope that bringing new trends to light will lead to improved anti-phishing measures.

This report seeks to understand trends and their significances by quantifying the scope of the global phishing problem. Specifically, this new report examines all the phishing attacks detected in the second half of 2011 ("2H2011", July 1, 2011 through December 31, 2011). 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.

Our major findings in this report include:

1. **In 2H2011, the average uptime of all phishing attacks dropped notably.** *(Pages 8-9)*
2. **For the first time, phishers registered more subdomains than regular domain names.** *(Pages 14-16)*
3. **Attacks by Chinese phishers have exploded. Chinese e-commerce site Taobao.com became the world's most-attacked target. Phishers attacking Chinese institutions were responsible for 70% of all malicious domain name registrations made in the world.** These phishers especially use free and low-priced domain providers outside of China. *(Pages 6-7)*
4. **The number of targeted institutions has dropped; phishers concentrated on larger or more popular targets.** *(Pages 5-7)*
5. **Malicious domain name registrations are concentrated by domain registrar, and by TLD.** *(Pages 12-14)*

Basic Statistics

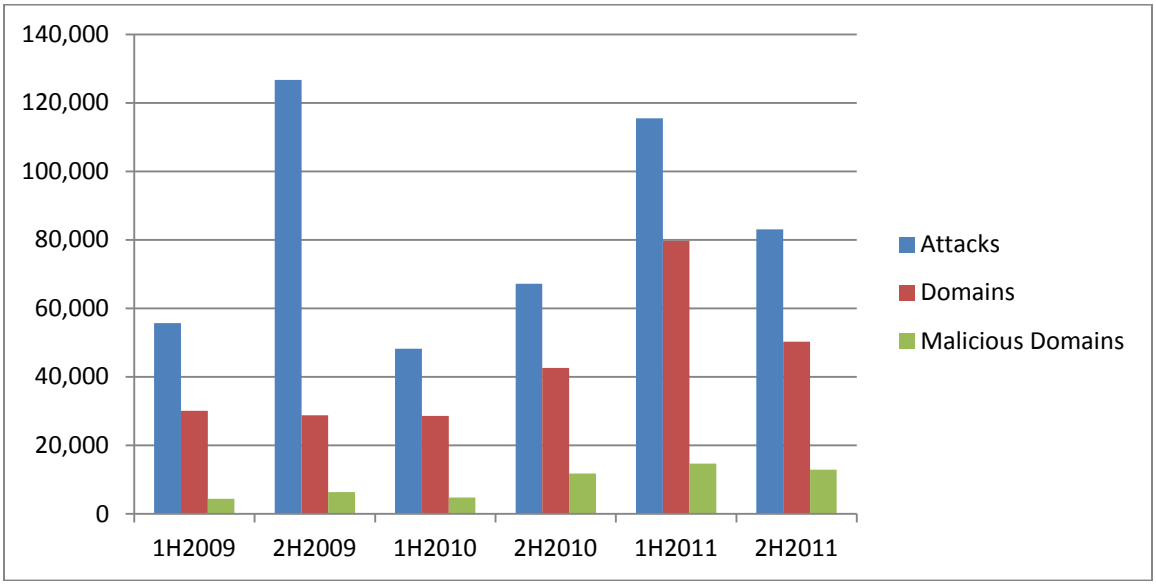
Millions of phishing URLs were reported in 2H2011, but the number of unique phishing attacks and domain names used to host them was much smaller.[1] The 2H2011 data set yields the following statistics:

- **There were at least 83,083 unique phishing attacks worldwide, in 200 top-level domains (TLDs).** This is far less than the 112,472 attacks we observed in the first half of 2011. The decrease is due in part to a decrease in phishing attacks that leveraged shared virtual servers to compromise multiple domains at once. An "attack" is defined as a phishing site that targets a specific brand or entity. One

[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.

domain name can host several discrete attacks against different banks, for example.

- **The attacks used 50,298 unique domain names**.[2] Again, this is down significantly from the 79,753 domains used in 1H2011. The number of domain names in the world grew from 218.8 million in May 2011 to 229.3 million in November 2011.[3]
- In addition, **2,288 attacks were detected on 1,681 unique IP addresses, rather than on domain names.** (For example: http://79.173.233.18/paypal/.) The number of attacks using IPs has remained consistent for two years, and is down just slightly from 2,960 attacks using 2,385 unique IPs recorded in 1H2012. None of these phish sat on IPv6 addresses.
- Of the 50,298 phishing domains, **we identified 12,895 that we believe were registered maliciously, by phishers.** This is down from 14,650 in 1H2011. Of those, 7,991 (62%) were registered to phish Chinese targets. The other 37,403 domains were hacked or compromised on vulnerable Web hosting.
- **We counted 487 target institutions, down from 587 in 2H2010**. Targets include the users of banks, e-commerce sites, social networking services, ISPs, government tax bureaus, online gaming sites, postal services, and securities companies.
- **Phishing is generally distributed by top-level domain market share, but 93% of the malicious domain registrations were in just four TLDs**: .TK, .COM, .INFO, and .IN.
- **Only about 4% of all domain names that were used for phishing contain a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations.")
- Only 36 of the 79,753 domain names we studied were internationalized domain names (IDNs), and three were homographic attacks.



[2] "Domain names" are defined as second-level domain names, plus third-level domain names if the relevant registry offers third-level registrations. An example is the .CN (China) registry, which offers both second-level registrations and third-level registrations (in zones such as com.cn, gov.cn, zj.cn, etc.). However, see the "Subdomains Used for Phishing" section for commentary about how these figures may undercount the phishing activity in a TLD.

[3] As per our research; including gTLD stats from ICANN.org and stats provided by the ccTLD registry operators.

Basic Statistics

	2H2011	1H2011	2H2010	1H2010	2H2009
Phishing domain names	50,298	79,753	42,624	28,646	28,775
Attacks	83,083	115,472	67,677	48,244	126,697
TLDs used	190	200	183	177	173
IP-based phish (unique IPs)	1,720	2,385	2,318	2,018	2,031
Maliciously registered domains	12,895	14,650	11,769	4,755	6,372
IDN domains	36	33	10	10	12

For most domain names in this report, the registrar of record was not reported at the time the phish was live. Obtaining accurate registrar sponsorship data for a domain name requires either time-of-attack WHOIS data, or historical registry-level data. This data has not been collected in a comprehensive manner by the anti-phishing community, and is typically unavailable, especially in the ccTLD space. However, we were able to obtain a significant amount of gTLD registrar information for this survey from DomainTools, a company that tracks WHOIS data, and were thus able to do some registrar-specific analysis for this report.

Shifting Targets

We have witnessed a reduction and concentration in the number of institutions that have been targeted recently by phishers, and a dramatic change in which institution is the world's most-targeted site.

In the second half of 2010, we saw phishers target 587 institutions and their users. In the first half of 2011, we recorded 520 targets. In the second half of 2011, the number dropped to 487 institutions. **In 2H2011, the top 20 targets accounted for 78% of the world's phishing attacks, and half of the targets were attacked only once or twice.** This is not to minimize the effects of a single phishing attack, which can be an enormous headache for a company, especially in these days when confused or irate consumers can express themselves via social media.

In those previous periods, phishers went after all kinds of sites that might offer some sort of value, including regional banks, credit unions, and mid-tier e-commerce sites. But phishers launched fewer attacks on such targets through 2011, concentrating on larger, more prominent targets. We believe they did so because:

1. There is less money to be made off the smaller targets. It is easier for phishers to sell stolen credentials associated with more popular institutions.
2. Phishers advertise via spam. It is less efficient for them to spam out lures related to smaller targets, unless the phishers possesses a qualified list of e-mail addresses.
3. There is a growing emphasis on gaining access to e-mail accounts, which enable phishers to spam from whitelisted services such as Gmail, Hotmail, and so on.

It will be interesting to see if phishing remains focused in this fashion. If so, it may be an indicator that the average return on phishing is being driven downward.

The second half of 2011 also marked the dominance of Chinese phishers. Beginning in our 2H2010 report, we have explored the rise of Chinese phishing -- phishing perpetrated largely by Chinese criminals, who victimize Chinese Internet users and steal the credentials they use on Chinese e-commerce and banking sites. Phishing in China has exploded as e-commerce has become commonplace there.

In 2H2011 there were 22,216 attacks against Chinese targets, versus 17,693 attacks in 1H2011 and 12,282 attacks in 2H2010. The rise indicates that the phishing is profitable. The rapid pace of Internet development in China produces a steady stream of novice users – 55.8 million new ones in 2011, according to the most recent government numbers.[4] This group is more vulnerable to online scams. Overall, the Chinese Internet user base is probably lower on the learning curve than the U.S. and Europe population, and can benefit from education about the dangers of phishing.

