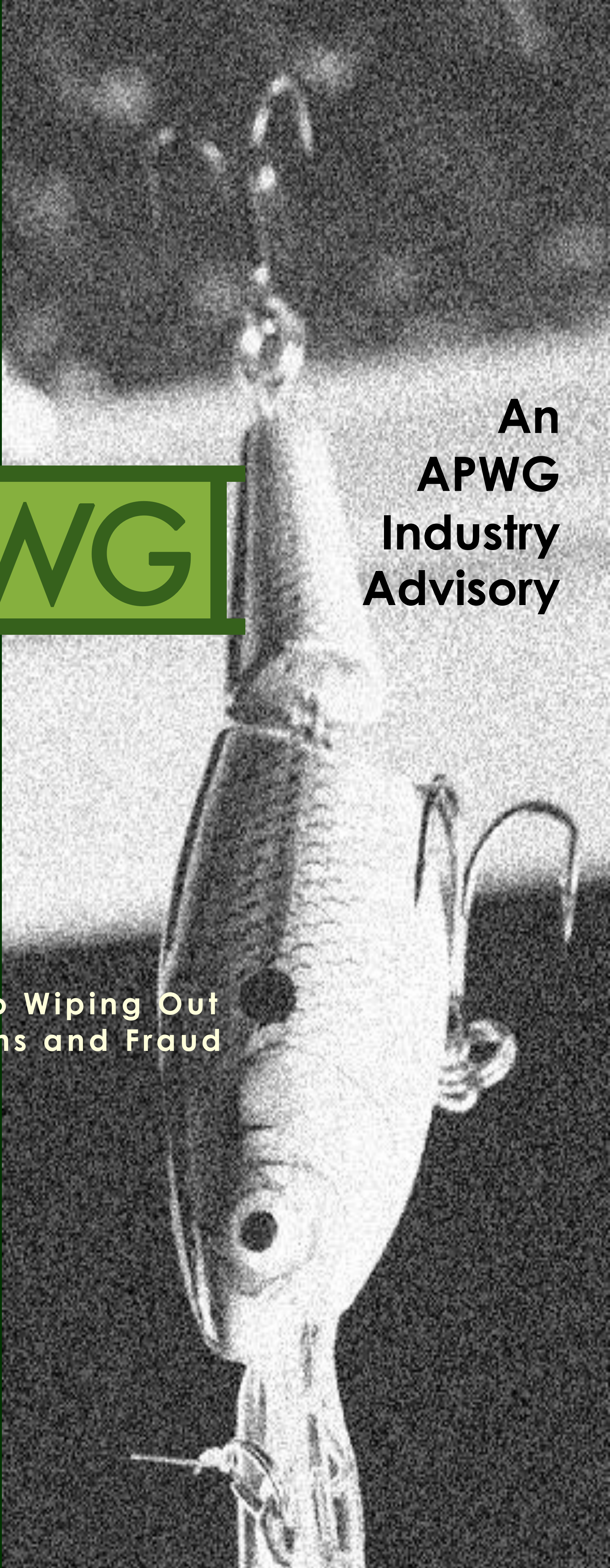
Global Phishing Survey: Trends and Domain Name Use in 1H2010



An APWG Industry Advisory

Committed to Wiping Out Internet Scams and Fraud

October 2010

Published October 18, 2010

Authors:

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

Greg Aaron
Afilias
<gaaron at afilias.info>

Research and Analysis Support:
Aaron Routt
Internet Identity

Table of Contents

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

Overview

The first half of 2010 marked the end of phishing by the world's largest phishing gang. While that may seem like good news, the change actually boded ill for Internet users. In late 2009, the "Avalanche" phishing operation was responsible for a staggering two-thirds of all phishing attacks. But like any professional operation, Avalanche adapted with the times, and by mid-2010 the group had largely abandoned phishing in favor of a better tool: the Zeus banking Trojan. This report takes a look at Avalanche's evolution, examining how these e-criminals have incorporated interrelated methods—including phishing, malware, botnets, and spam—into their work.

With Avalanche no longer dominating the scene, phishing fell back to historical levels in terms of the number of attacks observed and the number of Internet resources used. However, the uptimes of phishing sites headed higher.

This report seeks to understand such trends and their significances by quantifying the scope of the global phishing problem. Specifically, this new report examines all the phishing attacks detected in the first half of 2010 ("1H2010", or January 1, 2010 through June 30, 2010). The data was collected by the Anti-Phishing Working Group 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] We hope that bringing new trends to light will lead to improved anti-phishing measures.

Our major findings include:

1. **The Avalanche phishing gang abandoned its traditional phishing activities in favor of malware distribution.** *(Page 5)*
2. **Phishers continue to use subdomain services to host and manage phishing sites. Phishers use such services as often as they register domain names.** This activity shows phishers using services that cannot be taken down by domain registrars or registry operators, in the hopes of extending uptimes of attacks. *(Page 17)*
3. **In 1H2010, the average and median uptimes of all phishing attacks grew from previous periods.** Non-Avalanche phish stayed up noticeably longer. *(Page 8.)*
4. **The total of Internet domain names and numbers used for phishing has remained steady** over the past three years, a period in which the number of registered domain names in the world has grown significantly. *(Page 4)*
5. **Use of URL-shortening services (such as bit.ly and tinyurl.com) by phishers may be a growing trend.** URL shorteners can be useful for launching social engineering attacks via services such as Twitter. *(Page 19)*
6. **Phishers are not leveraging the unique characteristics of internationalized domain names (IDNs)**, and there are factors that may perpetuate this trend in the future. *(Page 16)*

[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: http://www.apwg.org/resources.html#apwg

Basic Statistics

Millions of phishing URLs were reported in 1H2010, but the number of unique phishing attacks and domain names used to host them was much smaller.[2] The 1H2010 data set yields the following statistics:

- **There were at least 48,244 phishing attacks. This is down significantly from the record 126,697 observed in 2H2009, and the fewest in any period since the first half of 2008.** 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. The decrease in attacks was due to reduced activity by the Avalanche phishing gang.
- The attacks occurred on **28,646 unique domain names.**[3] This is virtually unchanged from the 28,775 seen in 2H2009, and down from the 30,131 observed in 1H2009. The number of domain names in the world grew from 168 million in mid-2008 to 192 in late 2009 to 196 million in May 2010.[4]
- In addition, 2,538 attacks were detected on **2,018 unique IP addresses, rather than on domain names.** (For example: http://96.56.84.42/ClientHelp/ssl/index.htm.) This is comparable to the 2,031 unique IPs seen in 2H2009, and down significantly from the 3,563 in 1H2009. We did not observe any phishing on IPv6 addresses.
- 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 remarkably steady over the past three years.**
- Of the 28,646 phishing domains, **we identified 4,755 that we believe were registered maliciously, by the phishers. Of those, 1,624 (34%) were registered by Avalanche.** Virtually all of the other 23,891 domains were hacked or compromised on vulnerable Web hosting. Malicious registrations apparently took place in just 49 TLDs.
- **Phishing remains concentrated in certain namespaces.** 62% of the attacks occurred in just four TLDs: .COM, .NET, .KR, and .ORG. And 80% of the malicious domain registrations were made in just 5 TLDs: .COM, .KR, .PL, .NET, and .TK.

[2] 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 targets. Some phishers place several different phishing attacks on each domain name they register.
C) A phishing site may have multiple pages, each of which may be reported.

[3] "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.

[4] As per our research, and VeriSign Industry Briefs: http://www.verisign.com/domain-name-services/domain-information-center/industry-brief/index.html

- **Only about 5% of all domain names that were used for phishing contain a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations" on page 15.)
- Only 10 of the 28,647 domain names we studied were IDNs. See "Use of Internationalized Domain Names" below for more details.

Basic Statistics

	1H2010	2H2009	1H2009	2H2008	1H2008
Phishing domain names	28,646	28,775	30,131	30,454	26,678
Attacks	48,244	126,697	55,698	56,959	47,324
TLDs used	177	173	171	170	155
IP-based phish (unique IPs)	2,018	2,031	3,563	2,809	3,389
Maliciously registered domains	4,755	6,372	4,382	5,591	-
IDN domains	10	12	13	10	52

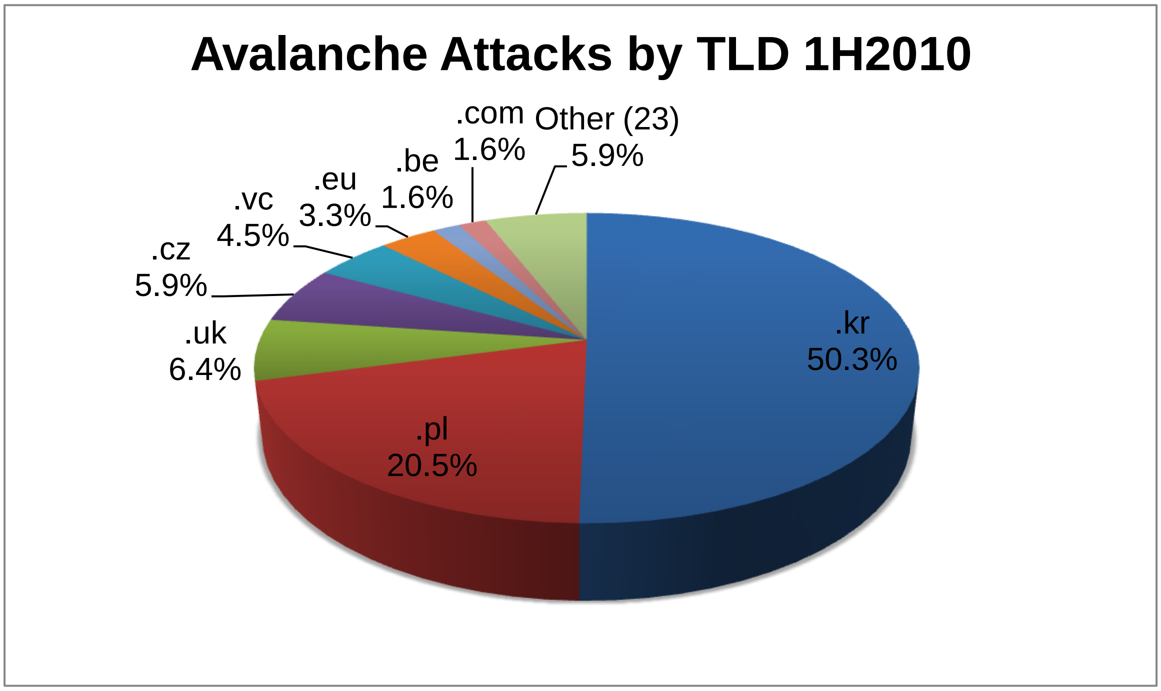
Each domain name's registrar of record was not reported at the time the phish was live. Obtaining accurate registrar sponsorship data for a domain name requires either time-of-attack WHOIS data, or historical registry-level data. This data has not been collected in a comprehensive manner by the anti-phishing community.

