Global Phishing Survey: Trends and Domain Name Use in 1H2011

January-June 2011

APWG

Unifying the
Global Response
To Cybercrime

An
APWG
Industry
Advisory

November 2011

Published November 7, 2011

Authors:

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

Greg Aaron
Afilias
<gaaron at afilias.info>

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

Table of Contents

OVERVIEW 3
BASIC STATISTICS 3
SHARED VIRTUAL SERVER HACKING 5
PHISHING IN CHINA 7
PHISHING BY UPTIME 8
PREVALENCE OF PHISHING BY TOP-LEVEL DOMAIN (TLD) 11
COMPROMISED DOMAINS VS. MALICIOUS REGISTRATIONS 14
USE OF SUBDOMAIN SERVICES FOR PHISHING 15
USE OF INTERNATIONALIZED DOMAIN NAMES (IDNS) 19
USE OF URL SHORTENERS FOR PHISHING 19
USE OF VIRTUAL HOSTS FOR PHISHING 20
CONCLUSIONS 21
APPENDIX: PHISHING STATISTICS AND UPTIMES BY TLD 22
ABOUT THE AUTHORS & ACKNOWLEDGMENTS 30

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

Overview

Phishers are an ingenious lot, and the successful ones develop their own specialties and business plans. For example, in this report we describe how Chinese phishers are using resources outside of their country to attack users and companies inside of China. And elsewhere, phishers have taken an old hacking trick and used it to great advantage, multiplying the number of phish they can deploy against their favorite targets. These and other tactics have significant implications for phishing targets, service providers, and anti-phishing responders.

This report seeks to understand trends and their significances by quantifying the scope of the global phishing problem. Specifically, this new report examines all the phishing attacks detected in the first half of 2011 ("1H2011", or January 1, 2011 through June 30, 2011). The data was collected by the Anti-Phishing Working Group, and supplemented with data from several phishing feeds, CNNIC, and private sources. The APWG phishing repository is the Internet's most comprehensive archive of phishing and e-mail fraud activity.[1] We hope that bringing new trends to light will lead to improved anti-phishing measures.

Our major findings in this report include:

1. **In 1H2011, the average and median uptimes of all phishing attacks dropped notably.** *(Pages 8-10)*
2. **More than a third of all phishing attacks involved hackings of shared virtual servers.** This formerly obscure attack vector involves large numbers of attacks and domain names, but these phish stayed up a much shorter time than average. *(Pages 5-6)*
3. **Attacks by Chinese phishers were up significantly. Phishers attacking Chinese institutions were responsible for 70% of all malicious domain name registrations made in the world.** These phishers especially use free and low-priced domain providers outside of China. *(Pages 7-8)*
4. **Otherwise, the number of malicious domain name registrations is down significantly from past periods. Phishers are also registering relatively few domain names that contain brand names in them.** This tactic has fallen out of favor. *(Pages 15-16)*
5. **Phishers continue to use subdomain registration services heavily.** *(Pages 15-17)*

Basic Statistics

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

[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

[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

yields the following statistics:

- **There were at least 112,472 unique phishing attacks worldwide, in 200 top-level domains (TLDs).** This is far greater than the 42,624 attacks we observed in 2H2010, but less than the record 126,697 observed in 2H2009 at the height of phishing on the Avalanche botnet**. The increase in 1H2011 consists largely of phishing attacks that leverage shared virtual servers to infect multiple domains at once, and attacks on Chinese targets.** 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 attacks used 79,753 unique domain names**.[3] This is a high in our reports going back to 2007, and the increase is due to two factors. Chinese phishers have been registering large numbers of domain names and increased their attacks. We also saw a massive increase in attacks against servers hosting multiple domains, where all domains on the server would be used for phishing. The number of domain names in the world grew from 205.6 million in October 2010 to 218.8 million in May 2011.[4]
- In addition, 2,960 attacks were detected on **2,385 unique IP addresses, rather than on domain names.** (For example: http://79.173.233.18/paypal/.) This is the highest number since early 2009. None were IPv6 addresses.
- Of the 79,753 phishing domains, **we identified 14,650 that we believe were registered maliciously, by phishers (18%).** This is down from 28% in 2H2010. **Of those, 10,441 (70%) were registered to phish Chinese targets.** The other 65,103 domains were hacked or compromised on vulnerable Web hosting. Malicious registrations took place in 43 TLDs.
- We counted **520 target institutions**. These included banks, e-commerce sites, social networking services, ISPs, lotteries, government tax bureaus, online gaming sites, postal services, and stock-holding securities companies.
- **Phishing is generally distributed by top-level domain market share, but there are a few exceptions.** 93% of the malicious domain registrations were made in just four TLDs: .TK, .INFO, .COM, and .NET.
- **Only about 2% of all domain names that were used for phishing contain a brand name or variation thereof**. (See "Compromised Domains vs. Malicious Registrations.")
- Only 33 of the 79,753 domain names we studied were internationalized domain names, and none were homographic attacks.

---

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; including gTLD stats from ICANN.org and stats provided by the ccTLD registry operators.

Basic Statistics

	1H2011	2H2010	1H2010	2H2009	1H2009
Phishing domain names	79,753	42,624	28,646	28,775	30,131
Attacks	115,472	67,677	48,244	126,697	55,698
TLDs used	200	183	177	173	171
IP-based phish (unique IPs)	2,385	2,318	2,018	2,031	3,563
Maliciously registered domains	14,650	11,769	4,755	6,372	4,382
IDN domains	33	10	10	12	13

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.

Shared Virtual Server Hacking

Nearly every year we see a new tactic being used by phishers that drastically affects our statistics. This year we've seen a dramatic rise in what is actually an old tactic, but one that has been obscure until recently. In this attack, a phisher breaks into a web server that hosts large numbers of domains – a "shared virtual server" in industry parlance. Once a phisher breaks into such a server, instead of putting his phishing site content on a web site or two, the phisher first uploads a single copy of his phishing content. He then updates the web server configuration to add that content to *every* hostname served by that web server, so that all web sites on that server start displaying the phishing pages via a custom subdirectory. This is a standard capability for web servers, which allows webmasters to set up shared "info" pages, administration facilities, and 404 ("not found") pages.

So instead of hacking sites one at a time, **the phisher can infect dozens, hundreds, or even thousands of web sites at a time, depending on the server. We identified 42,448 unique attacks that utilized this tactic, each using a different domain name. This was 37% of all phishing attacks worldwide.** This large number of domain names accounts for much of the increase in phishing we saw versus the second half of 2010.

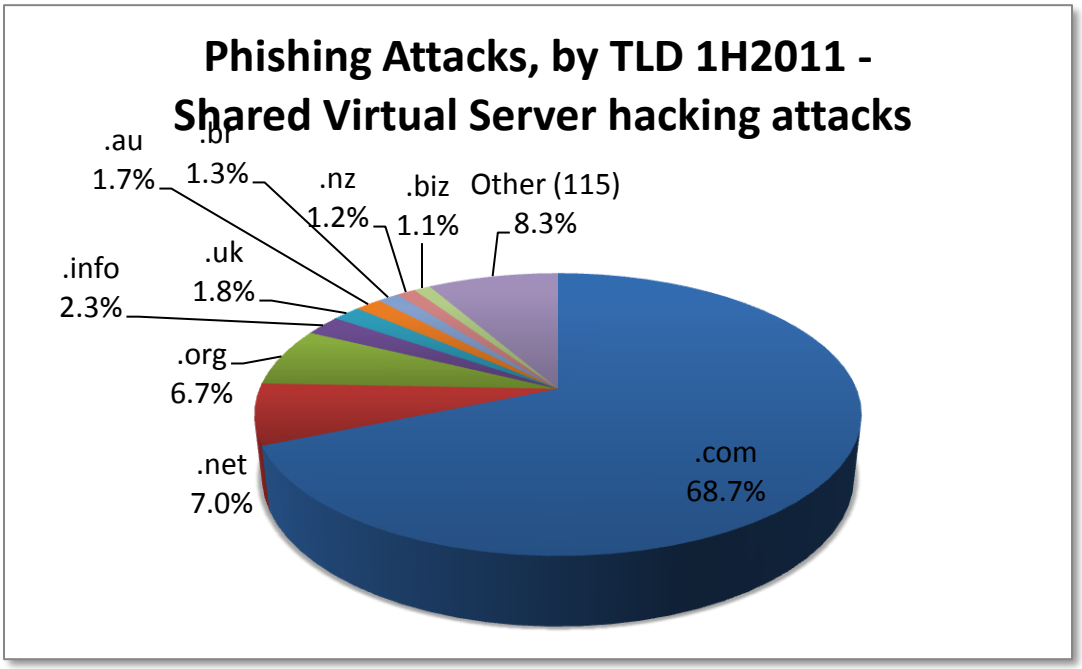
We were able to identify 122 of these mass attacks, each involving at least 50 domains. They targeted just 25 institutions, with PayPal (23,268 domains/attacks) and Wells Fargo (6,516 domains/attacks) being the most frequent targets.

The technique has several other advantages. Besides getting lots of different phishing pages for redundancy, the phisher can spam out e-mail lures using a wide range of domains, and thus circumvent phishing detection that is based on domain reputation

and/or the number of spam messages seen per domain. Another advantage is that it's difficult for a novice web site operator to figure out what's going on, since the offending content isn't in the directory that the owner uploaded, and the owner's personal web hosting account probably was never compromised. Instead, the overall system administrator has been compromised, and has to figure out that it's the web server configuration file that's been tampered with. In theory, this attack should therefore increase phishing site resiliency and get more spam into victims' mailboxes.

While there is some evidence that more lures are delivered, it is quite clear from our analysis that this type of phishing site generally stays alive for a shorter time than other phishing sites. **The median phishing site uptime for attacks using shared virtual servers was 9 hours and 45 minutes, versus 12 hours and 40 minutes for all other phishing sites.** This is likely due to multiple complaints coming into the hosting company. It becomes clear very quickly that something more serious than a simple site hack is occurring, especially when the offending directories don't exist.