In 2H2011, China's Taobao.com became the world's most frequent phishing target, far exceeding the previous #1 target, PayPal. Taobao.com is one of China's largest e-commerce sites, specializing in business-to-consumer and consumer-to-consumer transactions, similar to eBay and Amazon. For several years, PayPal had been far and away the world's #1 phishing target, due to PayPal's ubiquity and its popularity with

Above: an attack targeting users of Taobao.com, using a maliciously registered domain

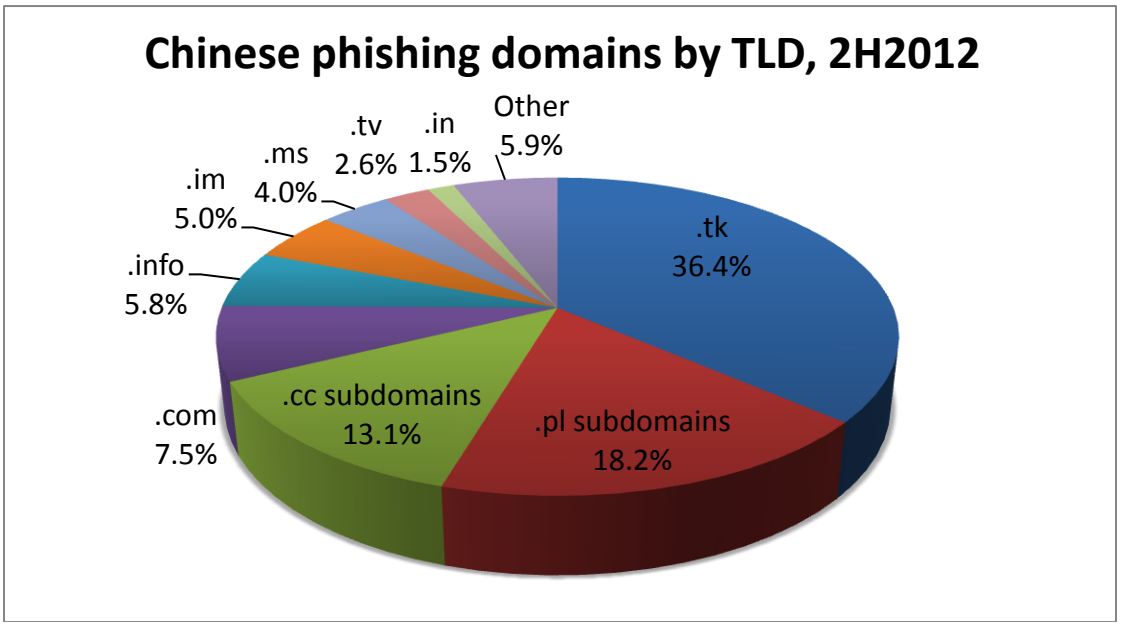
[4] http://www1.cnnic.cn/uploadfiles/pdf/2012/2/27/112543.pdf

consumers. In the first half of 2011, PayPal was still the number one target, attacked more than twice as often as Taobao.com, the world's second-most-frequent target. But through the second half of 2011, Taobao.com was attacked more than twice as much as PayPal. In 2H2011 there were 18,508 attacks against Taobao.com -- 22% of all the phishing attacks recorded worldwide. The flip is also due to a precipitous drop in attacks against PayPal, which dropped from 34,209 attacks in 1H2011 to just 7,169 in 2H2011.

Unlike most phishers, Chinese phishers do not use many hacked domains. Instead, they prefer to set up their phishing pages on domains and subdomains they register themselves. The 18,508 attacks against Taobao.com broke down thusly:

- 7,025 attacks used maliciously registered domains names. Most were in .TK, which offers free domain name registrations. Phishers registered just one .CN domain to attack Taobao.com.
- 10,840 attacks used subdomains, which were registered by the phishers at subdomain resellers.
- Only 639 attacks occurred on hacked or compromised domains.
- Four attacks used URL shortening services.

Much of the data about this Chinese phishing was contributed by CNNIC. CNNIC operates the .CN domain registry, and is also the secretariat of the Anti-Phishing Alliance of China (APAC, http://en.apac.cn/). APAC has more than 140 member institutions in the country, including banks, e-commerce sites, and domain registrars, and has an efficient reporting and domain suspension program. We are grateful to CNNIC and APAC for sharing their data. APAC members are detecting and reporting these attacks far more effectively than parties outside of China. Security observers in Europe and the Americas are evidently not receiving and/or parsing many of the Chinese-language phishing lure e-mails and instant messages that advertise most of these phishing attacks.

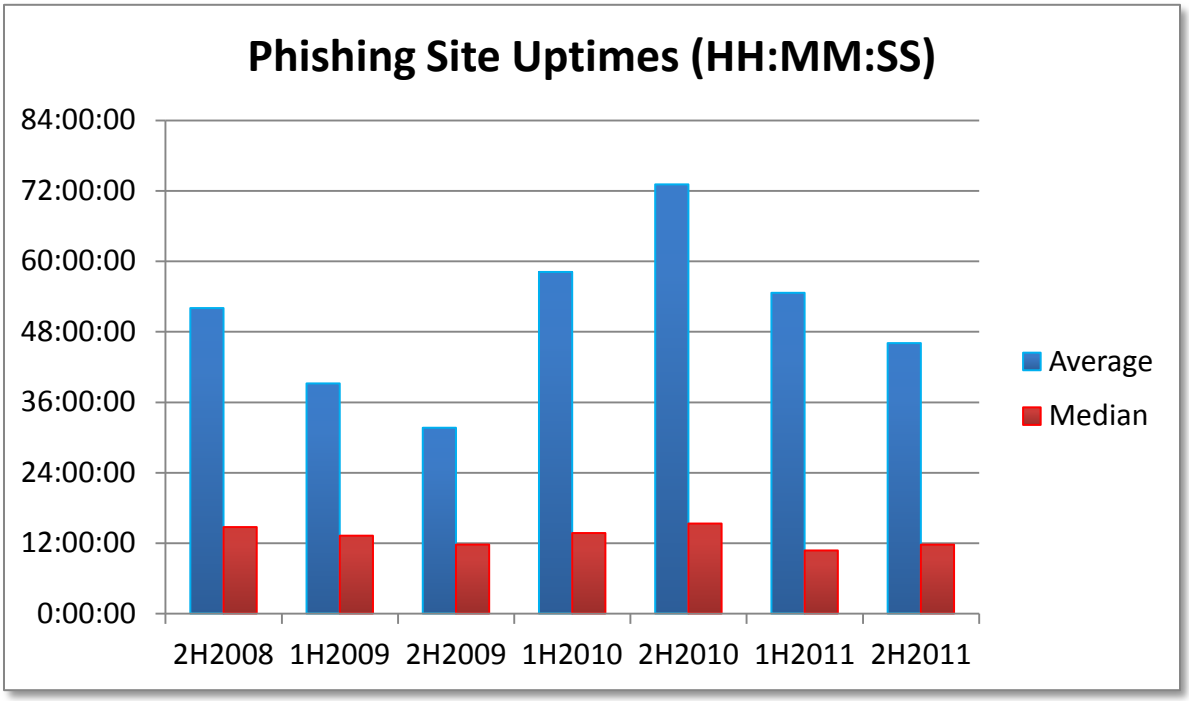


Phishing By Uptime

After reaching a high in 2H2010, the average uptimes of phishing attacks dropped through 2H2011. The average uptime in 2H2011 was 46 hours and 3 minutes, compared to a high of 73 hours in 2H2010. The median uptime in 2H2011 was 11 hours and 43 minutes, up slightly from the previous period.

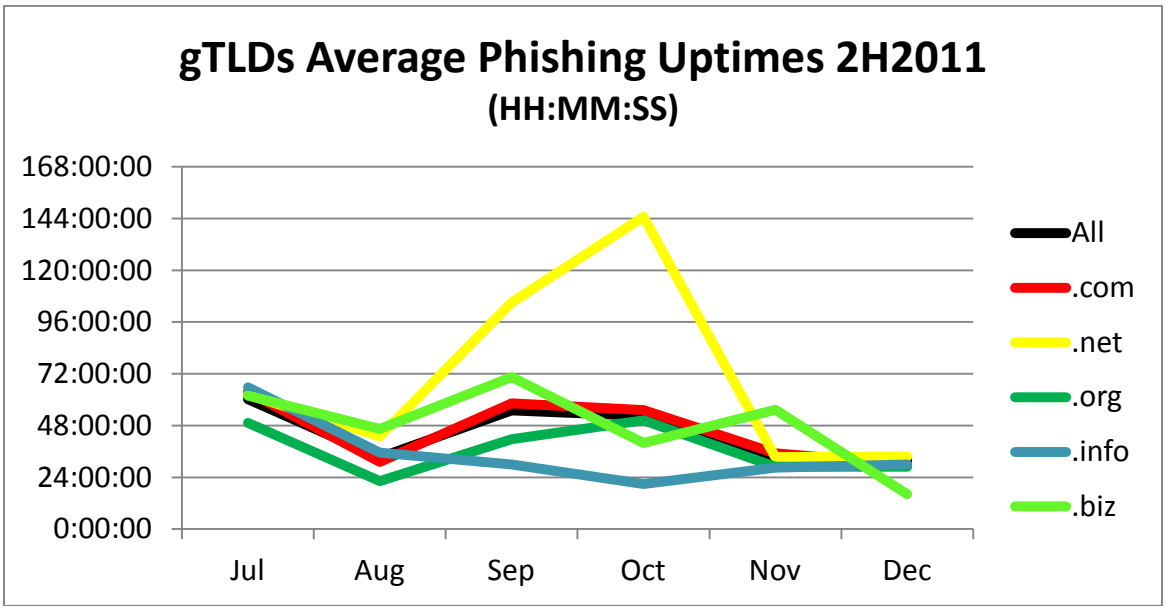
The "uptimes" or "live" times[5] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a measure of the success of mitigation efforts. The longer a phishing attack remains active, the more money the victims and target institutions lose.

