Global Phishing Survey: Trends and Domain Name Use in 2H2008

An APWG Industry Advisory

APWG

Committed to Wiping Out Internet Scams and Fraud

May 2009

Authors:

Greg Aaron
Afilias
<gaaron at afilias.info>

Rod Rasmussen
Internet Identity
<rod.rasmussen at internetidentity.com>

Table of Contents

Overview

Phishers are constantly experimenting, looking for better ways to defraud Internet users and reap more money from their crimes. The second half of 2008 found phishers adopting new strategies and tactics. To combat phishing, we seek to better understand how they are using domain names, and why. Domain name usage is an important measure of the scope of the global phishing problem, and examination of domain name system trends can provide effective new anti-abuse tools.

This study describes our analysis of a comprehensive database of the phishing that took place in the second half of 2008 (2H2008), and is a follow-up to our earlier studies of data stretching back to January 2007.[1] Specifically, this new report examines all the phishing attacks detected between July 1, 2008 and December 31, 2008, as collected by the APWG and supplemented with data from several phishing feeds and private sources. The APWG phishing repository is the Internet's most comprehensive archive of phishing and e-mail fraud activity.

New to this 2H2008 report is 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.

Our data reveals several new trends, and we hope that bringing them to light will lead to improved anti-phishing measures.

Our major findings include:

1. **Phishers are increasingly using subdomain services** to host and manage their phishing sites. Phishers use such services almost as often as they register domain names. And such attacks even account for the majority of phishing attacks in certain large TLDs. This trend shows phishers migrating to services that cannot be taken down by registrars or registry operators, thereby frustrating some takedowns and extending the uptimes of attacks.
2. **Phishers continue to target specific Top-Level Domains (TLDs) and specific domain name registrars**, and shift their preferences over time. 2H2008 demonstrated what can happen to registries and registrars who are not prepared to combat phishing with effective policies and procedures.
3. **The amount of Internet names and numbers used for phishing has remained fairly steady over the past two years**.
4. **Anti-phishing programs implemented by domain name registries can have a remarkable effect** on the up-times (durations) of phishing attacks.
5. There are decreases in **phishing on IP addresses and the use of brand names in domain names** to fool users. Phishers are **not using IDNs** (Internationalized Domain Names).

[1] The previous studies are available at:
1H2008: http://www.apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf
2007: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2007.pdf

Basic Statistics

Millions of phishing URLs were reported in 2H2008, but the number of phishing attacks and domain names used to host them is much smaller.[1] The 2H2008 data set yields the following statistics:

- There were at least **56,959 phishing attacks**. An "attack" is defined as a phishing site that targets a specific brand or entity. One domain name can host several discrete attacks against different banks, for example. This is up from the 47,324 attacks recorded in 1H2008.
- Those attacks occurred on **30,454 unique domain names**.[2] This is up slightly from previous periods.
- Of the 30,454 phishing domains, we identified **5,591 that we believe were registered by phishers. These "malicious" domain registrations represent about 18.5%** of the domain names involved in phishing. Virtually all the rest were hacked domains belonging to innocent site owners. Only about **3.5% of all domain names that were used for phishing contain a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations" below.)
- In addition, phish were detected on **2,809 unique IP addresses**, rather than on domain names. (For example: http://96.56.84.42/ClientHelp/ssl/index.htm.) This is down significantly from the 3,389 seen in 1H2008, the 5,217 in 2H2007, and the 6,336 in 1H2007. Phishing on IPv6 addresses was negligible.
- If unique domain names and unique IP addresses used for phishing are added together, **the amount of Internet names and numbers used for phishing has remained relatively steady** for the past two years.
- Phishing took place on domain names in **170 TLDs**. That number has grown steadily since mid-2007. During that time, the number of domain names registered in ccTLDs grew by 38%.
- Only 10 of the 30,454 domain names were Internationalized Domain Names (IDNs). All appear to be cases where phishers hacked the domains' servers. So in 2H2008, **phishers did not attempt to use IDNs** to spoof brand names.

[1] This is due to several factors: A) Some phishing involves customized attacks by incorporating unique numbers in the URLs (to track targeted victims, or to defeat spam filters). A single phishing attack can therefore manifest as thousands of individual URLs. B) Phishers often use one domain name to host simultaneous attacks against different target brands. Some phishers are known for placing four or more different phishing attacks on each domain name it registers. 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.

Basic Statistics:

	2H2008	1H2008	2H007
Phishing domain names	**30,454**	**26,678**	**28,818**
IP-based phish (unique IPs)	**2,809**	**3,389**	**5,217**
TLDs phished in	**170**	**155**	**145**
Attacks	**>56,969**	**>47,342**	
IDN domains	**10**	**52**	**10**

Each domain name's registrar of record was often not reported at the time of the phish. In most registries, a domain name can have multiple "lifetimes" as the name is registered, is deleted or expires, and is then registered anew. Obtaining accurate registrar sponsorship

of 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. Registrar-specific statistics and trends are certainly of interest, and are an opportunity for future studies.

Prevalence of Phishing by Top-Level Domain (TLD)

We analyzed the 30,454 phishing domains to see how many fell into which TLDs. The absolute counts by TLD are interesting, but the sizes of the various TLDs vary widely. To place 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" 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.[1] This metric is a way of revealing whether a TLD has a higher or lower incidence of phishing relative to others. In 2H2008, phishing occurred on domain names in 170 TLDs. Of these, we were able to obtain the domain count statistics for 138 TLD registries.[2] Those 138 TLDs contained 98.9% of the phishing domains in our data set (30,119 out of the 30,454), and a total of 179,913,118 domain names overall.

The complete tables are presented in Appendix A, including the scores and the number of phish in each TLD.

- The **median score was 2.7.**
- The **average score was 6.3**, which was skewed by a few high-scoring TLDs.
- .COM, the world's largest and most ubiquitous TLD, had a score of **1.8**. .COM contains 46% of the phishing domains in our data set, and 44.7% of the domains in the TLDs for which we have domains-in-registry statistics. In the ranking of TLDs by score, there are 63.6 million domains in the TLDs ranked below .COM, and 35.8 million in the TLDs ranked above .COM.

[1] Score = (phishing domains / domains in TLD) x 10,000
[2] For the purposes of this study, we used the number of domain names in each registry as of December 2008. Sources: ICANN.org (monthly registry reports), ccTLD registry operators.

We therefore suggest that scores between .COM's 1.8 and the median of 2.7 occupy the middle ground, with scores above 2.7 indicating TLDs with increasingly prevalent phishing.

The metric "Phishing Attacks per 10,000" provides insight into what TLDs are predominantly used by phishers who use subdomain services, and where high-volume phishers place multiple phish on one domain.

Notes regarding the statistics:

- A small number of phish can increase a small TLD's score significantly, and these pushed up the study's median score. The larger the TLD, the less a phish influences its score, and indeed 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 2007 study.