The Decline of Avalanche Phishing

"Avalanche" is the name given to what has been the world's most prolific phishing gang, and to the infrastructure it uses to host phishing sites. In the second half of 2009, this criminal enterprise accounted for two-thirds of all phishing attacks — 84,250 out of 126,697 attacks. Avalanche phishing dropped precipitously during the first half of 2010, down to just 4,272 phishing attacks on 1,624 domains. Unfortunately, the people behind Avalanche switched to distributing malware instead. Avalanche's targeting, attack methods, and volume changed several times in the first half of 2010, and its activities therefore deserve special examination.

Avalanche was first seen in December 2008, and introduced an unprecedented volume and sophistication to phishing. Avalanche was responsible for 24% of the phishing attacks recorded in 1H2009, growing to 67% of all phishing attacks in 2H2009. A typical Avalanche domain often hosted around 40 separate attacks at a time in 2009. This changed to just one or a handful of attacks per domain in 2010. Avalanche domains were usually hosted on a botnet comprised of compromised consumer-level computers. This "fast-flux" hosting made mitigation efforts more difficult – there was no ISP or hosting provider who had control of the hosting and could take the phishing pages down, and instead the domain name itself had to be suspended by the domain registrar or registry.

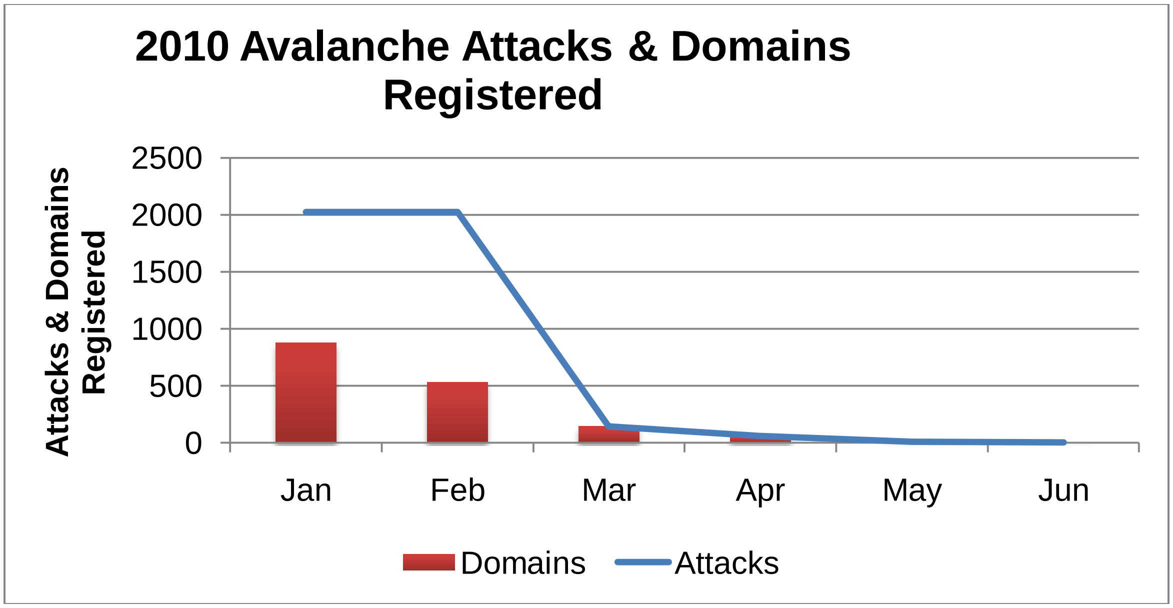
Avalanche continually registered domain names in TLDs where the domains were not taken down expeditiously. During 2010, two ccTLDs new to these attacks were abused heavily: .KR (South Korea) and .PL (Poland). Those domains accounted for over 70% of all Avalanche attacks. The registries did expedited domain takedowns in those hard-hit TLDs, often with support from their national CERTs. Avalanche used domains in 30 other TLDs for phishing in 1H2010, but at relatively low levels.



During the first half of 2010, Avalanche attacked just 14 targets (major financial institutions, online services, and social networks), down from 40 targets in 2H2009.

Avalanche attacks dwindled to just four per month by July 2010:

Month	Avalanche Attacks	Domain names
July 2009	12,793	498
August 2009	16,372	603
September 2009	18,633	656
October 2009	26,411	924
November 2009	7,089	523
December 2009	2,952	959
January 2010	2,028	877
February 2010	2,024	531
March 2010	146	145
April 2010	59	59
May 2010	11	8
June 2010	4	4



Because they were so damaging, prevalent, and recognizable, Avalanche phishing attacks received concentrated attention from the response community, including the target institutions, domain name registrars, registries, and other responders and service providers. As a result, Avalanche attacks had a much shorter average uptime than non-Avalanche phishing attacks, and community efforts partially neutralized the advantage of the fast-flux hosting. Uptimes for Avalanche phish were under 10 hours in 1H2010, compared to nearly 14 hours for non-Avalanche attacks.

Avalanche also dabbled in tactics other than directly registering malicious domains at registrars. We saw Avalanche host 26 attacks on a handful of subdomain resellers and URL shortening services in 1H2010. We saw also Avalanche make extensive use of URL shortening services for malware distribution at various times into October 2010.

During 1H2010, the criminals instead emphasized the Avalanche infrastructure as a major distribution point for the notorious Zeus Trojan. Zeus is a sophisticated piece of malware that is in the hands of many different e-criminals. The Avalanche gang started incorporating Zeus into its phishing and spamming campaigns in 2009. Zeus is *crimeware* – malware designed specifically to automate identity theft and facilitate unauthorized transactions.

The Avalanche gang used nearly every type of social engineering trick we've seen over the years in order to fool victims into receiving the Zeus crimeware. Avalanche sent false alerts/updates purporting to be from popular social networking sites, and lures that offered popular software upgrades, and fake downloadable forms from tax authorities. These lures took victims to "drive-by download" sites, where the criminals infected vulnerable machines. Once a machine is infected, the criminals can remotely access it, steal the personal information stored on it, and intercept passwords and online transactions. The criminals can even log into the victim's machine to perform online banking transactions using the victim's own account details, which is difficult for banks to detect as fraud. Recent reporting pegs losses due to this crimeware at more than $100 million annually. [5]

The shift from traditional phishing to crimeware distribution seems to have occurred because Zeus is more profitable. It is simply more profitable to control someone's computer remotely and move large amounts of money than to simply steal victims' online banking credentials.

At various times during the first half of 2010, members of the security community affected temporary shutdowns of all or part of the botnet infrastructure that the Avalanche "crew" relies on. Unfortunately, the crimeware attacks continue despite the disruptions. Ultimately, arrest and prosecution of the criminals behind these attacks will likely be necessary to completely end the attacks.

Events occurring concurrently with the drafting of this paper may have an impact on future Avalanche attacks. During the last week of September 2010, dozens of alleged cybercriminals in the United States, the United Kingdom, the Ukraine, and elsewhere were arrested for the use of Zeus crimeware – possibly the Zeus malware distributed by Avalanche. As of this writing it is too early to tell if key members of the core group behind these attacks were rounded up. But we are hopeful that this is the case, and we hope to see a dramatic decrease in Avalanche attacks in the future. We applaud law enforcement's efforts and recent successes.

