Global Phishing Survey: Trends and Domain Name Use in 1H2009

An APWG Industry Advisory

APWG

Committed to Wiping Out Internet Scams and Fraud

October 2009

Authors:

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

Greg Aaron
Afilias
<gaaron at afilias.info>

Table of Contents

Overview

The battle against phishing is a seesaw contest. On one side are the phishers, looking for better ways to steal money and Internet users' personal data. On the other side is an array of security and software providers, financial institutions, and other like-minded parties who fight back with counter-measures of their own. While phishing remains a dangerous criminal activity involving great losses of money and personal data, the latest statistics also show that phishing has not increased by some measures, and that some anti-phishing measures have had a beneficial impact.

This report attempts to understand the scope of the global phishing problem, especially by examining domain name usage and phishing site uptimes. Specifically, this new report examines all the phishing attacks detected in the first half of 2009 (1H2009) -- between January 1, 2009 and June 30, 2009. The data was 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.[1] Our data confirms new and ongoing trends, and we hope that bringing them to light will lead to improved anti-phishing measures.

Our major findings include:

1. **In 1H2009, the average uptime of all phishing attacks was noticeably shorter than in 2H2008.** This is an encouraging improvement, most likely reflecting efforts by providers and responders.
2. **The Avalanche phishing kit accounted for a whopping 24% of all phishing attacks launched in 1H2009.** This criminal operation is one of the most sophisticated and damaging on the Internet, and targets vulnerable or non-responsive registrars and registries.
3. **The great majority of phishing is also concentrated in certain namespaces -- just five TLDs**.
4. **The amount of Internet domain names and numbers used for phishing has remained fairly steady** over the past two years.
5. **Anti-phishing programs implemented by domain name registries can reduce the up-times of phishing attacks, and can reduce the number of malicious registrations made in those TLDs.**
6. **The unique characteristics of Internationalized Domain Names (IDNs) are not being used to facilitate phishing**, and there are factors that may perpetuate this trend in the future.
7. **Phishers continue to use subdomain services to host and manage their phishing sites.** Phishers used such services more often than they registered domain names via regular registrars. This trend shows phishers using services that cannot be taken down by domain registrars or registry operators.

[1] This new report is a follow-up to our earlier studies of data stretching back to January 2007. The previous studies are available at:
2H2008: http://www.apwg.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf
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 1H2009, but the number of unique phishing attacks and domain names used to host them is much smaller.[1] The 1H2009 data set yields the following statistics:

- There were at least **55,698 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 down insignificantly from the 56,959 attacks recorded in 2H2008.
- Those attacks occurred on **30,131 unique domain names**.[2] This is barely down from the 30,454 observed in 2H2008.
- Of the 30,454 phishing domains, **we identified 4,382 that we believe were registered by phishers. These "malicious" domain registrations represented about 14.5% of the domain names involved in phishing,** down from 18.5% in 2H2008. Virtually all the rest were hacked or "compromised" domains belonging to innocent site owners.
- Phishing took place on domain names in **171 TLDs**. However, malicious registrations apparently took place in just 57 TLDs. 86% of the 4,382 malicious domain registrations were made in just 5 TLDs.
- Only about **3.6% of all domain names that were used for phishing contained a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations" below.)
- In addition, phish were detected on **3,563 unique IP addresses**, rather than on domain names. (For example: http://96.56.84.42/ClientHelp/ssl/index.htm.) This is up from the 2,809 seen in 2H2008, and the 3,389 seen in 1H2008. 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-and-one-half years.**
- The unique characteristics of internationalized domain names (IDNs) are not being used to facilitate phishing, and there are factors that may perpetuate this trend in the future. Only 13 of the 30,131 domain names we studied were IDNs. See "Use of Internationalized Domain Names" below for more details.

---

[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. For an example of an apparently different tallying method, see page 4 at: http://apwg.org/reports/apwg_report_h1_2009.pdf

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.

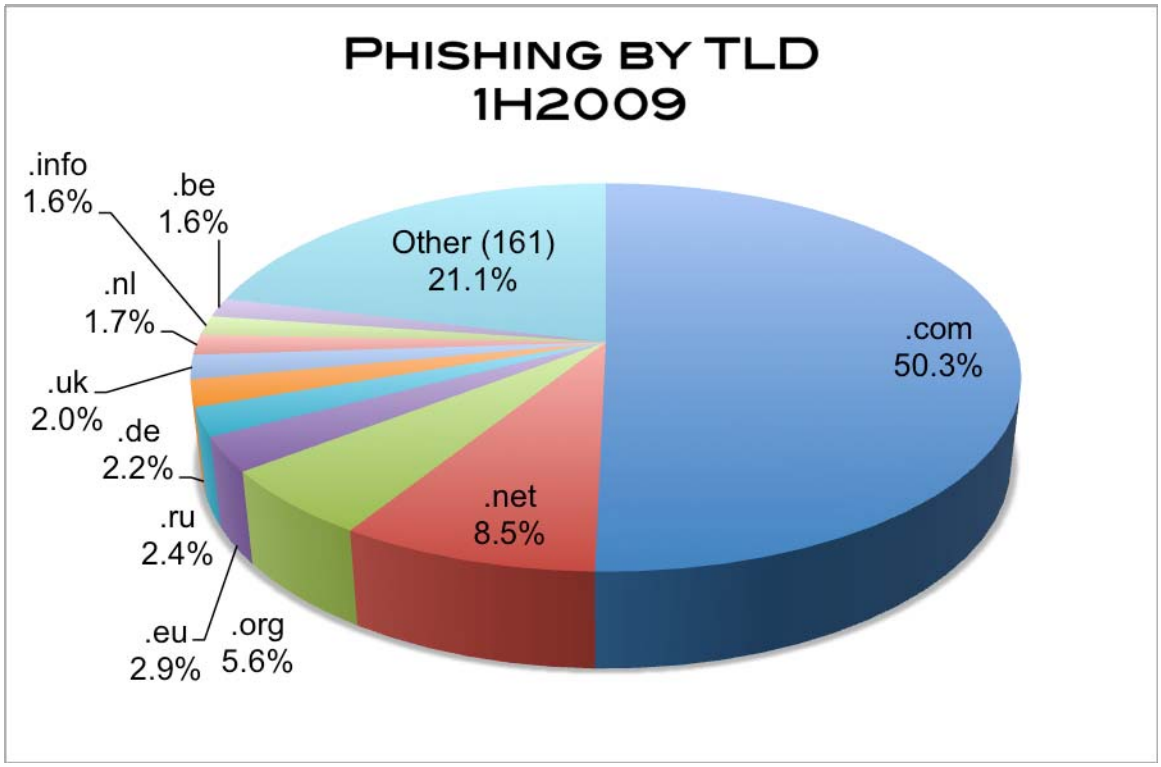
Basic Statistics:

	1H2009	2H2008	1H2008	2H2007
Phishing domain names	30,131	30,454	26,678	28,818
IP-based phish (unique IPs)	3,563	2,809	3,389	5,217
TLDs in phish URLs	171	170	155	145
Attacks	>55,698	>56,969	>47,342	
Maliciously registered domains	4,382	5,591		
IDN domains	13	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 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. 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 30,131 phishing domains to see how many fell into which TLDs. The complete tables are presented in the Appendix.