The first two days of a phishing attack are the most lucrative for the phisher, so quick takedowns are essential. Long-lived phish can skew the averages since some phishing sites may 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.

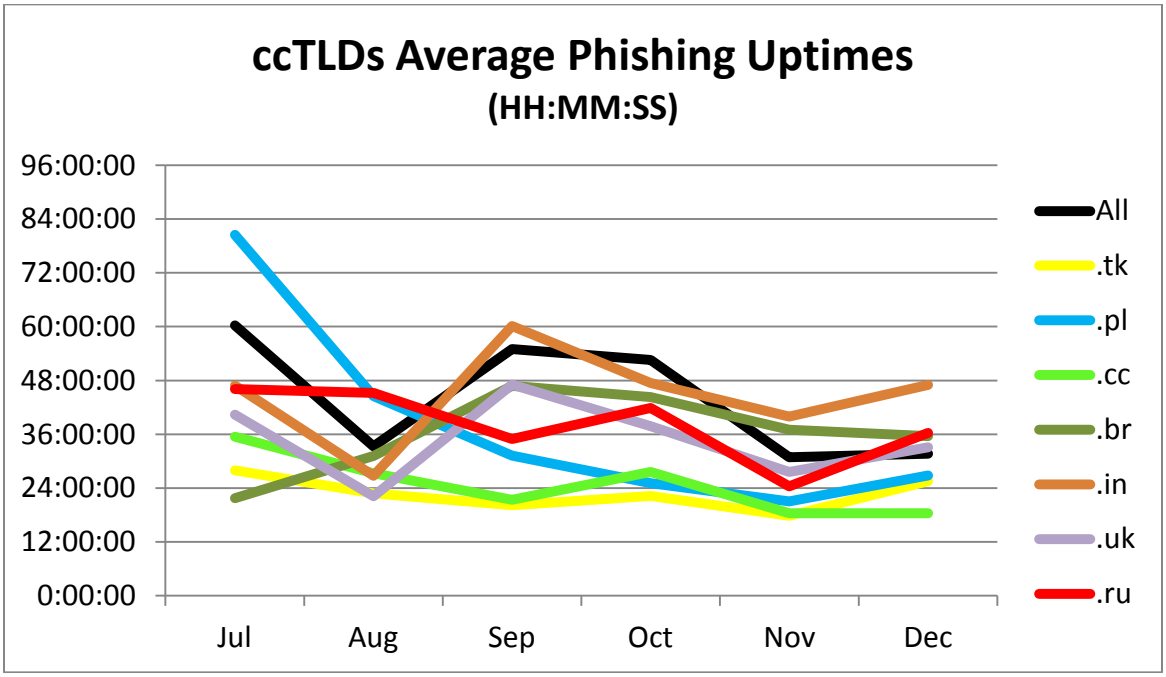


In the large generic top-level domains (gTLDs), .INFO and .ORG had the lowest uptimes, due to the aggressive notification and takedown programs at those registry operators:

[5] 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 large country-code TLDs (ccTLDs) generally tracked each other, with .TK and .CC phish having lower uptimes due to their mitigation programs:



For average and median uptime statistics for every TLD, 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 complete tables are presented in the Appendix.**

The majority of phishing continues to be concentrated in just a few namespaces. Except for.PL subdomains and .TK domains, which were taken advantage of extensively by phishers, phishing was roughly distributed by 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"[6] 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 scores and the number of phish in each TLD.

- **The median domains-per-10,000 score was 3.2**.
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 2.3.** .COM contained 40% of the phishing domains in our data set, and 44% of the domains in the world.

We therefore suggest that domains-per-10,000 scores between .COM's 2.3 and the median of 3.2 occupy the middle ground, with scores above 3.2 indicating TLDs with increasingly prevalent phishing. [7]

---

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

[7] 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, and the largest TLDs tend to appear lower in the rankings.
- 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.

Top 10 Phishing TLDs by Domain Score, 2H2011

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

RANK	TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry, Nov 2011	Score: Phish per 10,000 domains 2H2011
1	.tk	Tokelau	7,605	7,316	6,101,229	12.0
2	.in	India	1,613	1,314	1,122,549	11.7
3	.th	Thailand	110	69	65,309	10.6
4	.my	Malaysia	145	125	132,775	9.4
5	.rs	Serbia	77	51	68,643	7.4
6	.cl	Chile	333	260	361,650	7.2
7	.pe	Peru	83	38	56,655	6.7
8	.ph	Philippines *(domains estimated)*	31	20	30,000	6.7
9	.br	Brazil	2,210	1,691	2,832,270	6.0
10	.hr	Croatia	70	53	88,804	6.0

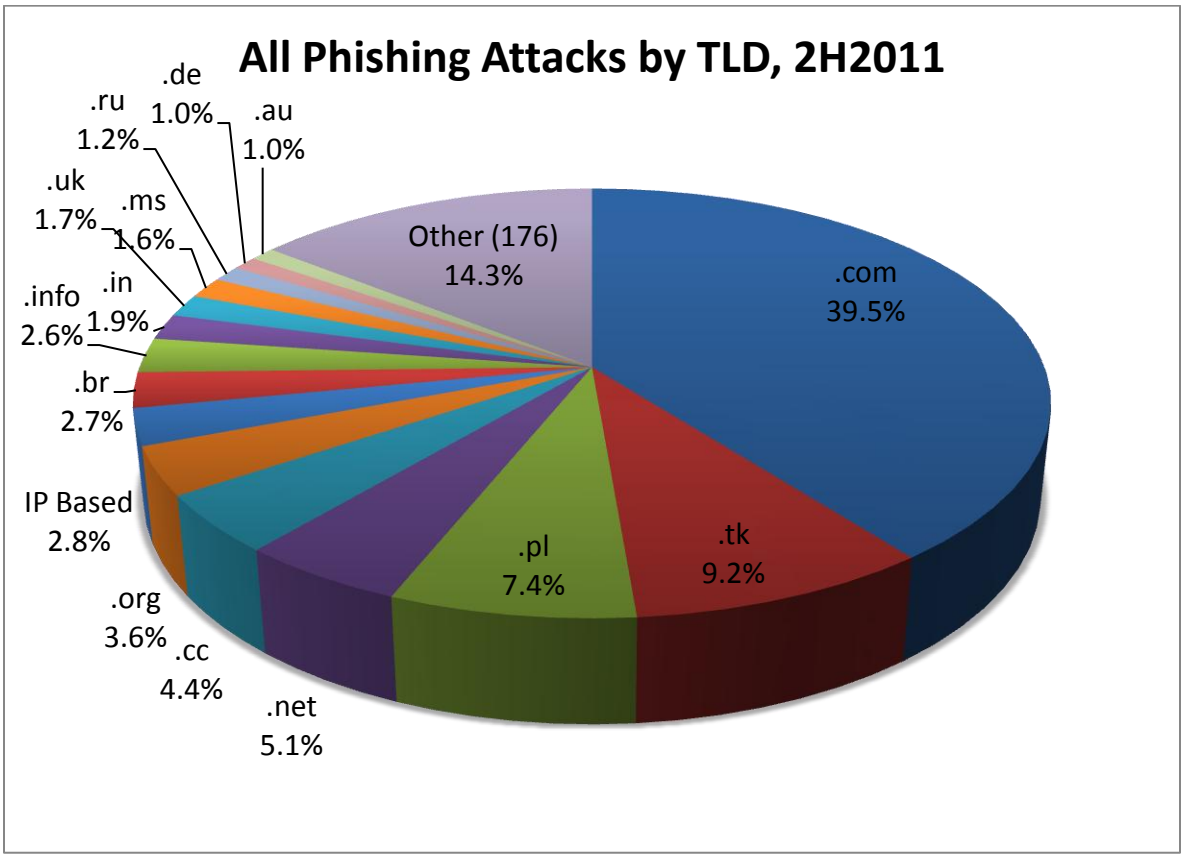
At the top of the list is .TK, which had an increase in phishing domains, from 6,214 in 1H2011 to 7,316 in 2H2011. Virtually all of the .TK phishing domains were maliciously registered by phishers. .TK is a liberalized country code domain, a joint venture of the small Pacific nation of Tokelau and Dot TK, a privately held company. By offering free domain names, .TK has become the third-largest ccTLD in the world, trailing only Germany's .DE and Great Britain's .UK.