Phishing By Uptime

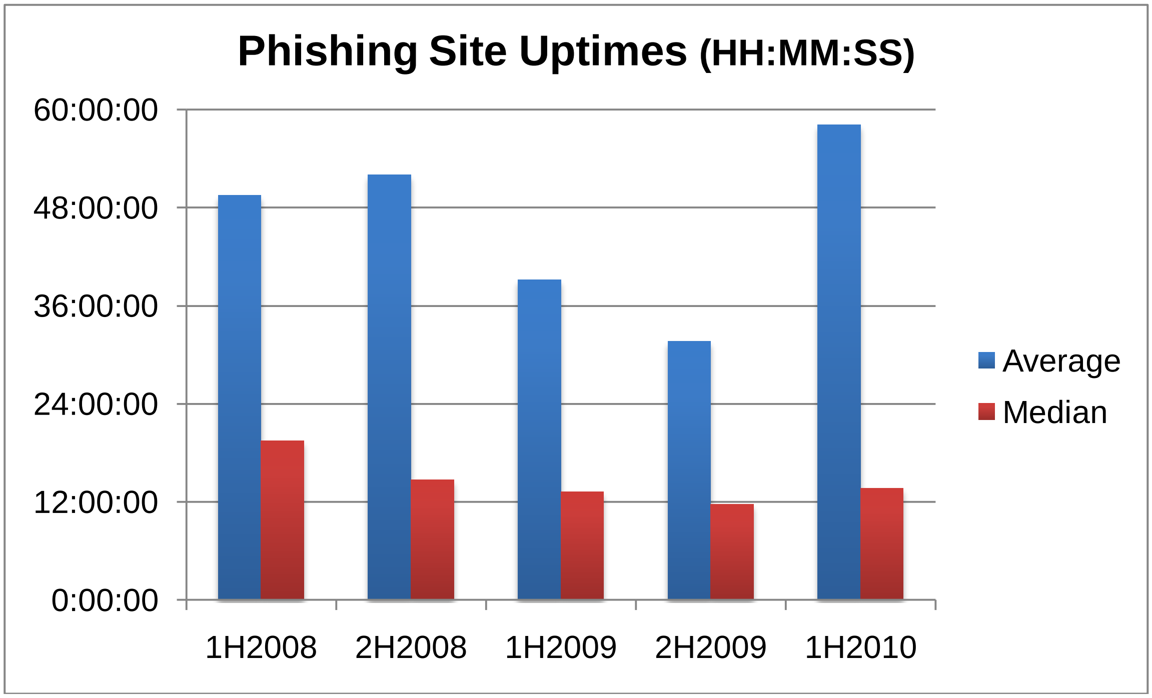
After reaching an historical low in 2H2009, the average and median uptimes of phishing attacks rose in the first half of 2010. This increase is attributable to the absence of Avalanche, since Avalanche domains were killed quickly and attracted a great deal of attention from the response community.

The "uptimes" or "live" times[6] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a measure of the success of mitigation efforts. The longer a phishing attack remains active, the more money the victims and target institutions lose, and the more money the phisher can make. Long-lived phish can skew the averages since some phishing sites may last weeks or even months, so medians are also a useful barometer of overall mitigation efforts.

[5] For more about how Zeus works, see: http://secureworks.com/research/threats/zeus/

[6] 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.

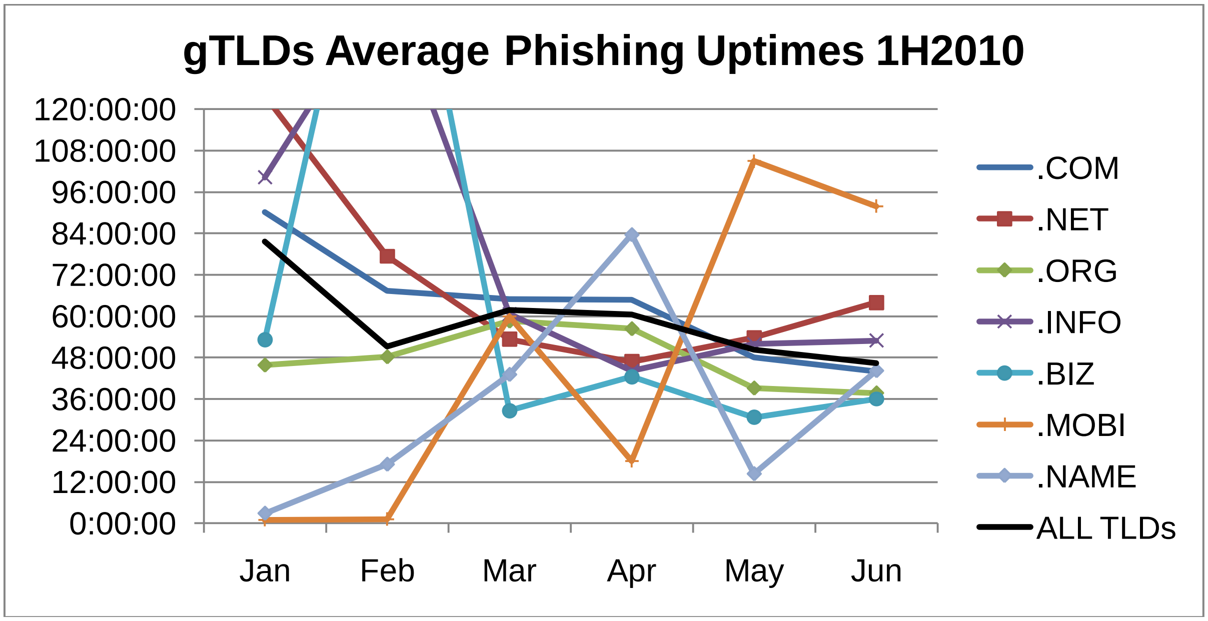
The historical trend is:

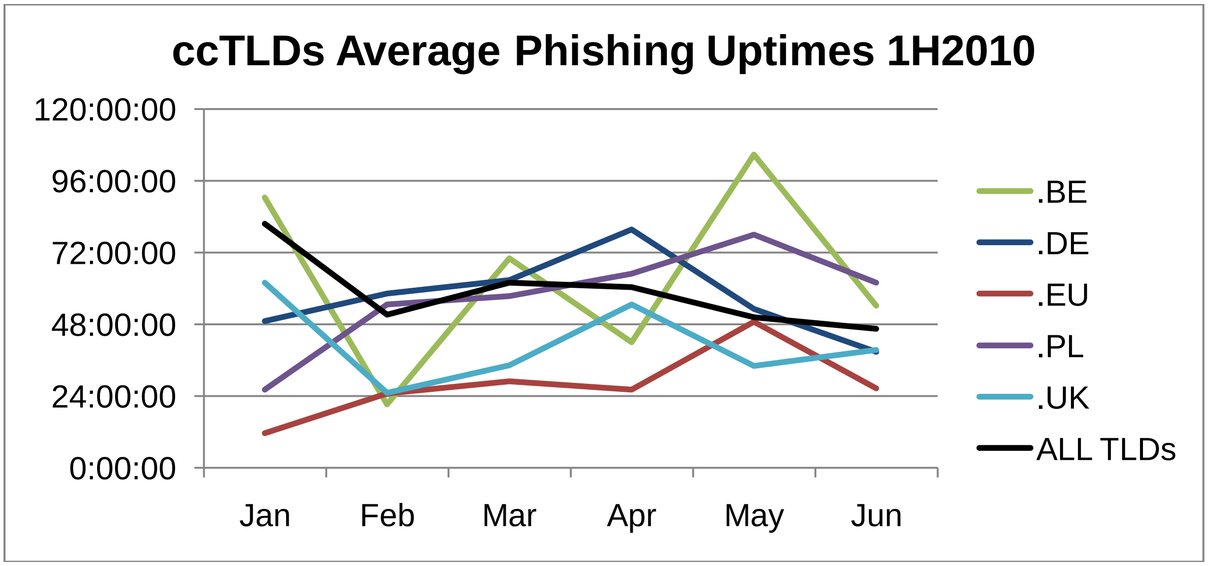


ALL PHISH, ALL TLDs	Average (HH:MM:SS)	Median (HH:MM:SS)
Jun 2010	46:26:52	16:22:07
May 2010	50:18:09	14:19:02
Apr 2010	60:28:10	15:15:34
Mar 2010	61:52:18	15:26:53
Feb 2010	51:09:00	10:51:44
Jan 2010	81:41:33	12:09:59
1H 2010	**58:10:16**	**13:42:16**
2H2009	31:38:00	11:44:15
1H2009	39:11:00	13:15:32
2H2008	52:01:58	14:43:15
1H2008	49:30:00	19:30:00

The median is still improved from where it was two years ago. Early 2008 was the heyday of the Rock Phish gang, which used a fast-flux botnet to extend the uptimes of its phish. Avalanche also used fast-flux, but Avalanche phishing sites were mitigated more quickly, and in batches. **The historical decrease was encouraging, but we must monitor uptimes into 2H2010 to see if uptimes continue to stay higher than in years past. Now that Avalanche phishing is gone, the field now consists overwhelmingly of phish on compromised domains, which are more difficult to mitigate.**

The uptimes for all phishing attacks in 1H2010, and for phish in some large TLDs, were as follows:





Uptimes: All Phish, 1H2010

	Average (HH:MM:SS)	Median (HH:MM:SS)
ALL TLDs	58:10:16	13:42:16
.COM	61:06:02	13:39:51
.NET	67:59:27	14:03:44
.ORG	46:39:14	13:01:58
.INFO	69:56:55	15:12:31
.BIZ	57:44:45	12:14:58
.UK	41:39:35	13:15:21
.CN	91:51:48	14:24:29
.EU	24:30:39	9:55:20
.RU	59:32:18	15:09:34
.BE	65:36:16	17:35:21
.KR	25:20:24	9:57:48
.PL	41:01:06	16:53:52
.BR	82:23:54	23:38:59
.DE	55:18:08	15:08:37
.FR	38:09:11	15:31:33
.VC	17:24:31	8:53:03
.CZ	31:26:37	8:56:48

Uptimes: Avalanche Phish Only, 1H2010

	Average (HH:MM:SS)	Median (HH:MM:SS)
ALL TLDs	12:28:12	9:55:23
.COM	29:43:49	7:49:05
.NET	14:06:23	6:49:05
.ORG	1:22:21	1:21:05
.INFO	n/a	n/a
.BIZ	n/a	n/a
.UK	10:51:36	3:41:32
.CN	n/a	n/a
.EU	7:56:13	5:47:14
.RU	17:48:16	17:22:34
.BE	12:41:23	12:24:01
.KR	10:22:52	9:53:04
.PL	18:04:57	17:15:25
.BR	n/a	n/a
.DE	n/a	n/a
.FR	n/a	n/a
.VC	17:25:17	8:53:21
.CZ	7:21:59	6:12:54

