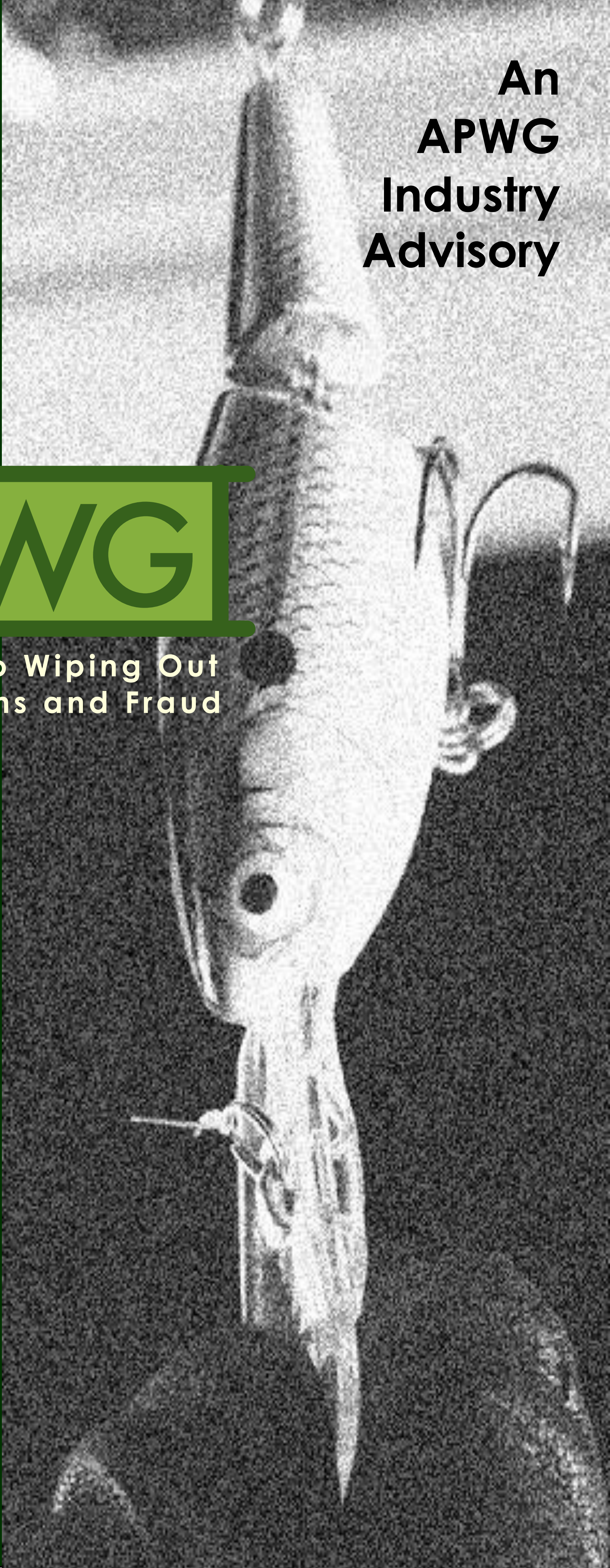
Global Phishing Survey: Trends and Domain Name Use in 2H2009

An APWG Industry Advisory



Committed to Wiping Out Internet Scams and Fraud

Spring edition
May 2010

Authors:

Greg Aaron
Afilias
<gaaron at afilias.info>

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

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

Phishing has always been attractive to criminals because it has low start-up costs and few barriers to entry. But by mid-2009, phishing was dominated by one player as never before—the "Avalanche" phishing operation. This criminal entity is one of the most sophisticated and damaging on the Internet, and perfected a mass-production system for deploying phishing sites and "crimeware" – malware designed specifically to automate identity theft and facilitate unauthorized transactions from consumer bank accounts. **Avalanche was responsible for two-thirds (66%) of all phishing attacks launched in the second half of 2009, and was responsible for the overall increase in phishing attacks recorded across the Internet.**

The statistics also show that **phishing remained highly localized in certain Internet namespaces, and that some anti-phishing measures had noticeable impacts.** While phishing remains a damaging phenomenon involving many millions of dollars in losses, the increasingly "concentrated" nature of much phishing offers some opportunities for improved response and mitigation.

This report seeks to understand such trends by quantifying 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 second half of 2009 ("2H2009", or July 1, 2009 through December 31 2009). The data was collected by the Anti-Phishing Working Group, 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 was responsible for two-thirds of all phishing attacks launched in 2H2009.** *(Page 5)* Avalanche successfully targeted vulnerable or non-responsive domain name registrars and registries. However, Avalanche changed its activities significantly in November 2009, and as of this writing has a different *modus operandi* and greatly reduced scale. *(Page 9)*
2. **In 2H2009, the average uptime of all phishing attacks continued to drop from previous periods.** *(Page 11)* Some of this improvement is due to the attention that Avalanche phishing received from the response community. The average uptime for Avalanche domains was less than half of that for non-Avalanche domains. Unfortunately, non-Avalanche phish stayed up noticeably longer in 2H2009 than they did in 1H2009.
3. **The amount of Internet domain names and numbers used for phishing has remained fairly steady** over the past two-and-one-half years, a period in which the number of registered domain names in the world has grown. *(Page 15)*

[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:
1H2009: http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf
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

4. **The great majority of phishing continued to be concentrated in certain namespaces -- just five top-level domains (TLDs)**. *(Page 15)*
5. **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 19)*
6. **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 20)*

Basic Statistics

Millions of phishing URLs were reported in 2H2009, but the number of unique phishing attacks and domain names used to host them is much smaller.[2] The 2H2009 data set yields the following statistics:

- **There were at least 126,697 phishing attacks. This is more than double the 55,698 attacks we recorded in 1H2009.** 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 increase in attacks was attributable to the Avalanche phishing gang.
- The attacks occurred on **28,775 unique domain names.**[3] **This is steadily down** from the 30,131 observed in 1H2009 and the 30,454 in 2H2008. During 2009, the number of registered domain names in the world grew from 179 million to 192 million.[4]
- In addition, phish were detected on **2,031 unique IP addresses, rather than on domain names.** (For example: http://96.56.84.42/ClientHelp/ssl/index.htm.) **This is down significantly** from the 3,563 in 1H2009 and the 2,809 in 2H2008. Phishing on IPv6 addresses remained 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 declined slightly over the past three years.**
- Of the 28,775 phishing domains, **we identified 6,372 that we believe were registered maliciously, by the phishers. Of those, 4,141 (66%) were registered by Avalanche.** Virtually all of the other 22,403 domains were hacked or compromised on

[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 it registers.
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 TL

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

vulnerable Web hosting. Malicious registrations apparently took place in just 51 TLDs.

- **Phishing remains highly concentrated in certain namespaces.** 76% of the attacks occurred in just four TLDs: .COM, .EU, .NET, and .UK. And 88% of the malicious domain registrations were made in just 5 TLDs: .BE, .COM, .EU, .NET, .EU, and .UK.
- **Only about 3.6% of all domain names that were used for phishing contain a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations" below.)
- Only 12 of the 28,775 domain names we studied were IDNs. See "Use of Internationalized Domain Names" below for more details.

Basic Statistics

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

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.

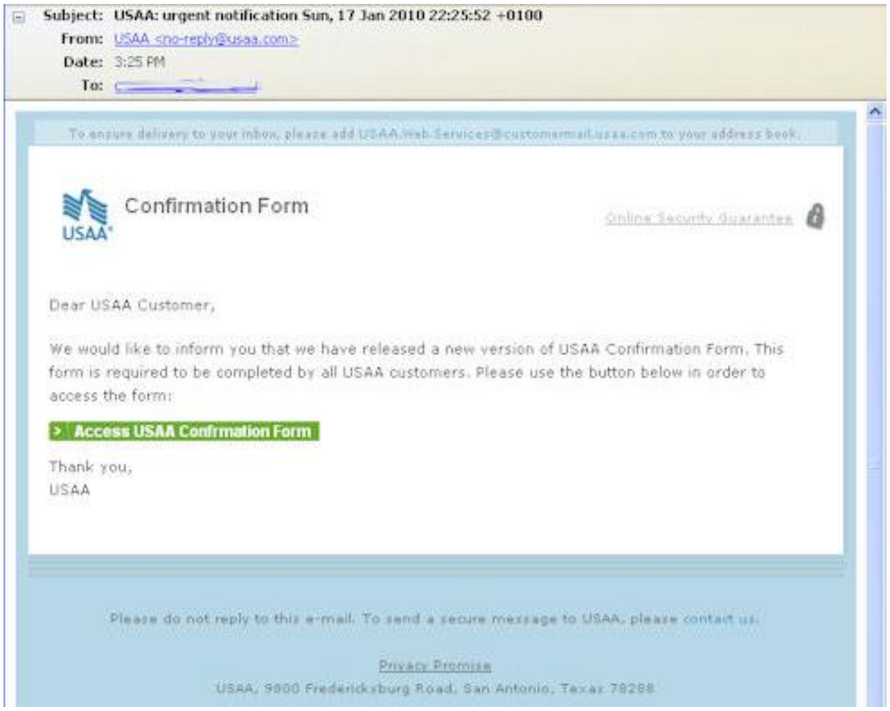
Avalanche Attacks

"Avalanche" is the name given to the world's most prolific phishing gang, and to the infrastructure it uses to host phishing sites. This criminal enterprise perfected a system for deploying mass-produced phishing sites, and for distributing malware that gives the gang additional capabilities for theft. Avalanche accounted for an incredible two-thirds of all the phishing attacks seen during 2H2009 (84,250 out of 126,697). During that time, it targeted the more than 40 major financial institutions, online services, and job search providers. The sheer volume of Avalanche attacks dominates some of our metrics, and makes it difficult or less useful to compare some metrics over time. Avalanche also changed significantly in late 2009, launching far fewer attacks. Avalanche's activities therefore deserve special examination.