Joost Zuurbier is CEO of Dot TK, and notes that "Dot TK is the only TLD that allows trusted partners to shut down immediately any domains that are abused in spam, phishing, copyright infringement, or fraud by using an anti-abuse API. We are actively looking for trusted partners that are willing to implement our anti-abuse API and make the world a safer place." These partners include Facebook, Internet Identity, and the Anti-Phishing Alliance of China (APAC). **.TK's rapid takedown program has resulted in lower-than-average uptimes, but has not prevented phishers from obtaining and using .TK domains in the first place.**

India's .IN TLD rose to the number two position. More than half of the attacks using .IN domains targeted users of Battle.net, the online gaming site. Online gaming credentials are valuable to certain criminals, who sell them on the black market. In-game items can also be sold for real-world cash.

Thailand's .TH continues to rank highly, as it has for several years. .TH suffers from compromised government and university Web servers. From August through December 2011, phishers broke into the Web site of the Senate of Thailand (senate.go.th) several times.

If TLDs are ranked by Attacks per 10,000, .CC continues to rank highly, due to attacks that used CO.CC, CU.CC, and CX.CC subdomains. (See "Use of Subdomain Services for Phishing" below).



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 50,281 domains used for phishing in 2H2011, **we identified 12,895 that we believe were registered maliciously, by phishers (25%). This number was down from 14,650 in 1H2011. The other 75% of domains used for phishing were compromised or hacked domains.**

57% of the world's malicious registrations were make in the .TK TLD. 93% of the malicious domain registrations were made in just four TLDs: TK, .COM, .INFO, and .IN.

Of the 12,895 maliciously registered domains, 8,000 of them (62%) were registered to phish Chinese targets, overwhelmingly Taobao.com. **Otherwise, phishers turned to subdomain services, which are more lightly defended than top-level domains, and offer cheaper (often free) registrations.**

Of the maliciously registered domains, 2,232 contained a relevant brand name or variation thereof—often a misspelling.[8] This represents just 4% of all domains that were used for phishing, and 17% of all maliciously registered domains.

Most maliciously registered domain strings offered nothing to confuse a potential victim. Placing brand names or variations thereof in the domain name itself is not a favored tactic, since brand owners are proactively scanning Internet zone files for such names. As we have observed in the past, **the domain name itself usually does not matter to phishers, and a domain name of any meaning, or no meaning at all, in any TLD, will usually do. Instead, phishers almost always place brand names in subdomains or subdirectories.** 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.

Registrars Used for Malicious Domain Registrations

This report marks the first time we have been able to perform systematic analysis of where phishers purchased domain names. This is made possible via WHOIS data captured by

DomainTools.com, recorded shortly after each domain was created. We thank DomainTools; its data covered 2,909 gTLD domains that were registered exclusively to support phishing. Unfortunately, we do not have statistics for ccTLDs, since many ccTLD registries restrict the data they publish. Most of the world's malicious registrations were made in the .TK registry.

The registrar marketplace is diverse, with one major player (GoDaddy) holding roughly half of the market share, then several large players, and then a long list of smaller registrars. As one may expect, some of the largest registrars -- GoDaddy, MelbourneIT, eNom, and Tucows -- appeared on the list of most-exploited registrars due to their market share. Some registrars also support reseller models, and some of these domains were sold via resellers, but we were not able to discern reseller identities for this survey.

In order to compare dissimilar registrars with each other, we used the same metric we use for comparing various TLDs – malicious domains per 10,000 under management. We then use this measure to identify registrars that may be exploited. The top 15 registrars on our list accounted for 85% (2,480) of the domains we had data for.

[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).

Top 15 gTLD Phishing Registrars by Malicious Domain Score, 2H2011

More than 25 phishing domains and 1,000 domain names at registrar

RANK	Registrar	Malicious Domain Names used for phishing 2H2011	gTLD domains at registrar, March 2012[9]	Score: Phish per 10,000 domains 2H2011
1	CHENGDU WEST DIMENSION DIGITAL TECHNOLOGY CO., LTD.	147	2,652	554.3
2	JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD	120	152,950	7.8
3	INTERNET.BS CORP.	35	117,883	3.0
4	HICHINA ZHICHENG TECHNOLOGY LTD.	243	935,347	2.6
5	UK2 GROUP LTD.	34	183,586	1.9
6	BIZCN.COM, INC.	58	383,047	1.5
7	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	322	3,491,724	0.9
8	XIN NET TECHNOLOGY CORPORATION	97	1,240,769	0.8
9	DIRECTI INTERNET SOLUTIONS PVT. LTD. D/B/A PUBLICDOMAINREGISTRY.COM	135	2,172,751	0.6
10	NAME.COM LLC	28	669,641	0.4
11	FASTDOMAIN, INC.	45	1,495,856	0.3
12	ENOM, INC.	230	9,225,304	0.2
13	GoDaddy.com LLC	856	34,696,655	0.2
14	REGISTER.COM, INC.	50	2,083,433	0.2
15	TUCOWS.COM CO.	80	7,197,121	0.1

Our analysis identified a handful of registrars with much higher relative levels of abuse than their peers. Five of the top eight registrars are located in China. One registrar stood far apart from the rest: Chengdu West Dimension Digital Technology (http://west263.com/), a small registrar with an exceptionally high score. Other domains sponsored by Chengdu West including hundreds of cybersquatting domains containing the brand-names of clothing lines, apparently supporting the sale of counterfeit goods.

A good rule of thumb for identifying a registrar that has a higher level of fraudulent registrations than normal would be more than one per 10,000 under management. We will continue to study this area and refine our methodologies as we gather more data for future reports.

Use of Subdomain Services for Phishing

We continue to see very high abuse of subdomain services. **For the first time, malicious use of subdomain registration services eclipsed the registration of regular domain names by phishers.**

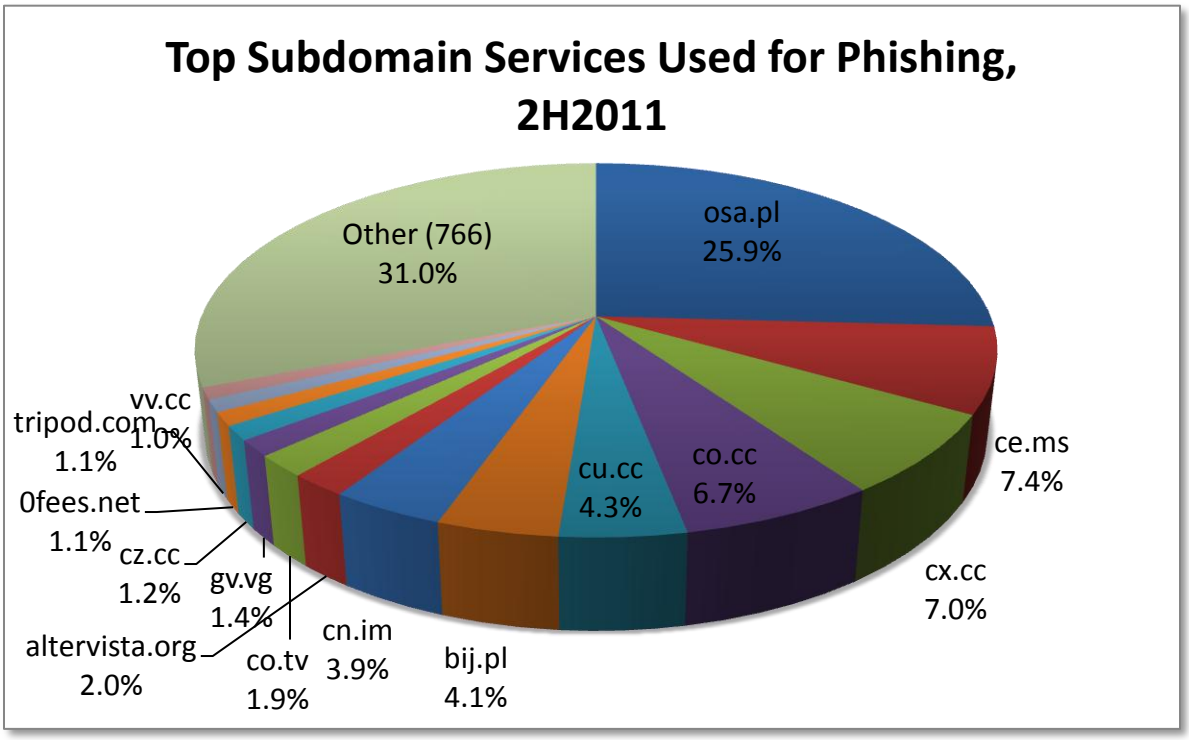
[9] Source: Webhosting.info

There were 17,390 phishing attacks hosted on subdomain services in the second half of 2011, using 16,664 unique subdomains. This was a 38% increase from the 12,574 attacks we recorded in 1H2011. This provides yet another clear example of phishers gravitating towards services they can readily abuse.