Uptimes: Non-Avalanche Phish Only, 1H2010

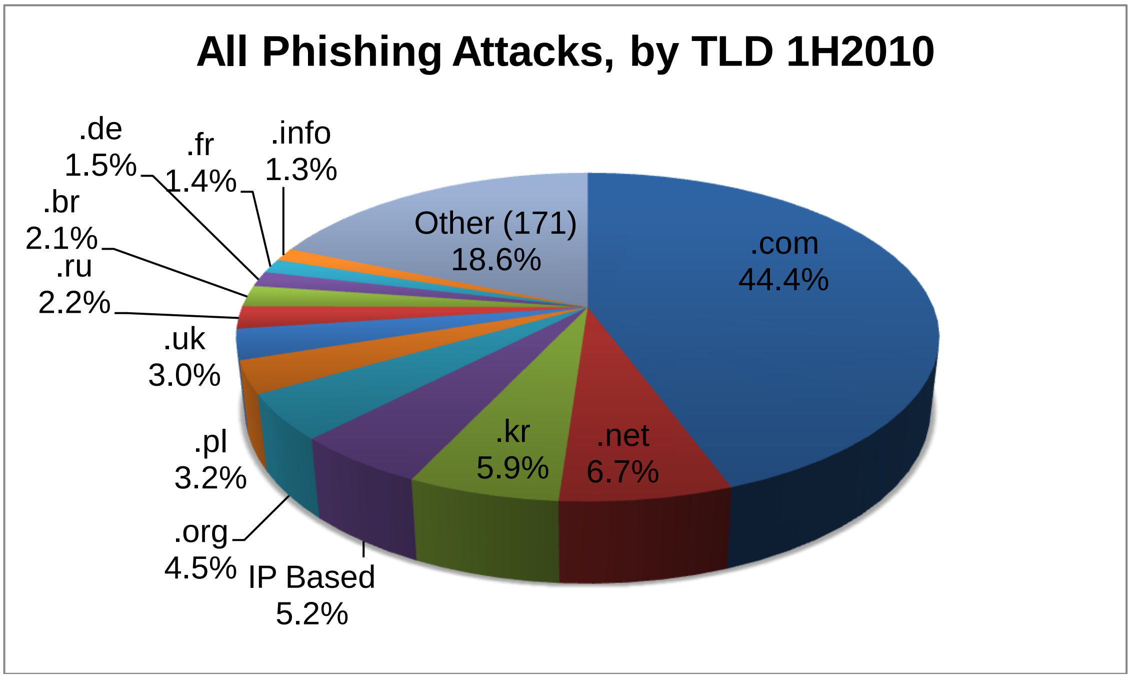
	Average (HH:MM:SS)	Median (HH:MM:SS)
ALL TLDs		
.COM	61:14:08	13:44:26
.NET	68:41:39	14:14:37
.ORG	46:51:39	13:10:42
.INFO	69:56:55	15:12:31
.BIZ	57:44:45	12:14:58
.UK	48:47:07	16:08:49
.CN	91:51:48	14:24:29
.EU	34:08:59	16:14:06
.RU	59:46:13	15:09:34
.BE	88:25:25	20:22:07
.KR	67:54:22	21:05:38
.PL	69:06:57	16:14:40
.BR	82:23:54	23:38:59
.DE	55:18:08	15:08:37
.FR	38:09:11	15:31:33
.VC	16:55:17	4:42:40
.CZ	58:03:18	14:46:18

Prevalence of Phishing by Top-Level Domain (TLD)

We analyzed the 28,646 phishing domains to see how they were distributed among the TLDs. The complete tables are presented in the Appendix. We were able to obtain the domain count statistics for TLDs containing 99% of the phishing domains in our data set, and a total of 194,824,738 domain names overall. [7]

The majority of phishing continues to be concentrated in just a few namespaces. Except for .KR, a TLD that was victimized by Avalanche in early 2010, phishing was roughly distributed by market share. 62% of the attacks occurred in just four TLDs: .COM, .NET, .KR, and .ORG. 80% of the malicious domain registrations were made in just 5 TLDs: .COM, .KR, .PL, .NET, and .TK.

[7] For the purposes of this study, we used the number of domain names in each registry as of May 2010. Sources: ICANN.org (monthly registry reports), ccTLD registry operators.



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"[8] is a ratio of the number of domain names used for phishing in a TLD to the number of registered domain names in that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of phishing relative to others.

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

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

- **The median domains-per-10,000 score was 2.7**.
- **The average domains-per-10,000 score of 8.4** was skewed by a few high-scoring TLDs.
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 1.6.** .COM contains 49% of the phishing domains in our data set, and 46% of the domains in the TLDs for which we have domains-in-registry statistics.

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

We therefore suggest that domains-per-10,000 scores between .COM's 1.6 and the median of 2.7 occupy the middle ground, with scores above 2.7 indicating TLDs with increasingly prevalent phishing. [9]

Top 10 Phishing TLDs by Domain Score

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

RANK	TLD	TLD Location	# Unique Phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010
1	th	Thailand	86	62	49,000	12.7	17.6
2	kr	Korea	2,888	989	1,079,298	9.2	26.8
3	ie	Ireland	102	79	145,724	5.4	7.0
4	pl	Poland	1,582	744	1,805,894	4.1	8.8
5	cl	Chile	159	111	282,526	3.9	5.6
6	my	Malaysia	61	39	99,736	3.9	6.1
7	gr	Greece	130	93	260,000	3.6	5.0
8	ro	Romania	324	156	443,700	3.5	7.3
9	vn	Vietnam	64	48	153,002	3.1	4.2
10	cz	Czech Republic	480	207	689,813	3.0	7.0

.TH (Thailand) has been at the top of our list for two years. Phishing in .TH takes place mostly on compromised academic (AC.TH) and government (GO.TH) Web servers, but also on commercial sites. There were even two phish on the military domain tdd.mi.th, which had been defaced prominently numerous times between May and December 2009. Such institutional servers in Thailand have been exploited repeatedly over the last three years, highlighting the need for server operators everywhere to follow good software update practices and maintain effective intrusion detection.

.KR, .PL , and .CZ were used for Avalanche attacks. The other TLDs in the Top 10 list experienced phishing on compromised domains almost exclusively.

The "generic" TLDs are open to registrants across the world without registration qualifications, while "sponsored" TLDs have eligibility requirements. All of the gTLDs and

[9] 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.

sTLDs had average-to-below-average scores:

Phishing in gTLDs and sTLDs by Score

TLD	TLD Type	# Unique Phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010
coop	sponsored	2	2	6,873	2.9	2.9
org	generic	2,199	1,469	8,354,701	1.8	2.6
net	generic	3,260	2,132	13,424,274	1.6	2.4
com	generic	21,673	13,947	89,712,873	1.6	2.4
aero	sponsored	1	1	6,881	1.5	1.5
biz	generic	227	171	2,076,973	0.8	1.1
info	generic	628	513	6,297,595	0.8	1.0
name	generic	17	14	245,326	0.6	0.7
pro	sponsored	3	2	46,381	0.4	0.6
travel	sponsored	1	1	43,488	0.2	0.2
mobi	sponsored	24	20	970,693	0.2	0.2
asia	sponsored	5	2	187,203	0.1	0.3
cat	sponsored	0	0	42,676	0.0	0.0
jobs	sponsored	0	0	33,009	0.0	0.0
museum	sponsored	0	0	556	0.0	0.0
tel	generic	0	0	287,755	0.0	0.0

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 their sites were 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.

Of the 28,647 domains used for phishing, **we identified 4,775 that we believe were registered by phishers.** Of those, 1,624 were registered by Avalanche early in 2010. If Avalanche registrations are discarded, the number of malicious domains was 3,151, up from the 2,221 in 2H2009.

The remaining 23,872 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. 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, 1,503 contained a relevant brand name or variation thereof – often a misspelling.[10] **This represents just 5% of all domains that were used for phishing, and 31% of the maliciously registered domains.** And 71% of those band-name-using domains victimized just four targets – PayPal, World of Warcraft/Battle.net, HSBC, and Google.

Most maliciously registered domain strings offered nothing to confuse a potential victim. Placing brand names or variations thereof in the domain name itself is not a favored tactic, since brand owners are proactively scanning Internet zone files for such names. As we have observed in the past, **the domain name itself usually does not matter to phishers, and a hacked domain name of any meaning, in any TLD, will usually do.** Instead, phishers almost always place brand names in subdomains or subdirectories. This puts the misleading string somewhere in the URL, where potential victims may see it and be fooled. Internet users are rarely knowledgeable enough to be able to pick out the "base" or true domain name being used in a URL.

Recent innovations in the browser market may change this equation, however, since browsers can highlight the "real" domain name in the address bar as a security enhancement. Time will tell if this is an effective countermeasure.

Use of Internationalized Domain names (IDNs)

An area of growing interest on the Internet is Internationalized Domain Names, or IDNs. **Data continues to show that the unique characteristics of IDNs are not being used to facilitate phishing.** We believe that this trend will continue.

IDNs are domain names that contain one or more non-ASCII characters. Such domain names can contain letters with diacritical marks such as ǎ and ü, or characters from non-Latin scripts such as Arabic, Chinese, Cyrillic, or Hindi. Over the past five years, IDNs have been available at the second and third levels in many domain name registries, with the majority registered in Asia. IDN TLDs allow the entire domain name to be in non-Latin characters. ICANN and IANA enabled the first three IDN TLDs on May 5, 2010, and applications for dozens more are in process.

The IDN homograph attack is a means by which a malicious party seeks to deceive computer users by exploiting the fact that characters in different language scripts may be nearly (or wholly) indistinguishable. The last true homograph attack we were able to identify appeared on January 16, 2009. The domain name was "xn--hotmal-t9a.net", which appeared as "hotmaıl.net" when rendered in a browser address bar. Note that the lower-case "i" has been replaced with a similar-looking substitute character.

[10] Examples of domain names we counted as containing brand names included: ardwords-n.com (Google Adwords), bid-pagz-yahoo.com (Yahoo!), battleuswow.net (World of Warcraft), ntwestsc.com (Natwest), and fbphonenumbers.tk (Facebook).