Even though it was really the "server" that was hacked, the fact unfortunately remains that the individual domains were all spammed as lures, and the web sites were used for phishing. So the bottom-line impact on our statistics is that some TLDs were heavily impacted based on the type of server that was hacked. .COM was proportionally more impacted than its relative size. A few TLDs suffered similarly if a hosting location in their country was compromised.



These attacks mostly involved consumer-grade servers. In contrast, most enterprise, government, and university servers are on dedicated rather than virtual hosts.

We will watch this trend closely going forward. Our goal is to continue reporting using our standard metrics, while at the same time providing background and analysis to make comparisons between reports meaningful.

Phishing in China

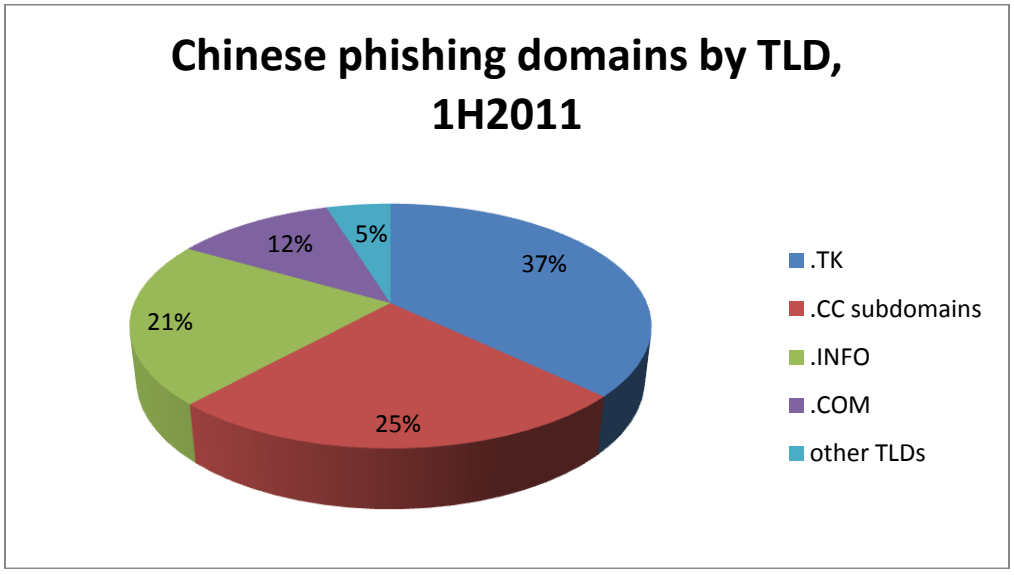
In our 2H2010 report, we explored the rise of Chinese phishing -- phishing perpetrated largely by Chinese criminals, who victimize Chinese Internet users and steal the credentials they use on Chinese e-commerce and banking sites. **In the first half of 2011, these phishing attacks increased by 44% over the previous period. And Chinese phishers were responsible for a startling 70% of all the domain names that were maliciously registered for phishing worldwide in 1H2011.**

In 2H2010 we counted 12,282 attacks on Chinese institutions, utilizing 6,382 unique domain names plus 4,737 CO.CC subdomains. In 1H2011 we recorded 17,693 such attacks, appearing on 11,192 unique domain names, plus 3,629 .CC subdomains.

Much of the data about this phishing was contributed by CNNIC. CNNIC operates the .CN domain registry, and is also the secretariat of the Anti-Phishing Alliance of China (APAC, http://en.apac.cn/). APAC has more than 140 member institutions in the country, including banks, e-commerce sites, and domain registrars, and has an efficient reporting and domain suspension program. We are grateful to CNNIC and APAC for sharing.

APAC members are detecting and reporting these attacks far more effectively than the APWG and the detection systems outside of China that we have access to, which detected only about 25% of the Chinese-target phishing that APAC did. Security observers in Europe and the Americas are evidently not receiving and/or parsing many of the Chinese-language phishing lure e-mails and instant messages that advertise most of these phishing attacks.

Unlike most phishers, Chinese phishers do not use many hacked domains. Instead, they prefer to set up their phishing pages on domains they register themselves. Of the 11,192 domains used in 1H2011, at least 10,179 of them (91%) were maliciously registered, up from 5,895 in 2H2010.



These phishers are especially attracted to cheap domain names, which they can obtain in

bulk. The low transaction amounts also fly below the fraud measures at payment processing companies and registrars. We saw that 5,459 of the maliciously registered domains were in the .TK top-level domain, which offers free registrations. An additional 3,181 malicious domains were in .INFO. All of the .INFO domains were obtained through just one American registrar that offers steep discounts, often as cheap as US$0.79 per .INFO domain. There were also 3,629 .CC subdomains. All of those were from subdomain resellers that offered free registrations—mostly CO.CC, plus VV.CC and CX.CC. Chinese phishers also registered 1,743 .COM domains.

The Chinese phishers targeted at least 36 Chinese institutions, including banks, securities firms, and CCTV, the major state television broadcaster. **But 15,554 of the attacks — a full 88% — targeted Taobao.com**. Taobao.com is one of China's largest e-commerce sites and specializes in business-to-consumer and consumer-to-consumer transactions, similar to eBay and Amazon. It is operated by the Alibaba Group, which also runs China's biggest third-party e-payment platform, Alipay. **It appears that Taobao.com is now the world's second-most-phished target, after PayPal.**

The domain names registered by these phishers usually bear addresses in China, although the truthfulness of the WHOIS data must be doubted. The domain registrars are not cancelling the domains for payment problems, which means that the payments are either being made with valid payment forms, or the payment processors and registrars are not catching fraudulent payments. We suspect that some of the domains are being paid for via Alipay; registrars do not reveal details about financial transactions and we are therefore unable to confirm this suspicion. The hosting location of these phishing sites is both inside and outside of China. Non-Chinese phishers continue to find hosting on Chinese networks, including Romanian criminals.

.CN domains were hardly used at all – only 101 attacks on 61 domains in 1H2011. In December 2009, new rules made it very difficult to register .CN domains. As a result, the number of names in the .CN registry fell from 13.5 million in late 2009 to just 3.4 million in March 2011. In 2H2010, our data showed 352 attacks on 278 .CN domains, with the increase due to CNNIC's superior data contribution. Half of those domains were used to attack non-Chinese targets.

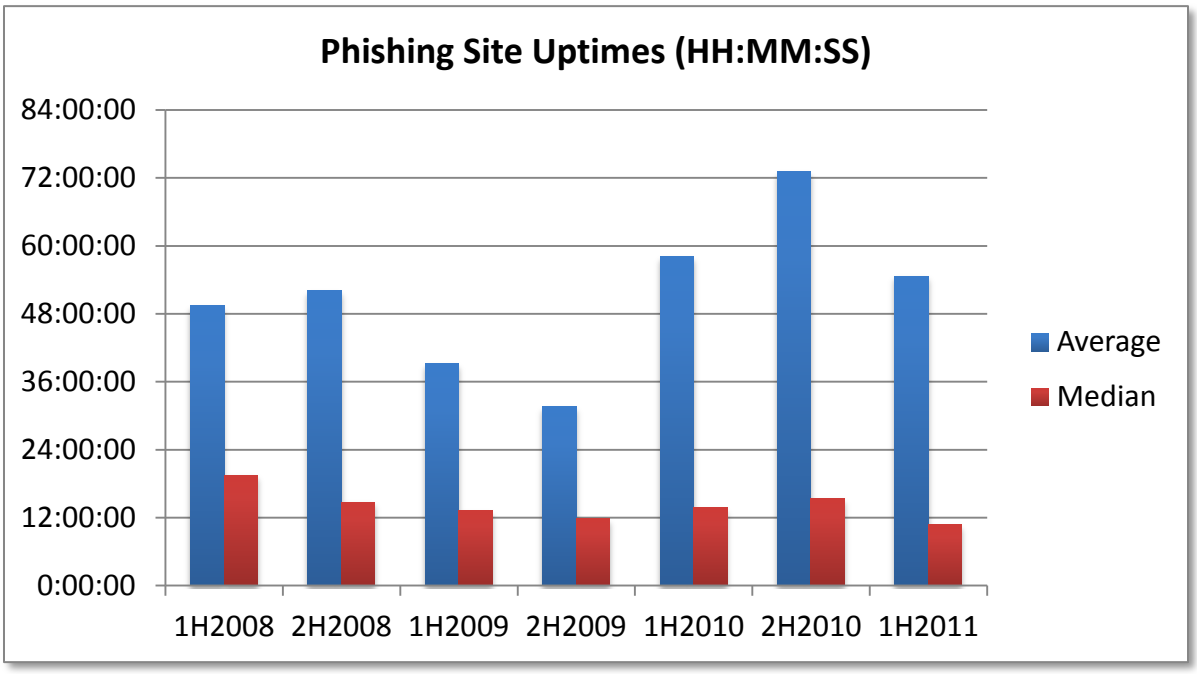
The current statistics confirm that while CNNIC and APAC have had admirable success preventing the use of .CN for phishing, **the phishers have simply gone to other TLDs and services to find resources.** Without outreach, data sharing, and strong anti-phishing efforts by the target institutions, Chinese consumers and institutions will remain at risk.

The above phishing is separate from the issue of spear-phishing attacks apparently originating in China in attempts to penetrate the personal e-mail accounts of government officials and journalists.

Phishing By Uptime

After reaching highs in 2H2010, the average and median uptimes of phishing attacks dropped notably in 1H2011. The average uptime was 54 hours and 37 minutes, compared to 73 hours in 2H2010. The median uptime was 10 hours and 44 minutes, the lowest median we have recorded in four years.

The "uptimes" or "live" times[5] of phishing attacks are a vital measure of how damaging phishing attacks are, and are a measure of the success of mitigation efforts. The longer a phishing attack remains active, the more money the victims and target institutions lose. The first two days of a phishing attack are believed to be the most lucrative for the phisher, so quick takedowns are essential. Long-lived phish can skew the averages since some phishing sites may last weeks or even months, so medians are also a useful barometer of overall mitigation efforts. CNNIC did not record the uptimes of the phish it documented, so those phish were not part of our uptime calculations.



