Global Phishing Survey: Trends and Domain Name Use in 2016

APWG

Unifying the
Global Response
To Cybercrime

An
APWG
Industry
Advisory

Published 26 June 2017

Authors:

Greg Aaron,

iThreat Cyber Group

and

Rod Rasmussen,

R2 Cyber

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.*

Table of Contents

OVERVIEW 4
KEY STATISTICS 5
TARGET DISTRIBUTION 7
PREVALENCE OF PHISHING BY TOP-LEVEL DOMAIN (TLD) 10
THE NEW TOP-LEVEL DOMAINS 14
MALICIOUS REGISTRATIONS VS. COMPROMISED DOMAINS 16
DOMAIN AGING 18
REGISTRARS USED FOR MALICIOUS DOMAIN REGISTRATIONS 19
THE RISE OF DOMAIN SHADOWING FOR PHISHING 21
USE OF SUBDOMAIN SERVICES FOR PHISHING 22
USE OF INTERNATIONALIZED DOMAIN NAMES (IDNS) 25
USE OF URL SHORTENERS FOR PHISHING 26
APPENDIX: PHISHING STATISTICS BY TLD 27
ABOUT THE AUTHORS & ACKNOWLEDGMENTS 48

Overview

This report comprehensively examines a large data set of more than 250,000 phishing attacks detected in 2015 and 2016. By quantifying this cybercrime activity and understanding the patterns that lurk therein, we have learned more about what phishers have been doing, and how they have accomplished their schemes.

Phishers prey on human trust and inattention, setting up web pages that masquerade as trustworthy entities such as a banks and well-known e-commerce sites. Phishers then lure victims to these fake sites through spam emails, IM messages, and other advertisements, and the users are tricked into providing sensitive information such as their usernames, passwords, and credit card details. To accomplish their work phishers often hack into web hosting and email accounts. They steal untold millions of dollars each year, ruin victims' credit ratings, defraud governments, and they leverage stolen credentials for more crimes.

The data used for this report consists of confirmed attacks only. Our statistics under-count the total amount of phishing that occurred in the wild—more attacks were undetected by our sources, and more attacks were reported but not confirmed. The numbers are a baseline compiled through collection and counting methods that have remained consistent over the years. This report measures attacks that broadly targeted the general public, and does not not attempt to quantify spear-phishing, which are attacks directed at a few specific individuals and more difficult to detect and count reliably.

The data was collected by the Anti-Phishing Working Group, and supplemented with data from several phishing feeds, CNNIC, and Internet Identity (now Infoblox). The APWG phishing repository is the Internet's most comprehensive archive of phishing and e-mail fraud activity. We are grateful to CNNIC and the Anti-phishing Alliance of China (APAC) for sharing their data with us. We are also grateful to DomainTools, which provided valuable domain registration data for our analysis.

Our major findings include:

1. **In 2016, the number of phishing attacks, and the number of domain names used for phishing, reached an all-time high.** (Page 5)
2. **Malicious domain name registrations are also at an all-time high, indicating detection and mitigation problems at certain registrars and registries.** (Pages 16-20)
3. **Phishing in the new top-level domains (nTLDS) is rising, but is not yet as pervasive as it is in the domain space as a whole. By the end of 2016, almost half of the nTLDs that were available for open registration had phishing in them. The nTLDs are also a place where phishers are purchasing domain names for themselves.** (Pages 14-15)
4. **New companies are constantly being targeted by phishers, while a few brands face an onslaught of thousands of attacks per year.** (Pages 7-9)
5. **Contrary to conventional wisdom, phishers often wait up to three weeks before using domain names they have registered.** (Page 18)

Key Statistics

Millions of phishing URLs were received by our sources each year, but the number of unique phishing attacks and domain names used to host them was much smaller.[1] Full statistics for 2015 and 2016 are in the Appendix. In 2016:

- **There were *at least* 255,065 unique phishing attacks worldwide**. This represents an increase of over 10% from the 230,280 attacks we identified in 2015. An *attack* is defined as a phishing site that targets a specific brand or entity. A single domain name can host several discrete phishing attacks against different banks, for example.
- **The attacks occurred on 195,475 unique domain names**.[2] **This is the most we have recorded in any year since we began these reports in 2007.** The number of domain names in the world grew from 287.3 million in December 2014 to 329.3 million in December 2016.[3]
- Of the 195,475 domains used for phishing, **we identified 95,424 domain names that we believe were registered maliciously by phishers. This is an all-time high, and almost three times as many as the number we found in 2015**. A little over half of these registrations were made by Chinese phishers. The other 100,051 domains were almost all hacked or compromised on vulnerable Web hosting. This means that **nearly half of all domains that hosted phishing sites were maliciously registered**. Please see pages 16-17 for more detail.
- **Seventy-five percent of the malicious domain registrations were in just four TLDs**: .COM, .CC, .PW, and .TK. More than 90% of malicious domains were found in just 14 TLDs. Please see pages 16-17 for more detail.
- In addition, 6,373 attacks were detected on 5,378 unique IP addresses, rather than on domain names. (For example: http://97.74.228.191/walmart.com/) We did not observe phish of any kind on IPv6 addresses.
- **We counted 679 targeted brands.** This dropped from 783 in 2015. Phishers are still creating kits dedicated to attacking both popular targets and new targets. Please see pages 7-8 for more detail.
- **Phishing occurred in 454 top-level domains (TLDs). Two-hundred twenty-nine (228) were new top-level domains launched since 2013.** Please see pages 14-15 for more detail.
- One-hundred and eighty-six of the 195,475 domain names were internationalized domain names (IDNs). None involved homographic attacks, but some displayed

[1] This is due to several factors: A) Some phishing involves customized attacks by incorporating unique numbers in the URLs, often to track targeted victims, or to defeat spam filters. A single phishing attack can therefore manifest as thousands of individual URLs, while leading to essentially one phishing site. Counting all URLs would therefore inflate some phishing campaigns. Our counting method de-duplicates in order to count unique attacks, and has remained consistent across this and our previous reports. 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.

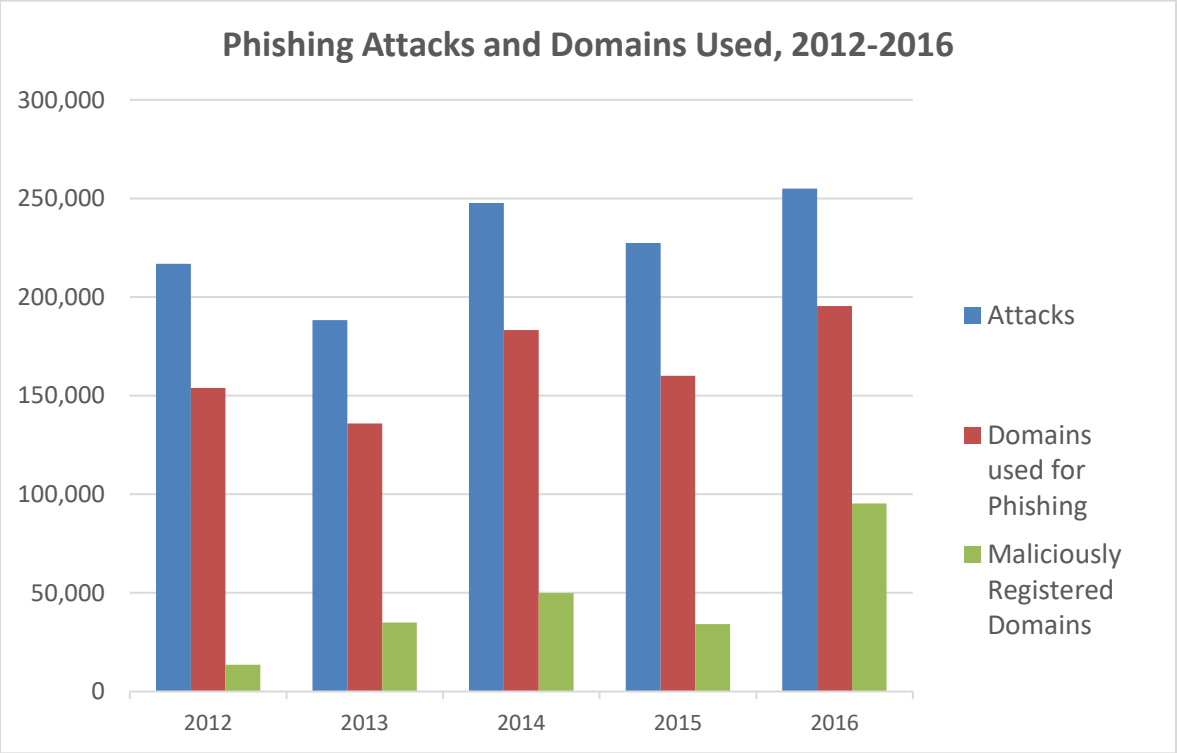
[2] "Domain names" are defined as second-level domain names, plus third-level domain names if the relevant registry offers third-level registrations. An example is the .CN (China) registry, which offers both second-level registrations and third-level registrations (in zones such as com.cn, gov.cn, zj.cn, etc.). However, see the "Subdomains Used for Phishing" section for commentary about how these figures may undercount the phishing activity in a TLD.