We saw no homographic attacks in the first half of 2010. Only ten of the 28,647 domain names we studied were IDNs, and those ten domains were all hacked by phishers.

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. Users therefore cannot see a homographic attack.

The new fast-track IDN TLD registries will be run by existing national ccTLD registry operators. We therefore do not believe that they will be more or less vulnerable to abuse than any other domain registry.

Use of Subdomain Services for Phishing

As we've tracked for the past few years, phishers make significant use of subdomain registration services to host phishing Web sites. **Malicious use of these services remained remarkably steady in the first half of 2010, and still accounts for the majority of phishing in some large TLDs**. In the first half of 2010, subdomain services hosted 6,761 phish (versus 6,734 phish in the second half of 2009, 6,441 phish in 1H2009, and the 6,339 in 2H2008). **This is significantly more than the number of maliciously registered domains names purchased by phishers at regular domain name registrars in 1H2010** (4,755). This continues to be a challenge, because only the subdomain providers themselves can effectively mitigate these phish.[11] Unfortunately, some of these services are unresponsive to complaints. We saw Avalanche phishing attacks taking advantage of subdomain resellers in limited numbers as well.

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

We have identified more than 570 subdomain registration providers, which offer services on more than 2,900 domain names. This is a space as rich as the current "regulated" domain space – each subdomain service is effectively its own "domain registry." The subdomain services have many business models, and are unregulated. 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. We are seeing some interesting changes in this market space as well. For example, many subdomain resellers

[11] Registrars or registry operators usually 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. If extensive abuse happens within a single domain, a registrar may still opt to suspend the domain based on numerous complaints. This has been observed on occasion, and could affect innocent parties with other subdomains on that domain.

now offer WHOIS services and anti-abuse support, and we've even seen "failures" of such services. Some base domains used by subdomain services appear to have been suspended for abuse, taking all the subdomains down as well.

Subdomain services remain a popular way for phishers to mount attacks. In our survey we positively identified **6,761 subdomain sites/accounts used for phishing, beneath 681 unique second-level domains.** This is nearly level from 2H2009, where we saw 6,734 subdomain sites/accounts used for phishing, beneath 658 unique second-level domains. Counting these unique subdomains as "regular" domain names, these types of domains would represent around 19% of all domains involved in phishing, and 20% of non-Avalanche phishing domains.

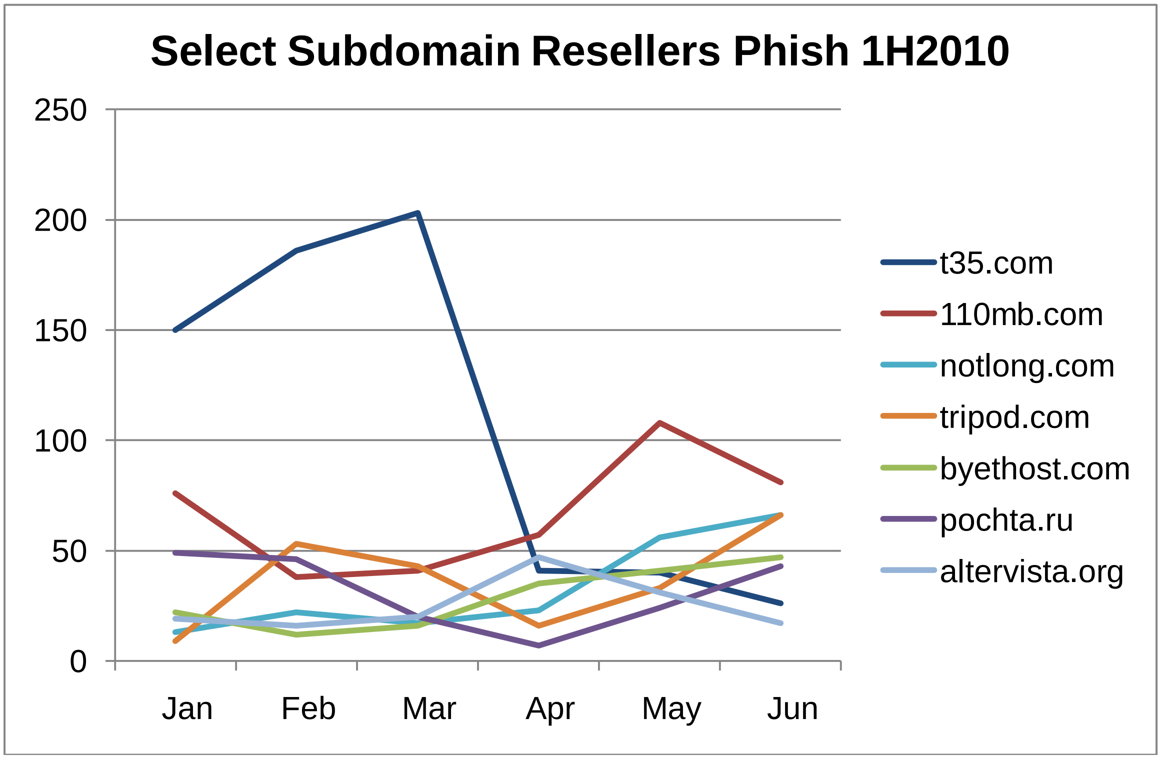
Top 20 Subdomain Services Used for Phishing 1H2010

Rank	Domain	Total Attacks	Provider
1	t35.com	646	t35.com
2	110mb.com	401	110mb.com
3	justfree.com	220	justfree.com
4	notlong.com	197	notlong.com
5	tripod.com	176	tripod.com
6	altervista.org	150	altervista.org
7	freewebhostx.com	142	freewebhostx.com
8	limewebs.com	107	limedomains.com
9	eb2a.com	100	eb2a.com
10	yourfreehosting.net	97	yourfreehosting.net
11	co.cc	89	php0h.com
12	freehostia.com	86	freehostia.com
13	50webs.com	70	50webs.com
14	hd1.com.br	66	hdfree.com.br
15	hdfree.com.br	65	hdfree.com.br
16	webcindario.com	60	webcindario.com
17	pochta.ru	54	pochta.ru
18	x10hosting.com	53	x10hosting.com
19	my3gb.com	49	my3gb.com
20	zapto.org	48	no-ip.com

Provider	Total Attacks
t35.com	646
110mb.com	401
justfree.com	220
Tripod	220

Overall, there were at least 279 different providers of subdomain registrations who had phishing subdomains on their services in the first half of 2010.

The good news for this report was that Russian free email provider Pochta.ru significantly curtailed phishing on its service, dropping to sixth place with 189 attacks in 1H2010, down from first place and 509 in 2H2009 and 822 in 1H2009. This left first place to the American provider **t35.com**, rising from second place in 2H2009. t35.com appears to have reacted—there was dramatic decrease in phishing attacks hosted on t35.com service during April 2010. Second place was occupied by 110mb.com. This provider may be heading for the top spot for the second half of 2010.



For more information about subdomain resellers and the unique challenges they pose for abuse mitigation, please see the APWG paper "Making Waves in the Phishers' Safest Harbors: Exposing the Dark Side of Subdomain Registries."[12]

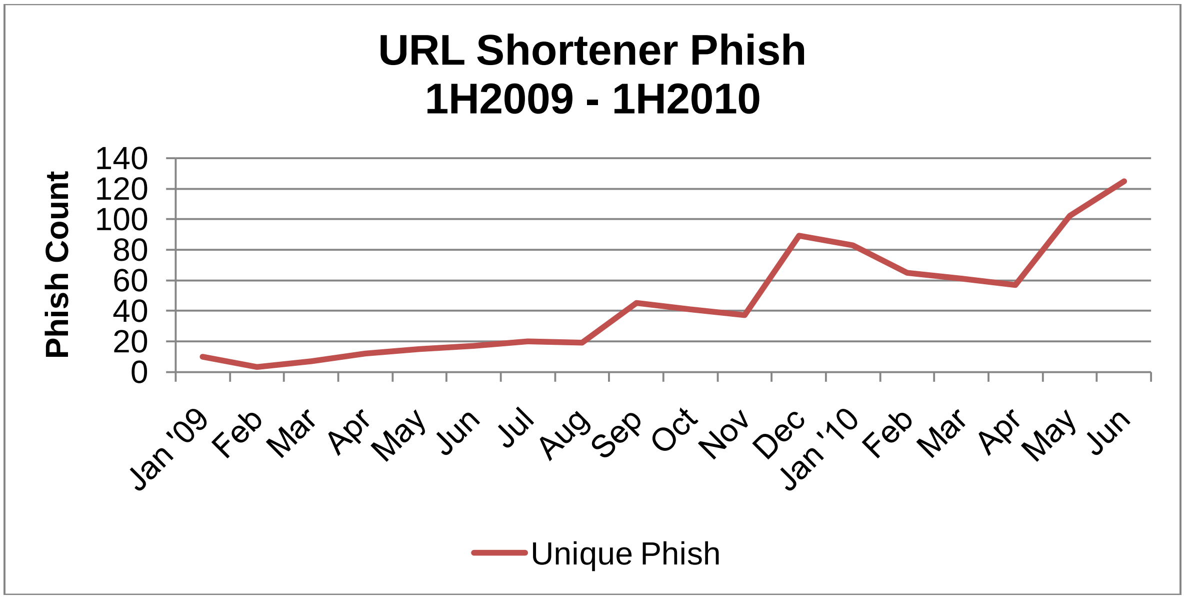
Use of Other Services for Phishing

Phishers use other tricks to get their sites onto the Internet, or to get around the spam filtering and browser-based protection mechanisms that protect users.