There are indications that Avalanche is a successor to the "Rock Phish" criminal operation, which was very prolific and successful from 2006 into the summer of 2008, when its activities ceased. The Rock was the first to bring significant scale and automation to phishing. The Rock registered domain names regularly and in large numbers, used fast-flux hosting to support its phishing Web sites and extend their uptimes, and usually placed about six discrete phishing attacks on each domain name.

Avalanche was first seen in December 2008, and was responsible for 24% of the phishing attacks recorded in 1H2009. Avalanche uses the Rock's techniques but improved upon them, introducing greater volume and sophistication. Avalanche domains are hosted on a botnet comprised of compromised consumer-level computers.[5] **This "fast-flux" hosting makes mitigation efforts more difficult – there is no ISP or hosting provider who has control of the hosting and can take the phishing pages down, and the domain name itself must be suspended by the domain registrar or registry.**

In 2H2009, a typical Avalanche domain often hosted around 40 separate attacks at a time. (So while the number of Avalanche attacks was enormous, Avalanche domains were only about 14% of all domains used for phishing.) If an Avalanche domain remained active over a long period of time, the gang sometimes placed new phish on that domain and advertised the new target via spam.



Subject: USAA: urgent notification Sun, 17 Jan 2010 22:25:52 +0100
From: USAA <no-reply@usaa.com>
Date: 3:25 PM
To: [redacted]

To ensure delivery to your inbox, please add USAA.Web.Services@customermail.usaa.com to your address book.

Confirmation Form

Online Security Guarantee

Dear USAA Customer,

We would like to inform you that we have released a new version of USAA Confirmation Form. This form is required to be completed by all USAA customers. Please use the button below in order to access the form:

Thank you,
USAA

Please do not reply to this e-mail. To send a secure message to USAA, please contact us.

Privacy Promise

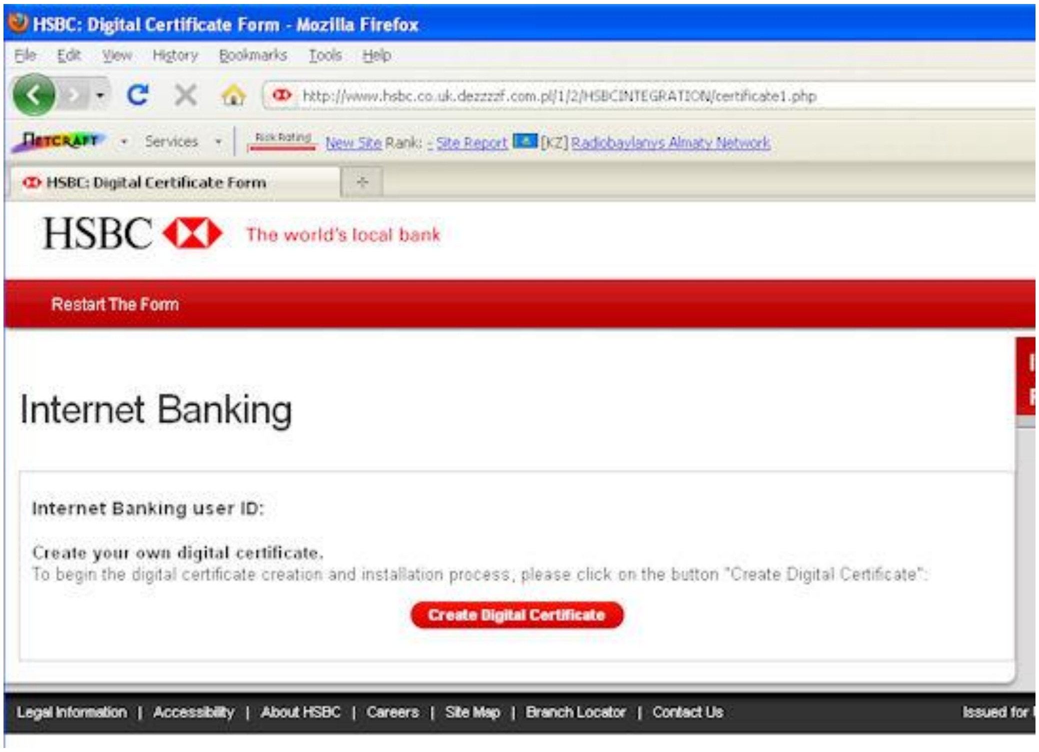
USAA, 9800 Fredericksburg Road, San Antonio, Texas 78288

A typical Avalanche phishing lure e-mail.

In addition, the criminals used the Avalanche infrastructure to distribute the notorious Zeus Trojan, a sophisticated piece of malware that the criminals incorporated into its phishing and spamming campaigns. Zeus is *crimeware* – malware designed specifically to

[5] For a description of the Avalanche botnet and the associated spamming and malware, please see: http://www.phishlabs.com/blog/archives/163

automate identity theft and facilitate unauthorized transactions. Potential victims are sent phishing-like lures that purport to offer popular software upgrades, file sharing services, and downloadable forms from tax authorities (such as the Internal Revenue Service in the United States, and Her Majesty's Revenue & Customs service in the United Kingdom). If a recipient takes this bait and his or her computer is infected, the criminals can remotely access that machine, steal the personal information stored on it, and intercept passwords and online transactions. The criminals can even log into a victim's machine to perform online banking transactions using the victim's own account details. This is difficult for the banks to detect as fraud. This combination of phishing and malware, advertised by spam, became one of the most insidious combinations on the Internet.



HSBC: Digital Certificate Form - Mozilla Firefox

http://www.hsbc.co.uk.dezzzzf.com.pl/1/2/HSBCINTEGRATION/certificate1.php

HSBC: Digital Certificate Form

Internet Banking

Internet Banking user ID:

Create your own digital certificate.
To begin the digital certificate creation and installation process, please click on the button "Create Digital Certificate":

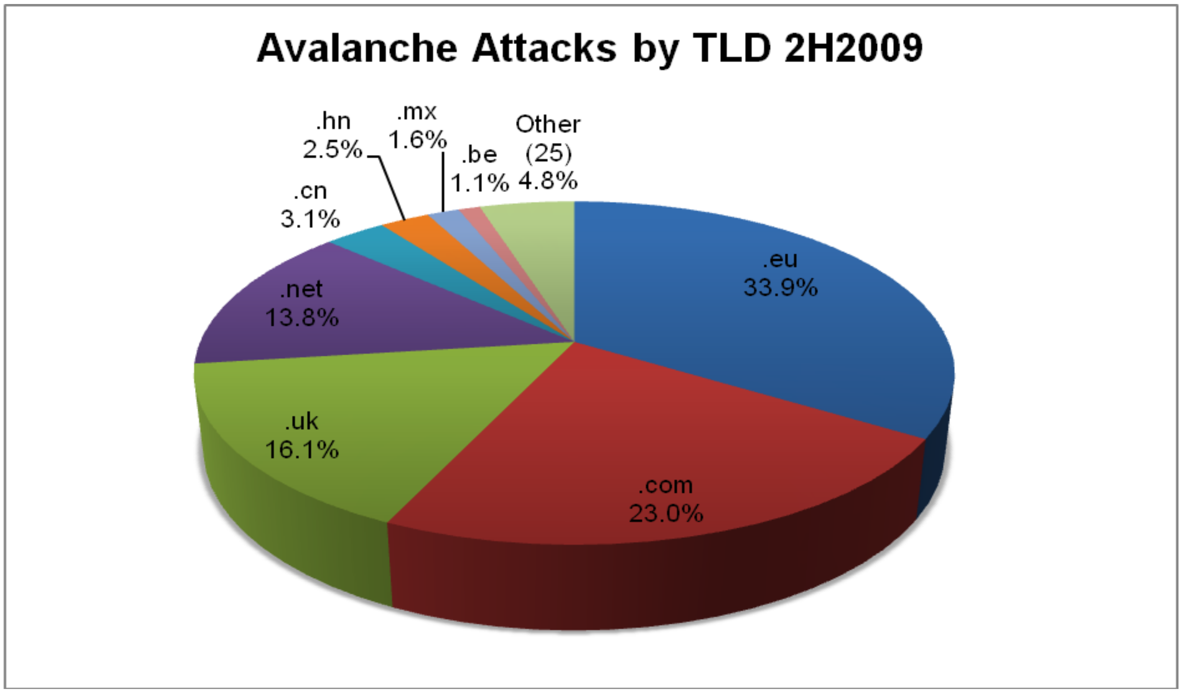
File Edit View History Bookmarks Tools Help
NETCRAFT
Services
Risk Rating
New Site Rank: - Site Report
[KZ] Radiobaylanys Almaty Network
HSBC
The world's local bank
Restart The Form
Create Digital Certificate
Legal Information | Accessibility | About HSBC | Careers | Site Map | Branch Locator | Contact Us
Issued for