[3] Our TLD domain counts come from the official gTLD registry reports published at ICANN.org, numbers published on ccTLD registry operators' web sites, and new gTLD statistics at ntldstats.com. When a registry does not publish its numbers, we rely on DomainTools' TLD statistics.

deceptive messages in the translated domains names. Please see page 25 for more detail.

Basic Statistics

	2012	2013	2014	2015	2016
Domain names used for phishing	153,952	135,848	183,222	160,155	195,475
Attacks	216,938	188,323	247,713	227,471	255,065
TLDs used	204	223	288	355	454
new gTLDs used	0	0	72	120	228
IP-based phish (unique IPs)	4,899	4,366	6,472	2,245	5,378
Maliciously registered domains	13,545	35,004	49,932	34,102	95,424



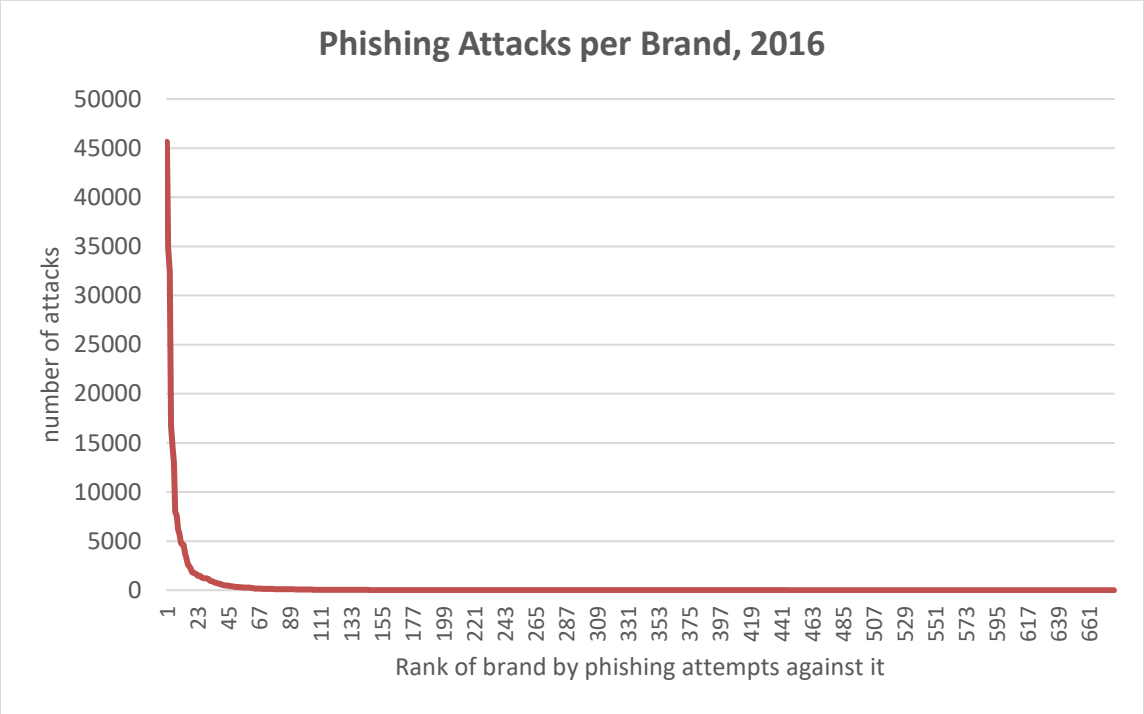
Target Distribution

We counted 679 unique target institutions during 2016, down about 12% from the 783 we found in 2015. Phishers are still creating phishing kits dedicated to attacking both popular targets and new targets. A few targets were extremely popular and accounted for the majority of phishing attacks.