One major factor for the drop was the use of shared virtual server hacking. Over a third of all phishing sites in the first half of 2011 were on shared virtual servers (see section above for more information), and the median phishing site uptime for attacks against shared virtual servers was 9 hours 45 minutes versus 12 hours 40 minutes for all other phishing sites. But even factoring out such sites, uptimes were still down from the prior period, and one of the lowest we've ever recorded. This is good news for the industry, as a majority of sites are now coming down in under 10 hours! That makes for fewer victims, which may partly explain why phishers are putting up more sites. However, if they continue to put up shorter-lived sites, their overall effectiveness is lower, and thus their "costs" are higher. Making things harder for criminals and raising their "cost of doing business" is a goal that all anti-abuse forces share.

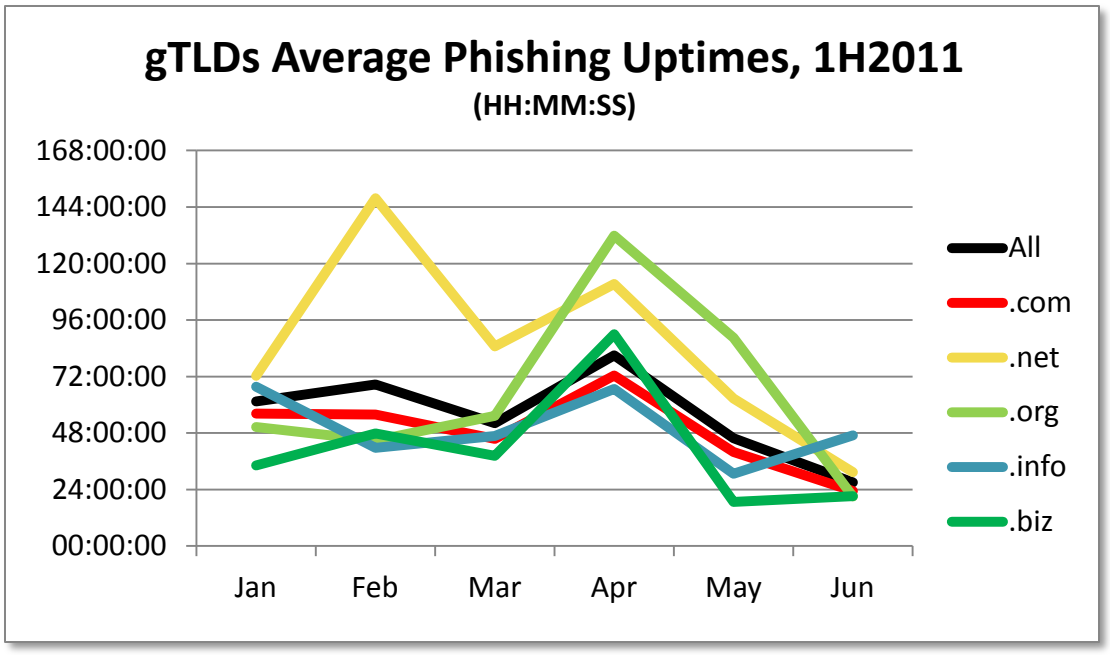
---

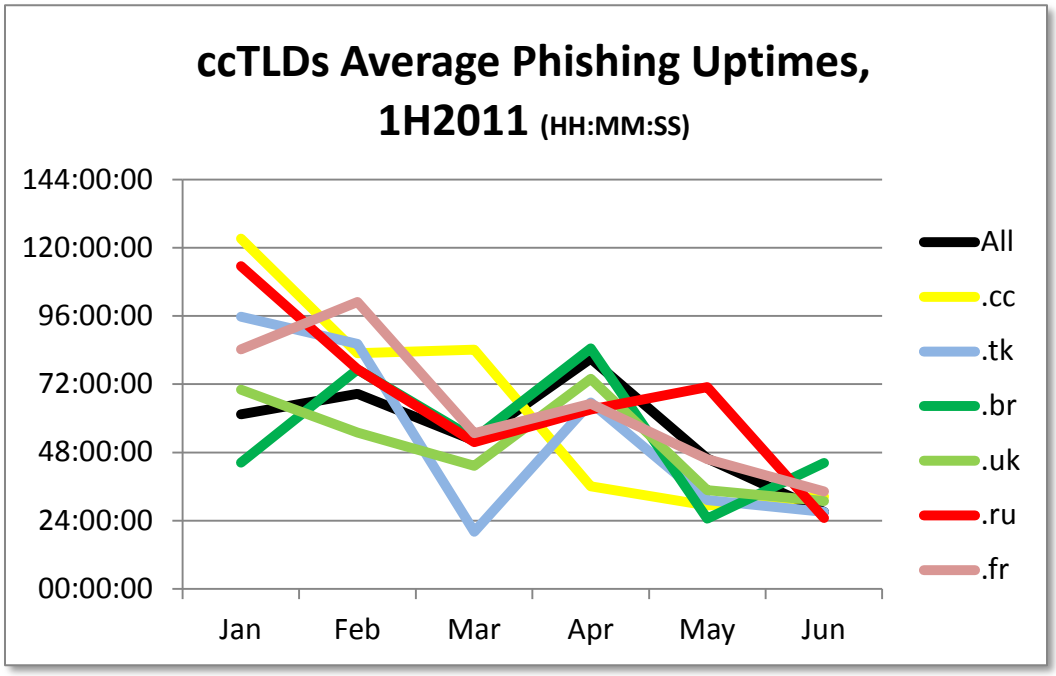
[5] The system used to track the uptimes automatically monitored the phishing sites, and monitoring began as soon as the system became aware of a phish via feeds or honeypots. Each phish was checked several times per hour to confirm its availability, and was not declared "down" until it had stayed down for at least one hour. (This requirement was used because some phish, especially those hosted on botnets, may not resolve on every attempt but in general remain live.) This estimate tends to under-count the "real" uptime of a phishing site, since more than 10% of sites "re-activate" after one hour of being down. However, our method is a consistent measure that allows direct comparison across incidents and should be fair for relative comparisons.

The uptimes for the last four years were:

All Phish, All TLDs	Average (HH:MM)	Median (HH:MM)
Jun 2011	27:04	9:55
May 2011	45:49	10:44
Apr 2011	80:57	13:38
Mar 2011	52:09	10:49
Feb 2011	68:36	12:40
Jan 2011	61:23	9:31
1H2011	**54:37**	**10:44**
2H2010	**73:05**	**15:19**
1H2010	**58:10**	**13:42**
2H2009	**31:38**	**11:44**
1H2009	**39:11**	**13:15**
2H2008	**52:01**	**14:43**
1H2008	**49:30**	**19:30**

The uptimes for all phishing attacks in 1H2011, and for phish in large TLDs, tracked similarly:





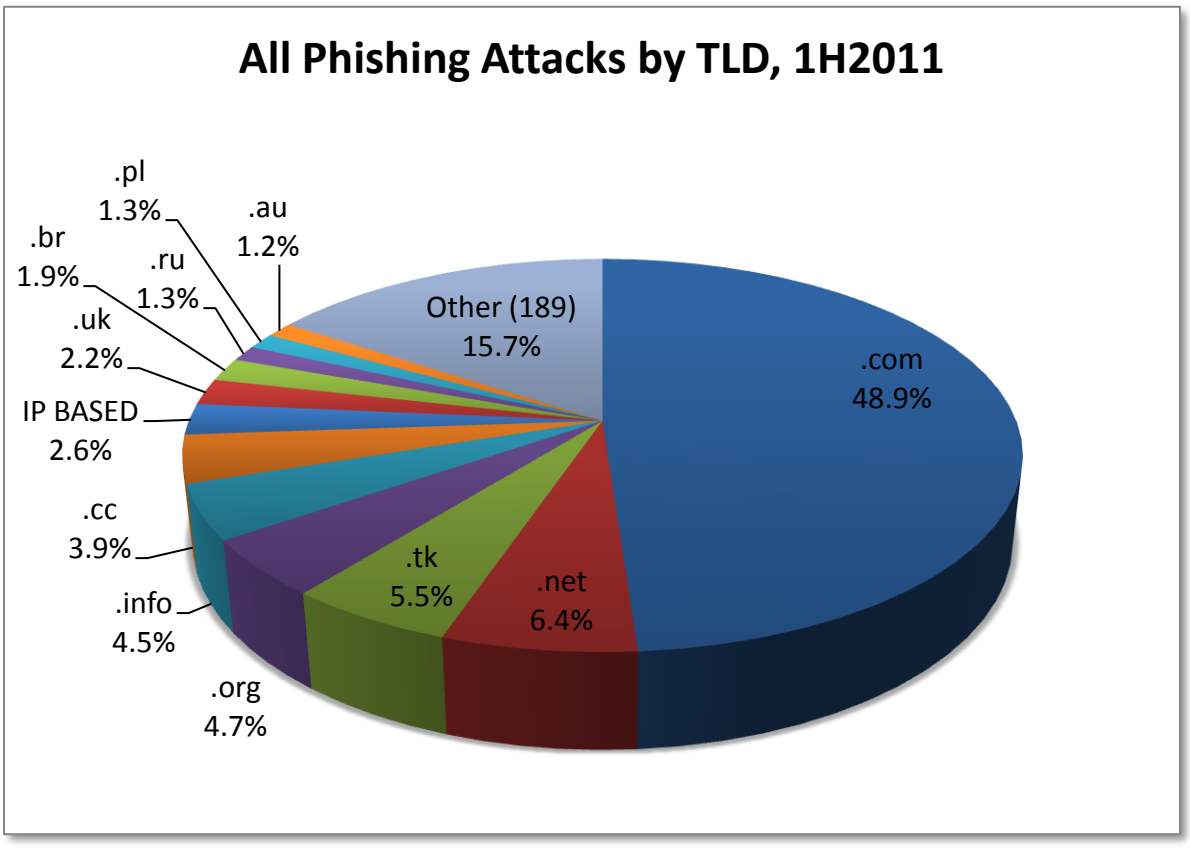
Uptimes by TLD, 1H2011

TLD	Average (HH:MM)	Median (HH:MM)
All	54:37	10:45
.com	47:33	9:55
.net	81:43	11:42
.org	60:32	9:55
.info	47:13	15:35
.biz	37:14	9:31
.tk	37:31	15:35
.cc	75:55	17:44
.br	52:10	13:40
.uk	50:40	11:37
.ru	61:41	12:40
.fr	62:10	17:31
.pl	57:43	14:11
.au	74:37	17:32

Prevalence of Phishing by Top-Level Domain (TLD)

We analyzed the phishing domains and attacks to see how they were distributed among the TLDs. **The complete tables are presented in the Appendix.**

The majority of phishing continues to be concentrated in just a few namespaces. Except for .TK and CO.CC, which were taken advantage of extensively by phishers, phishing was roughly distributed by market share.