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"[1] 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.

In 1H2009, phishing occurred on domain names in 171 TLDs. Of those registries, we were able to obtain the domain count statistics for 136. Those 136 TLDs contained 99% of the phishing domains in our data set (29,884 out of the 30,131), and a total of 184,233,568 domain names overall. [2]

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

- **The median score was 2.9**, up slightly from 2.7 in 2H2008 and 2.3 in 1H2008.
- **The average score was 6.9**, 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 50% of the phishing domains in our data set, and 45% of the domains in the TLDs for which we have domains-in-registry statistics.

[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 the end of March 2009. Sources: ICANN.org (monthly registry reports), ccTLD registry operators.

We therefore suggest that scores between .COM's 1.8 and the median of 2.9 occupy the middle ground, with scores above 2.9 indicating TLDs with increasingly prevalent phishing.

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.

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.

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 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009
1	pe	Peru	64	32,000	**20.0**
2	th	Thailand	68	42,594	**16.0**
3	bz	Belize	29	43,113	**6.7**
4	be	Belgium	484	892,267	**5.4**
5	ro	Romania	163	310,900	**5.2**
6	tw	Taiwan	194	425,551	**4.6**
7	kr	Korea	399	999,262	**4.0**
7	cl	Chile	97	243,701	**4.0**
9	ie	Ireland	48	122,374	**3.9**
10	my	Malaysia	31	80,949	**3.8**
11	su	Soviet Union	30	83,739	**3.6**
11	vn	Vietnam	36	100,979	**3.6**
13	ru	Russian Fed.	710	2,016,396	**3.5**
14	il	Israel	48	145,151	**3.3**
15	mx	Mexico	93	290,101	**3.2**

The "generic" TLDs (gTLDs) are open to registrants across the world without registration qualifications, while "sponsored" TLDs (sTLDs) have eligibility requirements:

Phishing in gTLDs and sTLDs by Score

Minimum 30,000 domain names in registry

Rank	TLD	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009
1	org	2,554	1,691	7,549,754	**2.2**
2	net	5,423	2,570	12,525,459	**2.1**
3	name	134	53	278,516	**1.9**
4	com	25,994	15,170	82,229,830	**1.8**
5	biz	395	225	2,075,159	**1.1**
6	mobi	206	87	847,332	**1.0**
7	info	600	493	5,390,206	**0.9**
8	asia	2	2	248,407	**0.1**
9	pro	1	1	35,694	**0.3**
10	travel	0	0	133,051	**0.0**
11	tel	0	0	129,562	**0.0**

If measured by Attack Score, certain TLDs vault into 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 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009
1	th	Thailand	128	68	42,594	**16.0**	**30.1**
2	pe	Peru	86	64	32,000	**20.0**	**26.9**
3	be	Belgium	1,813	484	892,267	**5.4**	**20.3**
4	bz	Belize	81	29	43,113	**6.7**	**18.8**
5	li	Liechtenstein	93	18	59,244	**3.0**	**15.7**
6	su	Soviet Union	125	30	83,739	**3.6**	**14.9**
7	eu	European Union	3,869	864	3,043,070	**2.8**	**12.7**
8	ru	Russian Fed.	1,982	710	2,016,396	**3.5**	**9.8**
9	ro	Romania	278	163	310,900	**5.2**	**8.9**
9	fr	France	1,214	340	1,367,333	**2.5**	**8.9**
11	kr	Korea	751	399	999,262	**4.0**	**7.5**
12	mx	Mexico	213	93	290,101	**3.2**	**7.3**
13	sk	Slovakia	132	46	184,943	**2.5**	**7.1**
14	tw	Taiwan	290	194	425,551	**4.6**	**6.8**
15	cl	Chile	144	97	243,701	**4.0**	**5.9**

.FR and .RU continue to receive 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.

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

- .EU and .BE: The "Avalanche" phishing gang registered large numbers of .EU and .BE domains, and this is reflected in those TLDs' elevated Attack Scores. Avalanche began attacks in December 2008 and ramped up significantly in early 2009, quickly becoming the most prolific and dangerous phishing operation on the Internet. This group uses infrastructure and methods very similar to the previous "Rock" gang, and added fast-flux hosting to sustain its attacks.

- .TH (Thailand): Phishing here takes place entirely on compromised Web sites in the AC.TH (academic) zone and the GO.TH (government) zone, and has been occurring regularly for two years. Although the number of attacks decreased from 2H2008 through 1H2009, phishers continued to have access into unsecure institutional servers in Thailand.

- .SU (Soviet Union) and .RU (Russia). .SU and .RU remain high in the rankings due to phishing at subdomain resellers (see more below). Only one malicious phishing registration was made in .SU in 1H2009, a notable reduction from the 55 made in 2H2008. .SU is notable because it was to have been phased out years ago, after the dissolution of the Soviet Union. However it has not been removed from the DNS root, and the registry operator has built new registrations.

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 (this is an indicator that the web server was not compromised), 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. There are some domains above and beyond the 4,382 we were not highly confident about classifying as malicious, and so we left them out of the count.

Of the 30,131 phishing domains, **we identified 4,382 that we believe were registered by phishers. These "malicious" or "evil" domains represent about 14.5% of the domain names involved in phishing. This is down from 5,591 domains (18.5%) in 2H2009. A staggering 43% of these maliciously registered domains (2,309) were Avalanche attack domains,** which we examine in more detail below.

86% of the 4,382 malicious domain registrations were made in just 5 TLDs -- .COM, .EU, .NET, .BE, and .ORG. (See the Appendix for breakdowns.) **By this measure, phishing is highly concentrated in just a few namespaces.**

Malicious Phishing Registrations by Volume

Minimum 30,000 domain names in registry

Rank	TLD	Malicious Domain Names used for phishing 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Malicious Domains per 10,000 domains 1H2009
1	be	293	484	892,267	**3.28**
2	eu	662	864	3,043,070	**2.18**
3	net	438	2,570	12,525,459	**0.35**
4	org	207	1,691	7,549,754	**0.27**
5	com	2,180	15,170	82,229,830	**0.27**

The remaining 85.5% 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.[1] Less than 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, 1,098 contained a relevant brand name, variation, or misspelling thereof.[2] This represents 25% of maliciously registered domains, and just 3.6% 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 h1jh1.eu, which offered nothing to confuse a potential victim.

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. As we have observed in the past, **the domain name itself usually does not matter to phishers, and a hacked domain name of any meaning, in any TLD, will usually 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.

TLDs that were heavily abused by malicious registrations in the past—such as .HK and .VE—had notably high phishing scores in our previous surveys. Those registries implemented better programs to prevent and respond to such attacks, and enjoy much better scores now. In fact, .HK and .VE each had only one malicious registration in 1H2009. CNNIC's

[1] A separate APWG report covering 1H2009 found that depending on the month, one-third to two-thirds of phishing URLs contain some form of target name: http://apwg.org/reports/apwg_report_h1_2009.pdf

[2] Examples of domain names we counted as containing brand names included: urvh-payspall.com, abbey-reademail.com, facebook-bonus-chips.tk, mailb0x-regi0ns.com, wellsfargo-online.us, mynetvisa.com.

anti-phishing program[1] bore results in 1H2009 also. Malicious registrations in .CN plummeted from 499 in 2H2008 to 115 in 1H2009.