The brunt of phishing is borne by the top ten targets, which suffered over three-quarters of all the phishing attacks mounted in 2016. Phishers continued to attack popular targets PayPal, Yahoo!, Apple, and Taobao.com heavily. Each of these four e-commerce giants suffered more than 30,000 phishing attacks against their respective services and brands in 2016. Together, these top four were the targets of over 57% of the world's phishing attacks. The next seven brands were targeted for a combined 21% of all phishing attacks -- meaning the top 10 targets accounted for 77% of all phishing attacks observed worldwide.

However, a brand can become a target at any time. Each year we observe some "churn" or new diversity in the list of targets. The phishers are looking for companies that have potentially lucrative user bases, are newly popular, and/or are not ready to respond to phishing attacks. If a site takes in personal data, then there may be phishers who want to exploit it.

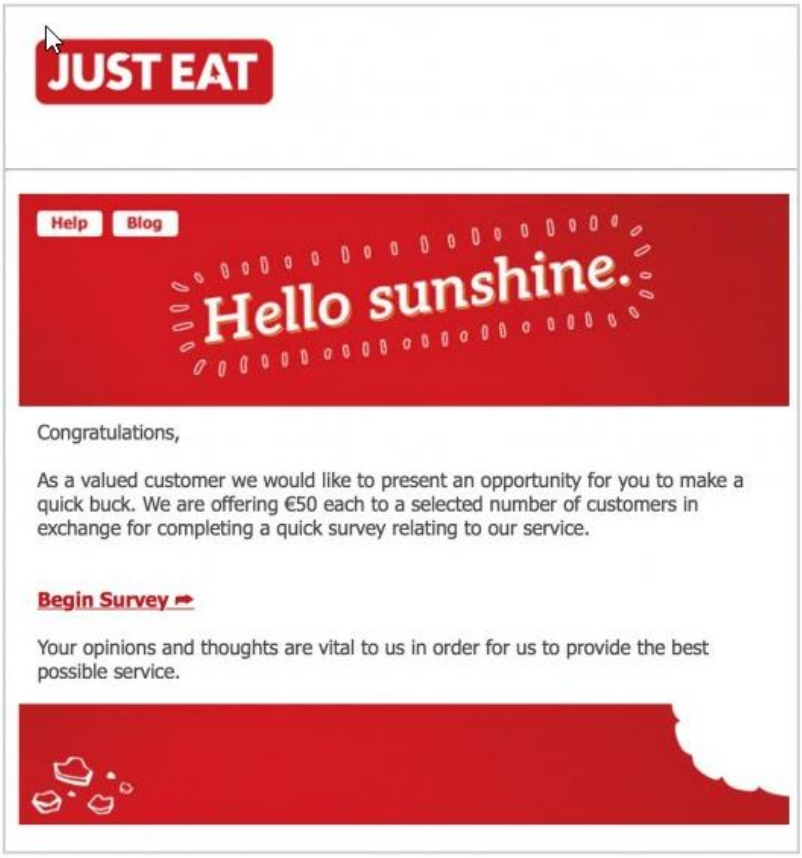
The number of times that the targets were attacked forms a long tail. More than half of the targets were attacked four or fewer times during the year. Two hundred and thirty-four targets were observed being attacked only once each in 2016.