To put the numbers in context and measure the prevalence of phishing in a TLD, we use the metrics "Phishing Domains per 10,000" and "Phishing Attacks per 10,000." "Phishing Domains per 10,000"[6] is a ratio of the number of domain names used for phishing in a TLD to the number of registered domain names in that TLD. This metric is a way of revealing whether a TLD has a higher or lower incidence of phishing relative to others.

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

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

- **The median domains-per-10,000 score was 4.6**.

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

- **The average domains-per-10,000 score of 11.3** 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 4.3.** .COM contains 53% 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 4.3 and the median of 4.6 occupy the middle ground, with scores above 4.6 indicating TLDs with increasingly prevalent phishing. [7]

Top 10 Phishing TLDs by Domain Score, 1H2011

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

RANK	TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing 1H2011	Domains in registry, May 2011	Score: Phish per 10,000 domains 1H2011
1	.ma	Morocco	305	182	39,448	**46.1**
2	.th	Thailand	151	89	54,744	**16.3**
3	.tk	Tokelau	6,333	6,214	5,240,299	**11.9**
4	.hr	Croatia	117	90	81,174	**11.1**
5	.ir	Iran	309	201	200,300	**10.0**
6	.pe	Peru	74	49	50,790	**9.6**
7	.in	India	942	781	968,952	**8.1**
8	.rs	Serbia	71	51	63,922	**8.0**
9	.nz	New Zealand	586	351*	440,576	**8.0**
10	.my	Malaysia	114	90	121,452	**7.4**

.MA (Morocco) was victimized by phishers with a taste for hacking; all the .MA domains were compromised, and 95% of those attacks targeted PayPal. .TH has been at the top of our list for three years. Phishing in .TH takes place mostly on compromised academic (AC.TH) and government (GO.TH) Web servers. There was even a phish on the domain rta.mi.th, the Web site of the Royal Thai Army.

The phishing on the other TLDs was on compromised domains almost exclusively, with the exceptions of .IN and .TK. More than a third of the attacks in .IN were attacks against Chinese institutions, using domains registered by Chinese phishers. The phishing on .NZ was

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

due almost entirely to shared virtual server hacking attacks, and .NZ was otherwise quite free of phishing problems.

.TK had more phishing domains than any TLD except .COM. .TK is a liberalized country code domain; the registry is a joint venture of the small Pacific nation of Tokelau and BV Dot TK, a privately held company. By offering free domain names, .TK has become the third-largest ccTLD in the world after Germany's .DE and Great Britain's .UK.

The downside is that the free .TK domain names became a popular resource for phishers in 2010. Every .TK domain used for phishing in 2H2010 and 1H2011 was maliciously registered. In 1H2011, most of the .TK domains—5,518 of the 6,333 —were used to phish Chinese institutions.

In an attempt to reduce phishing, BV Dot TK instituted a new program in 1H2011 that gives anti-phishing partners direct access to the registry, so that they can immediately suspend .TK names themselves. BV Dot TK notes that "With the API, we allow trusted partners to automatically cancel any domain name registrations which they find are abused for spam, phishing, or malware. We are actively looking for other trusted partners to add." These partners include Facebook, Internet Identity, and the Anti-Phishing Alliance of China (APAC). Preliminary reports indicate that .TK phishing has dropped 40% in the third quarter of 2011.

If TLDs are ranked by Attacks per 10,000, .CC continues to rank highly, due to the 4,547 attacks that used CO.CC subdomains. (See "Use of Subdomain Services for Phishing" below).

Compromised Domains vs. Malicious Registrations

We performed an analysis of how many domain names were registered by phishers, versus phish that appeared on compromised (hacked) domains. These different categories are important because they present different mitigation options for responders, and offer insights into how phishers commit their crimes. We flagged a domain as malicious if it was reported for phishing within a very short time of being registered, and/or contained a brand name or misleading string, and/or was registered in a batch or in a pattern that indicated common ownership or intent.

Of the 79,753 domains used for phishing in 1H2011, **we identified 14,650 that we believe were registered maliciously, by phishers (18.3%). The other 71.7% were compromised or hacked domains.** That percentage is the same as in 2H2010.

Of those 14,650 maliciously registered domains, 10,444 (70%) were registered to phish Chinese targets, overwhelmingly Taobao.com. **Otherwise, phishers turned away from registering domains names for their own use.**

Malicious registrations took place in 44 TLDs. **93% of the malicious domain registrations were made in just four TLDs: .TK, .INFO, .COM, and .NET.** All the phishing sites in .TK were on malicious domains, 6,214 total. The other 65,039 domains were hacked or compromised on vulnerable Web hosting.

About 12% of the malicious domains (1,803) were registered to phish World of Warcraft and Battle.net (the online gaming service that supports Warcraft). Online gaming credentials are valuable items for criminals, who sell them on the black market, with prices governed

by how well the associated characters are developed. In-game items can also be sold for real-world cash.

Top 10 TLDs for Maliciously Registered Phishing Domains, 1H2011

RANK	TLD	TLD Location	Unique Domain Names used for phishing 1H2011	Domains in registry, May 2011	# Total Malicious Domains Registered 1H2011	malicious registrations score/10,000 domains in registry
1	tk	Tokelau	6,214	5,240,299	6,214	11.9
2	info	generic TLD	4,705	7,853,775	3,325	4.2
3	com	generic TLD	42,548	97,968,486	3,307	0.3
4	net	generic TLD	5,279	14,344,083	891	0.6
5	in	India	781	968,952	259	2.7
6	uk	United Kingdom	1,882	9,603,189	257	0.3
7	org	generic TLD	3,866	9,270,722	161	0.2
8	cn	China	215	3,379,441	42	0.1
9	us	United States	292	1,732,009	26	0.2
10	br	Brazil	1,341	2,524,286	22	0.1

Of the maliciously registered domains, just 1,816 contained a relevant brand name or variation thereof—often a misspelling.[8] This represents just 2% of all domains that were used for phishing, and 12% of all maliciously registered domains. **These are the lowest numbers we have observed in the last past four years, and show that using domain names containing brand strings has fallen further out of favor among phishers.**

Most maliciously registered domain strings offered nothing to confuse a potential victim. Placing brand names or variations thereof in the domain name itself is not a favored tactic, since brand owners are proactively scanning Internet zone files for such names. As we have observed in the past, **the domain name itself usually does not matter to phishers, and a domain name of any meaning, or no meaning at all, in any TLD, will usually do. Instead, phishers almost always place brand names in subdomains or subdirectories.** This puts the misleading string somewhere in the URL, where potential victims may see it and be fooled. Internet users are rarely knowledgeable enough to be able to pick out the "base" or true domain name being used in a URL.

Use of Subdomain Services for Phishing

We continue to see very high abuse of subdomain services. **Malicious use of these services continued to increase during in the first half of 2011, and accounted for the majority of phishing in many TLDs.** There were 12,574 phish hosted on subdomain services in the first half of 2011, an increase of 7% from the 11,768 attacks we saw in 2H2010. **This is almost as many phish as were found on maliciously registered domain names purchased**

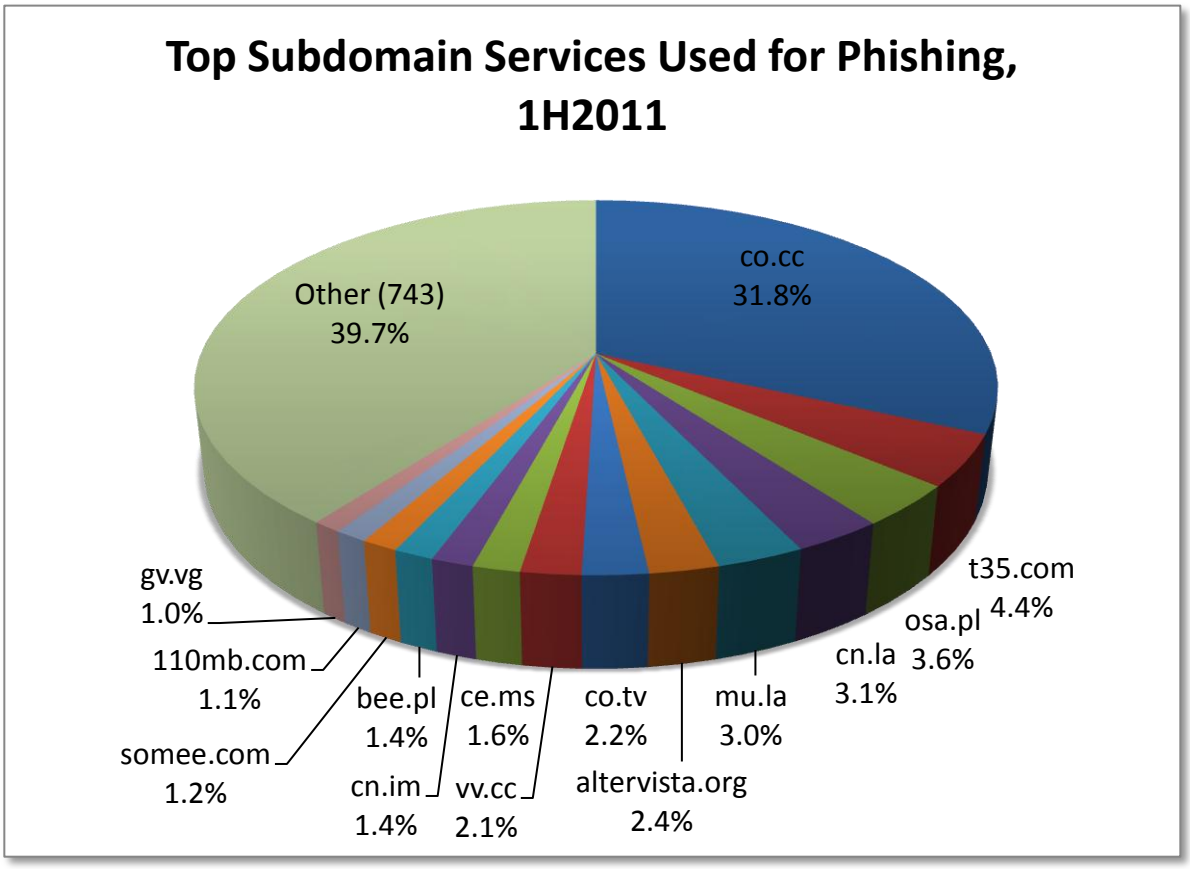
[8] Examples of domain names we have counted as containing brand names included: bid-pagz-yahoo.com (Yahoo!), battleuswow.net (World of Warcraft), ntwestsc.com (Natwest), and fbphonenumbers.tk (Facebook).

by phishers at regular domain name registrars (14,650). If we counted these unique subdomains as "regular" domain names, they would represent around 16% of all domains involved in phishing.