Avalanche Attacks

Avalanche sites are the latest in mass-production phishing and malware distribution techniques. Phishing sites on Avalanche domains target the commercial banking platforms of more than 30 financial institutions, major on-line services, and job search providers. Social-engineered malware downloads are also being distributed from these same domains. These attacks involve domain names registered by the phishers, set up on name servers controlled by the phishers, and hosted on a fast-flux network of apparently comprimised consumer-level machines. This fast-flux hosting makes mitigation efforts more difficult -- calling the Internet Service Provider to get a site or IP blocked is not effective, and the domain name itself must be suspended at the registrar or registry level.

The Avalanche phishing kit accounted for a whopping 24% (13,334) of all phishing attacks seen during 1H 2009. However, **since each domain is used to mount up to 30 attacks, this only represents about 8% of all domains used for phishing.** These large numbers of similar attacks can have a dramatic affect on phishing uptime – both overall (nearly a quarter of all phish) and for any targeted TLD (below).

An Avalanche attack campaign consists of many domain names that appear almost identical to each other (such as 11fjfhi.com, 11fjfhj.com, 11fjfh1.com, and 11fjfhl.com). These domain name groupings are therefore distinctive and recognizable to those who are looking for them. While only one or two brands are typically spammed at any one time during an Avalanche attack, the miscreants rotate back to older targets frequently. If an Avalanche domain remains active over a long period of time, spam for other targets may be sent using it.

When setting up an attack, the Avalanche registers domains at one to three registrars or resellers. They also target a small number of other registrars, testing to see if the registrar notices the registrations. If one registrar starts to quickly suspend the domains or implements other security procedures, Avalanche simply moves on to other vulnerable registrars. The phishers also employ additional tricks. For one batch of domain registrations, they chose a registrar located in a small country, and used credit card number stolen from consumers in that country in an attempt to avoid notice.

Avalanche does the same with top-level domains, registering in TLDs where the registry operator may not be an active or effective participant in mitigation efforts.

Avalanche attacks increased significantly into the third quarter of the year, and preliminary numbers indicate a possible doubling of attacks in the summer of 2009. Our next report will examine the data in detail.

For more about Avalanche and the efficacy of its attacks, continue to "Phishing by Uptime," below.

[1] In July 2008, an alliance of Chinese online commerce stakeholders, including CNNIC and several Chinese banks, founded the Anti-Phishing Alliance of China (APAC) in order to tackle phishing that abuses .CN sub-domain names, with CNNIC functioning as the secretariat of APAC.

Phishing By Uptime

In 1H2009, the average uptime of phishing attacks was noticeably shorter than in 2H2008. This is a significant event. 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. [1]

Phishers therefore strive for maximum uptime, and make choices accordingly. Phishers prefer vulnerable or inattentive registrars and registries, and the most sophisticated phishers use fast-flux hosting in an attempt to extend uptimes. (Phish hosted on fast-flux networks often stay up about 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.

In 1H2009, Internet Identity monitored the "uptimes" or "live" times of the phishing attacks in the data set.[2] **For the 55,698 attacks in 1H2009, the average uptime was 39 hours, with a median of 13 hours and 15 minutes. The average was down significantly from 2H2008's average of 52 hours, and the median dropped also, from 14 hours and 43 minutes in 2H2008.**

The major difference was the Avalanche attacks, which tended to attract a great deal of attention. Putting the Avalanche attacks aside, there was still a modest improvement over 2H2008. Without Avalanche attacks counted, 1H2009's average uptime was 45 hours and 36 minutes, and the median was 14 hours and 3 minutes. This is an encouraging improvement.

---

[1] 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, and drops off thereafter. Note that these may be 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.

[2] 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.

The uptimes for all phishing attacks in 1H2009, and for phish in large TLDs, were as follows:

Uptimes by TLD (HH:MM:SS)

ALL PHISH	Average	Median
Jan	41:57:27	12:51:49
Feb	38:17:27	13:49:33
Mar	36:00:14	13:25:08
Apr	40:42:42	11:35:26
May	37:50:11	13:31:39
June	40:01:22	12:08:19
1H2009	39:11:03	13:15:32

AVALANCHE	Average	Median
Jan	13:30:02	12:02:55
Feb	15:23:51	12:26:21
Mar	31:10:42	15:15:30
Apr	20:54:11	12:57:43
May	39:32:07	12:41:00
June	12:03:03	8:49:22
1H2009	18:45:44	12:23:43

Our theory is that malicious registrations are attracting more mitigation efforts for the following reasons:

a) Responders are highly aware of them—especially the Avalanche domains. And,

b) These domains are often registered using stolen credit cards. Registrars usually cancel fraudulently registered domains quickly. In most TLDs, a domain cancelled within 5 days of registration immediately exits the zone and stops resolving.

The average uptimes of Avalanche attacks were significantly lower than the norm, and the median was slightly lower than the norm, too:

Avalanche domains are hosted on fast-flux networks, which are designed to extend the uptimes of phish by making mitigation more difficult. But the uptimes numbers suggest that responders may be neutralizing the efficacy of Avalanche's fast-flux hosting.

In any case, the numbers show how Avalanche activity is a dominant factor, and how the *type* of phishing is a factor to be considered when examining uptimes.

.COM	Average	Median
Jan	55:30:32	12:44:47
Feb	48:33:56	13:11:22
Mar	36:23:57	13:42:49
Apr	46:22:38	11:49:19
May	39:32:07	12:41:00
June	42:27:14	13:01:30
1H2009	44:09:56	12:57:01

.NET	Average	Median
Jan	28:38:27	10:29:01
Feb	42:06:52	15:39:22
Mar	32:42:03	10:37:42
Apr	39:25:33	9:45:48
May	29:47:41	11:04:38
June	23:06:50	12:26:32
1H2009	29:45:58	11:25:24

.ORG	Average	Median
Jan	37:11:21	13:30:06
Feb	24:32:43	13:07:59
Mar	20:50:39	8:20:41
Apr	22:13:11	4:15:53
May	22:10:39	6:45:57
June	42:33:44	15:57:10
1H2009	27:54:08	8:55:25

.BIZ	Average	Median
Jan	20:46:51	5:34:57
Feb	35:35:54	13:55:20
Mar	27:32:42	9:39:49
Apr	30:14:59	14:24:42
May	36:34:38	12:13:32
June	31:34:13	14:12:20
1H2009	29:17:03	10:16:41

.INFO	Average	Median
Jan	21:10:44	11:34:41
Feb	22:58:58	11:29:37
Mar	25:00:35	7:10:07
Apr	33:20:24	11:34:28
May	28:06:36	28:06:36
June	20:53:40	13:02:51
1H2009	25:10:24	11:23:52

.UK	Average	Median
Jan	33:11:28	14:06:06
Feb	40:07:42	15:37:05
Mar	45:55:12	9:55:30
Apr	53:02:30	7:54:31
May	50:18:40	18:29:57
June	53:42:20	21:07:56
1H2009	45:23:09	14:10:28