Notably, there were 64,688 phishing sites targeting 79 different Chinese brands, representing 25% of all phishing attacks observed in 2016. Attacks on Chinese targets hit all sectors, from e-commerce giant Taobao to a plethora of Chinese banks and securities companies.

The 2016 target list featured many banks, including a notable list of banks in Latin America, but also throughout Europe, Southeast Asia, the Middle East, and of course, most large North American institutions. There were several targets in non-traditional sectors. Examples of new targets from 2016 include the following:

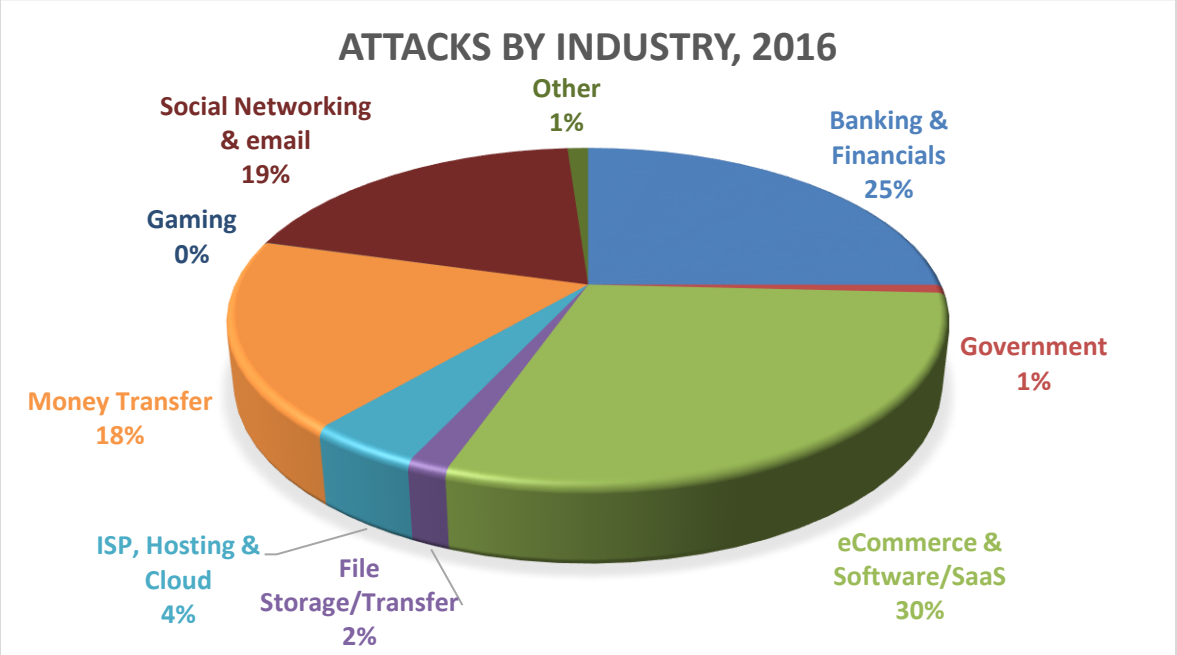
- The major universities in Switzerland
- Television stations throughout the world
- Energy companies
- Government agencies
- Airlines