Eliminating TLDs that had less than 30,000 domains under management or less than 25 phishing domains yields the following:

Top 15 Phishing TLDs by Score

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

Rank	TLD	TLD Location	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008
1	ve	Venezuela	1,504	82,500	**182.3**
2	th	Thailand	88	39,880	**22.1**
3	bz	Belize	55	43,377	**12.7**
4	su	Soviet Union	76	85,119	**8.9**
5	ro	Romania	188	310,114	**6.1**
6	cl	Chile	116	232,897	**5.0**
7	kr	Korea	413	983,626	**4.2**
8	vn	Vietnam	37	92,992	**4.0**
9	ru	Russia	676	1,860,179	**3.6**
10	tw	Taiwan	144	406,669	**3.5**
11	fr	France	430	1,289,559	**3.3**
12	my	Malaysia	25	80,786	**3.1**
13	mx	Mexico	80	277,652	**2.9**
14	be	Belgium	240	859,474	**2.8**
14	gr	Greece	71	250,000	**2.8**
14	ir	Iran	29	102,800	**2.8**

The "generic" TLDs are used by and are popular with registrants across the world. There is some variance in their scores:

Phishing in gTLDs by Score

Rank	TLD	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008
1	name	72	288,306	**2.5**
2	org	1,568	7,364,670	**2.1**
3	net	2,292	12,286,364	**1.9**
4	com	14,431	80,450,204	**1.8**
5	biz	222	2,077,413	**1.1**
6	info	508	5,138,132	**1.0**

If measured by Attack Score, certain TLDs vault into much higher rankings:

Top 15 Phishing TLDs by Attack Score

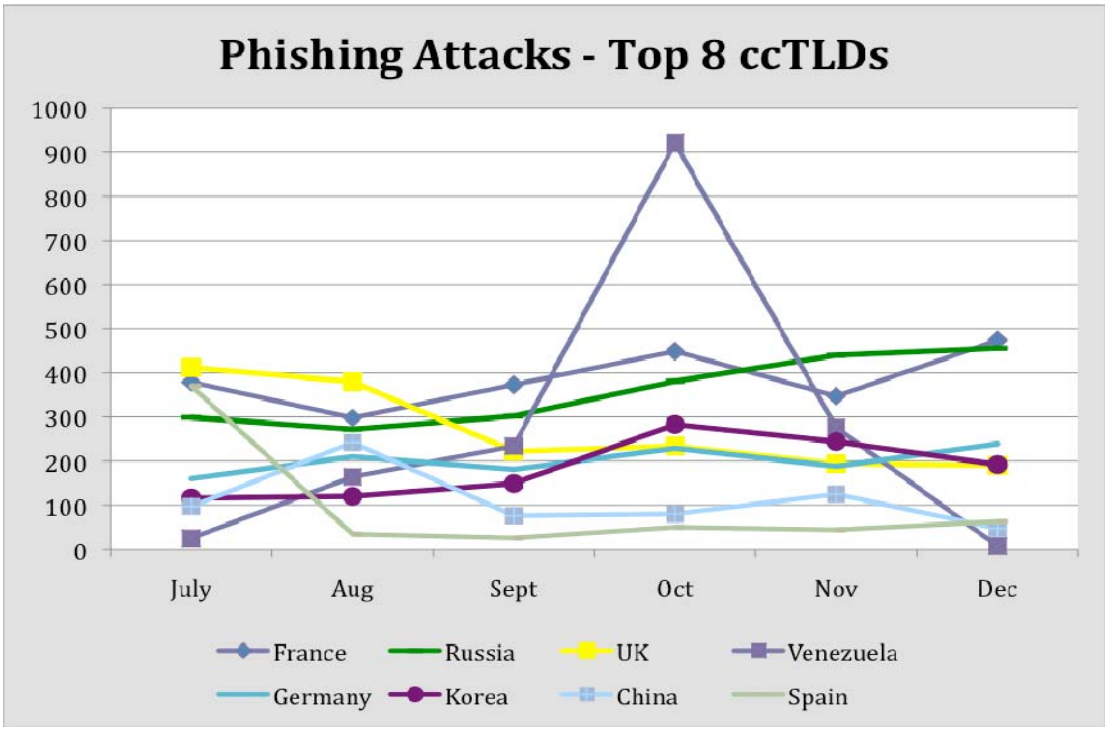
Minimum 50 phishing attacks and 30,000 domain names in registry

Rank	TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008
1	ve	Venezuela	1,627	1,504	82,500	**182.3**	**197.2**
2	th	Thailand	170	88	39,880	**22.1**	**42.6**
3	su	Soviet Union	271	76	85,119	**8.9**	**31.8**
4	fr	France	2,320	430	1,289,559	**3.3**	**18.0**
5	bz	Belize	69	55	43,377	**12.7**	**15.9**
6	ru	Russia	2,150	676	1,860,179	**3.6**	**11.6**
7	kr	Korea	1,104	413	983,626	**4.2**	**11.2**
8	ro	Romania	289	188	310,114	**6.1**	**9.3**
9	cl	Chile	211	116	232,897	**5.0**	**9.1**
10	vn	Vietnam	62	37	92,992	**4.0**	**6.7**
11	il	Israel	78	38	139,243	**2.7**	**5.6**
11	tw	Taiwan	226	144	406,669	**3.5**	**5.6**
13	es	Spain	586	253	1,082,757	**2.3**	**5.4**
14	gr	Greece	128	71	250,000	**2.8**	**5.1**
15	be	Belgium	430	240	859,474	**2.8**	**5.0**
15	ua	Ukraine	198	107	397,051	**2.7**	**5.0**
15	mx	Mexico	140	80	277,652	**2.9**	**5.0**
15	sk	Slovakia	87	31	172,500	**1.8**	**5.0**

.FR and .RU received high Attack Scores because phishers launched large numbers of attacks in these TLDs via subdomain hosting services. (For more, see "Use of Subdomains for Phishing," below.) Attack Score is therefore a useful measure of the pervasiveness of phishing in a namespace.

As in previous periods, phishing gang activity had a major impact on a few TLDs and registrars. In the first half of 2008, we saw how the notorious Rock phishing attacks affected .HK, .UK, and .ES, with severe impacts being felt by .HK until registry operator/registrar HKIRC put an industry-leading anti-abuse program in place.

In the summer of 2008, the Rock ceased activity and disappeared, and this is reflected in the drop-off in attacks using .UK and .ES domains in July and August:



However, a new phishing gang called "Avalanche" began attacks in December 2008, and ramped up significantly in early 2009. This group uses an infrastructure and methods very similar to the Rock, and has added fast-flux hosting to sustain its attacks. The "Avalanche" gang is having a major impact on some TLDs in 2009, including .BE and .EU.

High-scoring TLDs almost invariably suffered from the systematic exploitation by phishers. These cases highlight how vulnerabilities can lead to significant problems. Examples are:

- **.VE** (Venezuela. Score 182.3; 1,627 attacks on 1,504 domains.) Attacks using .VE domains went from virtually none to more than 900 in October, before nearly disappearing again by the end of the year. This is an example of how phishers target specific registries and registrars, seeking out ones they can exploit. Typically, such providers have weak or non-existent policies for mitigating fraudulent or

malicious domain registrations, weak credit-card verification processes to identify registrations using stolen credit cards, and modern systems that allow quick DNS updates.

In late 2008, the .VE registry was taken advantage of by phishers who registered .VE domains to mount attacks against eBay and PayPal, supported by fast-flux hosting. NIC.VE provides services under a combined registry/registrar model, and works under a branch of the Venezuelan government. The phishers began with a probing set of attacks in July. NIC.VE's policy required it to seek various authorizations before acting, and as a result phishing remediation times measured in weeks. There was also a shift in how the registry was managed within the government, exacerbating the situation. The phishers realized they had found a reliable and weakly defended source of domains.