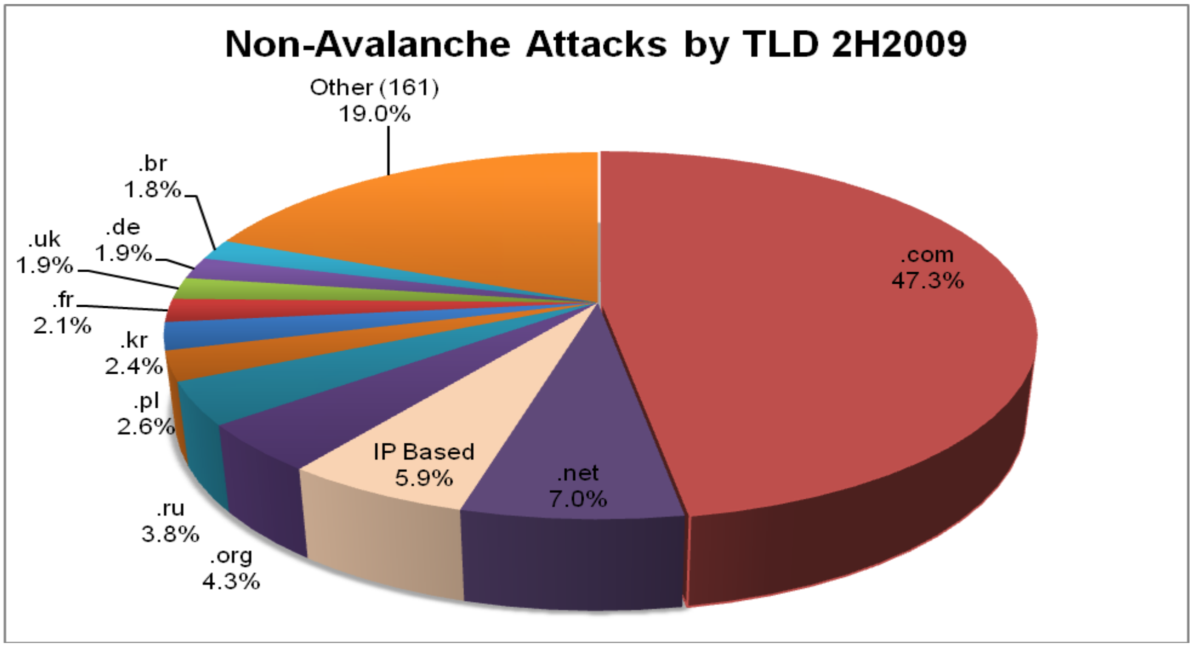
A page from an Avalanche phishing site. Clicking on the "Create Digital Certificate" button would download the Zeus trojan to the victim's computer.

An Avalanche attack campaign utilizes a set of domain names that appear almost identical each other (such as 11f1iili.com, 11t1jtiil.com, 11t1kt1il.com, and 11t1kt1pl.com). These domain name sets are therefore distinctive, and recognizable to those who are looking for them. When setting up an attack, Avalanche registered domains at one to three registrars or resellers. The gang often targets a small number of other registrars, testing to see if those registrars notice. If one registrar starts to quickly suspend the domains or implements other security procedures, the criminals simply move on to other vulnerable registrars. One unresponsive or vulnerable registrar can become a gateway for ongoing abuse. ICANN issued an alert about the Avalanche attacks on October 2, 2009[6], and this education made some registrars feel more comfortable about responding.

[6] http://www.icann.org/en/security/sa-2009-0002.htm

Avalanche did the same with top-level domains, continually registering in TLDs where the domains were not taken down expeditiously enough. Avalanche used domains in 33 TLDs in 2H2009, but in 2009 much of its activity took place in a few large TLDs, notably .BE, .COM, .EU, and .UK. (For example, Avalanche registered 645 .EU names in 1H2009, and increased that to 1,044 .EU names in 2H2009.) Domain takedowns in those hard-hit large TLDs depended mostly or entirely on the registrars.





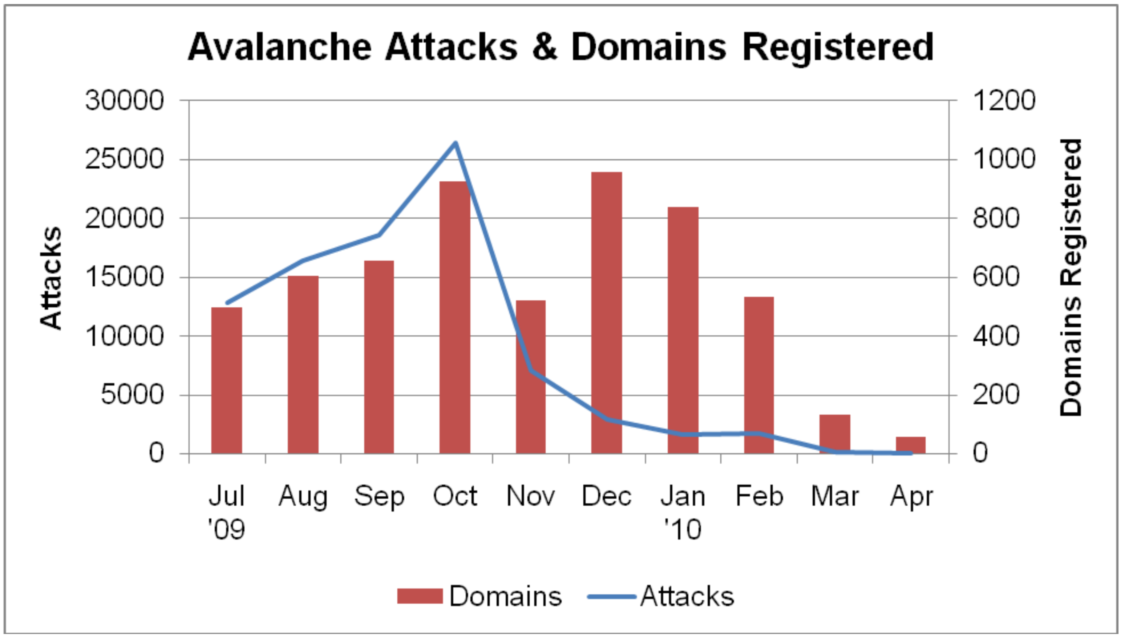
Other registries such as .BIZ, .HK, .INFO, and .ORG were almost untouched by Avalanche in 2H2009, probably because they had previously mounted effective defenses and made themselves unappealing targets. Those registries monitor for outbreaks and communicate them to their registrars, and are also willing to suspend domain names when a registrar is ineffective at doing so. Some other large, commonly available TLDs have not been used by Avalanche, for unknown reasons.

We saw several registries and registrars around the world update their anti-abuse procedures because of voluminous Avalanche attacks. For example, Nominet, the .UK registry, instituted outreach programs to registrars and now offers a new "phishing lock" status to make relevant domain suspensions easier for registrars.

Several smaller registries also responded effectively to Avalanche attacks in 2H2009. For example, the Honduran (.HN) domain registry was alerted as attacks hosted on .HN domains ramped up in July 2009. The registry worked with the affected registrar alertly until Avalanche moved away a week later. The Isle of Man (.IM) registry also worked effectively and is willing to suspended malicious registrations, and .IM has been touched by Avalanche only intermittently.

Because they were so damaging, prevalent, and recognizable, Avalanche attacks received concentrated attention from the response community. During an Avalanche campaign, it was not unusual for the target institutions, the relevant domain name registrar(s), a domain name registry, and other responders and service providers to all be aware of the campaign and working on mitigation at the same time. **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.** Despite this, the attacks were obviously profitable, and they continued in volume.

In mid-November 2009, members of the security community affected a temporary shut-down of the Avalanche botnet infrastructure. This lasted about a week before the criminals behind the attacks re-established their network. **After this event, Avalanche's activities changed significantly:**



Avalanche domain registrations hit a high in December 2009, but by then Avalanche was hosting fewer and fewer attacks overall. By March 2010, Avalanche was hosting only one phishing attack on each domain it registered, and **attacks dwindled to just 59 in the month of April 2010:**

Month	Attacks	Domains
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	1,654	839
February 2010	1,784	532
March 2010	133	133
April 2010	59	59

The old Rock Phish operation became quiescent in the summer of 2008, only to be re-born a few months later as the even worse Avalanche. As of this writing, Avalanche has dwindled to a shadow of its former self. Will Avalanche fade for good, or will it too be reborn as something new?