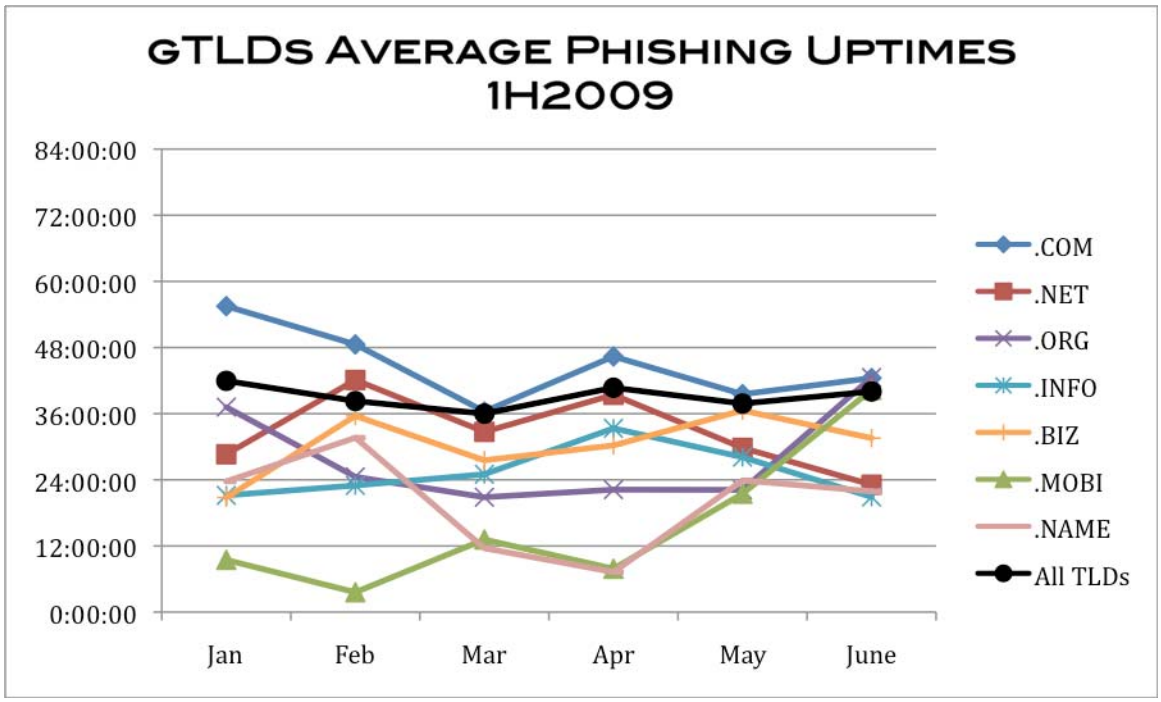
.EU	Average	Median
Jan	17:07:20	12:42:52
Feb	16:20:22	13:27:50
Mar	37:36:14	13:19:43
Apr	18:51:01	11:36:37
May	29:15:30	12:57:05
June	35:40:11	13:14:45
1H2009	23:31:14	13:16:01

.BE	Average	Median
Jan	12:48:28	11:22:38
Feb	22:51:20	15:03:58
Mar	16:50:58	12:26:13
Apr	18:54:20	11:44:09
May	42:10:47	24:33:11
June	24:08:57	11:45:10
1H2009	16:51:28	12:06:43

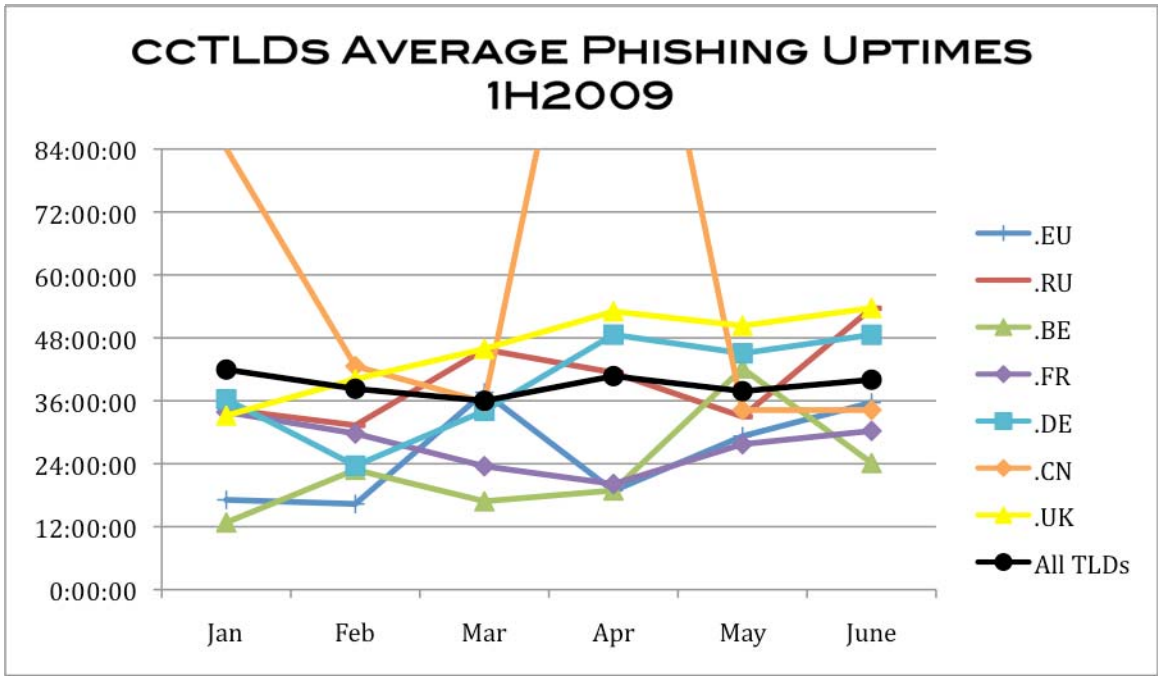
.RU	Average	Median
Jan	34:24:01	17:31:07
Feb	31:20:04	17:35:20
Mar	45:47:26	20:07:20
Apr	41:22:40	15:56:38
May	32:59:09	22:08:10
June	53:37:19	27:44:44
1H2009	39:46:08	19:33:42

.CN	Average	Median
Jan	84:02:07	57:37:18
Feb	42:36:42	20:16:48
Mar	35:45:22	19:38:15
Apr	153:32:09	60:16:29
May	34:14:18	24:09:36
June	34:14:18	24:09:36
Total	67:15:34	30:02:27

The average uptimes in gTLDs were:



The average uptimes in some major ccTLDs were:



TLDs with large percentages of malicious registrations had lower-than-average uptimes. Examples include .EU (662 out of its 864 phishing domains were malicious), .BE (293 out of 484), .NAME (44 out of 53), and .MOBI (62 out of 87).

A success story in 1H2009 was the new anti-phishing program put into place by The Public Interest Registry (PIR), the operator of the .ORG TLD. .ORG had average phishing uptimes

in 2H2008 and January 2009. Stating a desire for abuse response and heightened user protection, PIR announced a new anti-abuse policy to its registrars in late 2008, and it went into effect on February 5, 2009.[1] On that day, PIR began actively reporting phish to its registrars, helping them to alert their registrants about compromised phishing domains. PIR also reserved the option to suspend maliciously registered phishing domains, and did occasional outreach to the hosting providers of hacked phishing domains.[2] The impact was dramatic -- .ORG's phishing uptimes immediately dropped by a third.