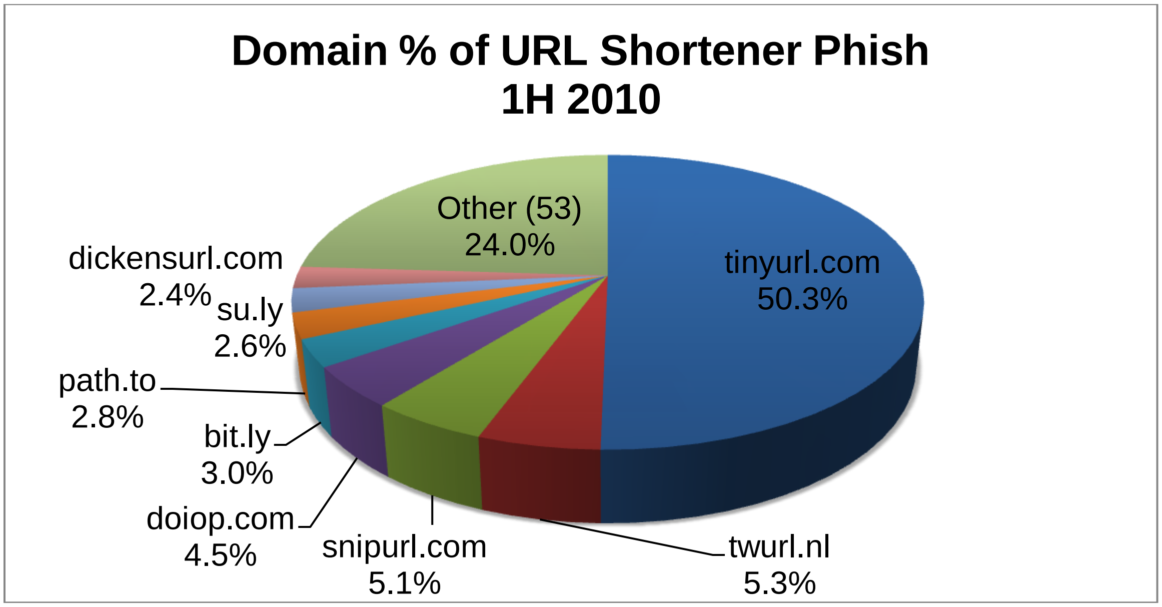
As we have reported previously, there is a continuing trend to use "URL shortening" services to obfuscate phishing URLs. Use of these URL shorteners has been driven by the popularity of Twitter and other social networking sites, and the continued shift to mobile phones and computing devices. Users of those services can obtain a very short URL to use in their limited-space posts, which automatically redirects the visitor to a much longer "hidden"

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

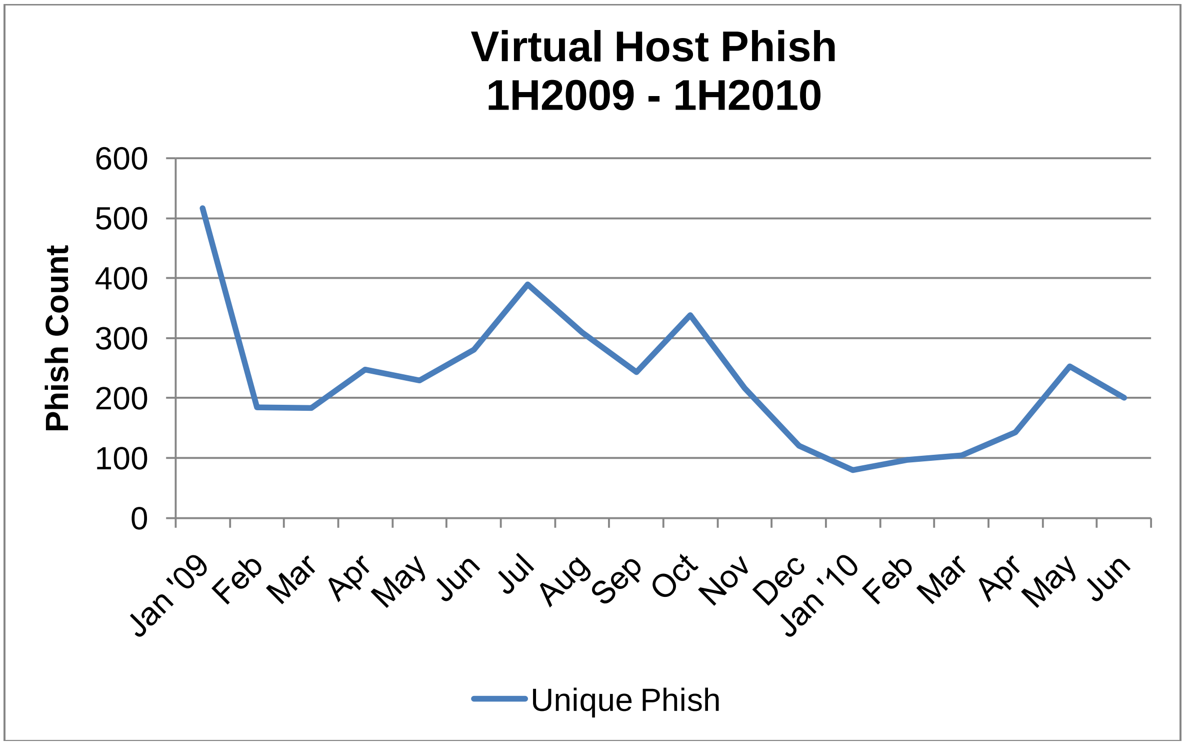
URL. This is a useful vector for abuse, since they redirect unsuspecting users to the truly malicious site based on a domain and service they are quite comfortable using.



We saw an uptick in usage of these services towards the end of 2009, and further abuse early in 2010. The absolute numbers remain small but continue to bear watching. We saw Avalanche hit these services with for malware attacks, and spammers using these services to obfuscate URLs to attempt to get past spam filters, and so we certainly will not be surprised to see phishers abusing these services more heavily. The other forms of abuse we observed on these services seemed to be successful in many cases, and imitation is almost certain to follow in the phishing world.



In past reports we also looked at how phishers have used "virtual hosting" services. These services allow Internet users to easily set up Web sites hosted on a central domain, and include providers such as Angelfire, FortuneCity.com, and multimania.co.uk. We saw a drop in attacks utilizing such services in 2009, but observed a rise and 877 attacks in 1H2010. While still not a large portion of phishing, this trend was unexpected.



Conclusions

The decreasing Avalanche uptimes in 2009 and 2010 showed that the domain name registration and response communities could make a difference by quickly suspending domain names. Avalanche has switched to distributing Zeus, but Zeus distribution also relies on the registration of domain names for spamming, drive-by-download sites, and Zeus command-and-control domains. We now wonder if domain takedown lessons are being applied to the Zeus distribution being perpetrated by Avalanche and other criminals who use the Zeus package.

Even including Avalanche's activity, the amount of phishing in the world in 1H2010 returned to the levels we observed in 2008 and early 2009, as measured by attacks and domains used. The majority of phishing continued to be concentrated in just a few namespaces overall, and the use of subdomain services was notable. We will continue to monitor the abuse of URL shortening services and subdomain services by phishers.

The average and median uptimes of phish rose in 1H2010, largely due to the disappearance of Avalanche from the phishing landscape. We are concerned, though, about the rise in phishing uptimes in 1H2010 over 2009, and we will analyze the ongoing trend in our next edition.

Appendix: Phishing Statistics and Uptimes by TLD

The column "# Total Malicious Domains Registered 1H2010" includes the number of Avalanche domains registered in 1H2010.