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

<customer_term>.<service_provider_sld>.TLD

Use of subdomain services continues to be a challenge, because only the subdomain providers themselves can effectively mitigate these phish.[9] While many of these services are responsive to complaints, very few take proactive measures to keep criminals from abusing their services in the first place.

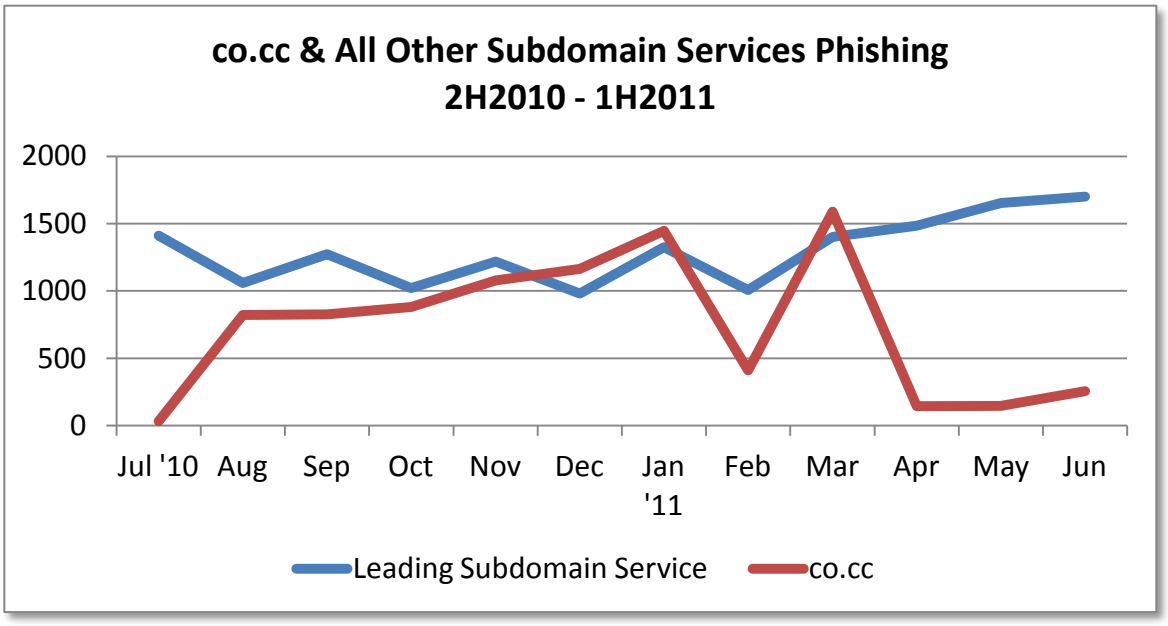


This behavior is exemplified by the top site for subdomain service abuse—the CO.CC service, based in Korea. **Over 30% of attacks using subdomain services occurred on CO.CC**, despite the fact that CO.CC is very responsive to abuse reports. This is actually

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

down from 2H2010. We also see that CO.CC dealt firmly with abuse starting in April 2011.

Volumes plummeted at that time, and while still not free of abuse, are more manageable. We covered phishing utilizing CO.CC extensively in our last report[10].



We have identified over 700 subdomain registration providers, which offer services on more than 3,200 domain names. This is a space as rich as the current "regulated" domain space as 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.

The American provider t35.com remained a distant second place in 1H2011. Third place was occupied by osa.pl, a domain run by the Polish company bee.pl, which runs dozens of domains dedicated to subdomain registration. We'll keep watch for more bee.pl subdomain abuse, since phishers tend to gravitate toward providers that offer very good tools and connectivity.

[10] http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

Top 20 Subdomain Services Used for Phishing, 1H2011

Rank	Domain	Total Attacks	Provider
1	co.cc	3993	CO.CC, Inc.
2	t35.com	554	t35.com
3	osa.pl	451	bee.pl
4	cn.la	389	cn.la
5	mu.la	377	mu.la
6	altervista.org	298	altervista.org
7	co.tv	281	co.tv
8	vv.cc	258	vv.cc
9	ce.ms	203	dotfree
10	cn.im	200	china0750.com
11	bee.pl	174	bee.pl
12	somee.com	157	somee.com
13	110mb.com	141	110mb.com
14	gv.vg	126	gv.vg
15	5gbfree.com	119	5gbfree.com
16	co.be	117	co.be
17	webcindario.com	116	webcindario.com
18	hdfree.com.br	109	HD Free Brazil
19	com3.tw	103	Shark Net
20	free.fr	101	free.fr

Of particular interest is the subdomain reseller CZ.CC. In September 2011, its president was named in a lawsuit brought by Microsoft, which sought to hold the subdomain reseller responsible for botnet activity using CZ.CC subdomains. The suit against the subdomain service was settled in October 2011, but the legal theory behind the suit is novel and has interesting implications.[11] There were 89 phishing sites on CZ.CC in 1H2011, plus extensive evidence from the anti-virus community pointing to malware activity. It will be very interesting to see future implications it has for subdomain providers and registrars who provide DNS naming services.

[11] See the court filing at:
http://media.scmagazineus.com/documents/29/8816kelihos_botnet_complaint_7090.pdf and Microsoft's blog about the settlement:
http://blogs.technet.com/b/microsoft_blog/archive/2011/10/26/microsoft-reaches-settlement-with-piatti-dotfree-group-in-kelihos-case.aspx

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.**

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 six years, IDNs have been available at the second and third levels in many domain name registries, with the majority registered in Asia. IDN TLDs allow the entire domain name to be in non-Latin characters, including the TLD extension. ICANN and IANA enabled the first IDN TLDs in May 2010, and as of this writing there are 38 approved IDN TLDs. While most IDN TLDs are not active, the .рф (.rf) TLD in the Russian Federation claims 839,000 domains.

The IDN homographic attack is a means by which a phisher seeks to deceive Internet users by exploiting the fact that characters in different language scripts may be nearly (or wholly) indistinguishable. Since January 2007, we have found only two homographic phishing attacks:

- On January 16, 2009 the domain name xn--hotmal-t9a.net appeared as "hotmaıl.net" when rendered in enabled browser address bars.
- On July 12, 2010 the domain name http://xn--fcebook-hwa.com appeared as "fácebook.com".

Only 33 other of the 79,742 domain names we studied in 1H2011 were IDNs, and they were all hacked domains. Most were .com domains in Thai characters, on hacked servers in Thailand. None were on IDN TLDs.

Given that IDNs have been widely available for years, why haven't phishers utilized IDN homographic attacks more often?

1. Phishers don't *need* to resort to such attacks. As noted elsewhere in this report, the domain name itself usually does not matter to a phisher.
2. By default, some browser manufacturers show the punycode version of the domain name (such as "xn--hotmal-t9a.net") in the address bar, instead of the native-character version. Users of those browsers therefore cannot see homographic attacks.

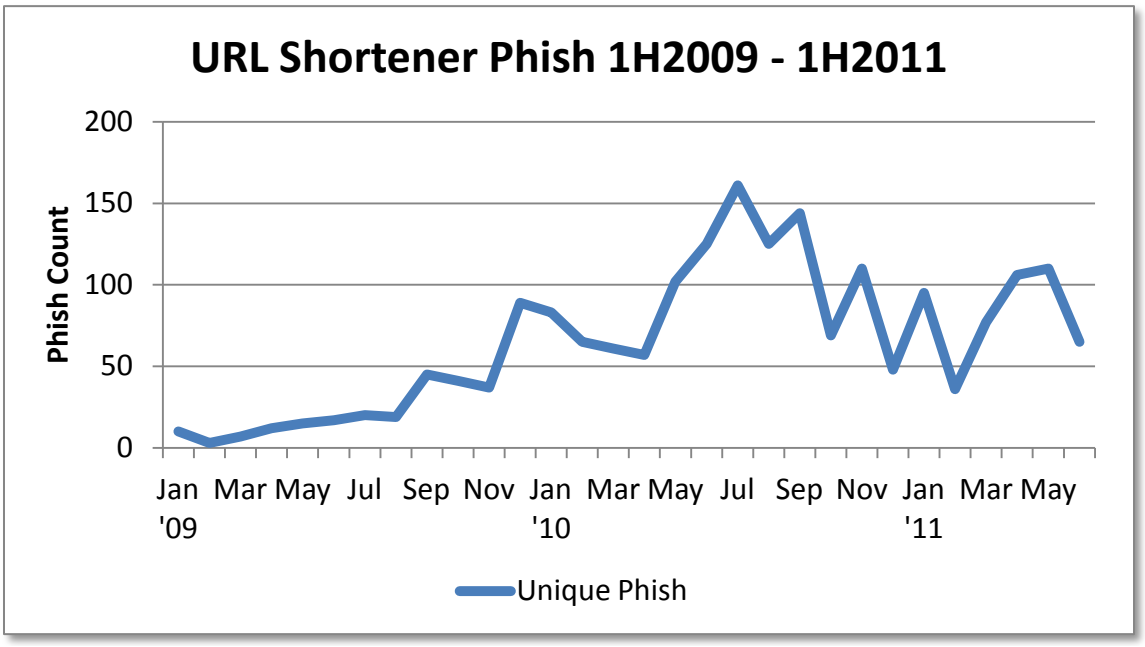
The new IDN TLD registries are being assigned to existing national ccTLD registry operators. We therefore do not believe that they will be more or less vulnerable to abuse than any other domain registry.