The attacks escalated to the point where they overwhelmed the registry operator, which had never seen these sorts of attacks. There was constructive outreach by many parties in the security community, including law enforcement, CERTs, other TLD operators, LACNIC, and security service providers. This helped NIC.VE put new policy and procedures in place, which allowed it to make rapid domain suspensions. This effective response drove the phishers away, and the attacks subsided. This case is an illustration of how other registries and registrars should put procedures, policies, personnel, and tools in place prior to being targeted.

- **.TH** (Thailand. Score: 22.1; 170 attacks; 88 phishing domains. Thirty-six of the phishing domains were in the AC.TH (academic) zone, and 15 more were in the GO.TH (government) zone. We highlighted these vulnerabilities in our last report, but it appears that phishers are still breaking into unsecure institutional servers in Thailand.

- **.SU** (Soviet Union. Score: 8.9; attack score 31.8). This TLD is notable because it was to have been phased out years ago, after the dissolution of the Soviet Union. However, it has not removed it from the DNS root, and the registry operator has been actively building new registrations.[1] .SU had significant phishing on malicious domain name registrations, and at subdomain resellers (see more below).

Compromised Domains vs. Malicious Registrations

Of the 30,454 phishing domains, **we identified 5,591 that we believe were registered by phishers. These "malicious" or "bad" domains represent about 18.5% of the domain names involved in phishing.**

We identified maliciously registered domains as those that were reported for phishing within a short time of being registered (this is an indicator that their sites were not compromised), and/or contained a brand name or misleading string, and/or were registered in batches or in patterns that indicated common ownership or intent. There are some domains above and beyond the 5,591 we were not highly confident about classifying as "malicious," and so we left them out of the count.

[1] .SU is managed by the Russian Institute for Public Networks, which also operates the .RU TLD.[1] http://en.wikipedia.org/wiki/.su and http://www.nic.ru/en/

Up to 81% of the domains used for phishing were "compromised" or hacked domains. Phishing most often takes place on compromised Web servers, where the phishers place their phishing pages unbeknownst to the site operators. This method gains the phishers free hosting, and complicates take-down efforts because suspending a domain name or hosting account also disables the resolution of the legitimate user's site. Phishing on a compromised Web site typically takes place on a subdomain or in a subdirectory, where the phish is not easily noticed by the site's operator or visitors.

The remaining <1% of the domains used for phishing were domains operated by subdomain resellers and sites that offer Web site hosting (such as ISPs, geocities.com, etc.).

Of the maliciously registered domains, **1,053 contained a relevant brand name, variation, or misspelling thereof.[1] This represents about 19% of maliciously registered domains, and 3.5% of all domains that were used for phishing**. 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. **Most maliciously registered domains were random strings**, such as *hodfw42hj.com.es*, that offered nothing to confuse a potential victim.

There were even 76 domains that contained a brand name, but were not used to phish that brand. Instead, the phishers used those domains to attack unrelated targets.[2]

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.

Of the malicious registrations, a significant number contained neither a brand name, nor any other inducement. Typical URLs were:

- http://www.001u6kyklskwn3rmnv.org.ve/cmd-confirm/
- http://whymanwand.es/olb/MemberForm.do

Clearly, the domain name itself usually does not matter to phishers, and a hacked domain name of any meaning, in any TLD, will do. Malicious domain name registrations do remain a damaging part of the current phishing problem, since they are used by the most prolific phishing gangs, which use them to harbor multiple phishing attacks.

Phishing By Uptime

How long did the phishing attacks last, and how damaging were they? To learn more, we analyzed uptimes.

[1] Examples of domain names we counted as containing brand names included: paiypaiypalsa.com (PayPal), poste-bpol-email.com (Poste Italiene), and capttall.com (Capital One).
[2] Examples included paypanl.net (used to attack Bank of America but not PayPal), and halifaax.com (used to attack PayPal France but not Halifax Bank).

In 2H2008, Internet Identity monitored the "uptimes" or "live" times of the phishing attacks in the data set.[1] Uptimes 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, and the more money the phisher can make. A top-ten American bank estimates that *at least US$300 is lost for every hour that a phishing site remains up*.[2]

Phishers therefore strive for maximum uptime, and make choices accordingly. Phishers prefer vulnerable or inattentive registrars and registries, and some phishers use fast-flux hosting to extend uptimes. (Phish hosted on fast-flux networks often stay up twice as long as those on conventional hosting.) Long-lived phish can skew the averages considerably, as some phishing sites may last weeks or even months. Thus medians may be a useful barometer of overall mitigation efforts.

We calculated the average and median uptimes for all of the 2H2008 attacks, and also for the attacks associated with some of the larger TLDs. For all 56,959 attacks, the **average uptime was 52 hours**, with a **median of 14 hours, 43 minutes**.

The uptimes for all phishing attacks in 2H2008, and for phish in large TLDs, were as follows:

ALL TLDs

	Average	Median
Uptimes	HH:MM:SS	HH:MM:SS
July	53:32:30	16:17:24
Aug	43:31:12	15:26:41
Sept	54:46:22	15:58:45
Oct	49:11:03	14:14:54
Nov	53:55:39	13:59:50
Dec	58:35:36	14:21:43
2H2008:	52:01:58	AVERAGE
	14:43:15	MEDIAN

[1] 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 has 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.

[2] This estimate posits that the average loss from a stolen bank access credential (either online account access, a debit card, or credit card) is US$400, and that the phisher steals two such valid credentials every three hours. This impact generally holds throughout the first 72 hours of phishing site uptime. Note these are conservative estimates since they measure only are bottom-line losses, and do not factor in "soft costs" like customer support calls, unseen losses through untracked channels, or the impact of ID theft upon the customer.

.COM

	Average	Median
Uptimes	HH:MM:SS	HH:MM:SS
July	56:18:31	14:55:42
Aug	48:48:51	14:56:39
Sept	56:50:21	15:03:33
Oct	53:38:33	14:16:10
Nov	55:34:17	13:23:32
Dec	64:16:52	13:38:25
2H2008:	56:11:11	AVERAGE
	14:20:27	MEDIAN

.NET

	Average	Median
Uptimes	HH:MM:SS	HH:MM:SS
July	62:11:06	16:47:04
Aug	37:20:42	13:24:33
Sept	52:40:10	16:56:44
Oct	36:25:42	13:54:32
Nov	51:38:22	13:52:58
Dec	49:27:24	14:13:50
2H2008:	48:10:49	AVERAGE
	14:38:28	MEDIAN

.ORG

Average	Median	HH:MM:SS
July	71:14:23	17:35:54
Aug	37:15:04	12:24:29
Sept	50:22:24	17:22:20
Oct	48:46:50	15:23:07
Nov	50:05:46	14:15:19
Dec	41:54:01	11:37:56
	49:27:43	AVERAGE
	14:55:17	MEDIAN

.INFO

	Average	Median
Uptimes	HH:MM:SS	HH:MM:SS
July	33:46:10	14:13:51
Aug	18:48:02	11:07:42
Sept	25:30:03	13:31:53
Oct	53:28:25	10:20:37
Nov	23:45:59	11:22:49
	28:21:22	AVERAGE
	11:09:25	MEDIAN