In March through May, PIR also responded to the Avalanche gang by quickly suspending maliciously registered .ORG domains, often within minutes of their activation. In mid-May the Avalanche gang stopped registering .ORG domains, and concentrated on registering in other TLDs instead. By June, .ORG was left with mostly phishing on compromised domains, which are harder to mitigate. .INFO and .BIZ continued their anti-phishing programs and recorded lower-than-average uptimes, and Avalanche almost completely avoided these TLDs.

Other major registry operators with active anti-phishing programs performed well by various measures.

.CN, .ORG, .INFO, and .BIZ now face mostly phishing on compromised domains, which are more difficult to fight. However, these TLDs are still turning in lower-than-average uptimes. The results show a correlation between lower phishing uptimes and proactive efforts by registry operators and the registrars they work with.

Use of Internationalized Domain Names (IDNs)

An area of growing interest on the Internet is Internationalized Domain Names, or IDNs. And there has been interest in how IDNs might enable phishing. Data shows that **the unique characteristics of IDNs are not being used to facilitate phishing at this time.** We think that there are factors that may perpetuate this trend in the future.

IDNs are domain names that contain one or more non-ASCII characters. Such domain names can contain letters with diacritical marks such as and , or characters from non-Latin scripts such as Arabic, Chinese, Cyrillic, or Hindi. Over the past four years, IDNs have been available at the second and third levels in many domain name registries, with the majority registered in Asia.

The IDN homograph attack is a means by which a malicious party may seek to deceive computer users by exploiting the fact that characters in different language scripts may be nearly (or wholly) indistinguishable. One such spoof was the registration of a domain that appeared in the browser address bar as:

http://www.paypal.com/

However, the first ASCII "a" was replaced by the virtually identical-looking Cyrillic "a", technically making it different domain name completely.

Are such tricks being used by phishers? From January 1, 2007 to June 30, 2009 only 85 IDNs were used for phishing. The majority were .HK domain names apparently used by the Rock Phish gang early in 2008. That batch presented as Chinese characters intermixed with latin

[1] http://www.pir.org/index.php?db=content/Website&tbl=About_Us&id=14
[2] PIR received assistance from Internet Identity and Afilias.

characters and were evidently not homographic attacks. (And they targeted Western banks and non-Chinese consumers.) Except for one, the rest appear to be compromised/hacked IDN domains owned by innocent parties.

The one true homograph attack we were able to identify appeared on January 16, 2009. The domain name was:

xn--hotmal-t9a.net

When it is rendered in a browser address bar, this IDN looks like this, with a deceptive character spoofing the lower-case "i":

hotmaıl.net

The phish appeared on the home page of the domain, and targeted users of Microsoft's Hotmail service.

Given that IDNs have been widely available for years, why haven't phishers utilized IDN homograph 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.

IDNs will remain an area of interest. On September 30, 2009 ICANN announced its new "fast track" process for top-level IDNs.[1] This will enable the introduction of a number of internationalized country-code top level domain names (IDN ccTLDs). Once implemented, this will be the first time that users will be able to obtain a domain name with the entire string in characters based on a native language.

Use of Subdomains for Phishing

As we wrote about in our last report, phishers are making significant use of subdomain registration services to host phish. Malicious use of these services remained remarkably steady in the first half of 2009, and still accounts for the majority of phishing in some large TLDs. **In the first half of 2009, subdomain services hosted 6,441 phish versus the 6,339 phish we saw in the second half of 2008. This is more than the number of domains registered by phishers at regular domain name registrars (4,382).** This is a disturbing trend, because phish on subdomain registration services can be effectively mitigated only by the subdomain providers themselves[2] – 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

[1] http://www.icann.org/en/topics/idn/

[2] 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.

Beyond uses for these services we've reported previously, there is a rapidly growing trend to use these kinds of services to provide URL "shortening" functionality. The popularity of the online service Twitter in particular and other social networking sites has driven a large part of this demand. Users of those services can obtain a very short URL to use on their limited space posts which redirects the visitor to a much longer "hidden" URL automatically. This is also an ideal vector for abuse, as they redirect unsuspecting users to the truly malicious site based on a domain and service they are quite comfortable using, thus potentially lowering their guard.

We have identified more than 465 subdomain registration providers, which offer services on nearly 2,600 domain names. This is a space as rich as the current "regulated" domain space, with as many or more 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.

Subdomain services remain a popular way for phishers to mount attacks. In our survey we positively identified **6,441 subdomain sites/accounts used for phishing, beneath 483 unique second-level domains.** This is remarkably similar to the second half of 2008, where we saw 6,339 subdomain sites/accounts used for phishing, beneath 480 unique second-level domains. Counting these unique subdomains as "regular" domain names, these types of domains would represent around 18% of all domains involved in phishing.

Top 20 Subdomain Services Used for Phishing 1H2009

Rank	Domain	Total	Provider
1	ns10-wistee.fr	453	wistee.fr
2	t35.com	243	t35.com
3	nm.ru	200	pochta.ru
4	blackapplehost.com	191	blackapplehost.com
5	110mb.com	176	110mb.com
6	pochta.ru	161	pochta.ru
7	pop3.ru	153	pochta.ru
8	justfree.com	150	justfree.com
9	by.ru	134	by.ru
10	free.fr	127	free.fr
10	freehostia.com	127	freehostia.com
12	tripod.com	117	tripod.com
13	aplus.net	106	aplus.net
14	land.ru	102	pochta.ru
15	uol.com.br	83	uol.com.br
16	bplaced.net	81	bplaced.net
17	altervista.org	77	altervista.org
18	co.cc	63	php0h.com
19	hostrator.com	61	hostrator.com
20	50webs.com	59	50Webs.com