Use of URL Shorteners for Phishing

Phishers continue to use "URL shortening" services to obfuscate phishing URLs, but such use is episodic and did not grow in 1H2011. Users of those services can obtain a very short URL to put in their limited-space posts, which automatically redirects the visitor to a much longer "hidden" URL. Use of these URL shorteners has been driven by the popularity of

Twitter and other social networking sites, and mobile phones and computing devices.

Some shortener providers like bit.ly are aggressively screening for malicious forwarding destinations and imposing rules to make it much harder to abuse their systems. But as of this writing, a number of URL shorteners remained blocklisted by Spamhaus, including StumbleUpon's SU.PR and GoDaddy's X.CO service. We encourage all URL shortener providers to implement similar tactics.



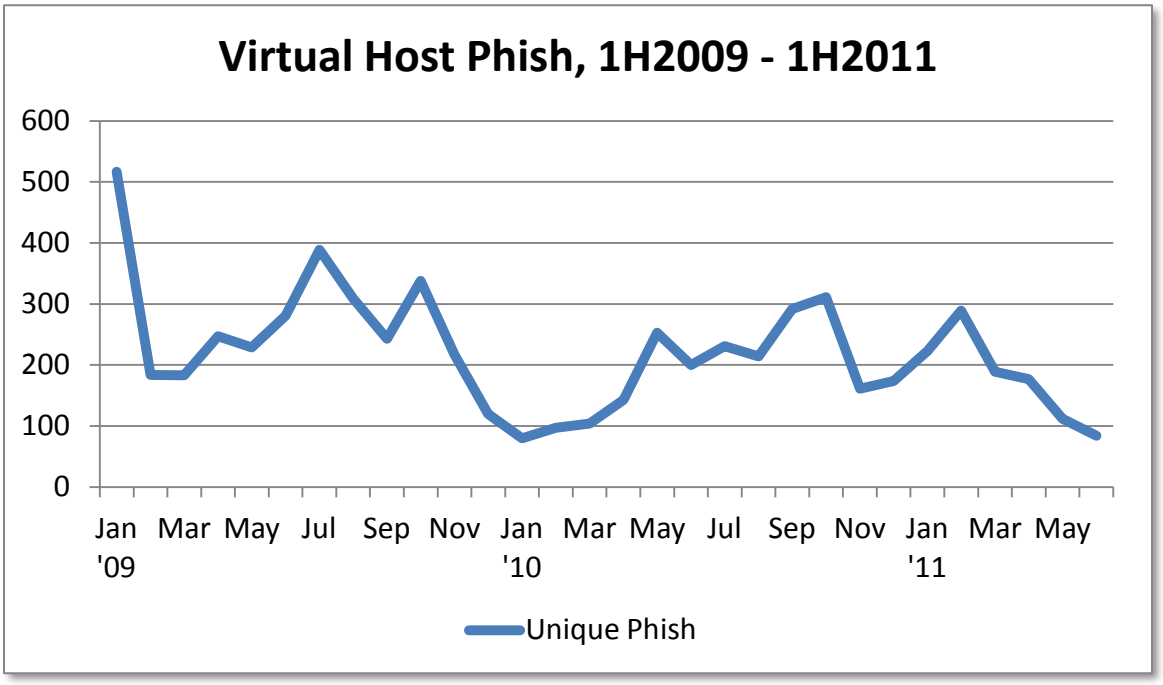
We have also seen criminals create their own fake URL shortener services. The domain's home page may look like any other URL shortener service, but the reality is that the criminals are using the domain strictly for their own purposes. We classify such sites used for phishing as malicious domains.

Use of Virtual Hosts for Phishing

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 Ripway, OVH,net, FortuneCity, and Multimania. We distinguish these types of sites from other shared virtual hosting environment servers where customers bring their own domains for hosting on a single server as discussed earlier in this report.

After a spike early in the year, attacks against such services have dropped to an all-time low. While still not a large portion of phishing, this area is still ripe for abuse, as many of these services are provided free to end-users and are a natural place for phishers to move to if significant pressure is applied elsewhere. Given that, it is interesting to see that such sites do not get abused very heavily, especially compared to hacking attacks against

individual domains/sites.



Conclusions

We're very happy to see that phishing times came down in the last period. Phish that were set up using virtual server hacking came down more quickly compared to other phish. But even factoring out those virtual server phish, phishing uptimes were still down from the prior period, and median uptimes were among the lowest we've ever recorded. This is encouraging news for the Internet. Raising the cost that criminals incur when "doing business" is a goal that all anti-abuse forces share.

The inclusion of phishing data from CNNIC and APAC continues to be a tremendous addition to this report. The Chinese phishers are using domains and subdomains outside of China. To thwart these phishers, institutions in China can share more data with the parties who can take down those domains and their hosting. As we have occasionally seen in the past, changes in TLD registration and security policies have not tended to reduce the overall amount of phishing in the world. Rather, it seems to shift the phishing to other TLDs and services. As we've seen in years past, phishers will gravitate towards certain services they can abuse in bulk, and those that offer low-cost or free resources.