We define "subdomain registration services" as providers that give customers subdomain "hosting accounts" beneath a domain name the provider owns. These services offer users the ability to define a "name" in their own DNS space for a variety of purposes. Thus a customer will obtain a hostname to use for his/her own Web site and/or e-mail of the form:

<customer_term>.<service_provider_sld>.TLD

Use of subdomain services continues to be a challenge, because only the subdomain providers themselves can effectively mitigate these phish.[10] While many of these services are responsive to complaints, very few take proactive measures to keep criminals from abusing their services in the first place.



This behavior is again exemplified by the top site for subdomain service abuse—the bee.pl service, based in Poland. **Over 30% of attacks using subdomain services occurred on subdomains provided by bee.pl**.

Second place went to ce.ms, where the count of malicious subdomains jumped from 203

[10] Standard domain name registrars or registry operators usually cannot mitigate these phish by suspending the main or "parent" domains as doing so would neutralize every subdomain hosted on the parent, thereby affecting innocent users as well. If extensive abuse happens on a single domain, a registrar may still opt to suspend the domain based on numerous complaints. This has been observed on occasion.

in 1H2011 to 1,288 in 2H2011. This was noticed throughout the security community, as malware authors also started pushing fake anti-virus software through subdomains on ce.ms.[11] The administrator of the subdomain claims to have implemented processes to curtail abuse, and we will be watching in 2012 to see if they were effective.

Dropping out of the top spot to fourth was the CO.CC service, based in Korea. Long abused by e-criminals, CO.CC is very responsive to abuse reports and it is good to see its volume down significantly.

We have identified over 700 subdomain registration providers, which offer services on more than 3,200 domain names. This is a space as rich as the current top-level domain space, since each subdomain service is effectively its own "domain registry." The subdomain services have many business models, and are unregulated. It has not been surprising to see criminals move into this space as some TLD registries and registrars have implemented better anti-abuse policies and procedures.

Top15 Subdomain Services Used for Phishing, 2H2011

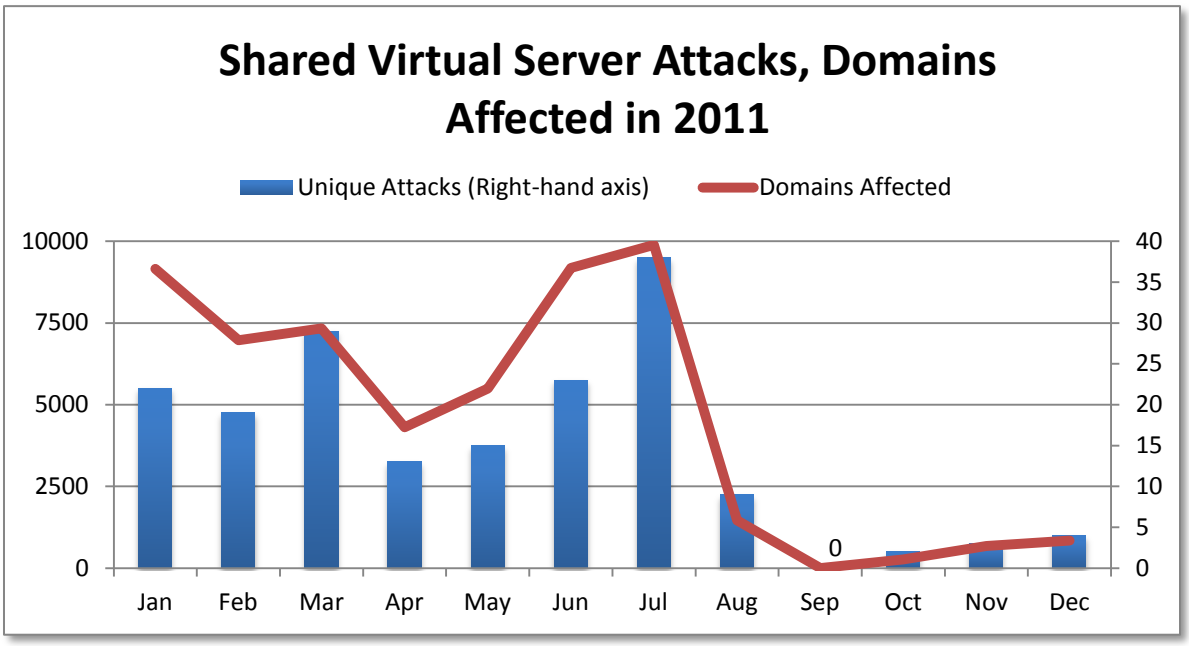
Rank	Domain	Total Attacks	Provider
1	osa.pl	4,500	bee.pl
2	ce.ms	1,288	ce.ms
3	cx.cc	1,214	cx.cc
4	co.cc	1,165	CO.CC, Inc.
5	cu.cc	749	cu.cc
6	bij.pl	720	bee.pl
7	cn.im	680	china0750.com
8	altervista.org	348	altervista.org
9	co.tv	324	co.tv
10	gv.vg	244	gv.vg
11	cz.cc	216	uni.me
12	0fees.net	199	II Hosting Media
13	tripod.com	184	Tripod
14	vv.cc	176	vv.cc
15	webs.com	128	Webs, Inc.

Shared Virtual Server Hacking

In the first half of 2011, a tactic used by phishers drastically affected our statistics. In this attack, a phisher breaks into a web server that hosts large numbers of domains – a "shared virtual server" in industry parlance. Once the phisher breaks into such a server, he first uploads a single copy of his phishing content. He then updates the web server configuration to add that content to *every* hostname served by that web server, so that all web sites on that server start displaying the phishing pages via a custom subdirectory.

[11] http://threatpost.com/en_us/blogs/attackers-moving-cems-domain-attack-sites-103111

So instead of hacking sites one at a time, the phisher can infect dozens, hundreds, or even thousands of web sites at a time, depending on the server. In 1H2011, we identified 42,488 phishing attacks that used this technique. **But in 2H2011, the number of shared virtual server phishing attacks dropped significantly, to 13,127. This was 16% of all phishing attacks worldwide.** The virtual server hacking dwindled to very low levels after July 2011, indicating a shift in tactics by the phishers using the tactic. We do not know why these attacks were mostly abandoned, and they could pop back up again at any point.



We will continue to watch this hacking closely to see if it recurs.

Use of Internationalized Domain Names (IDNs)

An area of growing interest on the Internet is Internationalized Domain Names, or IDNs. **Data continues to show that the unique characteristics of IDNs are not being used to facilitate phishing in a meaningful fashion.** But there was an interesting set of incidents caused by a sophisticated phisher.

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 characters from non-Latin scripts such as Arabic, Chinese, Cyrillic, or Hindi. Over the past seven years, IDNs have been available at the second and third levels in many domain name registries, with the majority registered in Asia. IDN TLDs allow the entire domain name to be in non-Latin characters, including the TLD extension. ICANN and IANA enabled the first IDN TLDs in May 2010, and as of this writing there are 38 approved IDN TLDs. While most IDN TLDs are not active, the .рф (.rf) TLD of the Russian Federation claims 940,000 domains.

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. Since January 2007, we had found only two homographic phishing attacks. In 2H2011, a phisher registered and used these three homographic domains:

- xn--mailchimp-7jfe.com (maĩlchĩmp.com)
- xn--verticalresponse-o8i.com (vertĩcalresponse.com)
- xn--icontact-o0e.com (ĩcontact.com)

These domains were all used in attacks against e-mail service providers (ESPs) that provide commercial e-mailing services for companies, including transactional e-mails and marketing campaigns. It is believed these domains were intended to "spear phish" employees and/or customers of these services, so the miscreants could then log into accounts there and send large volumes of spam. The attacks haven't been seen again, but this was certainly a troubling incident, showing sophistication on the part of the attacker.

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.

The new IDN TLD registries are being assigned to existing national ccTLD registry operators. We therefore do not believe that they will be more or less vulnerable to abuse than any other domain registry.

Use of URL Shorteners for Phishing

Phishers continue to use "URL shortening" services to obfuscate phishing URLs, but such use involved only 398 attacks in 2H2011. 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.

Some shortener providers like bit.ly have been aggressively screening for malicious forwarding destinations and imposing rules to make it much harder to abuse their systems. (And as a result, only 12 phishing attacks used bit.ly in 2H2011.) But as of this writing, a number of URL shorteners remained blocklisted by Spamhaus, including StumbleUpon's SU.PR and GoDaddy's X.CO service. We encourage all URL shortener providers to implement similar tactics. SURBL (http://www.surbl.org) provides free information on abusive use of shortener services, and all subdomain resellers should consider signing up for this feed of malicious URLs in order to mitigate abuse on their services.

We have also seen criminals create their own fake URL shortener services. The domain's home page may look like any other URL shortener service, but the reality is that the criminals are using the domain strictly for their own purposes. We classify such sites used for phishing as malicious domains.

Conclusions

As we have seen in the past, phishers shift toward the more economical options in their quest for profits. Changes in top-level-domain registration and security policies have tended to shift the phishing to other TLDs and services, and indeed in the second half of 2011, we saw phishers gravitate to subdomain registrations more than ever.