Provider	Total Attacks
Pochta.ru	822
Wistee.fr	475
t35.com	243

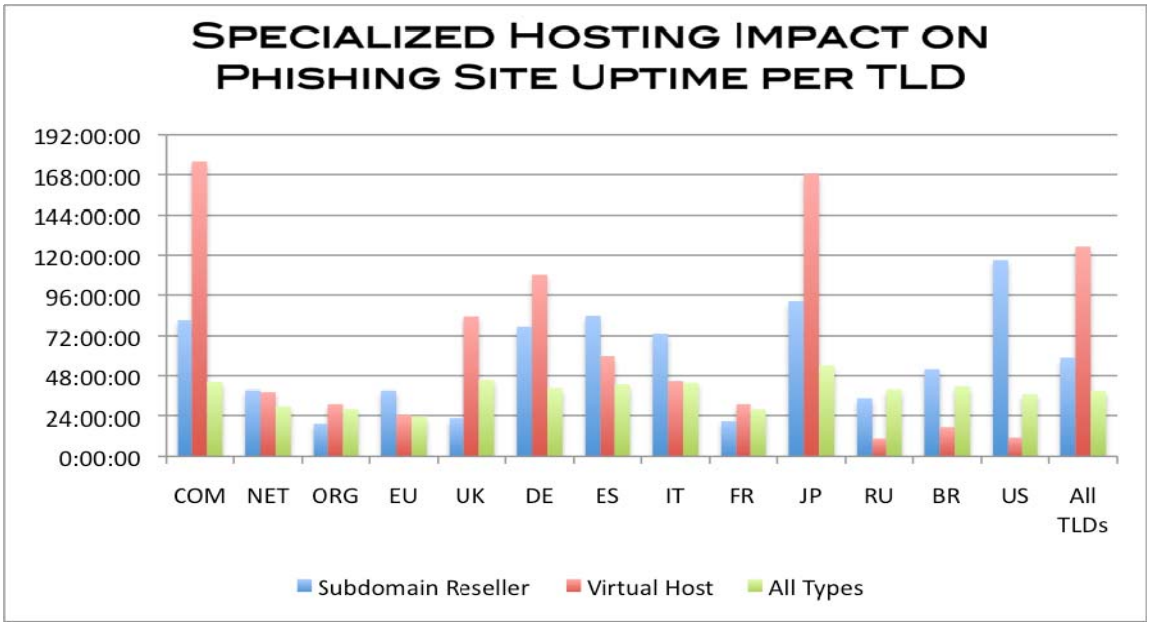
Overall, there were 288 different providers of subdomain registrations who had phishing subdomains on their services in first half of 2009. The Russian freemail provider **Pochta.ru** continued to lead the industry with at least 17 domains that were used to host phishing in 1H2009, and those domains were used to mount at least 822 phishing attacks. The good news is that this provider continues to quickly mitigate phish when reported.

For the second survey period in a row, second place belongs to the French hosting provider **Wistee.fr,** with four domains that hosted 475 phishing attacks during the first half of 2008.

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 that subdomain resellers and specific virtual hosting providers can have on an individual TLD's score, 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 via subdomain resellers and virtual private hosting companies that provide "personal Web hosting accounts" that were fraudulently purchased by phishers – typically in great numbers.



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,

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

depending on the responsiveness of the individual providers involved, 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, in .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. Some hosting companies 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.

Overall, in order for a TLD registry operator to understand how its overall score is affected by these specialized operators, it is important for the registry to know about these services within their TLD. Working with them when there is a persistent problem can sometimes quickly improve the situation.

Conclusions

We saw some evidence that the seesaw battle between phishers and anti-phishing forces has stabilized. The size of the battlefield – at least as measured by domain names and number of attacks – has remained nearly constant. On average, the attacks are not lasting as long as previously, indicating improving success by responders, domain registrars and registries, ISPs, and web hosting providers. Phishers are still obtaining takedown-resistant resources at subdomain resellers and by hacking domains, but they are also being denied resources by some major domain name registry operators and vigilant registrars. And the continued good efforts of spam filtering providers, browser manufacturers, and antivirus software vendors are undoubtedly aiding Internet users.

We also saw that a great deal of phishing is concentrated – the Avalanche gang is responsible for a quarter of phishing attacks, and most maliciously registered phishing domains are localized in only five TLDs. We can hope that focus on these areas of "low-hanging fruit" will lead to further improvements.

Appendix: Phishing Statistics and Uptimes by TLD

NOTE: The column "# Total Malicious Domains Registered 1H2009" includes the number of Avalanche domains registered in 1H2009.

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
ac	Ascension Island	0	0				0:00:00	0	0	0
ae	United Arab Emirates	4	3	87,000	0.3	0.5	6:00:32	0	0	0
aero	sponsored TLD	0	0	6,456	0.0		0:00:00	0	0	0
af	Afghanistan	0	0				0:00:00	0	0	0
ag	Antigua and Barbuda	1	1	15,928	0.6	0.6	17:37:02	0	0	0
ai	Anguilla	0	0				0:00:00	0	0	0
al	Albania	1	1				10:34:22	0	0	0
am	Armenia	11	7	10,834	6.5	10.2	26:34:51	1	0	0
an	Netherlands Antilles	1	1				4:18:59	0	0	0
ar	Argentina	207	159	1,837,779	0.9	1.1	41:26:32	1	0	0
as	American Samoa	5	4				8:51:43	1	0	0
asia	sponsored TLD	2	2	248,407	0.1	0.1	16:03:59	0	0	0
at	Austria	129	96	830,610	1.2	1.6	32:42:23	3	0	0
au	Australia	384	309	1,345,462	2.3	2.9	43:21:44	2	2	13
az	Azerbaijan	3	3	8,511	3.5	3.5	130:29:31	0	0	0
ba	Bosnia & Herzegovina	18	11	9,167	12.0	19.6	136:49:56	0	0	0
bd	Bangladesh	2	2	2,670	7.5	7.5	10:23:19	0	0	0
be	Belgium	1,813	484	892,267	5.4	20.3	16:51:27	293	276	1,540
bf	Burkina Faso	0	0				0:00:00	0	0	0
bg	Bulgaria	9	7	15,700	4.5	5.7	83:00:24	0	0	0
bh	Bahrain	0	0				0:00:00	0	0	0
biz	generic TLD	395	225	2,075,159	1.1	1.9	29:17:02	46	17	76

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
bm	Bermuda	1	1	5,250	1.9	1.9	3:02:48	0	0	0
bn	Brunei Darussalam	4	2				23:31:48	0	0	0
bo	Bolivia	7	5	4,700	10.6	14.9	52:44:08	0	0	0
br	Brazil	654	381	1,675,918	2.3	3.9	41:30:24	1	0	0
bs	Bahamas	38	1	2,228	4.5	170.6	215:54:07	0	0	0
bt	Bhutan	0	0				0:00:00	0	0	0
bw	Botswana	1	1				72:28:08	0	0	0
by	Belarus	19	16				71:23:03	0	0	0
bz	Belize	81	29	43,113	6.7	18.8	20:39:06	13	10	51
ca	Canada	291	226	1,198,350	1.9	2.4	42:21:03	1	0	0
cat	sponsored TLD	6	5	35,591	1.4	1.7	22:34:43	0	0	0
cc	Cocos (Keeling) Islands	130	39	registry declined to provide			70:12:17	5	0	0
cd	Congo, Democratic Repub.	0	0				0:00:00	0	0	0
ch	Switzerland	243	139	1,278,125	1.1	1.9	35:37:02	7	6	69
ci	Côte d'Ivoire	10	3	1,195	25.1	83.7	47:06:06	0	0	0
cl	Chile	144	97	243,701	4.0	5.9	47:39:54	1	0	0
cm	Cameroon	1	1	625	16.0	16.0	3:13:44	0	0	0
cn	China	159	115	13,843,548	0.1	0.1	67:15:34	22	3	13
co	Colombia	31	22	25,750	8.5	12.0	40:06:28	0	0	0
com	generic TLD	25,994	15,170	82,229,830	1.8	3.2	44:09:56	2,180	758	4,992
coop	sponsored TLD	1	1	5,843	1.7	1.7	11:22:38	0	0	0
cr	Costa Rica	1	1	11,739	0.9	0.9	17:55:53	0	0	0
cu	Cuba	2	1	1,500	6.7	13.3	11:18:16	0	0	0
cx	Christmas Island	27	3	4,800	6.3	56.3	53:10:35	0	0	0
cy	Cyprus	9	6	6,500	9.2	13.8	42:53:05	0	0	0