Appendix: Phishing Statistics and Uptimes by TLD

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
ac	Ascension Island	5	5	16,000	3.1	3.1	5:49:21	3:30:41	0	0.0
ad	Andorra	16	1	1,440	6.9	111.1	6:50:36	6:52:17	0	0.0
ae	United Arab Emirates	20	9	87,000	1.0	2.3	20:46:12	11:42:16	0	0.0
aero	sponsored TLD	2	1	7,520	1.3	2.7	20:18:36	20:18:36	0	0.0
af	Afghanistan	4	4	2,000	20.0	20.0	29:00:20	37:52:01	0	0.0
ag	Antigua and Barbuda	0	0	17,921	0.0	0.0			0	0.0
ai	Anguilla	0	0	2,010	0.0	0.0			0	0.0
al	Albania	35	27	5,658	47.7	61.9	45:01:28	12:40:30	0	0.0
am	Armenia	8	7	15,343	4.6	5.2	22:56:36	6:23:03	0	0.0
an	Netherlands Antilles	2	1	1,040	9.6	19.2	1:22:46	1:22:47	0	0.0
ao	Angola	1	1	261	38.3	38.3	62:04:14	62:04:14	0	0.0
ar	Argentina	406	346	2,283,391	1.5	1.8	61:04:04	10:44:18	7	0.0
arpa	Advanced Research Project Agency	1	1				2:59:56	2:59:56	0	0.0
as	American Samoa	1	1				24:16:12	24:16:12	0	0.0
asia	sponsored TLD	35	30	190,690	1.6	1.8	30:54:55	10:49:10	1	0.1
at	Austria	110	87	1,067,665	0.8	1.0	34:42:39	8:29:12	1	0.0
au	Australia	1,431	1,190	2,080,467	5.7	6.9	74:37:28	17:31:40	0	0.0
aw	Aruba	0	0	519	0.0	0.0			0	0.0
az	Azerbaijan	31	18	11,839	15.2	26.2	175:32:21	10:39:33	0	0.0
ba	Bosnia and Herzegovina	28	19	11,640	16.3	24.1	19:03:11	7:09:46	0	0.0
bd	Bangladesh	9	8	4,923	16.3	18.3	79:13:36	23:19:58	0	0.0
be	Belgium	350	158	1,147,315	1.4	3.1	84:19:17	19:27:17	7	0.1
bf	Burkina Faso	1	1				3:29:30	3:29:30	0	0.0
bg	Bulgaria	52	30	24,397	12.3	21.3	22:40:43	4:55:38	0	0.0
bh	Bahrain	1	1				55:03:36	55:03:36	0	0.0
biz	generic TLD	817	586	2,158,857	2.7	3.8	37:14:25	9:31:24	13	0.1
bm	Bermuda	1	1	7,599	1.3	1.3	1:03:37	1:03:37	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
bn	Brunei Darussalam	0	0	1,100	0.0	0.0			0	0.0
bo	Bolivia	36	31	5,942	52.2	60.6	473:37:37	841:07:41	0	0.0
br	Brazil	2,224	1,341	2,524,286	5.3	8.8	52:09:40	13:40:25	22	0.1
bs	Bahamas	1	1	2,300	4.3	4.3	23:14:50	23:14:51	0	0.0
bt	Bhutan	1	1				25:18:02	25:18:02	0	0.0
bw	Botswana	2	2				14:17:54	14:17:55	0	0.0
by	Belarus	33	24				129:11:33	36:44:56	0	0.0
bz	Belize	35	18	47,575	3.8	7.4	90:57:00	15:30:01	0	0.0
ca	Canada	670	515	1,701,378	3.0	3.9	48:23:15	10:49:10	1	0.0
cat	sponsored TLD	9	6	4,709	12.7	19.1	14:40:29	17:46:55	0	0.0
cc	Cocos (Keeling) Islands	4,547	87	1,086,372	0.8	41.9	75:55:05	17:44:06	12	0.1
cd	Congo, Democratic Republic	1	1	5,160	1.9	1.9	1:03:16	1:03:17	0	0.0
cg	Congo	1	1				11:42:23	11:42:23	0	0.0
ch	Switzerland	251	194	1,459,660	1.3	1.7	86:19:53	14:36:57	0	0.0
ci	Côte d'Ivoire	24	15	1,750	85.7	137.1	157:55:48	44:30:39	0	0.0
cl	Chile	311	207	326,175	6.3	9.5	47:45:05	15:18:46	0	0.0
cm	Cameroon	8	5	620	80.6	129.0	14:41:12	3:02:02	0	0.0
cn	China	294	215	3,379,441	0.6	0.9	65:48:57	24:14:30	42	0.1
co	Colombia	251	145	980,000	1.5	2.6	37:58:19	12:26:50	8	0.1
com	generic TLD	56,428	42,548	97,968,486	4.3	5.8	47:33:16	9:55:10	3,307	0.3
coop	sponsored TLD	0	0	9,198	0.0	0.0			0	0.0
cr	Costa Rica	19	13	13,535	9.6	14.0	29:56:49	11:42:31	0	0.0
cu	Cuba	1	1				1:03:33	1:03:34	0	0.0
cx	Christmas Island	17	8	5,200	15.4	32.7	61:23:51	10:39:03	0	0.0
cy	Cyprus	6	6	6,900	8.7	8.7	214:20:00	46:05:21	0	0.0
cz	Czech Republic	198	128	805,281	1.6	2.5	61:45:23	15:29:55	0	0.0
de	Germany	896	610	14,416,242	0.4	0.6	56:02:35	11:40:26	13	0.0
dj	Djibouti	0	0		0.0	0.0			0	0.0
dk	Denmark	188	141	1,124,850	1.3	1.7	58:01:29	23:19:47	1	0.0
dm	Dominica	1	1	14,500	0.7	0.7	35:55:09	35:55:09	0	0.0
do	Dominican Republic	3	3	15,103	2.0	2.0	24:17:17	23:19:43	0	0.0
dz	Algeria	0	0	1,800	0.0	0.0			0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
ec	Ecuador	67	53	22,927	23.1	29.2	22:54:27	6:46:20	1	0.4
edu	U.S. higher education	34	27	7,588	35.6	44.8	52:02:53	40:38:57	0	0.0
ee	Estonia	18	10	62,000	1.6	2.9	17:06:51	4:55:60	0	0.0
eg	Egypt	7	3	5,970	5.0	11.7	46:54:45	37:38:01	0	0.0
er	Eritrea	0	0	105	0.0	0.0			0	0.0
es	Spain	232	186	1,335,603	1.4	1.7	62:38:09	12:40:43	1	0.0
et	Ethiopia	0	0		0.0	0.0			0	0.0
eu	European Union	320	250	3,346,401	0.7	1.0	45:21:16	11:42:11	9	0.0
fi	Finland	85	65	265,066	2.5	3.2	19:36:06	7:50:19	0	0.0
fj	Fiji	0	0	4,000	0.0	0.0			0	0.0
fk	Falkland Islands	0	0		0.0	0.0			0	0.0
fm	Micronesia, Fed. States	7	5				20:15:09	11:37:27	0	0.0
fo	Faroe Islands	0	0	3,000	0.0	0.0			0	0.0
fr	France	680	360	2,034,518	1.8	3.3	62:09:36	17:30:45	8	0.0
gd	Grenada	29	4	3,900	10.3	74.4	22:36:27	8:48:20	0	0.0
ge	Georgia	18	15	18,600	8.1	9.7	65:08:30	17:02:01	0	0.0
gg	Guernsey	11	2				13:02:55	6:52:19	0	0.0
gh	Ghana	3	3				8:33:11	10:49:10	0	0.0
gi	Gibraltar	0	0	1,803	0.0	0.0			0	0.0
gl	Greenland	1	1	4,475	2.2	2.2	9:40:28	9:40:29	0	0.0
gov	U.S. government	0	0	5,000	0.0	0.0			0	0.0
gp	Guadeloupe	26	14	1,475	94.9	176.3	32:57:04	8:24:09	0	0.0
gr	Greece	233	182	323,100	5.6	7.2	69:29:32	8:52:33	0	0.0
gs	South Georgia & Sandwich Is.	2	2	8,100	2.5	2.5	7:15:36	7:15:37	0	0.0
gt	Guatemala	14	10	9,501	10.5	14.7	58:01:55	20:33:24	0	0.0
gy	Guyana	5	1	1,388	7.2	36.0	28:55:29	20:25:00	0	0.0
hk	Hong Kong	56	45	202,338	2.2	2.8	59:04:52	14:31:44	4	0.2
hm	Heard and McDonald Is.	1	1				0:58:32	0:58:32	0	0.0
hn	Honduras	6	5	5,635	8.9	10.6	11:48:54	7:50:02	0	0.0
hr	Croatia	117	90	81,174	11.1	14.4	39:43:11	6:51:43	0	0.0
ht	Haiti	3	3	2,100	14.3	14.3	8:53:19	6:52:07	0	0.0
hu	Hungary	366	260	561,000	4.6	6.5	55:40:56	9:22:36	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
id	Indonesia	99	63				33:27:55	11:42:38	0	0.0
ie	Ireland	145	101	162,546	6.2	8.9	26:18:56	7:50:26	0	0.0
il	Israel	81	60	217,670	2.8	3.7	52:37:34	11:43:35	0	0.0
im	Isle of Man	221	10				29:56:55	11:26:57	1	0.0
in	India	942	781	968,952	8.1	9.7	56:39:27	11:32:45	259	2.7
info	generic TLD	5,199	4,705	7,853,775	6.0	6.6	57:32:26	12:40:45	3,325	4.2
int	sponsored TLD	1	1							
io	British Indian Ocean Terr.	14	14	3,300	42.4	42.4			14	42.4
IP address		2,960	0		0.0	0.0			0	0.0
iq	Iraq	7	4				27:55:42	20:26:07	0	0.0
ir	Iran	309	201	200,300	10.0	15.4	177:49:25	16:27:27	7	0.3
is	Iceland	14	12	33,112	3.6	4.2	27:34:41	8:56:28	0	0.0
it	Italy	450	291	2,195,861	1.3	2.0	98:19:56	16:46:51	5	0.0
je	Jersey	4	3				4:55:20	4:53:07	0	0.0
jm	Jamaica	1	1	6,230	1.6	1.6	21:18:08	21:18:09	0	0.0
jo	Jordan	2	2	4,200	4.8	4.8	7:20:16	7:20:16	0	0.0
jobs	sponsored TLD	0	0	44,482	0.0	0.0			0	0.0
jp	Japan	169	98	1,214,101	0.8	1.4	48:51:37	29:07:13	0	0.0
ke	Kenya	35	29	16,200	17.9	21.6	133:05:02	6:27:45	0	0.0
kg	Kyrgyzstan	6	5	5,000	10.0	12.0	18:31:20	12:58:30	0	0.0
kh	Cambodia	2	1	1,400	7.1	14.3	39:17:50	39:17:51	0	0.0
ki	Kiribati	0	0	250	0.0	0.0			0	0.0
kr	Korea	261	128	1,091,521	1.2	2.4	89:06:23	17:31:20	0	0.0
kw	Kuwait	0	0	2,925	0.0	0.0			0	0.0
ky	Cayman Islands	2	2	6,750	3.0	3.0	15:55:40	15:55:40	0	0.0
kz	Kazakhstan	30	19	58,149	3.3	5.2	39:55:58	11:42:45	0	0.0
la	Lao People's Demo. Rep. *(domains estimated)*	805	13	9,500	13.7	847.4	78:51:09	17:34:33	0	0.0
lb	Lebanon	6	5	2,965	16.9	20.2	85:19:16	8:52:17	0	0.0
lc	St. Lucia	16	7	2,600	26.9	61.5	14:58:30	8:20:01	1	3.8
li	Liechtenstein	6	4	65,995	0.6	0.9	446:48:53	44:37:21	0	0.0
lk	Sri Lanka	20	18	7,775	23.2	25.7	195:16:49	211:33:14	0	0.0
lr	Liberia	1	1							