We also saw phishers gravitate toward victims that can be monetized effectively. Phishers in China are having some success victimizing Chinese citizens, particularly those who use Taobao.com. And in general, phishers concentrated on a smaller number of targets, perhaps because it was not economical to reach users of smaller institutions, or because user credentials at certain targets command a better price.

Appendix: Phishing Statistics and Uptimes by TLD

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
ac	Ascension Island	5	4	16,000	2.5	3.1	11:10:03	16:32:40	0	0.0
ad	Andorra	2	1	1,440	6.9	13.9	57:59:59	57:59:60	0	0.0
ae	United Arab Emirates	26	13	87,000	1.5	3.0	56:19:41	23:20:36	0	0.0
aero	sponsored TLD	3	1	7,718	1.3	3.9	23:12:24	11:44:44	0	0.0
af	Afghanistan	3	3	2,000	15.0	15.0	90:34:54	13:25:25	0	0.0
ag	Antigua and Barbuda	1	1	18,540	0.5	0.5	5:20:35	5:20:36	0	0.0
ai	Anguilla	2	2	3,250	6.2	6.2	9:11:19	9:11:20	0	0.0
al	Albania	4	2	6,500	3.1	6.2	24:57:56	28:40:03	0	0.0
am	Armenia	24	9	16,500	5.5	14.5	18:24:06	3:09:26	0	0.0
an	Netherlands Antilles	0	0	1,000	0.0	0.0			0	0.0
ao	Angola	3	3	260	115.4	115.4	36:56:35	38:00:42	0	0.0
ar	Argentina	300	236	2,393,873	1.0	1.3	46:56:38	15:13:56	2	0.0
arpa	Advanced Research Project Agency	0	0		0.0	0.0			0	0.0
as	American Samoa	2	1		0.0	0.0	18:29:13	18:29:13	0	0.0
asia	sponsored TLD	28	13	196,884	0.7	1.4	41:57:26	12:05:59	0	0.0
at	Austria	96	67	1,077,573	0.6	0.9	25:57:56	10:44:19	2	0.0
au	Australia	843	624	2,268,671	2.8	3.7	45:59:26	11:04:10	1	0.0
aw	Aruba	0	0	550					0	0.0
az	Azerbaijan	11	8	12,662	6.3	8.7	23:13:03	13:18:11	0	0.0
ba	Bosnia and Herzegovina	9	9	12,860	7.0	7.0	32:28:34	28:16:18	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
bd	Bangladesh	7	4	4,950	8.1	14.1	21:54:02	16:17:33	0	0.0
be	Belgium	241	118	1,210,530	1.0	2.0	45:41:15	19:12:41	2	0.0
bf	Burkina Faso	19	6		0.0	0.0	9:42:23	9:26:24	0	0.0
bg	Bulgaria	67	32	24,400	13.1	27.5	49:46:31	3:57:34	0	0.0
bh	Bahrain	0	0		0.0	0.0			0	0.0
bi	Burundi	8	8		0.0	0.0	14:58:20	4:11:23	0	0.0
biz	generic TLD	410	264	2,222,920	1.2	1.8	52:38:02	9:45:56	19	0.1
bm	Bermuda	0	0	7,800	0.0	0.0			0	0.0
bn	Brunei Darussalam	0	0	1,100	0.0	0.0			0	0.0
bo	Bolivia	11	4	7,500	5.3	14.7	79:05:25	91:26:51	0	0.0
br	Brazil	2,210	1,691	2,832,270	6.0	7.8	32:41:57	9:46:32	11	0.0
bs	Bahamas	0	0	2,200	0.0	0.0			0	0.0
bt	Bhutan	1	1		0.0	0.0	6:56:34	6:56:34	0	0.0
bw	Botswana	1	1		0.0	0.0	228:04:04	228:04:04	0	0.0
by	Belarus	45	32		0.0	0.0	65:14:01	21:31:50	0	0.0
bz	Belize	21	5	47,470	1.1	4.4	30:21:54	21:16:32	1	0.2
ca	Canada	340	253	1,803,381	1.4	1.9	41:09:38	13:04:12	0	0.0
cat	sponsored TLD	8	8	51,845	1.5	1.5	18:21:03	7:30:13	0	0.0
cc	Cocos (Keeling) Islands (domains estimated)	3,650	67	1,075,000	0.6	34.0	23:41:51	13:38:37	4	0.0
cd	Congo, Democratic Repub.	0	0	5,160	0.0	0.0			0	0.0
cg	Congo	0	0		0.0	0.0			0	0.0
ch	Switzerland	86	68	1,629,512	0.4	0.5	23:35:53	14:36:30	0	0.0
ci	Côte d'Ivoire	2	1	1,800	5.6	11.1	169:36:22	169:36:23	0	0.0
cl	Chile	333	260	361,650	7.2	9.2	32:27:48	8:48:55	0	0.0
cm	Cameroon	10	5	630	79.4	158.7	20:50:23	6:52:19	0	0.0
cn	China	173	128	3,413,127	0.4	0.5	30:16:30	15:02:54	8	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
co	Colombia	183	100	1,138,699	0.9	1.6	24:32:55	9:27:39	8	0.1
com	generic TLD	32,802	23,042	101,161,004	2.3	3.2	49:15:56	10:39:41	2,798	0.3
coop	sponsored TLD	1	1	9,470	1.1	1.1	69:36:54	69:36:54	0	0.0
cr	Costa Rica	14	12	13,750	8.7	10.2	71:18:24	14:54:17	0	0.0
cu	Cuba	0	0	1,550					0	0.0
cv	Cape Verde	1	1		0.0	0.0	16:19:23	16:19:23	0	0.0
cx	Christmas Island	142	4	5,200	7.7	273.1	13:28:52	10:39:24	0	0.0
cy	Cyprus	3	3	9,100	3.3	3.3	11:32:33	11:53:17	0	0.0
cz	Czech Republic	171	105	871,572	1.2	2.0	41:10:54	14:46:02	1	0.0
de	Germany	853	507	14,707,765	0.3	0.6	41:01:15	12:33:30	11	0.0
dj	Djibouti	0	0		0.0	0.0			0	0.0
dk	Denmark	127	93	1,160,592	0.8	1.1	38:38:29	20:24:56	0	0.0
dm	Dominica	1	1	14,500	0.7	0.7	7:49:59	7:49:59	0	0.0
do	Dominican Republic	9	8	16,500	4.8	5.5	44:29:00	9:45:50	0	0.0
dz	Algeria	1	1	1,800	5.6	5.6	59:37:41	59:37:42	0	0.0
ec	Ecuador	30	22	28,672	7.7	10.5	79:27:48	25:57:12	0	0.0
edu	U.S. higher education	22	16	7,588	21.1	29.0	33:25:25	11:25:03	0	0.0
ee	Estonia	24	18	64,021	2.8	3.7	28:50:52	12:10:39	0	0.0
eg	Egypt	2	2	5,975	3.3	3.3	56:06:56	56:06:57	0	0.0
er	Eritrea	0	0	108	0.0	0.0			0	0.0
es	Spain	209	166	1,147,150	1.4	1.8	53:31:51	15:34:24	1	0.0
et	Ethiopia	0	0	1,000	0.0	0.0			0	0.0
eu	European Union	261	188	3,503,500	0.5	0.7	49:55:50	12:40:31	9	0.0
fi	Finland	20	16	275,997	0.6	0.7	22:09:25	7:44:16	0	0.0
fj	Fiji	0	0	4,000	0.0	0.0			0	0.0
fk	Falkland Islands	0	0	100	0.0	0.0			0	0.0
fm	Micronesia, Fed. States	2	2		0.0	0.0	18:42:11	18:42:12	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
fo	Faroe Islands	0	0	3,000	0.0	0.0			0	0.0
fr	France	529	313	2,206,550	1.4	2.4	42:29:39	15:35:54	8	0.0
gd	Grenada	26	3	4,100	7.3	63.4	7:29:45	6:46:59	0	0.0
ge	Georgia	48	42	19,700	21.3	24.4	330:41:18	415:22:24	0	0.0
gg	Guernsey	64	6		0.0	0.0	1:43:08	0:10:00	0	0.0
gh	Ghana	6	6		0.0	0.0	83:14:48	83:14:48	0	0.0
gi	Gibraltar	1	1	1,831	5.5	5.5	23:24:29	23:24:29	0	0.0
gl	Greenland	3	1	4,600	2.2	6.5	1:00:03	0:58:30	0	0.0
gov	U.S. government	1	1	5,000	2.0	2.0	6:54:05	6:54:05	0	0.0
gp	Guadeloupe	22	14	1,475	94.9	149.2	19:20:11	9:23:56	0	0.0
gr	Greece	159	127	323,174	3.9	4.9	56:12:09	15:29:04	0	0.0
gs	South Georgia & Sandwich Is.	0	0	8,158	0.0	0.0			0	0.0
gt	Guatemala	6	6	9,600	6.3	6.3	36:01:48	13:36:59	0	0.0
gy	Guyana	2	2	1,811	11.0	11.0	33:54:24	33:54:24	0	0.0
hk	Hong Kong	38	29	226,505	1.3	1.7	87:11:06	12:01:06	1	0.0
hm	Heard and McDonald Is.	21	2		0.0	0.0	33:08:52	4:30:06	0	0.0
hn	Honduras	6	6	5,935	10.1	10.1	13:54:27	13:22:39	0	0.0
hr	Croatia	70	53	88,804	6.0	7.9	16:42:23	5:28:26	0	0.0
ht	Haiti	6	5	2,100	23.8	28.6	86:03:39	4:45:10	0	0.0
hu	Hungary	185	140	602,500	2.3	3.1	172:50:22	34:58:14	0	0.0
id	Indonesia	132	85		0.0	0.0	29:21:07	12:36:40	0	0.0
ie	Ireland	69	52	172,859	3.0	4.0	39:27:36	15:11:06	0	0.0
il	Israel	51	45	225,500	2.0	2.3	48:44:40	17:05:12	1	0.0
im	Isle of Man	685	4		0.0	0.0	33:16:35	18:57:37	0	0.0
in	India	1,613	1,314	1,122,549	11.7	14.4	45:55:37	18:10:24	950	8.5
info	generic TLD	2,173	1,825	8,694,417	2.1	2.5	46:24:31	11:52:52	952	1.1