.BIZ

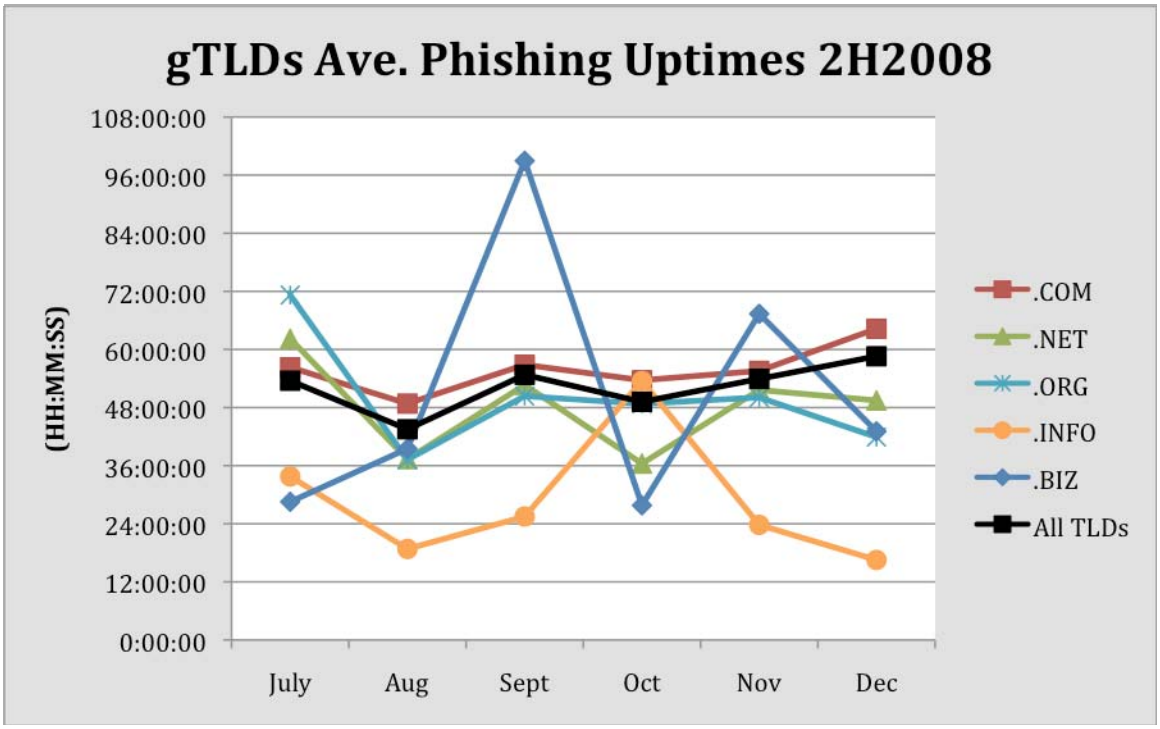
	Average	Median
Uptimes	HH:MM:SS	HH:MM:SS
July	28:32:20	14:28:53
Aug	39:30:09	18:34:03
Sept	98:57:29	24:02:39
Oct	27:48:05	14:26:11
Nov	67:21:03	24:26:24
Dec	43:05:32	1611:52:20
	52:07:59	AVERAGE
	16:45:48	MEDIAN

.CN

	Average	Median
Uptimes	HH:MM:SS	HH:MM:SS
July	33:46:10	14:13:51
Aug	27:10:04	12:03:43
Sept	47:48:51	14:15:33
Oct	34:26:21	19:55:56
Nov	24:33:36	7:37:59
Dec	69:18:31	17:13:01
	34:15:09	AVERAGE
	12:43:10	MEDIAN

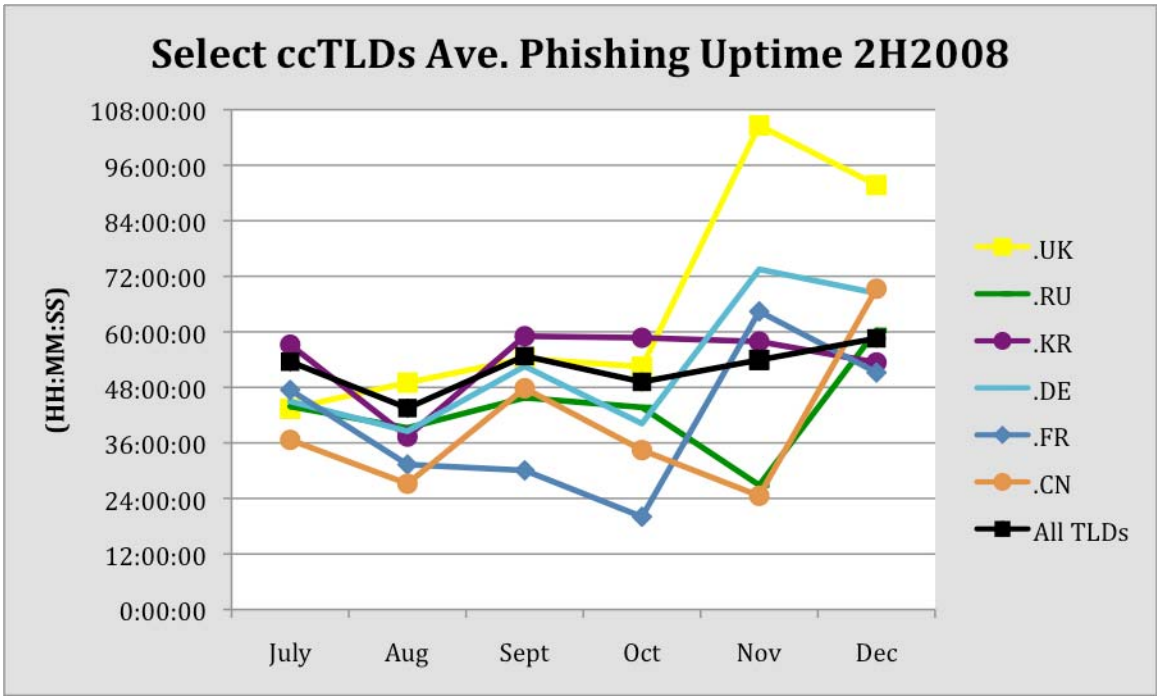
	.RU			.UK	
	Average	Median		Average	Median
Uptimes	HH:MM:SS	HH:MM:SS	***Uptimes***	HH:MM:SS	HH:MM:SS
July	July	12:54:54	July	43:23:58	18:16:21
Aug	Aug	18:15:11	Aug	49:00:15	29:33:04
Sept	Sept	20:30:22	Sept	54:15:10	19:54:54
Oct	Oct	19:26:47	Oct	52:27:22	15:40:18
Nov	Nov	15:04:47	Nov	104:36:29	14:36:31
Dec	Dec	16:51:49	Dec	91:43:24	15:32:47
	43:32:08	AVERAGE		59:08:16	AVERAGE
	17:00:53	MEDIAN		19:03:46	MEDIAN

The major TLD with significantly better performance than the others was .INFO, which had uptimes about half of the world average.



The .INFO registry operator, Afilias, has a multi-pronged anti-phishing approach that includes:

- An anti-abuse policy. The registry relies on the policy to suspend domain names obviously registered by phishers.
- Actively reporting phish to its registrars. This allows the registrars to alert their registrants about compromised domains.
- Occasional outreach to the hosting providers and ISPs of hacked phishing domains.