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
ls	Lesotho	0	0		0.0	0.0			0	0.0
lt	Lithuania	58	47	130,100	3.6	4.5	64:10:30	14:34:13	2	0.2
lu	Luxembourg	9	7	60,955	1.1	1.5	20:15:41	7:50:24	0	0.0
lv	Latvia	14	14	89,600	1.6	1.6	43:44:35	8:42:33	0	0.0
ly	Libya	60	11	9,900	11.1	60.6	26:26:41	6:53:17	0	0.0
ma	Morocco	305	182	39,448	46.1	77.3	26:51:51	5:54:25	0	0.0
mc	Monaco	2	2	1,920	10.4	10.4	178:21:05	178:21:05	0	0.0
md	Moldova	10	7	19,857	3.5	5.0	29:36:17	16:04:13	0	0.0
me	Montenegro	120	78	513,953	1.5	2.3	34:39:21	8:32:07	9	0.2
mg	Madagascar	3	3	1,000	30.0	30.0	22:13:56	16:27:53	0	0.0
mk	Macedonia	10	9				24:20:17	5:14:15	0	0.0
ml	Mali	0	0		0.0	0.0			0	0.0
mn	Mongolia	9	8	9,995	8.0	9.0	10:08:10	7:50:17	0	0.0
mo	Macao	1	1	290	34.5	34.5	16:46:50	16:46:51	0	0.0
mobi	sponsored TLD	38	28	1,044,829	0.3	0.4	167:17:02	12:09:06	2	0.0
mp	Northern Mariana Islands	36	2				8:49:14	3:02:30	0	0.0
mr	Mauritania	0	0		0.0	0.0			0	0.0
ms	Montserrat	217	11	9,000	12.2	241.1	22:22:28	12:40:41	5	5.6
mt	Malta	3	3	12,000	2.5	2.5	3:14:21	2:59:53	0	0.0
mu	Mauritius	30	7	7,500	9.3	40.0	8:54:19	3:30:41	0	0.0
museum	sponsored TLD	0	0	447	0.0	0.0			0	0.0
mv	Maldives	1	1							
mx	Mexico	404	295	498,656	5.9	8.1	37:15:39	9:46:11	1	0.0
my	Malaysia	114	90	121,452	7.4	9.4	69:28:49	8:47:51	1	0.1
mz	Mozambique	2	2	1,885	10.6	10.6	55:36:45	55:36:46	0	0.0
na	Namibia	0	0		0.0	0.0			0	0.0
name	generic TLD	43	32	228,076	1.4	1.9	97:06:31	13:38:30	3	0.1
nc	New Caledonia	0	0		0.0	0.0			0	0.0
ne	Niger	0	0		0.0	0.0			0	0.0
net	generic TLD	7,348	5,279	14,344,083	3.7	5.1	81:43:15	11:42:29	891	0.6
nf	Norfolk Island	10	2	1,600	12.5	62.5	35:32:21	9:31:03	0	0.0
ng	Nigeria	13	10	1,350	74.1	96.3	27:29:13	9:55:10	0	0.0
ni	Nicaragua	2	2	5,900	3.4	3.4	17:31:05	17:31:06	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
nl	Netherlands	520	417	4,486,891	0.9	1.2	61:16:01	14:23:38	0	0.0
no	Norway	91	66	516,359	1.3	1.8	67:46:20	27:45:18	0	0.0
np	Nepal	44	27	25,250	10.7	17.4	43:04:17	26:28:04	0	0.0
nr	Nauru	1	1	450	22.2	22.2	138:30:59	138:30:59	0	0.0
nu	Niue *(domains estimated)*	88	30	59,385	5.1	14.8	39:58:55	15:34:31	0	0.0
nz	New Zealand	586	351	440,576	8.0	13.3	123:58:44	56:13:32	1	0.0
om	Oman	1	1				0:40:50	0:40:50	0	0.0
org	generic TLD	5,438	3,866	9,270,722	4.2	5.9	60:32:11	9:55:10	161	0.2
pa	Panama	1	1	6,295	1.6	1.6	1:03:47	1:03:48	0	0.0
pe	Peru	74	49	50,790	9.6	14.6	55:25:08	17:30:51	0	0.0
pf	French Polynesia	2	2	180	111.1	111.1	8:48:20	8:48:21	0	0.0
pg	Papau New Guinea	3	1							
ph	Philippines *(domains estimated)*	113	49	29,737	16.5	38.0	42:24:14	11:42:45	0	0.0
pk	Pakistan *(domains estimated)*	122	97	17,860	54.3	68.3	22:46:26	9:31:24	0	0.0
pl	Poland	1,486	553	2,110,472	2.6	7.0	57:42:58	14:11:08	1	0.0
pn	Pitcairn	6	3	860	34.9	69.8	163:38:45	11:41:33	0	0.0
pro	sponsored TLD	7	7	110,609	0.6	0.6	6:37:15	6:06:48	0	0.0
ps	Palestinian Territory	15	15	7,450	20.1	20.1	47:44:43	3:30:41	0	0.0
pt	Portugal	74	54	370,830	1.5	2.0	33:38:57	12:38:39	0	0.0
py	Paraguay	21	20	12,155	16.5	17.3	82:11:37	124:01:35	0	0.0
qa	Qatar	3	1				23:10:25	33:15:44	0	0.0
re	Réunion	4	3	7,006	4.3	5.7	49:07:01	49:35:54	0	0.0
rf (.рф)	Russian Federation IDN (.xn--p1ai)	0	0	839,394	0.0	0.0			0	0.0
ro	Romania	324	194	524,310	3.7	6.2	92:20:33	14:06:48	0	0.0
rs	Serbia	71	51	63,922	8.0	11.1	36:58:02	13:31:36	0	0.0
ru	Russian Fed.	1,509	894	3,280,386	2.7	4.6	61:40:32	12:40:10	3	0.0
rw	Rwanda	3	2				90:02:13	89:57:59	0	0.0
sa	Saudi Arabia	41	26	24,600	10.6	16.7	36:17:40	10:49:10	0	0.0
sc	Seychelles	0	0	4,569	0.0	0.0			0	0.0
sd	Sudan	29	26				254:20:33	114:17:03	0	0.0
se	Sweden	173	126	1,087,662	1.2	1.6	113:39:51	27:32:31	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
sg	Singapore	61	50	129,221	3.9	4.7	38:02:18	15:34:07	0	0.0
sh	Saint Helena	1	1				40:45:35	40:45:36	0	0.0
si	Slovenia	36	23	99,500	2.3	3.6	45:33:56	7:18:28	0	0.0
sk	Slovakia	81	65	246,461	2.6	3.3	82:22:44	49:26:12	0	0.0
sl	Sierra Leone	0	0	850	0.0	0.0			0	0.0
sm	San Marino	0	0	1,900	0.0	0.0			0	0.0
sn	Senegal	0	0	3,010	0.0	0.0			0	0.0
so	Somalia	3	3							
sr	Suriname	5	4							
st	Sao Tome and Principe	17	7				17:42:57	11:42:29	0	0.0
su	Soviet Union	40	19	93,967	2.0	4.3	46:04:36	14:14:30	0	0.0
sv	El Salvador	7	5	5,000	10.0	14.0	38:50:11	16:32:28	0	0.0
sy	Syria	3	2				537:08:00	7:45:07	0	0.0
sz	Swaziland	0	0	1,095	0.0	0.0			0	0.0
tc	Turks and Caicos	34	16	10,400	15.4	32.7	14:50:39	7:26:52	0	0.0
tel	generic TLD	0	0	275,781	0.0	0.0			0	0.0
tf	French Southern Territories	6	5	1,550	32.3	38.7			0	0.0
tg	Togo	1	1				132:41:58	132:41:59	0	0.0
th	Thailand	151	89	54,744	16.3	27.6	135:19:59	24:17:55	0	0.0
tj	Tajikistan	9	2	18,700	1.1	4.8	66:50:07	1:51:46	0	0.0
tk	Tokelau	6,333	6,214	5,240,299	11.9	12.1	37:31:10	15:35:29	6,214	11.9
tl	Timor-Leste	8	3	1,795	16.7	44.6	62:00:24	9:21:12	0	0.0
tm	Turkmenistan	1	1	3,775	2.6	2.6	10:33:20	10:33:20	0	0.0
tn	Tunisia	1	1	9,705	1.0	1.0	53:14:09	53:14:10	0	0.0
to	Tonga	92	28	14,000	20.0	65.7	119:24:50	8:48:43	1	0.7
tp	Portuguese Timor	0	0		0.0	0.0			0	0.0
tr	Turkey	74	60	258,248	2.3	2.9	88:09:21	17:23:48	0	0.0
travel	sponsored TLD	3	3	26,675	1.1	1.1	15:11:06	11:42:10	0	0.0
tt	Trinidad and Tobago	1	1	2,200	4.5	4.5	8:47:58	8:47:59	0	0.0
tv	Tuvalu *(domains est.)*	379	81	214,788	3.8	17.6	23:01:06	9:45:35	0	0.0
tw	Taiwan	383	121	499,831	2.4	7.7	67:49:30	20:25:53	0	0.0
tz	Tanzania	20	16	4,130	38.7	48.4	15:21:51	8:07:09	0	0.0
ua	Ukraine	266	190	551,653	3.4	4.8	54:10:06	13:40:11	0	0.0

TLD	TLD Location	# Unique Phishing attacks 1H2011	Unique Domain Names used for phishing, 1H2011	Domains in registry, May 2011	Score: Phish domains per 10,000 domains, 1H2011	Score: Attacks per 10,000 domains, 1H2011	Average Uptime, 1H2011 (hh:mm:ss)	Median Uptime, 1H2011 (hh:mm:ss)	# Total Malicious Domains Registered 1H2010	Malicious registrations score/10,000 domains in registry
ug	Uganda	15	9	3,250	27.7	46.2	54:31:32	45:34:54	0	0.0
uk	United Kingdom	2,490	1,882	9,603,189	2.0	2.6	50:40:29	11:37:04	257	0.3
us	United States	387	292	1,732,009	1.7	2.2	58:54:51	9:45:46	26	0.2
uy	Uruguay	16	12	31,448	3.8	5.1	37:02:18	24:57:21	0	0.0
uz	Uzbekistan	4	3	12,101	2.5	3.3	11:27:40	10:44:16	0	0.0
vc	St. Vincent and Grenadines	8	4	6,756	5.9	11.8	8:08:46	5:51:15	0	0.0
ve	Venezuela	25	23	145,761	1.6	1.7	58:24:38	37:52:01	0	0.0
vg	British Virgin Islands	135	5	8,438	5.9	160.0	18:08:55	13:26:22	0	0.0
vi	Virgin Islands	0	0	17,060	0.0	0.0			0	0.0
vn	Vietnam	144	92	228,900	4.0	6.3	46:49:48	15:32:35	0	0.0
vu	Vanuatu	4	2				57:14:09	19:18:06	0	0.0
ws	Samoa	128	56	544,500	1.0	2.4	21:24:55	6:52:03	1	0.0
xxx	sponsored TLD	0	0	0	0.0	0.0			0	0.0
ye	Yemen	0	0	835	0.0	0.0			0	0.0
yu	Yugoslavia (TLD deprecated March 2010)	0	0	0	0.0	0.0			0	0.0
za	South Africa	412	315	660,224	4.8	6.2	51:36:40	12:40:43	1	0.0
zm	Zambia	0	0		0.0	0.0			0	0.0
zw	Zimbabwe	4	4	11,923	3.4	3.4	92:03:08	41:15:41	0	0.0
	TOTALS	**115,472**	**79,753**	**218,811,649**					**14,650**	

About the Authors & Acknowledgments

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

Rod Rasmussen is President and CTO of Internet Identity (www.internetidentity.com), and has served as its technical leader since he co-founded the company in 2001. He is widely recognized as a leading expert on the abuse of the domain name system by 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, its 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 President of Illumintel Inc., which provides advising to existing and new operators of top-level domains. He was previously the Director of Key Account Management and Domain Security at Afilias (www.afilias.info), and Greg continues to contribute to Afilias' security programs, including anti-abuse services for the .ORG registry. Greg is an authority on the use of domain names for e-crime, and works with registrars, registries, law enforcement, and researchers regarding phishing, malware, spam, and child pornography cases. In 2010, Greg accepted an OTA Excellence in Online Trust Award for Afilias' anti-abuse programs. He was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG), and joined ICANN's Security and Stability Advisory Committee (SSAC) in October 2011. 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.

#