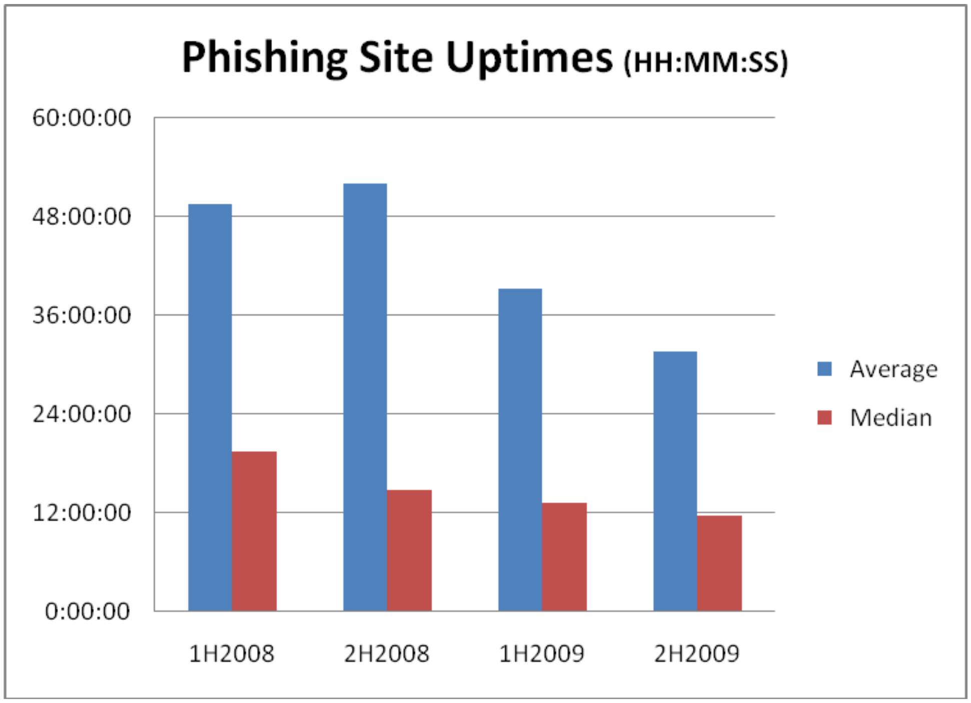
Phishing By Uptime

The average uptimes of phishing attacks has fallen steadily, and reached a notable low in 2H2009. This is a welcome trend attributable to mitigation efforts by the response community.

The "uptimes" or "live" times[7] 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.

[7] 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 overall trend is quite encouraging:



ALL PHISH, ALL TLDs	Average (HH:MM:SS)	Median (HH:MM:SS)
July 2009	43:53:24	13:49:19
Aug 2009	35:50:53	14:31:35
Sept 2009	30:06:14	12:07:14
Oct 2009	16:59:37	8:18:35
Nov 2009	34:57:35	11:46:49
Dec 2009	42:42:41	13:05:25
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

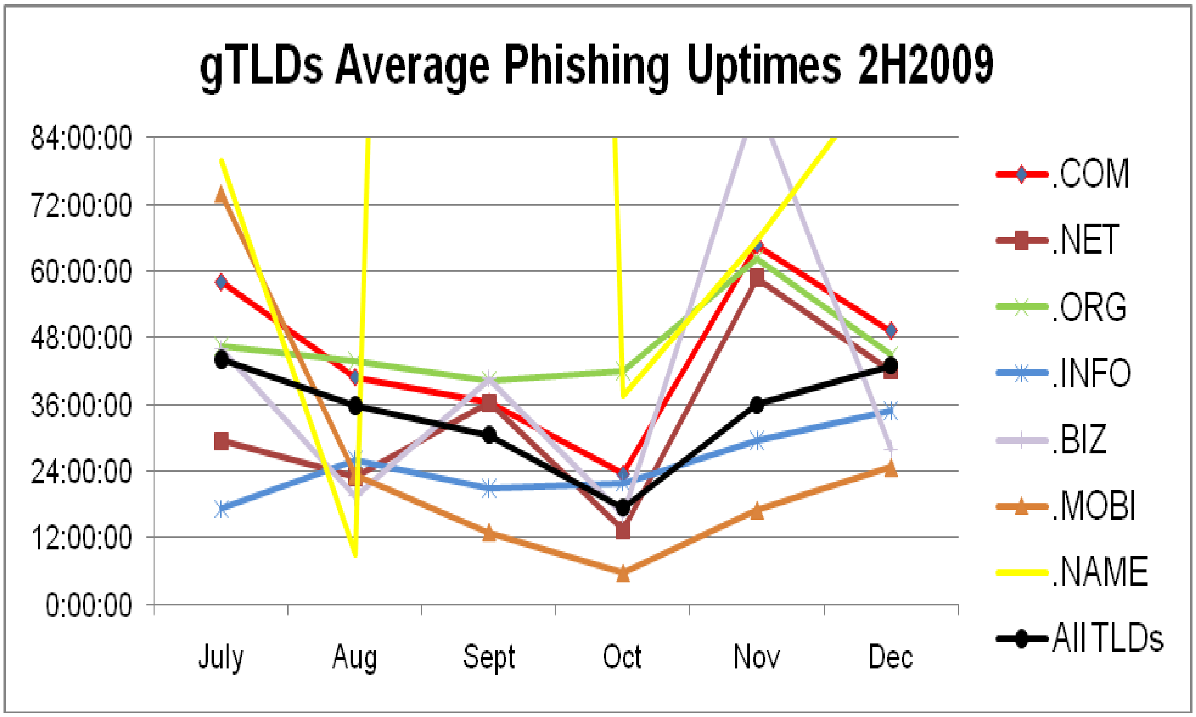
The median has fallen remarkably over the past two years, from 19 hours 30 minutes in 1H2008 to 11 hours 44 minutes in 2H2009. Early 2008 was the heyday of the Rock Phish gang, which used a fast-flux botnet to extend the uptimes of its phish. Avalanche also used fast-flux, but Avalanche phishing sites came down much faster on average. As noted previously, Avalanche attacks tended to be mitigated more quickly, and in batches. **This points to some improved awareness and responsiveness by domain name registrars and registries, which are the parties that can suspend Avalanche's domain names.**

Notably, the average uptime for Avalanche domains was less than half of that for non-Avalanche domains. On the other hand, non-Avalanche phish stayed up noticeably longer in 2H2009 than they did in 1H2009:

	Average	Median
Avalanche 2H2009	15:35:51	10:32:35
Non-Avalanche 2H2009	63:27:46	17:49:01
Non-Avalanche 1H2009	45:36:00	14:03:00

This raises the possibility that responders concentrated their resources on Avalanche, and less on smaller phishers.

The uptimes for all phishing attacks in 2H2009, and for phish in some large TLDs, were as follows:



Uptimes: All Phish

ALL PHISH 2H2009	Average (HH:MM:SS)	Median (HH:MM:SS)
ALL TLDs	**31:38:00**	**11:44:15**
.COM	42:15:40	12:11:33
.NET	24:58:25	13:12:35
.ORG	46:39:50	14:26:16
.INFO	23:51:09	9:23:14
.BIZ	38:38:03	11:28:56
.UK	15:41:22	10:55:04
.CN	15:32:32	4:52:35
.EU	15:59:18	10:55:38
.RU	54:34:19	17:35:25
.BE	15:11:00	10:15:08

Uptimes: Avalanche Phish Only

AVALANCHE ONLY 2H2009	Average (HH:MM:SS)	Median (HH:MM:SS)
ALL TLDs	**15:35:51**	**10:32:35**
.COM	31:16:11	9:56:20
.NET	33:33:02	12:45:49
.ORG	6:10:13	3:57:42
.INFO	7:27:49	1:54:52
.BIZ	5:54:23	3:49:59
.UK	27:30:47	10:46:58
.CN	23:57:27	4:31:17
.EU	31:14:18	10:55:06
.RU	n/a	n/a
.BE	21:02:04	10:04:14

Uptimes: Non-Avalanche Phish Only

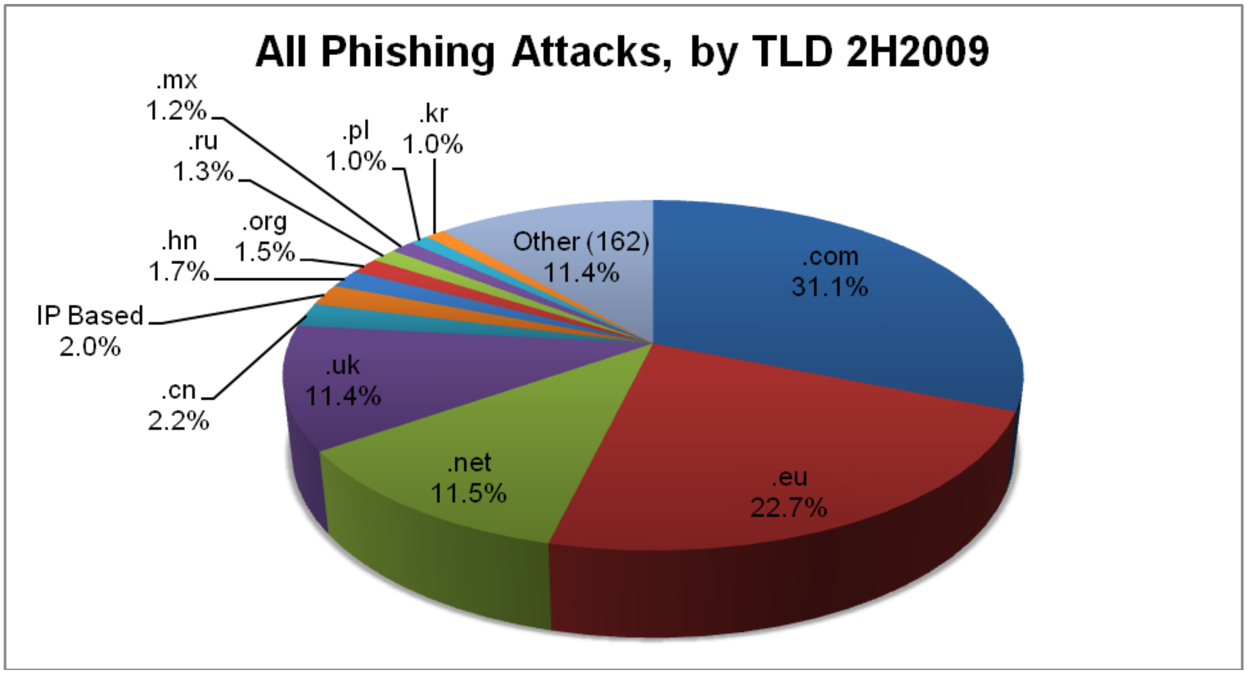
NON-AVALANCHE 2H2009	Average (HH:MM:SS)	Median (HH:MM:SS)
ALL TLDs	**63:27:46**	**17:49:03**
.COM	68:01:58	16:01:04
.NET	57:25:30	17:50:39
.ORG	47:58:05	15:23:57
.INFO	26:47:04	9:59:32
.BIZ	44:54:25	17:14:57
.UK	47:44:12	18:39:37
.CN	64:38:27	18:50:41
.EU	56:36:46	22:39:52
.RU	54:34:19	17:35:25
.BE	36:54:44	20:25:49