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
cz	Czech Republic	195	99	550,328	1.8	3.5	31:25:40	3	3	16
de	Germany	886	667	12,760,000	0.5	0.7	40:30:42	8	0	0
dj	Djibouti	0	0				0:00:00	0	0	0
dk	Denmark	182	106	996,329	1.1	1.8	49:22:52	1	0	0
dm	Dominica	2	1	14,500	0.7	1.4	12:32:09	0	0	0
do	Dominican Republic	14	7	10,100	6.9	13.9	81:33:47	0	0	0
dz	Algeria	1	1				53:19:05	0	0	0
ec	Ecuador	12	10	17,900	5.6	6.7	36:40:05	0	0	0
edu	U.S. higher education	26	21	Registry declined to provide			49:04:33	0	0	0
ee	Estonia	11	9	65,500	1.4	1.7	68:59:49	0	0	0
eg	Egypt	2	2	4,000	5.0	5.0	107:41:23	0	0	0
er	Eritrea	1	1	120	83.3	83.3	74:57:08	0	0	0
es	Spain	254	164	1,130,650	1.5	2.2	42:43:41	13	11	58
et	Ethiopia	1	1				519:12:24	0	0	0
eu	European Union	3,869	864	3,043,070	2.8	12.7	23:31:13	662	645	3,522
fi	Finland	31	26	211,510	1.2	1.5	90:38:23	0	0	0
fj	Fiji	3	2				29:44:27	0	0	0
fk	Falkland Islands	0	0				0:00:00	0	0	0
fm	Micronesia, Fed. States	9	7				19:00:59	0	0	0
fo	Faroe Islands	3	1				56:50:57	0	0	0
fr	France	1,214	340	1,367,333	2.5	8.9	27:52:10	11	0	0
gd	Grenada	9	3	2,100	14.3	42.9	14:23:59	1	1	4
ge	Georgia	11	8	13,050	6.1	8.4	122:36:17	0	0	0
gg	Guernsey	4	1				159:48:30	0	0	0
gh	Ghana	2	2				50:18:26	0	0	0

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
gi	Gibraltar	0	0	1,695	0.0		0:00:00	0	0	0
gl	Greenland	1	1				1:24:02	0	0	0
gov	U.S. government	3	3	registry declined to provide			471:01:26	0	0	0
gp	Guadeloupe	0	0	1,100	0.0		0:00:00	0	0	0
gr	Greece	116	75	240,000	3.1	4.8	30:02:21	4	4	24
gs	South Georgia & Sandwich Is.	3	2	8,200	2.4	3.7	91:50:26	1	1	1
gt	Guatemala	8	3	6,809	4.4	11.7	159:08:02	0	0	0
hk	Hong Kong	28	23	176,446	1.3	1.6	55:25:57	1	0	0
hm	Heard and McDonald Is.	6	3				14:14:29	0	0	0
hn	Honduras	0	0	3,972	0.0		0:00:00	0	0	0
hr	Croatia	11	9	66,754	1.3	1.6	28:57:19	0	0	0
ht	Haiti	0	0	1,110	0.0		0:00:00	0	0	0
hu	Hungary	127	91	430,000	2.1	3.0	59:56:04	0	0	0
id	Indonesia	96	61				44:46:17	0	0	0
ie	Ireland	59	48	122,374	3.9	4.8	41:48:03	1	0	0
il	Israel	82	48	145,151	3.3	5.6	45:43:46	2	2	10
im	Isle of Man	6	3	14,500	2.1	4.1	8:46:09	1	1	4
in	India	107	83	485,210	1.7	2.2	43:33:29	8	3	11
info	generic TLD	600	493	5,390,206	0.9	1.1	25:10:24	68	4	14
io	British Indian Ocean Terr.	0	0				0:00:00	0	0	0
ir	Iran	47	34	112,491	3.0	4.2	67:43:49	0	0	0
is	Iceland	9	7	24,041	2.9	3.7	22:41:30	0	0	0
it	Italy	373	215	1,685,845	1.3	2.2	43:33:02	0	0	0

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
je	Jersey	0	0				0:00:00	0	0	0
jm	Jamaica	1	1	4,600	2.2	2.2	10:34:35	0	0	0
jo	Jordan	5	4	2,715	14.7	18.4	11:41:46	0	0	0
jobs	sponsored TLD	0	0	15,597	0.0		0:00:00	0	0	0
jp	Japan	173	125	1,082,514	1.2	1.6	54:24:17	0	0	0
ke	Kenya	3	3	10,696	2.8	2.8	29:21:09	0	0	0
kg	Kyrgyzstan	0	0	3,230	0.0		0:00:00	0	0	0
kh	Cambodia	0	0	829	0.0		0:00:00	0	0	0
ki	Kiribati	0	0	4,350	0.0		0:00:00	0	0	0
kr	Korea	751	399	999,262	4.0	7.5	54:36:18	17	17	75
kw	Kuwait	0	0				0:00:00	0	0	0
ky	Cayman Islands	0	0	5,800	0.0		0:00:00	0	0	0
kz	Kazakhstan	21	15	35,298	4.2	5.9	58:18:50	0	0	0
la	Lao People's Demo. Rep.	16	7				22:54:11	1	1	4
lb	Lebanon	0	0	2,850	0.0		0:00:00	0	0	0
lc	St. Lucia	1	1	1,972	5.1	5.1	6:09:43	0	0	0
li	Liechtenstein	93	18	59,244	3.0	15.7	14:41:04	11	9	81
lk	Sri Lanka	9	7	5,921	11.8	15.2	22:41:57	0	0	0
lt	Lithuania	16	15	101,711	1.5	1.6	73:17:14	0	0	0
lu	Luxembourg	5	5	43,853	1.1	1.1	11:31:44	0	0	0
lv	Latvia	19	13	50,000	2.6	3.8	45:31:05	0	0	0
ly	Libya	3	2	5,851	3.4	5.1	7:31:05	0	0	0
ma	Morocco	37	13	29,581	4.4	12.5	43:50:14	0	0	0
md	Moldova	7	6				67:36:09	0	0	0
me	Montenegro	84	30	211,899	1.4	4.0	33:07:00	12	11	33
mg	Madagascar	1	1				2:44:39	0	0	0