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
ac	Ascension Island	1	1	15,050	0.7	0.7	101:53:57	101:53:58		0		
ad	Andorra	0	0		0.0	0.0				0		
ae	United Arab Emirates	8	5	87,000	0.6	0.9	12:47:42	5:52:44		0		
aero	sponsored TLD	1	1	6,881	1.5	1.5	4:22:01	4:22:02		0		
af	Afghanistan	0	0		0.0	0.0				0		
ag	Antigua and Barbuda	0	0	15,928	0.0	0.0				0		
ai	Anguilla	0	0	2,010	0.0	0.0				0		
al	Albania	5	5	2,530	19.8	19.8	8:04:13	7:29:20		0		
am	Armenia	22	9	12,952	6.9	17.0	19:25:28	19:13:00	1	1	1	1
an	Netherlands Antilles	1	1	1,033	9.7	9.7	98:31:28	98:31:29		0		
ao	Angola	1	1	245	40.8	40.8	8:13:38	8:13:39		0		
ar	Argentina	194	128	2,101,162	0.6	0.9	61:44:49	26:07:13		0		
as	American Samoa	0	0		0.0	0.0				0		
asia	sponsored TLD	5	2	187,203	0.1	0.3	183:29:35	82:05:00		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
at	Austria	87	81	937,403	0.9	0.9	98:13:15	22:17:33		0		
au	Australia	476	345	1,730,920	2.0	2.7	64:58:20	16:38:36		0		
az	Azerbaijan	8	6	9,899	6.1	8.1	91:45:42	64:06:06		0		
ba	Bosnia and Herzegovina	8	7	10,650	6.6	7.5	41:18:22	20:03:46		0		
bd	Bangladesh	8	6	4,900	12.2	16.3	97:13:57	58:01:16		0		
be	Belgium	229	162	1,037,018	1.6	2.2	65:36:15	17:35:21	45	0	41	69
bf	Burkina Faso	1	1				4:17:33	4:17:33		0		
bg	Bulgaria	30	20	22,783	8.8	13.2	83:14:19	22:09:15		0		
bh	Bahrain	0	0		0.0	0.0				0		
biz	generic TLD	227	171	2,076,973	0.8	1.1	57:44:44	12:14:58	12	0		
bm	Bermuda	1	1	6,580	1.5	1.5	59:47:20	59:47:20		0		
bn	Brunei Darussalam	0	0	817	0.0	0.0				0		
bo	Bolivia	7	6	5,942	10.1	11.8	115:14:38	43:26:05		0		
br	Brazil	1,046	627	2,101,233	3.0	5.0	82:23:53	23:38:59	4	0		
bs	Bahamas	1	1				14:16:50	14:16:51		0		
bt	Bhutan	0	0		0.0	0.0				0		
bw	Botswana	1	1				13:16:14	13:16:15		0		
by	Belarus	12	9				99:17:17	44:49:39		0		
bz	Belize	24	10	43,533	2.3	5.5	69:52:33	21:27:51	1	0	1	2
ca	Canada	267	189	1,411,029	1.3	1.9	73:43:38	14:08:30	2	0		
cat	sponsored TLD	0	0	42,676	0.0	0.0				0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
cc	Cocos (Keeling) Islands	200	35	registry declined to provide			54:41:29	14:04:56	3		1	3
cd	Congo, Democratic Repub.	0	0		0.0	0.0				0		
cg	Congo	1	1				21:58:29	21:58:29				
ch	Switzerland	204	132	1,241,500	1.1	1.6	53:20:12	26:47:03		0		
ci	Côte d'Ivoire	1	1	1,519	6.6	6.6	2:43:36	2:43:36		0		
cl	Chile	159	111	282,526	3.9	5.6	101:31:24	26:14:09		0		
cm	Cameroon	2	2	620	32.3	32.3	7:56:11	7:56:12		0		
cn	China	162	120	7,620,043	0.2	0.2	91:51:47	14:24:29	2	0		
co	Colombia	38	27	28,000	9.6	13.6	48:03:21	15:03:48		0		
com	generic TLD	21,673	13,947	89,712,873	1.6	2.4	61:06:01	13:39:51	2,179	0	45	93
coop	sponsored TLD	2	2	6,873	2.9	2.9	9:53:04	9:53:05		0		
cr	Costa Rica	5	5	12,100	4.1	4.1	25:11:37	22:44:24		0		
cu	Cuba	2	1	2,100	4.8	9.5	103:06:43	103:06:44		0		
cx	Christmas Island	13	4	5,100	7.8	25.5	100:06:35	18:37:53		0		
cy	Cyprus	0	0	6,817	0.0	0.0				0		
cz	Czech Republic	480	207	689,813	3.0	7.0	31:26:36	8:56:48	100	1	100	252
de	Germany	737	559	13,580,111	0.4	0.5	55:18:08	15:08:37	17	0		
dj	Djibouti	0	0		0.0	0.0				0		
dk	Denmark	206	134	1,070,517	1.3	1.9	82:04:12	32:07:29		0		
dm	Dominica	0	0		0.0	0.0				0		
do	Dominican Republic	4	4	15,103	2.6	2.6	7:52:35	7:01:11		0		
dz	Algeria	3	3	1,800	16.7	16.7	13:11:00	4:21:46		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
ec	Ecuador	18	9	22,200	4.1	8.1	28:44:15	19:58:26		0		
edu	U.S. higher education	17	13				36:16:40	29:19:13		0		
ee	Estonia	17	15	78,075	1.9	2.2	54:33:50	27:59:45		0		
eg	Egypt	5	2	5,950	3.4	8.4	35:11:07	40:52:26		0		
er	Eritrea	1	1	120	83.3	83.3	4:59:38	4:59:38		0		
es	Spain	132	110	1,196,617	0.9	1.1	91:38:41	18:25:15	8	0		
et	Ethiopia	1	1				2:11:33	2:11:33		0		
eu	European Union	378	242	3,201,948	0.8	1.2	24:30:38	9:55:20	75	0	60	139
fi	Finland	28	19	225,325	0.8	1.2	42:33:36	15:49:35		0		
fj	Fiji	0	0	3,900	0.0	0.0				0		
fk	Falkland Islands	0	0		0.0	0.0				0		
fm	Micronesia, Fed. States	14	7				96:43:26	14:26:15		0		
fo	Faroe Islands	0	0		0.0	0.0				0		
fr	France	680	375	1,716,308	2.2	4.0	38:09:10	15:31:33	13	0		
gd	Grenada	6	3	3,450	8.7	17.4	17:55:59	16:08:43		0		
ge	Georgia	23	13	15,960	8.1	14.4	77:38:31	46:46:16		0		
gg	Guernsey	12	6				77:13:37	9:06:12		0		
gh	Ghana	0	0		0.0	0.0				0		
gi	Gibraltar	0	0	1,718	0.0	0.0				0		
gl	Greenland	0	0	4,239	0.0	0.0				0		
gov	U.S. government	3	1	5,000	2.0	6.0	2:13:53	1:37:10		0		
gp	Guadeloupe	4	3	1,496	20.1	26.7	18:00:03	13:45:03		0		
gr	Greece	130	93	260,000	3.6	5.0	50:34:49	13:46:18		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
gs	South Georgia & Sandwich Is.	10	3	8,154	3.7	12.3	478:02:00	216:44:01	1	1	1	2
gt	Guatemala	2	1	8,200	1.2	2.4	3:08:13	3:08:13		0		
gy	Guyana	1	1				36:07:49	36:07:49				
hk	Hong Kong	41	33	187,680	1.8	2.2	33:57:33	23:21:55		0		
hm	Heard and McDonald Is.	1	1				90:10:26	90:10:26		0		
hn	Honduras	28	15	4,015	37.4	69.7	10:50:10	12:24:28	15	37	15	28
hr	Croatia	27	18	76,500	2.4	3.5	60:40:39	33:41:34		0		
ht	Haiti	3	2	2,000	10.0	15.0	51:01:40	1:31:39	1	5		
hu	Hungary	94	73	493,000	1.5	1.9	88:27:03	19:25:42		0		
id	Indonesia	76	48				49:40:45	23:41:01		0		
ie	Ireland	102	79	145,724	5.4	7.0	56:36:00	24:07:21		0		
il	Israel	46	36	167,643	2.1	2.7	139:42:47	19:21:07		0		
im	Isle of Man	62	28	26,000	10.8	23.8	15:56:49	4:37:56	20	8	19	47
in	India	146	116	677,170	1.7	2.2	134:52:17	18:02:53	8	0	2	2
info	generic TLD	628	513	6,297,595	0.8	1.0	69:56:55	15:12:32	62	0		
io	British Indian Ocean Terr.	2	1	3,043	3.3	6.6	30:52:49	30:52:49	1	3	1	2
IP address		2,018	0	n/a			68:16:41	16:03:19		0		
iq	Iraq	0	0		0.0	0.0				0		
ir	Iran	64	41	160,982	2.5	4.0	42:29:29	22:33:24		0		
is	Iceland	8	5	30,000	1.7	2.7	52:57:46	27:26:45		0		
it	Italy	376	222	1,800,000	1.2	2.1	89:33:14	28:19:55	1	0		
je	Jersey	5	2				96:22:03	31:50:44		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
jm	Jamaica	0	0	4,975	0.0	0.0				0		
jo	Jordan	0	0	3,850	0.0	0.0				0		
jobs	sponsored TLD	0	0	33,009	0.0	0.0				0		
jp	Japan	141	85	1,164,295	0.7	1.2	51:29:02	29:05:10		0		
ke	Kenya	10	8	12,750	6.3	7.8	20:53:45	19:27:01		0		
kg	Kyrgyzstan	1	1	4,340	2.3	2.3	1:11:02	1:11:02		0		
kh	Cambodia	3	3	1,157	25.9	25.9	7:11:31	6:44:10		0		
ki	Kiribati	3	2	315	63.5	95.2	237:18:33	338:51:46		0		
kr	Korea	2,888	989	1,079,298	9.2	26.8	25:20:23	9:57:48	616	6	616	2,137
kw	Kuwait	2	1	2,250	4.4	8.9	344:20:32	344:20:33		0		
ky	Cayman Islands	0	0	6,760	0.0	0.0				0		
kz	Kazakhstan	21	15	42,027	3.6	5.0	51:39:41	17:20:20	1	0		
la	Lao People's Demo. Rep.	23	9				58:22:01	6:11:48	2		2	3
lb	Lebanon	4	2	3,050	6.6	13.1	36:58:18	39:37:21		0		
lc	St. Lucia	4	4	1,977	20.2	20.2	79:43:16	72:28:08		0		
li	Liechtenstein	5	3	61,060	0.5	0.8	28:57:14	25:52:23		0		
lk	Sri Lanka	7	3	6,415	4.7	10.9	9:55:39	6:13:57		0		
lt	Lithuania	15	13	115,298	1.1	1.3	73:20:46	6:14:45		0		
lu	Luxembourg	17	12	52,350	2.3	3.2	87:49:57	21:19:44		0		
lv	Latvia	35	22	81,759	2.7	4.3	66:22:40	18:08:30		0		
ly	Libya	30	3	8,408	3.6	35.7	16:33:19	5:43:40		0		
ma	Morocco	42	20	35,824	5.6	11.7	82:23:11	14:46:35		0		
mc	Monaco	1	1	1,680	6.0	6.0	34:15:24	34:15:25		0		
md	Moldova	16	16				23:38:59	9:44:35	15		15	15
me	Montenegro	37	29	402,177	0.7	0.9	63:13:42	11:17:01	5	0	1	2