Prevalence of Phishing by Top-Level Domain (TLD)

We analyzed the 28,775 phishing domains to see how many fell into which 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 191,771,389 domain names overall. [8]

The great majority of phishing continues to be concentrated in just a few namespaces. 76% of all phishing attacks occurred in just four TLDs: .COM, .EU, .NET, and .UK:

[8] For the purposes of this study, we used the number of domain names in each registry as of the end of November 2009. 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"[9] 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 into 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 2.9**, the same as in 1H2009.
- **The average domains-per-10,000 score of 7.2** 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 46% of the phishing domains in our data set, and 45% of the domains in the TLDs for which we have domains-in-registry statistics.

We therefore suggest that domains-per-10,000 scores between .COM's 1.6 and the median of 2.9 occupy the middle ground, with scores above 2.9 indicating TLDs with increasingly prevalent phishing.

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

Notes regarding the statistics:

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

Top 10 Phishing TLDs by Domain Score

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

	TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009
1	.th	Thailand	117	60	48,111	**12.5**	**24.3**
2	.kr	Korea	1,278	580	1,061,187	**5.5**	**12.0**
3	.ie	Ireland	100	65	135,177	**4.8**	**7.4**
4	.be	Belgium	1,111	444	966,679	**4.6**	**11.5**
5	.ro	Romania	295	134	325,000	**4.1**	**9.1**
6	.my	Malaysia	45	36	89,798	**4.0**	**5.0**
7	.eu	European Union	28,793	1,234	3,140,216	**3.9**	**91.7**
8	.ir	Iran	68	43	144,865	**3.0**	**4.7**
9	.pl	Poland	1,329	470	1,638,550	**2.9**	**8.1**
10	.mx	Mexico	1,466	104	376,455	**2.8**	**38.9**

Phishing in .TH (Thailand) took place mostly on compromised academic (AC.TH) and government (GO.TH) Web servers – and even on a hacked military zone (MI.TH) Web site. Such institutional servers in Thailand have been exploited repeatedly over the last two-and-one-half years, highlighting the need for server operators everywhere to follow good software update practices and maintain effective intrusion detection.

As previously noted, .EU and .BE domains were used frequently for Avalanche attacks. In contrast, phishing in .IE, .KR, and .RO took place mostly on compromised domains.

The "generic" TLDs are open to registrants across the world without registration qualifications, while "sponsored" TLDs have eligibility requirements. All of them had average-to-below-average scores:

Phishing in gTLDs and sTLDs by Score

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009
.net	generic TLD	14,609	2,400	12,910,298	**1.9**	**11.3**
.coop	sponsored TLD	1	1	6,166	**1.6**	**1.6**
.com	generic TLD	39,355	13,351	85,715,975	**1.6**	**4.6**
.org	generic TLD	1,857	1,235	7,948,804	**1.6**	**2.3**
.aero	sponsored TLD	1	1	6,764	**1.5**	**1.5**
.biz	generic TLD	354	218	2,046,387	**1.1**	**1.7**
.info	generic TLD	771	573	5,402,824	**1.1**	**1.4**
.cat	sponsored TLD	5	3	39,219	**0.8**	**1.3**
.name	generic TLD	18	14	258,660	**0.5**	**0.7**
.mobi	sponsored TLD	122	51	947,015	**0.5**	**1.3**
.asia	sponsored TLD	11	8	219,384	**0.4**	**0.5**
.jobs	sponsored TLD	0	0	9,002	**0.0**	**0.0**
.museum	sponsored TLD	0	0	553	**0.0**	**0.0**
.pro	sponsored TLD	0	0	42,783	**0.0**	**0.0**
.tel	generic TLD	0	0	255,289	**0.0**	**0.0**
.travel	sponsored TLD	0	0	137,039	**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 28,775 domains used for phishing, **we identified 6,372 that we believe were registered by phishers. Malicious registrations were concentrated in certain namespaces: 88% of them made in just 5 TLDs: .BE, .COM, .EU, .NET, .EU, and .UK. This is partly because two-thirds of the maliciously registered domains (4,151) were Avalanche attack domains.** If Avalanche registrations are discarded, the number of malicious domains was 2,221, up slightly from the 2,073 in 1H2009.

The remaining 22,403 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, 1,063 contained a relevant brand name or variation thereof – often a misspelling.[10] This represents just 17% of maliciously registered domains, and just 3.6% of all domains that were used for phishing, a percentage unchanged from 1H2009.

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.

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 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 ă 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. ICANN recently launched a program that will make IDN TLDs available to countries and territories, so that the entire domain name will be in non-Latin characters. Hong Kong, Sri Lanka, Thailand, Qatar, and others have already had their IDN TLD applications evaluated.

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

We saw no homographic attacks in the second half of 2009. Only 12 of the 28,764 domain names we studied were IDNs, and those 12 domains were all hacked by phishers.

[10] Examples of domain names we counted as containing brand names included: emesboaonlinesupport.com, enrol-online-usb.com, faceblooknm.org, and free-steam-community-games.tk

From January 1, 2007 to December 31, 2009 only 97 IDNs were used for phishing. The majority were .HK domain names (non-homographic), apparently used by the Rock Phish gang early in 2008, with the rest being compromised/hacked IDN domains owned by innocent parties.

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 generally be run by existing national ccTLD registry operators. They therefore may not be more or less vulnerable to abuse than any other domain registry.

Use of Subdomain Services for Phishing

Phishers continue making significant use of subdomain registration services to host phishing Web sites. **Malicious use of these services remained steady in the second half of 2009, and still accounts for the majority of phishing in some large TLDs**. **In the second half of 2009, subdomain services hosted 6,734 phish** (versus 6,441 phish in the first half of 2009 and the 6,339 phish we saw in the second half of 2008). This is more than the number of maliciously registered domains names purchased by phishers at regular domain name registrars (6,372). 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 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 560 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

[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.

interesting changes in this market space as well. For example, many subdomain resellers now offer WHOIS services, 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 **6,734 subdomain sites/accounts used for phishing, beneath 658 unique second-level domains.** This is up from the first half of 2009, where we saw 6,441 subdomain sites/accounts used for phishing, beneath 483 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 22% of non-Avalanche phishing domains.

Top 20 Subdomain Services Used for Phishing 2H2009

Rank	Domain	Total	Provider
1	t35.com	385	t35.com
2	110mb.com	293	110mb.com
3	ns11-wistee.fr	177	wistee.fr
4	tripod.com	160	tripod.com
5	justfree.com	125	justfree.com
6	co.cc	100	php0h.com
6	freehostia.com	100	freehostia.com
8	angelfire.com	94	angelfire.com
9	50webs.com	90	50Webs.com
9	dezigner.ru	90	NextMail.ru
9	freewebhostx.com	90	freewebhostx.com
12	hostrator.com	88	hostrator.com
13	free.fr	84	free.fr
14	pochta.ru	78	pochta.ru
15	blackapplehost.com	74	blackapplehost.com
16	hd1.com.br	70	hdfree.com.br
17	atspace.com	69	atspace.com
17	pisem.su	69	pochta.ru
19	w.interia.pl	65	interia.pl
20	rbcmail.ru	64	pochta.ru