.CN operator CNNIC continues to do well compared to its peers in both phishing domain numbers and uptimes. The .CN registry's anti-phishing program appears to be providing better response to phishing attacks. Two other registries with fairly high volumes of phishing attacks are also seeing quicker mitigations: .FR (France) and .RU (Russia). However, as we discuss below in the section "Impact of Specialized Providers on Phishing Uptimes," a very small number of Internet providers that are responsible for the lion's share of phishing on those TLDs. Those providers respond quickly to complaints, and while they allow many phishing attacks to launch, they actually improve the uptime statistics for their TLDs.

The .INFO, .BIZ, and .CN results seem to show a clear correlation between lower phishing uptimes and proactive efforts by registry operators and the registrars they work with. In an environment where anti-spam and other security vendors use systems to automatically protect customers from abuse, TLD has become one of several metrics upon which to base the "reputation" of a domain name or URL. So for those service providers who are impacting their abuse statistics, there is a potential pay-off for having their TLDs treated favorably by such systems, and in the marketplace. This is especially important going into 2010, when ICANN plans to open a new round of TLD applications, which may add scores of new TLDs to the Internet. As applicants prepare their business plans and proposals for running new registries, there is compelling evidence that provisions for e-crime response and prevention will have a positive impact for everyone.

Use of Subdomains for Phishing

As we wrote about in our last report, phishers are increasingly using subdomain registration services to host phish. **Malicious use of these services continued to grow throughout the second half of 2008, and now accounts for the majority of phishing in some large TLDs. In the second half of 2008, subdomain services hosted 6,339 phish** – almost as many as the number of domains we verified were registered by phishers at regular domain name registrars (7,204). This is a disturbing trend, because phish on subdomain registration services can be effectively mitigated only by the subdomain providers themselves[1] – and some of these services are unresponsive to complaints.

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

Subdomain registration services include Web hosting companies that provide free subdomain space under their domains, dynamic IP allocation services that supplement their offerings with customizable subdomains, and companies that provide "affinity" subdomains (such as "myfavoriteteam.fan.org"). Some offer DNS services that allow users to redirect their domain names anywhere at any time.

We have identified more than 360 subdomain registration providers, which offer services on more than 2,300 domain names. This is a space as rich as the current "regulated" domain space, with as many business models and no real rules or oversight. It is not surprising to see criminals gravitating towards this space as registries and registrars in the gTLD and ccTLD spaces implement better anti-abuse policies and procedures. There are lessons to be learned here for potential new TLD operators, and challenges for future policy making.

Subdomain services are a popular way for phishers to mount attacks. In our survey we positively identified **6,339 subdomain sites/accounts used for phishing, beneath 480 unique second-level domains.** This is up significantly from the first half of the year, where we saw 4,512 subdomain sites/accounts used for phishing, beneath 274 unique second-level domains. There are likely even more within the data set, as it is often difficult to separate them out from other kinds of domains that have hacked hosts or were registered independently by phishers and set up with special subdomains. Even with that caveat, counting these unique subdomains as "regular" domain names, these types of domains would represent nearly 12% of all domains involved in phishing.

[1] Registrars or registry operators cannot mitigate these phish by suspending the main or "parent" domains – doing so would neutralize every subdomain hosted on the parent, thereby affecting many innocent users.

Top 20 Subdomain Services Used for Phishing 2H2008

Rank	Domain	Total	Provider
1	ns10-wistee.fr	321	wistee.fr
2	olympe-network.com	273	olympe-network.com
3	by.ru	272	by.ru
4	t35.com	267	t35.com
5	powa.fr	242	allo-heberge.com
6	nm.ru	221	pochta.ru
7	free.fr	204	free.fr
8	altervista.org	169	altervista.org
9	javabien.fr	147	javabien.fr
10	ns8-wistee.fr	146	wistee.fr
11	cfun.fr	139	Tripod
12	tripod.com	121	Tripod
13	freehostia.com	114	freehostia.com
14	pochta.ru	103	pochta.ru
15	9k.com	103	9k.com
16	bluechiphosting.com	99	bluechiphosting.com
17	siteburg.com	94	siteburg.com
18	110mb.com	92	110mb.com
19	land.ru	88	pochta.ru
20	vndv.com	80	zymic.com

The Russian freemail provider Pochta.ru continued to lead the industry with at least 12 domains that were used to host phishing in 2H2008, and those domains were used to mount at least 716 phishing attacks. The good news is that this was down from 1,446 attacks during 1H2008, and this provider continues to quickly mitigate phish when reported.

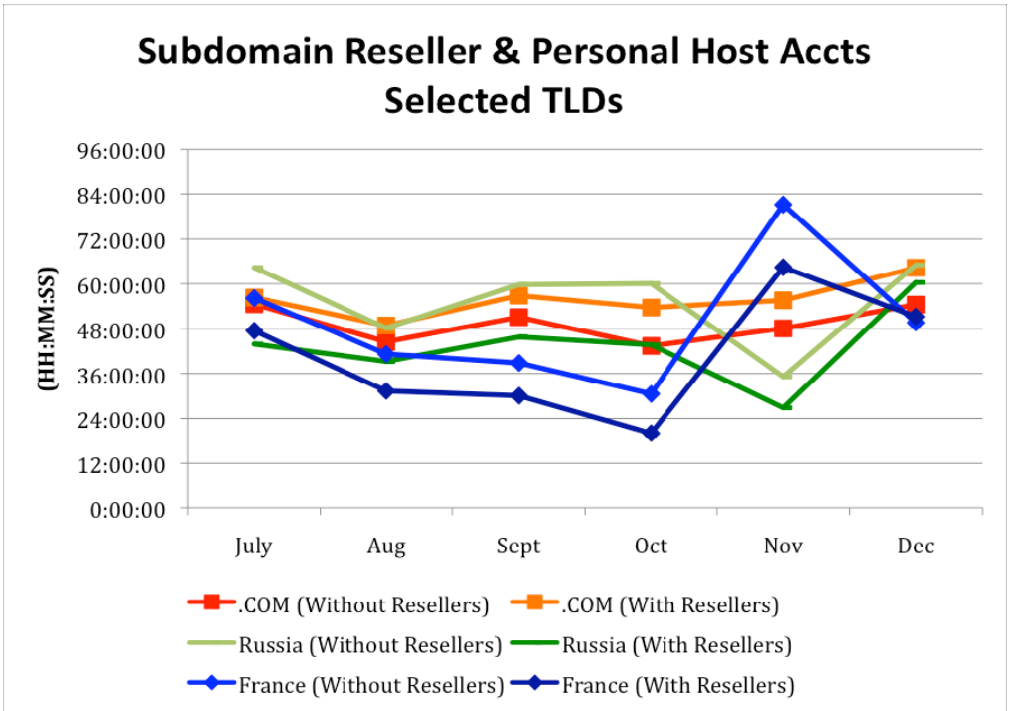
Second place belongs to the French hosting provider Wistee.fr, with three domains that hosted 468 phishing attacks during the second half of 2008. Mitigation was quick when Wistee.fr was notified, but some phishing sites lasted many days, indicating that this provider is not being notified by some affected phishing targets and brand owners.