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
mg	Madagascar	1	1				0:12:55	0:12:55		0		
mk	Macedonia	8	7				8:03:16	5:51:12		0		
ml	Mali	1	1				29:01:40	29:01:40		0		
mn	Mongolia	22	11	7,428	14.8	29.6	49:36:44	9:45:09	2	3	2	2
mo	Macao	0	0		0.0	0.0				0		
mobi	sponsored TLD	24	20	970,693	0.2	0.2	48:31:00	7:39:55	6	0	1	1
mp	Northern Mariana Islands	2					6:16:17	6:16:17				
mr	Mauritania	0	0		0.0	0.0				0		
ms	Montserrat	3	3	12,209	2.5	2.5	51:04:03	26:43:46		0		
mt	Malta	0	0	11,750	0.0	0.0				0		
mu	Mauritius	4	4	7,500	5.3	5.3	44:57:41	20:06:53		0		
museum	sponsored TLD	0	0	556	0.0	0.0				0		
mx	Mexico	111	80	420,556	1.9	2.6	49:35:36	14:59:11	2	0		
my	Malaysia	61	39	99,736	3.9	6.1	55:33:09	17:20:57		0		
mz	Mozambique	0	0	1,850	0.0	0.0				0		
na	Namibia	2					38:28:44	38:28:44				
name	generic TLD	17	14	245,326	0.6	0.7	46:22:45	11:39:41	2	0		
nc	New Caledonia	3	2				11:07:41	12:54:31		0		
net	generic TLD	3,260	2,132	13,424,274	1.6	2.4	67:59:27	14:03:44	337	0	23	42
nf	Norfolk Island	2	1	5,000	2.0	4.0	2:18:07	2:18:07		0		
ng	Nigeria	4	3	1,350	22.2	29.6	396:41:59	88:16:33		0		
ni	Nicaragua	1	1	5,475	1.8	1.8	21:58:50	21:58:50		0		
nl	Netherlands	496	377	3,902,356	1.0	1.3	53:43:24	16:28:37		0		
no	Norway	101	67	473,575	1.4	2.1	73:43:50	23:35:37		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
np	Nepal	17	11	21,272	5.2	8.0	26:20:37	25:18:32		0		
nr	Nauru	4	2	445	44.9	89.9	179:12:54	14:47:11		0		
nu	Niue	35	18				62:51:59	24:28:25	1		1	1
nz	New Zealand	106	61	399,151	1.5	2.7	71:24:26	8:37:02	9	0	9	34
org	generic TLD	2,199	1,469	8,354,701	1.8	2.6	46:39:14	13:01:58	106	0	5	10
pa	Panama	0	0		0.0	0.0				0		
pe	Peru	37	21	42,375	5.0	8.7	76:09:19	51:28:01	1	0		
pf	French Polynesia	1	1				79:16:39	79:16:39		0		
ph	Philippines	12	12	registry declined to provide			16:55:36	5:46:57		0		
pk	Pakistan	32	21	registry declined to provide			60:47:27	20:13:25		0		
pl	Poland	1,582	744	1,805,894	4.1	8.8	41:01:06	16:53:53	368	2	368	871
pn	Pitcairn	17	7	877	79.8	193.8	115:17:42	4:17:42		0		
pro	sponsored TLD	3	2	46,381	0.4	0.6	11:15:13	10:14:11		0		
ps	Palestinian Territory	9	8	5,150	15.5	17.5	108:11:46	57:39:22		0		
pt	Portugal	67	51	313,044	1.6	2.1	82:46:52	15:16:31		0		
py	Paraguay	3	3	10,496	2.9	2.9	6:39:18	6:30:45		0		
qa	Qatar	0	0		0.0	0.0				0		
re	Réunion	1	1	5,500	1.8	1.8	16:16:15	16:16:16		0		
ro	Romania	324	156	443,700	3.5	7.3	55:49:51	12:13:44	2	0		
rs	Serbia	13	10	56,000	1.8	2.3	24:54:37	8:08:58		0		
ru	Russian Fed.	1,085	516	2,797,837	1.8	3.9	59:32:17	15:09:34	16	0	5	6
rw	Rwanda	2					17:45:56	17:45:56				
sa	Saudi Arabia	7	6	18,868	3.2	3.7	62:15:18	20:31:13		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
sc	Seychelles	17	11	6,415	17.1	26.5	48:14:25	13:24:32	10	16	8	14
sd	Sudan	2					30:34:50	30:34:50				
se	Sweden	76	59	962,360	0.6	0.8	57:34:43	21:36:57		0		
sg	Singapore	52	27	116,439	2.3	4.5	46:42:22	22:37:32		0		
sh	Saint Helena	4	4	2,900	13.8	13.8	5:18:13	5:09:46	3	10	3	3
si	Slovenia	23	18	78,099	2.3	2.9	107:21:34	34:52:33		0		
sk	Slovakia	57	35	213,045	1.6	2.7	56:50:58	17:17:55		0		
sl	Sierra Leone	0	0	700	0.0	0.0				0		
sm	San Marino	0	0	1,900	0.0	0.0				0		
sn	Senegal	2	2				31:37:11	31:37:12		0		
st	Sao Tome and Principe	8	4				727:05:02	331:15:26		0		
su	Soviet Union	62	15	93,491	1.6	6.6	31:31:35	8:48:09		0		
sv	El Salvador	0	0	4,650	0.0	0.0				0		
sy	Syria	0	0		0.0	0.0				0		
sz	Swaziland	1	1				8:17:23	8:17:23				
tc	Turks and Caicos	36	22				177:54:43	19:09:07	3		3	3
tel	generic TLD	0	0	287,755	0.0	0.0				0		
tf	French Southern Territories	54	14				57:21:54	28:22:24		0		
tg	Togo	1	1				45:25:53	45:25:53		0		
th	Thailand	86	62	49,000	12.7	17.6	190:31:46	39:33:32		0		
tj	Tajikistan	0	0	18,600	0.0	0.0				0		
tk	Tokelau	352	336				32:04:54	11:52:38	336		1	1
tl	Timor-Leste	13	6	1,800	33.3	72.2	33:06:27	9:34:39		0		
tm	Turkmenistan	1	1	3,650	2.7	2.7	9:13:32	9:13:32		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
tn	Tunisia	0	0	50	0.0	0.0				0		
to	Tonga	75	23	13,300	17.3	56.4	104:05:18	8:13:38		0		
tp	Portuguese Timor	10	6				72:01:45	15:32:27		0		
tr	Turkey	40	35	220,000	1.6	1.8	112:49:17	25:07:59		0		
travel	sponsored TLD	1	1	43,488	0.2	0.2	6:13:38	6:13:39		0		
tt	Trinidad and Tobago	23	3	2,200	13.6	104.5	4:14:12	2:59:33		0		
tv	Tuvalu	68	49	registry declined to provide			30:39:33	5:33:12	10		10	20
tw	Taiwan	121	85	449,332	1.9	2.7	54:25:46	13:30:54		0		
tz	Tanzania	0	0		0.0	0.0				0		
ua	Ukraine	118	87	507,603	1.7	2.3	67:50:06	14:16:09		0		
ug	Uganda	2	2	3,258	6.1	6.1	28:08:17	28:08:17		0		
uk	United Kingdom	1,453	864	8,582,295	1.0	1.7	41:39:34	13:15:21	199	0	155	273
us	United States	197	147	1,657,480	0.9	1.2	42:18:11	15:27:58	20	0		
uy	Uruguay	15	10	25,353	3.9	5.9	21:34:09	20:30:16		0		
uz	Uzbekistan	4	2	10,480	1.9	3.8	116:35:28	117:42:36		0		
vc	St. Vincent and Grenadines	196	110	6,112	180.0	320.7	17:24:30	8:53:03	107	175	106	191
ve	Venezuela	23	22	145,761	1.5	1.6	70:27:09	21:20:20		0		
vg	British Virgin Islands	10	4	8,300	4.8	12.0	118:24:28	18:01:46		0		
vi	Virgin Islands	0	0	1,000	0.0	0.0				0		
vn	Vietnam	64	48	153,002	3.1	4.2	41:48:03	17:28:57	1	0		
vu	Vanuatu	7	3				114:59:47	14:21:37		0		

TLD	TLD Location	# Unique phishing attacks 1H2010	Unique Domain Names used for phishing 1H2010	Domains in registry May 2010	Score: Phish per 10,000 domains 1H2010	Score: Attacks per 10,000 domains 1H2010	Average Uptime 1H2010 hh:mm:ss	Median Uptime 1H2010 hh:mm:ss	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry	AVALANCHE Domains Registered 1H2010	AVALANCHE Attacks 1H2010
ws	Samoa	48	27	544,443	0.5	0.9	46:46:38	20:58:37	4	0	3	3
ye	Yemen	0	0	750	0.0	0.0				0		
yu	Yugoslavia (TLD deprecated 30 March 2010)	0	0	0	0.0	0.0				0		
za	South Africa	164	132	581,453	2.3	2.8	36:07:10	15:12:19		0		
zm	Zambia	0	0		0.0	0.0				0		
zw	Zimbabwe	2	2	10,148	2.0	2.0	6:17:29	6:17:29		0		
	TOTALS	**48,244**	**28,646**	**194,824,747**					**4,755**		**1,624**	**4,272**

About the Authors & Acknowledgments

The authors wish to thank the following for their support: Peter Cassidy, Foy Shiver, Dave Jevans, and Laura Mather of the APWG; and Ram Mohan and Bruce Reeser of Afilias. 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. Aaron Routt of Internet Identity performed data analysis to support this paper, and designed the charts and graphs.

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, it's Registration Abuse Policy Working Group (RAPWG), and is co-chairing a special ICANN working group looking into provision of zone file access for new gTLDs. 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.

Greg Aaron is Director of Key Account Management and Domain Security at Afilias (www.afilias.info). Greg oversees .INFO operations and Afilias' security programs, including domain name abuse policy and practices, and Afilias also provides anti-abuse services to the .ORG registry. Greg is an authority on the use of domain names for e-crime, and works with registrars, registries, law enforcement, and researchers regarding phishing, malware, spam, and child pornography cases. He was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG), and served on ICANN's Fast-Flux Working Group. Greg also serves on the Steering Committee of the Anti-Phishing Working Group (APWG). Greg has advised governments, ccTLD operators, and ICANN regarding registry policies and operations, and he oversaw the launches of the .MOBI, .IN, and .ME TLDs. He also has significant experience with Sunrises and Internationalized Domain Names (IDNs). Greg is a magna cum laude graduate of the University of Pennsylvania.

#