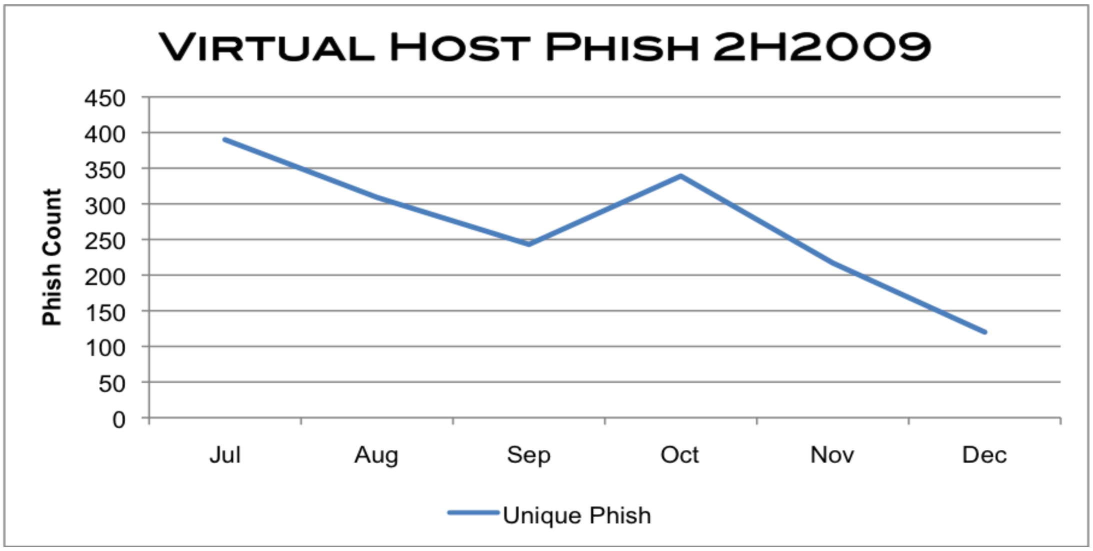
Provider	Total Attacks
pochta.ru	509
t35.com	385
NextMail.ru	302
110mb.com	293

Overall, there were 354 different providers of subdomain registrations who had phishing subdomains on their services in the second 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 2H2009, and those domains were used to mount at least 509 phishing attacks. The good news is that this provider continues to quickly mitigate phish when reported, and this number is quite a bit down from the 822 in the first half of 2009. Second place belongs to the American provider t35.com, rising from third place in 1H2009.

For more information on subdomain resellers and the unique challenges they pose for phishing and 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

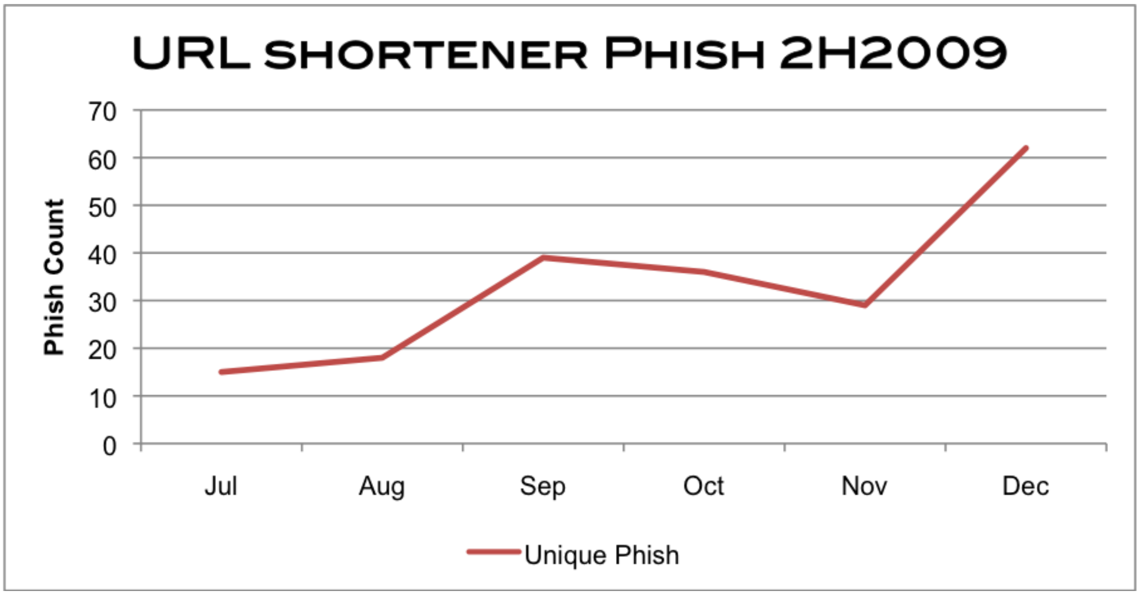
Phishers use other tricks to get their sites onto the Internet, or to get around the spam filtering and browser-based protection mechanisms that protect users. In past reports we have looked at the role that various "virtual hosting" services have played in phishing. With the shuttering of GeoCities, one of the largest providers in this area, and the rise in popularity of social networking sites like FaceBook to host small Web sites, there appears to be a trend away from abuse of virtual hosting services to host malicious content.



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 on their limited-space posts, which redirects the visitor to a much longer "hidden" URL automatically. 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.

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

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 bear watching:



Conclusions

In the second half of 2009, Avalanche cast a shadow over the landscape. While Avalanche launched a record number of attacks, responders took significant bites out of Avalanche's uptimes. The decreasing Avalanche uptimes showed that the domain name registration community responded with an increasing effectiveness. Some registrars and registries remained ineffective, though, and after failing to mount quick defenses became victimized on a continuing basis. Avalanche's infrastructure was temporarily disabled late in 2009, and the phishers behind it changed their tactics and launched decreasing numbers of attacks through April 2010. We will continue to monitor this situation with interest.

Avalanche aside, the amount of phishing remained steady from previous periods, as measured by attacks and domains used. The vast majority of phishing continued to be concentrated in just a few namespaces overall, and the use of subdomain services rose only slightly. Phishers still do not tend to abuse Internationalized domain names (IDNs). Abuse of URL shortening services by phishers may be a new trend to watch going forward. The average and median uptimes of non-Avalanche phish rose in 2H2009, perhaps because some brand owners and responders were concentrating their efforts on Avalanche. Brand owners must continue to protect themselves and not become complacent.