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
int	sponsored TLD	1	1		0.0	0.0	18:25:39	18:25:39	0	0.0
io	British Indian Ocean Terr.	0	0	3,300	0.0	0.0			0	0.0
IP address	(no domain name used)	2,288			0.0	0.0				
iq	Iraq	0	0		0.0	0.0			0	0.0
ir	Iran	170	109	224,155	4.9	7.6	30:23:05	14:07:01	4	0.2
is	Iceland	11	10	36,051	2.8	3.1	84:08:26	17:05:32	0	0.0
it	Italy	442	243	3,655,000	0.7	1.2	66:04:23	24:22:31	1	0.0
je	Jersey	5	2		0.0	0.0	5:29:45	3:36:10	0	0.0
jm	Jamaica	181	179	6,380	280.6	283.7	82:23:52	83:14:48	0	0.0
jo	Jordan	2	2	4,200	4.8	4.8	42:20:35	42:20:36	0	0.0
jobs	sponsored TLD	0	0	41,453	0.0	0.0			0	0.0
jp	Japan	136	97	1,242,941	0.8	1.1	60:27:53	26:34:12	0	0.0
ke	Kenya	11	10	18,659	5.4	5.9	11:50:01	4:56:14	0	0.0
kg	Kyrgyzstan	5	4	5,300	7.5	9.4	25:08:35	27:12:31	0	0.0
kh	Cambodia	1	1	1,500	6.7	6.7	49:12:03	49:12:04	0	0.0
ki	Kiribati	0	0	250	0.0	0.0			0	0.0
kr	Korea	174	94	1,093,547	0.9	1.6	33:44:42	13:02:42	0	0.0
kw	Kuwait	2	2	3,040	6.6	6.6	1:15:15	1:15:15	0	0.0
ky	Cayman Islands	1	1	9,500	1.1	1.1	12:40:31	12:40:31	0	0.0
kz	Kazakhstan	37	18	42,055	4.3	8.8	71:06:40	42:43:41	0	0.0
la	Lao People's Demo. Rep. *(domains estimated)*	31	15	9,500	15.8	32.6	43:43:07	25:23:14	0	0.0
lb	Lebanon	1	1	2,975	3.4	3.4	309:38:38	309:38:38	0	0.0
lc	St. Lucia	7	7	2,801	25.0	25.0	11:33:31	8:47:59	0	0.0
li	Liechtenstein	4	4	67,099	0.6	0.6	12:24:14	8:50:17	0	0.0
lk	Sri Lanka	5	5	8,375	6.0	6.0	71:09:35	17:43:53	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
ls	Lesotho	0	0		0.0	0.0			0	0.0
lt	Lithuania	50	36	137,215	2.6	3.6	34:27:09	13:58:59	2	0.1
lu	Luxembourg	8	7	64,555	1.1	1.2	7:07:21	4:12:38	0	0.0
lv	Latvia	54	30	93,100	3.2	5.8	29:59:46	17:40:29	1	0.1
ly	Libya	27	6	11,333	5.3	23.8	16:49:47	1:55:36	0	0.0
ma	Morocco	27	21	41,144	5.1	6.6	38:25:24	12:40:31	0	0.0
mc	Monaco	0	0	2,050	0.0	0.0			0	0.0
md	Moldova	9	7		0.0	0.0	23:10:04	13:46:35	0	0.0
me	Montenegro	111	55	576,844	1.0	1.9	393:45:03	18:05:04	5	0.1
mg	Madagascar	5	3	1,000	30.0	50.0	12:39:36	12:09:51	0	0.0
mk	Macedonia	12	9		0.0	0.0	14:06:37	8:06:57	0	0.0
ml	Mali	0	0		0.0	0.0			0	0.0
mn	Mongolia	19	15	11,189	13.4	17.0	60:58:18	13:36:44	1	0.9
mo	Macao	0	0	310	0.0	0.0			0	0.0
mobi	sponsored TLD	15	15	1,010,544	0.1	0.1	23:08:59	3:34:10	0	0.0
mp	Northern Mariana Islands	1	1		0.0	0.0	43:39:51	43:39:52	0	0.0
mr	Mauritania	0	0		0.0	0.0			0	0.0
ms	Montserrat	1,307	8	9,700	8.2	1347.4	24:39:59	12:27:28	0	0.0
mt	Malta	0	0	6,000	0.0	0.0			0	0.0
mu	Mauritius	47	4	7,500	5.3	62.7	36:56:07	36:57:50	0	0.0
museum	sponsored TLD	0	0	438	0.0	0.0			0	0.0
mx	Mexico	309	185	527,626	3.5	5.9	36:34:20	13:30:24	0	0.0
my	Malaysia	145	125	132,775	9.4	10.9	39:35:54	12:05:59	0	0.0
mz	Mozambique	2	2	1,885	10.6	10.6	8:31:27	8:31:27	0	0.0
na	Namibia	0	0	220	0.0	0.0			0	0.0
name	generic TLD	18	14	235,672	0.6	0.8	73:04:15	16:35:05	1	0.0
nc	New Caledonia	0	0		0.0	0.0			0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
ne	Niger	0	0	140	0.0	0.0			0	0.0
net	generic TLD	4,211	2,740	14,678,203	1.9	2.9	68:37:36	11:43:03	519	0.4
nf	Norfolk Island	10	3	1,600	18.8	62.5	10:07:29	2:44:32	0	0.0
ng	Nigeria	19	13	1,355	95.9	140.2	29:47:44	13:20:53	1	7.4
ni	Nicaragua	2	1	6,300	1.6	3.2	22:03:52	22:03:53	0	0.0
nl	Netherlands	462	332	4,778,280	0.7	1.0	37:08:44	14:08:21	1	0.0
no	Norway	74	49	532,583	0.9	1.4	63:32:15	21:22:06	0	0.0
np	Nepal	34	23	27,516	8.4	12.4	38:15:38	8:48:06	0	0.0
nr	Nauru	6	1	460	21.7	130.4	6:56:34	8:02:06	0	0.0
nu	Niue *(domains estimated)*	186	29	60,000	4.8	31.0	23:26:39	10:44:28	0	0.0
nz	New Zealand	81	67	463,960	1.4	1.7	38:24:13	9:41:57	0	0.0
om	Oman	0	0	50					0	0.0
org	generic TLD	3,010	1,981	9,636,087	2.1	3.1	39:08:04	9:39:16	68	0.1
pa	Panama	0	0	6,551	0.0	0.0			0	0.0
pe	Peru	83	38	56,655	6.7	14.7	35:58:08	16:03:17	1	0.2
pf	French Polynesia	0	0	210	0.0	0.0			0	0.0
pg	Papua New Guinea	3	1		0.0	0.0	35:25:30	44:37:34	0	0.0
ph	Philippines *(domains estimated)*	31	20	30,000	6.7	10.3	18:49:39	7:49:59	0	0.0
pk	Pakistan *(domains estimated)*	67	63	18,000	35.0	37.2	27:14:50	3:58:51	0	0.0
pl	Poland	6,158	514	2,217,465	2.3	27.8	29:58:39	13:03:38	2	0.0
pn	Pitcairn	13	5	870	57.5	149.4	60:25:07	14:34:59	0	0.0
pr	Puerto Rico	1	1		0.0	0.0	83:14:48	83:14:48	0	0.0
pro	sponsored TLD	4	4	120,610	0.3	0.3	4:35:08	2:50:50	0	0.0
ps	Palestinian Territory	27	7	3,190	21.9	84.6	8:07:06	1:47:11	0	0.0
pt	Portugal	85	56	233,483	2.4	3.6	33:27:23	9:46:29	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
py	Paraguay	11	10	12,775	7.8	8.6	21:40:53	13:11:19	0	0.0
qa	Qatar	3	2		0.0	0.0	36:23:19	18:28:42	0	0.0
re	Réunion	5	3	10,013	3.0	5.0	50:45:50	25:49:03	0	0.0
rf (.рф)	Russian Federation IDN (.xn--p1ai)	1	1	940,050	0.0	0.0	37:09:27	37:09:27	0	0.0
ro	Romania	259	194	557,413	3.5	4.6	40:40:38	10:44:24	1	0.0
rs	Serbia	77	51	68,643	7.4	11.2	86:41:46	49:20:27	0	0.0
ru	Russian Fed.	989	627	3,540,500	1.8	2.8	39:03:37	14:10:29	8	0.0
rw	Rwanda	1	1		0.0	0.0	1:44:43	1:44:43	0	0.0
sa	Saudi Arabia	22	14	26,427	5.3	8.3	47:49:45	19:50:56	0	0.0
sc	Seychelles	3	3	4,658	6.4	6.4	9:01:17	8:32:57	0	0.0
sd	Sudan	3	3		0.0	0.0	14:19:19	16:32:16	0	0.0
se	Sweden	168	120	1,152,411	1.0	1.5	32:42:03	12:40:31	0	0.0
sg	Singapore	37	31	135,220	2.3	2.7	27:24:25	11:57:38	0	0.0
sh	Saint Helena	1	1	2,966	3.4	3.4	37:16:49	37:16:49	0	0.0
si	Slovenia	57	49	100,724	4.9	5.7	203:51:30	37:28:26	0	0.0
sk	Slovakia	49	32	256,849	1.2	1.9	34:42:02	14:51:59	0	0.0
sl	Sierra Leone	0	0	856	0.0	0.0			0	0.0
sm	San Marino	0	0	1,905	0.0	0.0			0	0.0
sn	Senegal	0	0	3,562	0.0	0.0			0	0.0
so	Somalia	4	4		0.0	0.0	8:25:41	8:25:41	1	0.0
st	Sao Tome and Principe	5	4		0.0	0.0	33:28:50	31:07:51	0	0.0
su	Soviet Union	21	16	100,367	1.6	2.1	21:15:48	8:28:39	2	0.2
sv	El Salvador	2	2	5,300	3.8	3.8	8:22:35	8:22:36	0	0.0
sy	Syria	0	0		0.0	0.0			0	0.0
sz	Swaziland	0	0	1,148	0.0	0.0			0	0.0
tc	Turks and Caicos	57	16	10,758	14.9	53.0	86:51:17	9:59:53	1	0.9