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
mk	Macedonia	5	4				7:21:06	0	0	0
ml	Mali	2	1				100:55:18	0	0	0
mn	Mongolia	9	9	7,333	12.3	12.3	76:58:21	0	0	0
mo	Macao	0	0	2,599	0.0		0:00:00	0	0	0
mobi	sponsored TLD	206	87	847,332	1.0	2.4	10:43:31	62	35	154
mr	Mauritania	0	0				0:00:00	0	0	0
ms	Montserrat	5	3	11,650	2.6	4.3	13:58:17	0	0	0
mt	Malta	2	2	11,750	1.7	1.7	32:41:11	0	0	0
mu	Mauritius	0	0	8,700	0.0		0:00:00	0	0	0
museum	sponsored TLD	0	0	545	0.0		0:00:00	0	0	0
mx	Mexico	213	93	290,101	3.2	7.3	36:00:52	30	14	109
my	Malaysia	40	31	80,949	3.8	4.9	59:10:40	0	0	0
mz	Mozambique	0	0	1,800	0.0		0:00:00	0	0	0
name	generic TLD	134	53	278,516	1.9	4.8	14:26:27	44	26	106
net	generic TLD	5,423	2,570	12,525,459	2.1	4.3	29:45:58	438	317	1,785
nf	Norfolk Island	11	3	5,000	6.0	22.0	2:34:10	0	0	0
ng	Nigeria	6	4	1,350	29.6	44.4	19:29:03	0	0	0
ni	Nicaragua	0	0	23,000	0.0		0:00:00	0	0	0
nl	Netherlands	610	509	3,323,308	1.5	1.8	46:39:41	3	0	0
no	Norway	52	43	428,123	1.0	1.2	54:22:04	0	0	0
np	Nepal	4	2	11,900	1.7	3.4	12:41:47	0	0	0
nr	Nauru	4	2	425	47.1	94.1	90:43:43	0	0	0
nu	Niue	117	32				36:05:15	13	13	72
nz	New Zealand	53	45	353,430	1.3	1.5	30:00:07	0	0	0
org	generic TLD	2,554	1,691	7,549,754	2.2	3.4	27:54:07	207	99	374
pa	Panama	5	3	4,800	6.3	10.4	37:53:18	0	0	0
pe	Peru	86	64	32,000	20.0	26.9	33:56:47	24	0	0

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
ph	Philippines	27	18	registry declined to provide			18:19:47	0	0	0
pk	Pakistan	75	16	28,200	5.7		30:17:13	2	2	37
pl	Poland	573	359	1,416,565	2.5	4.0	43:26:33	4	0	0
pn	Pitcairn	5	4				152:21:27	0	0	0
pro	sponsored TLD	1	1	35,694	0.3	0.3	5:46:22	0	0	0
ps	Palestinian Territory	3	2	4,315	4.6	7.0	2:03:35	0	0	0
pt	Portugal	61	46	296,871	1.5	2.1	61:28:35	0	0	0
py	Paraguay	3	2	8,834	2.3	3.4	39:45:27	0	0	0
qa	Qatar	1	1				16:38:12	0	0	0
ro	Romania	278	163	310,900	5.2	8.9	68:01:07	2	1	7
rs	Serbia	20	13	45,000	2.9	4.4	26:39:43	0	0	0
ru	Russian Fed.	1,982	710	2,016,396	3.5	9.8	39:46:07	3	0	0
sa	Saudi Arabia	11	9	15,946	5.6	6.9	122:22:13	0	0	0
sc	Seychelles	1	1	6,543	1.5	1.5	20:43:35	1	0	0
se	Sweden	94	72	853,802	0.8	1.1	61:07:32	0	0	0
sg	Singapore	24	18	109,823	1.6	2.2	30:47:30	1	0	0
sh	Saint Helena	0	0				0:00:00	0	0	0
si	Slovenia	23	19	67,207	2.8	3.4	56:31:34	0	0	0
sk	Slovakia	132	46	184,943	2.5	7.1	49:04:53	0	0	0
sl	Sierra Leone	0	0	1,200	0.0		0:00:00	0	0	0
sm	San Marino	0	0	1,905	0.0		0:00:00	0	0	0
st	Sao Tome & Principe	9	3	5,660	5.3	15.9	49:09:03	0	0	0
su	Soviet Union	125	30	83,739	3.6	14.9	37:26:53	1	0	0
sv	El Salvador	2	2	4,292	4.7	4.7	57:05:31	0	0	0
sy	Syria	2	2				22:08:33	0	0	0
tc	Turks and Caicos	35	10	9,700	10.3	36.1	111:36:58	1	1	3

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
tel	generic TLD	0	0	129,562	0.0		0:00:00	0	0	0
tf	French Southern Territories	4	3	1,557	19.3	25.7	74:32:27	0	0	0
th	Thailand	128	68	42,594	16.0	30.1	64:08:22	0	0	0
tj	Tajikistan	5	2	4,681	4.3	10.7	72:32:02	0	0	0
tk	Tokelau	166	135	1,780,000	0.8	0.9	40:36:12	73	2	19
tl	Timor-Leste	5	2				36:37:39	0	0	0
tm	Turkmenistan	1	1				0:44:13	0	0	0
tn	Tunisia	1	1	50	200.0	200.0	3:05:43	0	0	0
to	Tonga	11	11	13,250	8.3	8.3	47:26:02	0	0	0
tp	Portuguese Timor	1	1				40:00:06	0	0	0
tr	Turkey	52	35	191,193	1.8	2.7	59:58:35	0	0	0
travel	sponsored TLD	0	0	133,051	0.0		0:00:00	0	0	0
tt	Trinidad & Tobago	5	4	2,202	18.2	22.7	106:26:11	0	0	0
tv	Tuvalu	42	35	registry declined to provide			49:51:56	0	0	0
tw	Taiwan	290	194	425,551	4.6	6.8	47:52:21	3	3	12
tz	Tanzania	4	3				21:58:28	0	0	0
ua	Ukraine	146	104	403,456	2.6	3.6	45:19:40	0	0	0
ug	Uganda	11	6	3,100	19.4	35.5	30:15:35	0	0	0
uk	United Kingdom	823	605	7,665,754	0.8	1.1	45:23:09	45	10	41
us	United States	200	153	1,392,657	1.1	1.4	37:14:16	17	0	0
uy	Uruguay	15	13	18,622	7.0	8.1	17:21:42	0	0	0
uz	Uzbekistan	3	3	8,284	3.6	3.6	5:07:00	0	0	0

TLD	TLD Location	# Unique Phishing attacks 1H2009	Unique Domain Names used for phishing 1H2009	Domains in registry at end March 2009	Score: Phish per 10,000 domains 1H2009	Score: Attacks per 10,000 domains 1H2009	Average Uptime 1H2009 hh:mm:ss	# Total Malicious Domains Registered 1H2009	AVALANCHE Domains Registered 1H2009	AVALANCHE Attacks 1H2009
vc	St. Vincent & Grenadines	1	1	6,259	1.6	1.6	12:56:35	0	0	0
ve	Venezuela	24	15	130,000	1.2	1.8	111:19:13	1	0	0
vg	British Virgin Islands	7	4	8,900	4.5	7.9	10:21:43	1	1	4
vi	Virgin Islands	0	0	457	0.0		0:00:00	0	0	0
vn	Vietnam	52	36	100,979	3.6	5.1	48:53:00	0	0	0
vu	Vanuatu	0	0				0:00:00	0	0	0
ws	Samoa	57	34	540,000	0.6	1.1	52:24:00	3	0	0
yu	Yugoslavia (being deprecated)	6	4	4,500	8.9		128:55:28	0	0	0
za	South Africa	91	64	476,607	1.3	1.9	36:42:16	0	0	0
zm	Zambia	1	1				75:42:51	0	0	0
zw	Zimbabwe	10	5	8,328	6.0	12.0	43:56:16	0	0	0
	TOTALS	55,698	30,131	184,583,376				4,382	2,309	13,334

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), served on ICANN's Fast-Flux Working Group, 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 served 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. A very special thank-you to Aaron Routt of Internet Identity for his tireless work in ensuring the accuracy of the data in the report, and for preparing the many charts and graphs. 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.

#