Appendix: Phishing Statistics and Uptimes by TLD

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

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
ac	Ascension Island	2	2	14,938	**1.3**	**1.3**	17:30:10	0	0.0	0	0
ad	Andorra	1	1				3:27:01	0			
ae	United Arab Emirates	8	7	87,000	**0.8**	**0.9**	80:20:47	0	0.0	0	0
aero	sponsored TLD	1	1	6,764	**1.5**	**1.5**	13:40:41	0	0.0	0	0
af	Afghanistan	1	1				6:20:17	0		0	0
ag	Antigua and Barbuda	1	1	15,921	**0.6**	**0.6**	26:32:04	0	0.0	0	0
ai	Anguilla	0	0	390	**0.0**	**0.0**		0	0.0	0	0
al	Albania	0	0	1,670	**0.0**	**0.0**		0	0.0	0	0
am	Armenia	12	8	11,700	**6.8**	**10.3**	50:15:51	0	0.0	0	0
an	Netherlands Antilles	0	0		**0.0**	**0.0**		0		0	0
ao	Angola	1	1				1:56:24	0			
ar	Argentina	162	118	1,990,085	**0.6**	**0.8**	65:07:27	1	0.0	0	0
as	American Samoa	0	0		**0.0**	**0.0**		0		0	0
asia	sponsored TLD	11	8	219,384	**0.4**	**0.5**	106:04:56	0	0.0	0	0
at	Austria	84	63	906,036	**0.7**	**0.9**	54:46:53	0	0.0	0	0
au	Australia	302	217	1,585,558	**1.4**	**1.9**	73:55:30	0	0.0	0	0
az	Azerbaijan	4	3	9,201	**3.3**	**4.3**	17:29:30	0	0.0	0	0
ba	Bosnia and Herzegovina	9	3	9,858	**3.0**	**9.1**	44:54:19	0	0.0	0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
bd	Bangladesh	4	4	4,031	**9.9**	**9.9**	9:58:37	0	0.0	0	0
be	Belgium	1,111	444	966,679	**4.6**	**11.5**	15:10:59	297	3.1	287	915
bf	Burkina Faso	0	0		**0.0**	**0.0**		0		0	0
bg	Bulgaria	24	16	15,700	**10.2**	**15.3**	95:48:38	0	0.0	0	0
bh	Bahrain	1	1				80:43:05	0		0	0
biz	generic TLD	354	218	2,046,387	**1.1**	**1.7**	38:38:02	16	0.1	3	53
bm	Bermuda	2	2	5,580	**3.6**	**3.6**	1:23:19	0	0.0	0	0
bn	Brunei Darussalam	1	1	760	**13.2**	**13.2**	31:58:18	0	0.0	0	0
bo	Bolivia	3	3	5,300	**5.7**	**5.7**	298:05:35	0	0.0	0	0
br	Brazil	774	426	1,949,550	**2.2**	**4.0**	62:36:53	2	0.0	0	0
bs	Bahamas	9	2	2,260	**8.8**	**39.8**	59:44:57	0	0.0	0	0
bt	Bhutan	5	2				54:25:32	0		0	0
bw	Botswana	0	0		**0.0**	**0.0**		0		0	0
by	Belarus	34	16				79:29:06	0		0	0
bz	Belize	50	15	44,478	**3.4**	**11.2**	7:19:48	9	2.0	1	34
ca	Canada	266	197	1,300,378	**1.5**	**2.0**	49:54:48	0	0.0	0	0
cat	sponsored TLD	5	3	39,219	**0.8**	**1.3**	118:53:28	0	0.0	0	0
cc	Cocos (Keeling) Islands	169	40	registry declined to provide			42:10:36	6		0	0
cd	Congo, Democratic Repub.	0	0		**0.0**	**0.0**		0		0	0
ch	Switzerland	179	97	1,340,198	**0.7**	**1.3**	48:04:15	1	0.0	1	33
ci	Côte d'Ivoire	3	2	1,340	**14.9**	**22.4**	26:21:41	0	0.0	0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
cl	Chile	119	70	268,333	2.6	4.4	65:31:30	0	0.0	0	0
cm	Cameroon	1	1	625	16.0	16.0	0:57:42	0	0.0	0	0
cn	China	2,826	228	13,680,727	0.2	2.1	15:32:32	104	0.1	85	2,635
co	Colombia	42	23	27,700	8.3	15.2	60:15:17	0	0.0	0	0
com	generic TLD	39,355	13,351	85,715,975	1.6	4.6	42:14:52	2,164	0.3	830	19,352
coop	sponsored TLD	1	1	6,166	1.6	1.6	30:24:45	0	0.0	0	0
cr	Costa Rica	0	0	11,977	0.0	0.0		0	0.0	0	0
cu	Cuba	3	2	2,100	9.5	14.3	19:05:21	0	0.0	0	0
cx	Christmas Island	22	6	5,100	11.8	43.1	55:21:09	0	0.0	0	0
cy	Cyprus	2	2	6,750	3.0	3.0	40:56:33	0	0.0	0	0
cz	Czech Republic	207	71	624,893	1.1	3.3	46:12:09	2	0.0	2	67
de	Germany	809	584	13,276,820	0.4	0.6	48:16:11	9	0.0	0	0
dj	Djibouti	0	0		0.0	0.0		0		0	0
dk	Denmark	161	126	1,010,070	1.2	1.6	71:28:00	0	0.0	0	0
dm	Dominica	0	0	14,603	0.0	0.0		0	0.0	0	0
do	Dominican Republic	4	2	10,550	1.9	3.8	90:09:45	0	0.0	0	0
dz	Algeria	2	1	1,800	5.6	11.1	96:15:19	0	0.0	0	0
ec	Ecuador	11	10	20,000	5.0	5.5	25:43:00	0	0.0	0	0
edu	U.S. higher education	35	27				52:27:09	0		0	0
ee	Estonia	13	7	72,190	1.0	1.8	27:43:37	1	0.1	0	0
eg	Egypt	5	4	5,900	6.8	8.5	62:51:11	0	0.0	0	0
er	Eritrea	0	0	120	0.0	0.0		0	0.0	0	0
es	Spain	430	122	1,199,422	1.0	3.6	37:30:49	15	0.1	8	259
et	Ethiopia	0	0		0.0	0.0		0		0	0
eu	European Union	28,793	1,234	3,140,216	3.9	91.7	15:59:18	1,070	3.4	1,044	28,534
fi	Finland	49	36	224,000	1.6	2.2	110:42:42	0	0.0	0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
fj	Fiji	0	0	3,800	**0.0**	**0.0**		0	0.0	0	0
fk	Falkland Islands	0	0		**0.0**	**0.0**		0		0	0
fm	Micronesia, Fed. States	1	1				74:34:18	0		0	0
fo	Faroe Islands	3	3	3,000	**10.0**	**10.0**	20:38:24	0	0.0	0	0
fr	France	868	337	1,599,200	**2.1**	**5.4**	41:18:42	17	0.1	0	0
gd	Grenada	2	2	2,701	**7.4**	**7.4**	6:26:54	0	0.0	0	0
ge	Georgia	29	15	15,057	**10.0**	**19.3**	103:02:48	0	0.0	0	0
gg	Guernsey	2	1				302:00:44	0		0	0
gh	Ghana	1	1				45:09:38	0		0	0
gi	Gibraltar	0	0	1,764	**0.0**	**0.0**		0	0.0	0	0
gl	Greenland	0	0	4,120	**0.0**	**0.0**		0	0.0	0	0
gov	U.S. government	2	2	registry declined to provide			11:01:09	0		0	0
gp	Guadeloupe	0	0	1,400	**0.0**	**0.0**		0	0.0	0	0
gr	Greece	91	47	260,000	**1.8**	**3.5**	50:51:19	0	0.0	0	0
gs	South Georgia & Sandwich Is.	69	6	8,200	**7.3**	**84.1**	8:10:35	2	2.4	2	65
gt	Guatemala	10	7	7,500	**9.3**	**13.3**	31:38:05	0	0.0	0	0
hk	Hong Kong	34	29	179,731	**1.6**	**1.9**	41:58:11	0	0.0	0	0
hm	Heard and McDonald Is.	0	0		**0.0**	**0.0**		0		0	0
hn	Honduras	2,128	98	4,339	**225.9**	**4904.4**	11:48:57	98	225.9	98	2,128
hr	Croatia	15	14	69,333	**2.0**	**2.2**	106:54:04	0	0.0	0	0
ht	Haiti	0	0	1,601	**0.0**	**0.0**		0	0.0	0	0
hu	Hungary	119	88	473,000	**1.9**	**2.5**	97:00:21	0	0.0	0	0
id	Indonesia	73	49				72:58:07	0		0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
ie	Ireland	100	65	135,177	**4.8**	**7.4**	64:33:41	0	0.0	0	0
il	Israel	55	40	157,259	**2.5**	**3.5**	43:38:41	0	0.0	0	0
im	Isle of Man	350	67	25,000	**26.8**	**140.0**	11:03:17	64	25.6	63	344
in	India	176	66	570,523	**1.2**	**3.1**	28:48:21	5	0.1	3	97
info	generic TLD	771	573	5,402,824	**1.1**	**1.4**	23:51:08	133	0.2	6	117
io	British Indian Ocean Terr.	0	0		**0.0**	**0.0**		0		0	0
IP address		2,498		n/a				n/a		0	0
iq	Iraq	1	1				5:59:49	0			
ir	Iran	68	43	144,865	**3.0**	**4.7**	114:45:02	0	0.0	0	0
is	Iceland	5	4	27,100	**1.5**	**1.8**	34:57:25	0	0.0	0	0
it	Italy	373	232	1,790,100	**1.3**	**2.1**	72:04:39	1	0.0	0	0
je	Jersey	0	0		**0.0**	**0.0**		0		0	0
jm	Jamaica	0	0	4,844	**0.0**	**0.0**		0	0.0	0	0
jo	Jordan	1	1	3,609	**2.8**	**2.8**	3:54:56	0	0.0	0	0
jobs	sponsored TLD	0	0	9,002	**0.0**	**0.0**		0	0.0	0	0
jp	Japan	164	126	1,132,000	**1.1**	**1.4**	60:19:49	1	0.0	0	0
ke	Kenya	13	10	12,557	**8.0**	**10.4**	45:21:46	0	0.0	0	0
kg	Kyrgyzstan	2	2	3,900	**5.1**	**5.1**	355:23:13	0	0.0	0	0
kh	Cambodia	0	0	1,013	**0.0**	**0.0**		0	0.0	0	0
ki	Kiribati	0	0		**0.0**	**0.0**		0		0	0
kr	Korea	1,278	580	1,061,187	**5.5**	**12.0**	58:05:05	35	0.3	34	172
kw	Kuwait	2	2				331:46:23	0		0	0
ky	Cayman Islands	0	0	6,314	**0.0**	**0.0**		0	0.0	0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
kz	Kazakhstan	31	17	38,122	**4.5**	**8.1**	103:09:12	1	0.3	0	0
la	Lao People's Demo. Rep.	48	7				77:34:30	1		1	32
lb	Lebanon	0	0		**0.0**	**0.0**		0		0	0
lc	St. Lucia	0	0	1,924	**0.0**	**0.0**		0	0.0	0	0
li	Liechtenstein	238	14	58,310	**2.4**	**40.8**	10:21:58	8	1.4	7	231
lk	Sri Lanka	5	4	6,278	**6.4**	**8.0**	57:12:57	0	0.0	0	0
lt	Lithuania	18	16	110,212	**1.5**	**1.6**	37:05:21	0	0.0	0	0
lu	Luxembourg	5	4	47,647	**0.8**	**1.0**	41:57:46	0	0.0	0	0
lv	Latvia	57	10	79,513	**1.3**	**7.2**	179:24:34	0	0.0	0	0
ly	Libya	15	2	5,965	**3.4**	**25.1**	107:29:05	0	0.0	0	0
ma	Morocco	21	14	31,920	**4.4**	**6.6**	109:50:03	0	0.0	0	0
mc	Monaco	1	1				34:48:46	0			
md	Moldova	5	3				185:29:58	0		0	0
me	Montenegro	636	38	335,191	**1.1**	**19.0**	38:51:39	27	0.8	23	602
mg	Madagascar	0	0		**0.0**	**0.0**		0		0	0
mk	Macedonia	6	5				93:52:18	0		0	0
ml	Mali	0	0		**0.0**	**0.0**		0		0	0
mn	Mongolia	372	26	7,645	**34.0**	**486.6**	3:08:45	15	19.6	13	352
mo	Macao	0	0		**0.0**	**0.0**		0		0	0
mobi	sponsored TLD	122	51	947,015	**0.5**	**1.3**	11:55:41	20	0.2	2	68
mr	Mauritania	1	1				7:43:27	0		0	0
ms	Montserrat	71	8	12,107	**6.6**	**58.6**	9:45:49	2	1.7	2	62
mt	Malta	1	1	11,750	**0.9**	**0.9**	1:00:56	0	0.0	0	0
mu	Mauritius	4	3	7,500	**4.0**	**5.3**	37:46:05	0	0.0	0	0
museum	sponsored TLD	0	0	553	**0.0**	**0.0**		0	0.0	0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
mx	Mexico	1,466	104	376,455	**2.8**	**38.9**	44:46:38	60	1.6	57	1,373
my	Malaysia	45	36	89,798	**4.0**	**5.0**	52:53:32	0	0.0	0	0
mz	Mozambique	0	0	1,825				0	0.0	0	0
name	generic TLD	18	14	258,660	**0.5**	**0.7**	123:19:14	1	0.0	0	0
nc	New Caledonia	7	2				10:23:01	0			
net	generic TLD	14,609	2,400	12,910,298	**1.9**	**11.3**	24:58:29	637	0.5	509	11,663
nf	Norfolk Island	5	3	5,000	**6.0**	**10.0**	14:10:59	0	0.0	0	0
ng	Nigeria	1	1	1,350	**7.4**	**7.4**	8:11:08	0	0.0	0	0
ni	Nicaragua	4	3	5,300	**5.7**	**7.5**	150:52:02	0	0.0	0	0
nl	Netherlands	328	253	3,632,580	**0.7**	**0.9**	55:12:45	0	0.0	0	0
no	Norway	56	48	455,377	**1.1**	**1.2**	62:54:54	0	0.0	0	0
np	Nepal	7	6	18,000	**3.3**	**3.9**	57:38:03	0	0.0	0	0
nr	Nauru	0	0	425				0	0.0	0	0
nu	Niue	26	16				60:20:30	0		0	0
nz	New Zealand	65	24	380,015	**0.6**	**1.7**	22:04:40	1	0.0	1	34
org	generic TLD	1,857	1,235	7,948,804	**1.6**	**2.3**	46:38:19	102	0.1	4	54
pa	Panama	0	0	5,103				0	0.0	0	0
pe	Peru	134	21	37,500	**5.6**	**35.7**	42:58:19	3	0.8	3	93
pf	French Polynesia	1	1				14:54:24	0			
ph	Philippines	17	13	registry declined to provide			84:02:12	0		0	0
pk	Pakistan	11	9	registry declined to provide			24:56:02	0		0	0
pl	Poland	1,329	470	1,638,550	**2.9**	**8.1**	88:49:44	76	0.5	75	298
pn	Pitcairn	2	2				1:25:12	0		0	0
pro	sponsored TLD	0	0	42,783	**0.0**	**0.0**		0	0.0	0	0
ps	Palestinian	3	3	5,100	**5.9**	**5.9**	19:05:34	0	0.0	0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
	Territory										
pt	Portugal	49	29	285,275	**1.0**	**1.7**	53:17:51	0	0.0	0	0
py	Paraguay	1	1	9,485	**1.1**	**1.1**	0:29:03	0	0.0	0	0
qa	Qatar	0	0					0		0	0
re	Réunion	2	2	4,450	**4.5**	**4.5**	32:28:28	0	0.0	0	0
ro	Romania	295	134	325,000	**4.1**	**9.1**	76:06:32	0	0.0	0	0
rs	Serbia	7	5	49,000	**1.0**	**1.4**	48:38:07	0	0.0	0	0
ru	Russian Fed.	1,592	623	2,493,601	**2.5**	**6.4**	54:34:19	31	0.1	0	0
sa	Saudi Arabia	12	7	17,543	**4.0**	**6.8**	59:16:41	0	0.0	0	0
sc	Seychelles	2	2	6,169	**3.2**	**3.2**	36:04:08	0	0.0	0	0
se	Sweden	110	64	912,300	**0.7**	**1.2**	102:49:31	0	0.0	0	0
sg	Singapore	12	11	108,700	**1.0**	**1.1**	47:32:45	1	0.1	0	0
sh	Saint Helena	31	1	2,750	**3.6**	**112.7**	23:39:42	1	3.6	1	31
si	Slovenia	9	7	72,000	**1.0**	**1.3**	96:08:40	0	0.0	0	0
sk	Slovakia	58	26	202,000	**1.3**	**2.9**	53:50:54	0	0.0	0	0
sl	Sierra Leone	7	7	1,100	**63.6**	**63.6**	1:40:28	2	18.2	0	0
sm	San Marino	0	0	1,903				0	0.0	0	0
sn	Senegal	1	1				166:42:26	0			
st	Sao Tome and Principe	11	7				103:00:04	0		0	0
su	Soviet Union	267	22	91,250	**2.4**	**29.3**	40:23:46	0	0.0	0	0
sv	El Salvador	4	3	4,395	**6.8**	**9.1**	59:20:23	0	0.0	0	0
sy	Syria	1	1				7:54:35	0		0	0
tc	Turks and Caicos	198	16	9,700	**16.5**	**204.1**	18:16:57	6	6.2	6	186
tel	generic TLD	0	0	255,289	**0.0**	**0.0**		0	0.0	0	0
tf	French Southern Territories	29	9	1,550	**58.1**	**187.1**	500:43:57	0	0.0	0	0