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
tel	generic TLD	0	0	280,502	0.0	0.0			0	0.0
tf	French Southern Territories	5	4	1,550	25.8	32.3	5:09:14	2:37:02	0	0.0
tg	Togo	1	1		0.0	0.0	177:41:17	177:41:18	0	0.0
th	Thailand	110	69	65,309	10.6	16.8	36:59:18	12:14:39	0	0.0
tj	Tajikistan	1	1	18,796	0.5	0.5	1:03:21	1:03:22	0	0.0
tk	Tokelau	7,605	7,316	6,101,229	12.0	12.5	22:46:06	11:43:02	7,308	12.0
tl	Timor-Leste	7	5	1,795	27.9	39.0	19:56:38	15:45:05	0	0.0
tm	Turkmenistan	4	1	3,775	2.6	10.6			0	0.0
tn	Tunisia	0	0	9,700	0.0	0.0			0	0.0
to	Tonga	50	17	14,500	11.7	34.5	58:00:51	15:58:40	2	1.4
tp	Portuguese Timor	0	0		0.0	0.0			0	0.0
tr	Turkey	97	80	275,141	2.9	3.5	121:26:52	20:54:39	0	0.0
travel	sponsored TLD	3	3	26,796	1.1	1.1	16:58:14	10:18:48	0	0.0
tt	Trinidad and Tobago	0	0	2,375					0	0.0
tv	Tuvalu *(domains est.)*	379	38	215,000	1.8	17.6	31:09:10	15:45:05	1	0.0
tw	Taiwan	273	115	509,943	2.3	5.4	96:58:47	14:44:30	16	0.3
tz	Tanzania	2	1	4,341	2.3	4.6	10:44:20	10:44:21	0	0.0
ua	Ukraine	261	188	617,251	3.0	4.2	39:46:37	13:03:14	1	0.0
ug	Uganda	1	1	3,258	3.1	3.1	17:31:01	17:31:02	0	0.0
uk	United Kingdom	1,413	1,095	9,802,638	1.1	1.4	35:16:16	9:45:56	124	0.1
us	United States	301	177	1,701,186	1.0	1.8	40:53:32	10:11:24	21	0.1
uy	Uruguay	7	4	34,507	1.2	2.0	19:04:00	11:36:39	0	0.0
uz	Uzbekistan	2	2	13,221	1.5	1.5	13:56:49	13:56:49	0	0.0
vc	St. Vincent and Grenadines	5	3	7,443	4.0	6.7	203:13:32	203:13:33	0	0.0
ve	Venezuela	34	28	199,000	1.4	1.7	23:35:52	6:44:07	0	0.0
vg	British Virgin Islands	250	5	8,400	6.0	297.6	28:51:23	17:34:51	0	0.0

TLD	TLD Location	# Unique Phishing attacks 2H2011	Unique Domain Names used for phishing 2H2011	Domains in registry Nov 2011	Score: Phishing domains per 10,000 domains 2H2011	Score: Attacks per 10,000 domains 2H2011	Average Uptime 2H2011 hh:mm:ss	Median Uptime 2H2011 hh:mm:ss	# Malicious Domains Registered 2H2011	Malicious registrations score/10,000 domains in registry
vi	Virgin Islands	0	0	17,091	0.0	0.0			0	0.0
vn	Vietnam	103	74	253,319	2.9	4.1	35:20:55	17:12:09	0	0.0
vu	Vanuatu	42	14		0.0	0.0	11:24:51	7:52:47	0	0.0
ws	Samoa	63	38	544,500	0.7	1.2	43:38:16	13:25:19	10	0.2
xxx	sponsored TLD	0	0	1,310	0.0	0.0			0	0.0
ye	Yemen	0	0	800					0	0.0
yu	Yugoslavia (TLD deprecated March 2010)	0	0	0	0.0	0.0			0	0.0
za	South Africa	237	191	685,046	2.8	3.5	47:09:43	11:22:50	2	0.0
zm	Zambia	2	2		0.0	0.0	12:05:40	12:05:40	0	0.0
zw	Zimbabwe	2	2	7,500	2.7	2.7	15:21:53	15:21:54	0	0.0
	TOTALS	**83,082**	**50,298**	**229,288,823**					**12,895**	

About the Authors & Acknowledgments

The authors wish to thank the following for their support: Peter Cassidy and Foy Shiver of the APWG; Aaron Routt of Internet Identity; and Ram Mohan and Bruce Reeser of Afilias. The authors thank Liming Wang and Wang Wei at CNNIC for the contribution of APAC phishing data for this report. The authors thank DomainTools for their contribution of WHOIS data to help identify trends in malicious registrations. The authors also thank the members of the security industry, the domain name industry, and the law enforcement community who have contributed to anti-phishing programs and research.

Rod Rasmussen is President and CTO of Internet Identity (www.internetidentity.com), and has served as its technical leader since he co-founded the company in 2001. He is widely recognized as a leading expert on the abuse of the domain name system by criminals. Rasmussen is co-chair of the Anti-Phishing Working Group's (APWG) Internet Policy Committee and serves as the APWG's Industry Liaison, representing and speaking on behalf of the organization at events around the world. In this role, he works closely with ICANN, the international oversight body for domain names, and is a member of ICANN's Security and Stability Advisory Committee (SSAC). Rasmussen is a member of the Online Trust Alliance's (OTA) Steering Committee and was recently appointed to the FCC's Communications Security, Reliability and Interoperability Council (FCC CSRIC). He is also an active member of the Digital PhishNet, a collaboration between industry and law enforcement, and is an active participant in the Messaging Anti-Abuse Working Group (MAAWG), and is IID's FIRST representative (Forum of Incident Response and Security Teams). He also is a regular participant in DNS-OARC meetings, the worldwide organization for major DNS operators, registries and interested parties, and in ICANN's series of DNS Security, Stability, and Resiliency Symposiums. Rasmussen earned an MBA from the Haas School of Business at UC-Berkeley and holds two bachelor's degrees, in Economics and Computer Science, from the University of Rochester.

Greg Aaron is President of Illumintel Inc., which provides advising and security services to top-level domain registry operators and other Internet companies. He was previously the Director of Key Account Management and Domain Security at Afilias (www.afilias.info), and Greg continues to contribute to Afilias' security programs, including anti-abuse services for the .ORG registry. Greg is an authority on the use of domain names for e-crime, and works with registrars, registries, law enforcement, and researchers regarding phishing, malware, spam, and child pornography cases. In 2010, Greg accepted an OTA Excellence in Online Trust Award for Afilias' anti-abuse programs. He was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG), and joined ICANN's Security and Stability Advisory Committee (SSAC) in 2011. Greg also serves on the Steering Committee of the Anti-Phishing Working Group (APWG) and is a participant in MAAWG. 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.

#