For more information on subdomain resellers and the unique challenges they pose for phishing and abuse mitigation, please see the recent APWG paper "Making Waves in the Phisher' Safest Harbors: Exposing the Dark Side of Subdomain Registries."[1]

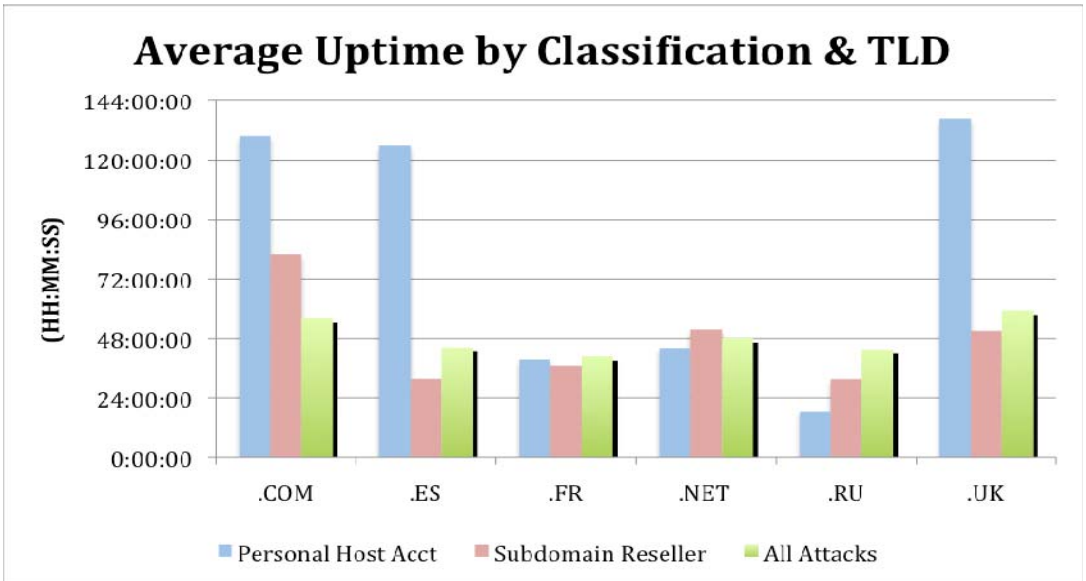
Impact of Specialized Providers on Phishing Uptimes

Because of the impact subdomain resellers and specific hosting providers can have on certain TLDs' scores and questions from some ccTLD operators about this issue, we have taken a deeper look at a few TLDs that saw a prevalence of "alternative" phishing attack activities in this period. This includes phishing on subdomain resellers and virtual private hosting companies that provide "personal Web hosting accounts" that were fraudulently purchased by phishers.

[1] http://apwg.com/reports/APWG_Advisory_on_Subdomain_Registries.pdf



This subcategory of attacks does seem to have a consistent impact over time and can affect a specific TLD's score. The impact can be either positive or negative, though, depending on the responsiveness of the providers, and a single provider can have a major impact upon an entire TLD. For comparison, we looked at .COM, as there are many such providers in that dominant TLD. The impact on .COM was significantly negative, with average uptimes nearly 7 hours longer with those attacks included in .COM's overall average. However, for .FR and .RU, the providers were actually significantly faster than their counterparts at removing phishing sites. So while they contributed large numbers of phishing sites to their respective TLDs, they improved the uptime scores for those TLDs.



Breaking out the individual attack types by TLD shows the opposing impacts the various providers can have on a TLD's score. Hosting companies in some TLDs are very quick to mitigate attacks, while others take many days in some cases. Subdomain resellers tend to do a better job, but can still have an impact in average uptime for a TLD.

Conclusions

This updated study shows that phishers are finding new opportunities, and are reacting to anti-phishing efforts. This study has documented some of their recent moves, including their continued abuse of subdomain services, their systematic exploitation of vulnerable registrars and registries, and how they are abandoning some tactics that are no longer as fruitful as they once were.

The statistics about domain registrations and site uptimes show correlations between the efforts of several large gTLD and ccTLD operators and the amount of time phishing sites remained live within their TLDs. The uptime results show that such efforts can lead to significant reduction in the amount of time phishing sites stay live, thus greatly reducing exposure to potential victims of these attacks. While registrars and registry operators have no control over the security of the Web sites hosted on the domains they sponsor, and have more limited options when vulnerable sites are compromised for phishing, they are in an excellent position to address malicious domain name registrations, which remain a damaging part of the current phishing problem. Registry operators can disseminate information to their registrars, and registrars and hosting providers can mitigate malicious domain name registrations quickly, thereby reducing all phishing up-times and reducing the options available to phishers.

We see some evidence that the "broken window" theory applies to online service providers. Sociologists created the "broken window" theory to explain why some neighborhoods thrive, while others decay. The theory posits that ignoring the little problems—graffiti, litter, shattered glass—creates a sense of decline that attracts bad elements and leads the law-abiding to stay away. On the Internet, we think that inattentive subdomain providers, registrars, and resellers are attracting bad actors into certain spaces.

We hope this study will spur further research on these and related topics and help the community create improved anti-phishing measures.

Appendix A: Phishing Statistics and Up-Times by TLD

TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008	Average Uptime 2H2008 (Hours)	# Malicious Phishing Domains 2H2008
ac	Ascension Island	3	2				51.8	1
ae	United Arab Emirates	10	7	87,000	**0.8**	**1.1**	46.5	
aero	sponsored TLD		0	6,008	**0.0**	**0.0**		
af	Afghanistan	4	2				27.8	1
ag	Antigua and Barbuda		0	15,638	**0.0**	**0.0**		
ai	Anguilla	5	1				16.4	
al	Albania	2	1				29.5	
am	Armenia	30	14	10,403	**13.5**	**28.8**	66.5	1
ar	Argentina	265	149	1,826,634	**0.8**	**1.5**	70.8	2
as	American Samoa	12	3				32.5	
asia	sponsored TLD	21	19	244,676	**0.8**	**0.9**	8.0	17
at	Austria	221	116	799,562	**1.5**	**2.8**	50.4	4
au	Australia	379	250	1,286,439	**1.9**	**2.9**	44.0	1
az	Azerbaijan	8	3	8,000	**3.8**	**10.0**	25.3	
ba	Bosnia and Herzegovina	24	10	8,463	**11.8**	**28.4**	56.2	
bd	Bangladesh	4	4				93.7	
be	Belgium	430	240	859,474	**2.8**	**5.0**	60.5	53
bf	Burkina Faso		0					
bg	Bulgaria	13	5	15,721	**3.2**	**8.3**	25.4	
bh	Bahrain	1	1				27.7	
biz	generic TLD	336	222	2,077,413	**1.1**	**1.6**	52.1	37
bm	Bermuda	4	2	5,152	**3.9**	**7.8**	15.5	
bo	Bolivia	21	7	4,623	**15.1**	**45.4**	55.0	
br	Brazil	452	273	1,535,117	**1.8**	**2.9**	49.4	1
bs	Bahamas	5	1	1,870	**5.3**	**26.7**	63.1	
bt	Bhutan	1	1				119.9	
by	Belarus	10	8				53.2	
bz	Belize	69	55	43,377	**12.7**	**15.9**	20.9	44

TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008	Average Uptime 2H2008 (Hours)	# Malicious Phishing Domains 2H2008
ca	Canada	334	212	1,136,411	**1.9**	**2.9**	52.2	6
cat	sponsored TLD	15	7	33,397	**2.1**	**4.5**	52.6	
cc	Cocos (Keeling) Islands	200	71	registry declined to provide			49.0	36
cd	Congo, Democratic Repub.	1	1				26.1	
ch	Switzerland	198	110	1,244,567	**0.9**	**1.6**	87.9	4
ci	Côte d'Ivoire	2	2				6.6	
cl	Chile	211	116	232,897	**5.0**	**9.1**	70.2	
cn	China	667	499	13,572,326	**0.4**	**0.5**	34.3	367
co	Colombia	83	44	24,867	**17.7**	**33.4**	62.8	
com	generic TLD	24,162	14,431	80,450,204	**1.8**	**3.0**	56.2	2,187
coop	sponsored TLD	9	5	5,921	**8.4**	**15.2**	27.2	
cr	Costa Rica	1	1	11,988	**0.8**	**0.8**	42.3	
cx	Christmas Island	34	5	4,800	**10.4**	**70.8**	14.3	
cy	Cyprus	5	2	6,341	**3.2**	**7.9**	21.2	
cz	Czech Republic	159	111	506,258	**2.2**	**3.1**	99.2	33
de	Germany	1,207	834	12,402,383	**0.7**	**1.0**	53.1	1
dj	Djibouti		0					
dk	Denmark	218	107	965,816	**1.1**	**2.3**	46.3	
dm	Dominica		0					
do	Dominican Republic	3	1	10,048	**1.0**	**3.0**	63.5	
dz	Algeria	2	1				1.5	
ec	Ecuador	48	17	179,500	**0.9**	**2.7**	51.6	5
edu	U.S. higher education	48	30	7,000	**42.9**	**68.6**	23.9	
ee	Estonia	42	19	63,100	**3.0**	**6.7**	30.2	
eg	Egypt	4	3	3,839	**7.8**	**10.4**	42.4	
es	Spain	586	253	1,082,757	**2.3**	**5.4**	44.4	126
eu	European Union	315	234	2,988,269	**0.8**	**1.1**	53.9	35

TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008	Average Uptime 2H2008 (Hours)	# Malicious Phishing Domains 2H2008
fi	Finland	43	31	198,000	**1.6**	**2.2**	66.9	
fk	Falkland Islands		0					
fm	Micronesia, Fed. States	6	4				9.4	
fr	France	2,320	430	1,289,559	**3.3**	**18.0**	40.6	21
gd	Grenada	15	4	1,600	**25.0**	**93.8**	43.2	
ge	Georgia	10	8	12,376	**6.5**	**8.1**	111.6	
gg	Guernsey		0					
gh	Ghana	3	1				23.9	
gi	Gibraltar		0	1,729	**0.0**	**0.0**		
gov	U.S. government	4	3	registry declined to provide			7.9	
gp	Guadeloupe			1,050	**0.0**	**0.0**		
gr	Greece	128	71	250,000	**2.8**	**5.1**	37.0	1
gs	South Georgia & Sandwich Is.	27	18				24.2	16
gt	Guatemala	3	2	6,695	**3.0**	**4.5**	0.9	
hk	Hong Kong	65	38	173,651	**2.2**	**3.7**	35.9	6
hm	Heard and McDonald Is.	10	1				23.6	
hn	Honduras	4	2	3,934	**5.1**	**10.2**	34.0	
hr	Croatia	27	17	59,901	**2.8**	**4.5**	68.2	
ht	Haiti		0	1,100	**0.0**	**0.0**		
hu	Hungary	106	69	400,000	**1.7**	**2.7**	111.3	
id	Indonesia	64	38				67.8	
ie	Ireland	42	23	115,836	**2.0**	**3.6**	109.7	
il	Israel	78	38	139,243	**2.7**	**5.6**	43.3	
im	Isle of Man	1	1	14,000	**0.7**	**0.7**	3.1	
in	India	174	105	501,155	**2.1**	**3.5**	44.9	38
info	generic TLD	649	508	5,138,132	**1.0**	**1.3**	28.4	82
io	British Indian Ocean Terr.	4	3				57.3	
IP address	IP address / no domain name		2,809 unique IPs	n/a				

TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008	Average Uptime 2H2008 (Hours)	# Malicious Phishing Domains 2H2008
ir	Iran	38	29	102,800	**2.8**	**3.7**	107.9	
is	Iceland	13	12	23,500	**5.1**	**5.5**	60.5	
it	Italy	452	214	1,622,938	**1.3**	**2.8**	57.7	
je	Jersey	1	1				133.8	
jo	Jordan	3	1	2,582	**3.9**	**11.6**	40.1	
jobs	sponsored TLD		0	15,072	**0.0**	**0.0**		
jp	Japan	408	242	1,062,731	**2.3**	**3.8**	47.4	16
ke	Kenya	11	4	9,909	**4.0**	**11.1**	33.6	
kg	Kyrgyzstan	37	18	3,080	**58.4**	**120.1**	75.6	17
kh	Cambodia		0					
ki	Kiribati		0	4,350	**0.0**	**0.0**		
kr	Korea	1,104	413	983,626	**4.2**	**11.2**	55.2	1
ky	Cayman Islands		0	5,773	**0.0**	**0.0**		
kw	Kuwait	3	1				30.4	
kz	Kazakhstan	18	10	30,019	**3.3**	**6.0**	45.9	
la	Lao People's Demo. Rep.	19	5				15.9	1
lb	Lebanon	2	1	2,700	**3.7**	**7.4**	34.4	
lc	St. Lucia		0	1,982	**0.0**	**0.0**		
li	Liechtenstein	13	9	60,082	**1.5**	**2.2**	19.3	3
lk	Sri Lanka	3	1	5,897	**1.7**	**5.1**	49.9	
lt	Lithuania	40	25	94,000	**2.7**	**4.3**	19.5	
lu	Luxembourg	4	3	42,001	**0.7**	**1.0**	27.1	
lv	Latvia	21	13	49,000	**2.7**	**4.3**	256.6	
ly	Libya	21	3	4,196	**7.1**	**50.0**	14.0	
ma	Morocco	16	11	28,101	**3.9**	**5.7**	74.9	1
md	Moldova	7	6				38.6	1
me	Montenegro	34	24	183,232	**1.3**	**1.9**	15.7	14
mk	Macedonia	1	1	11,027	**0.9**	**0.9**	4.5	
ml	Mali	1	1				522.1	
mn	Mongolia	14	7	7,257	**9.6**	**19.3**	38.4	1
mo	Macao	1	1	2,529	**4.0**	**4.0**	7.6	
mobi	sponsored TLD	54	43	876,151	**0.5**	**0.6**	15.1	36
mr	Mauritania	1	1				7.7	
ms	Montserrat	3	3	11,000	**2.7**	**2.7**	4.5	1

TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008	Average Uptime 2H2008 (Hours)	# Malicious Phishing Domains 2H2008
mu	Mauritius	1	1				5.4	
museum	sponsored TLD		0	545	**0.0**	**0.0**		
mx	Mexico	140	80	277,652	**2.9**	**5.0**	51.6	
my	Malaysia	49	25	80,786	**3.1**	**6.1**	113.8	
mz	Mozambique	2	2				169.0	
name	generic TLD	101	72	288,306	**2.5**	**3.5**	19.9	51
net	generic TLD	4,068	2,292	12,286,364	**1.9**	**3.3**	48.2	161
nf	Norfolk Island	2	2	6,238	**3.2**	**3.2**	21.8	
ng	Nigeria	3	1	1,170	**8.5**	**25.6**	232.0	
ni	Nicaragua	3	1	4,750	**2.1**	**6.3**	18.5	
nl	Netherlands	461	338	3,191,127	**1.1**	**1.4**	66.4	2
no	Norway	78	50	412,839	**1.2**	**1.9**	42.3	
np	Nepal	9	8	11,039	**7.2**	**8.2**	28.3	
nr	Nauru	8	5				51.7	3
nu	Niue	56	24				28.3	
nz	New Zealand	71	37	348,769	**1.1**	**2.0**	44.0	
org	generic TLD	2,589	1,568	7,364,670	**2.1**	**3.5**	49.5	117
pa	Panama	2	2				106.8	
pe	Peru	31	15	29,516	**5.1**	**10.5**	42.1	
ph	Philippines	64	32	registry declined to provide			32.6	5
pk	Pakistan	25	19				70.1	8
pl	Poland	551	303	1,350,138	**2.2**	**4.1**	54.0	5
pro	sponsored TLD	1	1	29,917	**0.3**	**0.3**	628.1	
ps	Palestinian Territory	4	3	4,278	**7.0**	**9.4**	11.6	
pt	Portugal	53	34	275,972	**1.2**	**1.9**	33.6	
py	Paraguay	6	5	8,384	**6.0**	**7.2**	87.7	
ro	Romania	289	188	310,114	**6.1**	**9.3**	77.2	1
rs	Serbia	2	2	44,500	**0.4**	**0.4**	29.2	
ru	Russian Fed.	2,150	676	1,860,179	**3.6**	**11.6**	43.5	34

TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008	Average Uptime 2H2008 (Hours)	# Malicious Phishing Domains 2H2008
sa	Saudi Arabia	6	5	14,983	**3.3**	**4.0**	15.3	
sc	Seychelles	1	1	7,067	**1.4**	**1.4**	14.1	
se	Sweden	116	71	834,886	**0.9**	**1.4**	68.0	
sg	Singapore	38	31	114,549	**2.7**	**3.3**	57.3	
sh	Saint Helena	1	1				10.3	
si	Slovenia	12	8	63,265	**1.3**	**1.9**	44.9	
sk	Slovakia	87	31	172,500	**1.8**	**5.0**	48.5	1
sl	Sierra Leone	1	1				0.4	1
sm	San Marino	1	1	1,900	**5.3**	**5.3**	19.5	
st	Sao Tome and Principe	9	7	5,600	**12.5**	**16.1**	57.5	
su	Soviet Union	271	76	85,119	**8.9**	**31.8**	42.1	55
sv	El Salvador	5	3	4,051	**7.4**	**12.3**	13.6	
sy	Syria	1	1				56.7	
tc	Turks and Caicos	24	15	9,882	**15.2**	**24.3**	38.8	
tf	French Southern Territories	3	3	1,557	**19.3**	**19.3**	14.1	
th	Thailand	170	88	39,880	**22.1**	**42.6**	47.7	
tj	Tajikistan		0	4,681	**0.0**	**0.0**		
tk	Tokelau	204	132	1,880,000	**0.7**	**1.1**	29.7	107
tl	Timor-Leste	12	4				146.6	
tm	Turkmenistan	2	2				2.4	
tn	Tunisia		0					
to	Tonga	36	14	13,200	**10.6**	**27.3**	15.3	
tp	Portuguese Timor	2	2				214.3	
tr	Turkey	49	33	180,065	**1.8**	**2.7**	31.9	
travel	sponsored TLD	1	1	214,719	**0.0**	**0.0**	35.7	
tt	Trinidad and Tobago	6	3	2,202	**13.6**	**27.2**	242.7	
tv	Tuvalu	109	71	registry declined to provide			56.0	21
tw	Taiwan	226	144	406,669	**3.5**	**5.6**	69.2	8
tz	Tanzania		0					

TLD	TLD Location	# Unique Phishing attacks 2H2008	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008	Score: Attacks per 10,000 domains 2H2008	Average Uptime 2H2008 (Hours)	# Malicious Phishing Domains 2H2008
ua	Ukraine	198	107	397,051	**2.7**	**5.0**	54.2	2
ug	Uganda	4	3				31.0	
uk	United Kingdom	1,632	886	7,310,000	**1.2**	**2.2**	59.1	236
us	United States	304	216	1,434,301	**1.5**	**2.1**	49.6	44
uy	Uruguay	8	7	18,115	**3.9**	**4.4**	11.5	
uz	Uzbekistan	9	4	7,575	**5.3**	**11.9**	128.7	
vc	St. Vincent and Grenadines	1	1	6,283	**1.6**	**1.6**	39.9	
ve	Venezuela	1,627	1,504	82,500	**182.3**	**197.2**	7.3	1,490
vg	British Virgin Islands	7	7	9,173	**7.6**	**7.6**	12.6	1
vi	Virgin Islands	2	2				62.6	
vn	Vietnam	62	37	92,992	**4.0**	**6.7**	44.6	1
vu	Vanuatu	2	1				6.9	1
ws	Samoa	63	40	544,000	**0.7**	**1.2**	24.1	18
yu	Yugoslavia	15	8	TLD being deprecated			28.9	
za	South Africa	90	66	437,000	**1.5**	**2.1**	30.6	1
zm	Zambia		0					
zw	Zimbabwe		0	8,345	**0.0**	**0.0**		
	GRAND TOTALS	**56,959**	**30,454**	**179,913,118**				**5,591**

About the Authors & Acknowledgments

Greg Aaron is Director of Key Account Management and Domain Security at Afilias (www.afilias.info). Afilias operates the .INFO top-level domain (TLD) and provides technical and advising services for thirteen other TLDs, including .ORG, .MOBI, .ASIA, .ME, and .IN (India). Greg oversees .INFO operations and Afilias' security programs, including domain name abuse policy and practices. He is also an expert on domain name intellectual property issues and Internationalized Domain Names (IDNs). He is the Chair of ICANN's Registration Abuse Working group (RAPWG), serves on the steering committee of the Anti-Phishing Working Group (APWG), and has advised the Government of India regarding domain and related Internet policies. He previously worked at Internet companies such as Travelocity, and graduated magna cum laude from the University of Pennsylvania.

Rod Rasmussen is President and CTO of Internet Identity (www.internetidentity.com), and has served as its technical leader since he co-founded the company in 2001. He is widely recognized as a leading expert on the abuse of the domain name system by phishing criminals. Rasmussen is co-chair of the Anti-Phishing Working Group's (APWG) Internet Policy Committee (IPC), and serves as the APWG's Industry Liaison to various groups around the world, including ICANN, the international oversight body for domain names. He serves on ICANN's Fast-Flux Working Group. He is also a member of the Steering Committee for the Authentication and Online Trust Alliance (AOTA), and an active member of the Digital PhishNet, a collaboration between industry and law enforcement. Prior to starting Internet Identity, Rasmussen held product management roles for LanQuest, a network equipment testing company, and networking product manufacturer Global Village. Rasmussen earned an MBA from the Haas School of Business at the University of California, Berkeley and holds two bachelor's degrees, in Economics and Computer Science, from the University of Rochester.

The authors wish to thank the following for their support: Peter Cassidy, Foy Shiver, and Laura Mather of the APWG; Ram Mohan and Bruce Reeser of Afilias, and Aaron Routt of Internet Identity. 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.

#