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
tg	Togo	3	2				69:28:48	0			
th	Thailand	117	60	48,111	**12.5**	**24.3**	88:25:31	0	0.0	0	0
tj	Tajikistan	3	1	5,270	**1.9**	**5.7**	151:15:48	0	0.0	0	0
tk	Tokelau	303	280				40:05:26	280		0	0
tl	Timor-Leste	5	5	1,750	**28.6**	**28.6**	34:53:06	2	11.4	0	0
tm	Turkmenistan	1	1	3,500	**2.9**	**2.9**	0:27:41	0	0.0	0	0
tn	Tunisia	0	0	50				0	0.0	0	0
to	Tonga	23	13	13,250	**9.8**	**17.4**	53:20:26	0	0.0	0	0
tp	Portuguese Timor	12	7				104:10:00	0		0	0
tr	Turkey	52	33	205,493	**1.6**	**2.5**	107:51:25	0	0.0	0	0
travel	sponsored TLD	0	0	137,039	**0.0**	**0.0**		0	0.0	0	0
tt	Trinidad and Tobago	15	7	2,100	**33.3**	**71.4**	8:42:33	0	0.0	0	0
tv	Tuvalu	62	39	registry declined to provide			48:07:19	0		0	0
tw	Taiwan	168	108	440,000	**2.5**	**3.8**	51:42:12	0	0.0	0	0
tz	Tanzania	1	1				1:54:56	0		0	0
ua	Ukraine	111	78	476,864	**1.6**	**2.3**	58:04:51	0	0.0	0	0
ug	Uganda	5	3	3,200	**9.4**	**15.6**	41:28:43	0	0.0	0	0
uk	United Kingdom	14,387	1,554	8,098,544	**1.9**	**17.8**	15:41:22	995	1.2	953	13,569
us	United States	261	159	1,570,106	**1.0**	**1.7**	32:19:21	17	0.1	1	32
uy	Uruguay	13	8	22,859	**3.5**	**5.7**	23:52:00	0	0.0	0	0
uz	Uzbekistan	3	3	9,450	**3.2**	**3.2**	18:55:44	0	0.0	0	0
vc	St. Vincent and Grenadines	594	23	6,054	**38.0**	**981.2**	6:12:00	20	33.0	20	590

TLD	TLD Location	# Unique Phishing attacks 2H2009	Unique Domain Names used for phishing 2H2009	Domains in registry November 2009	Score: Phish per 10,000 domains 2H2009	Score: Attacks per 10,000 domains 2H2009	Average Uptime 2H2009 hh:mm:ss	# Total Malicious Domains Registered 2H2009	Malicious registrations score/10,000 domains in registry	Avalanche Domains Registered 2H2009	Avalanche Attacks 2H2009
ve	Venezuela	22	12	150,000	**0.8**	**1.5**	31:19:03	1	0.1	0	0
vg	British Virgin Islands	4	3				57:15:32	0		0	0
vi	Virgin Islands	0	0	500				0	0.0	0	0
vn	Vietnam	49	31	128,799	**2.4**	**3.8**	103:26:28	0	0.0	0	0
vu	Vanuatu	177	8				11:20:38	6		6	175
ws	Samoa	56	32	540,443	**0.6**	**1.0**	44:46:38	2	0.0	0	0
ye	Yemen	2	1				236:05:20	0			
yu	Yugoslavia (being deprecated)	1	1	2,000	**5.0**	**5.0**	33:49:00	0	0.0	0	0
za	South Africa	114	92	499,950	**1.8**	**2.3**	100:58:22	1	0.0	0	0
zm	Zambia	0	0					0		0	0
zw	Zimbabwe	0	0	9,600				0	0.0	0	0
	TOTALS	**126,697**	**28,775**	**191,771,389**			**31:38:00**	**6,372**		**4,151**	**84,250**

About the Authors & Acknowledgments

The authors wish to thank the following for their support: Dave Jevans, Peter Cassidy, Foy Shiver, 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. We would like to extend a special thanks to Aaron Routt of Internet Identity, who performed much of the data analysis to support this paper, along with design of the included 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 is 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.

#