A phishing lure e-mail targeting Just Eat, a London-based online food delivery service, in January 2016. Credit: Michele Neylon

Overall, phishing still targeted the primary industry sectors we have seen for over a decade, with financial institutions, e-commerce, social networking, and money transfer companies being targeted in over three-quarters of phishing attacks. Attacks where money is handled or moves in commerce are typically designed to directly defraud

victims. Attacks on social networks, e-mail systems usually are attempts to harvest credentials for further use. We are seeing further attacks being launched from such compromised accounts, and we are also seeing continued attacks on ISP's and other Internet services companies to obtain Internet resources to launch further attacks. We are also seeing interesting attacks on File Transfer/Storage services which may well be tied towards attempted data breach.

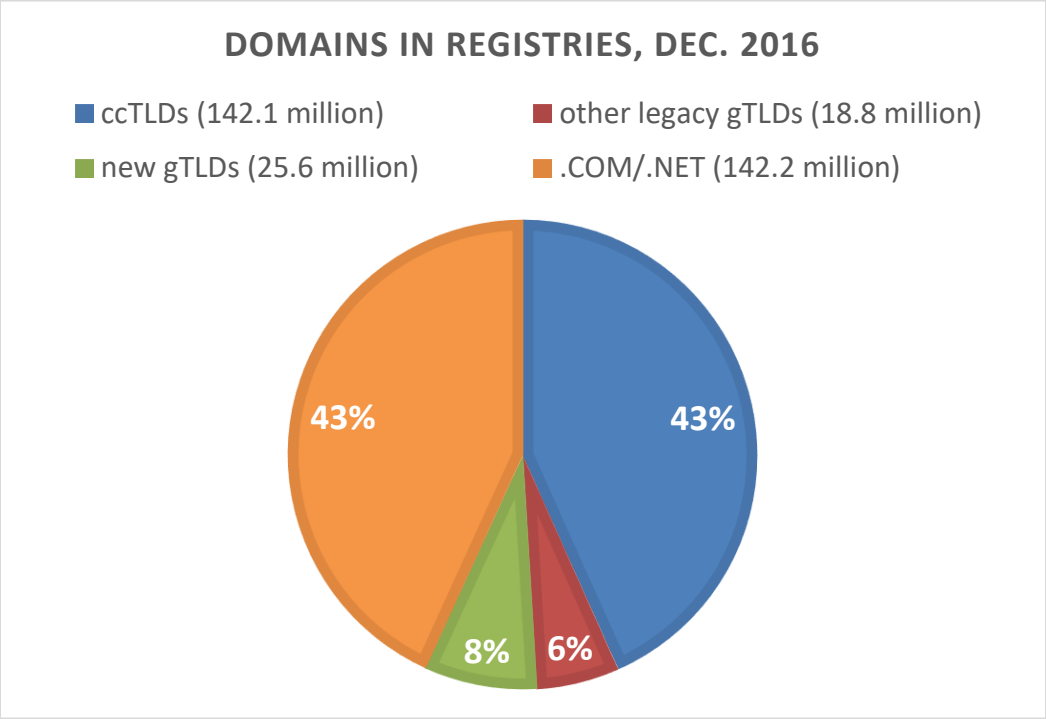


These show criminals seeking the credentials of victims in places where victims may least expect it. With some critical infrastructure and government organizations showing up in reports to the APWG, there is some indication that spear-phishing continues to grow as a problem. Phishers target wide-ranging targets for several reasons. One is to perform credit card theft, and hitting new targets may lull consumers into a false sense of security. The phishers can also monetize stolen data through reshipping fraud, a tactic that remains popular. Phishers also steal usernames and passwords from one site to try those credential on other sites. Many consumers re-use usernames and passwords, and this poor habit can be costly. If a site is getting phished for the first time, it may have been targeted by a more sophisticated phisher, who had the skill to design a new phishing template.

Prevalence of Phishing by Top-Level Domain (TLD)

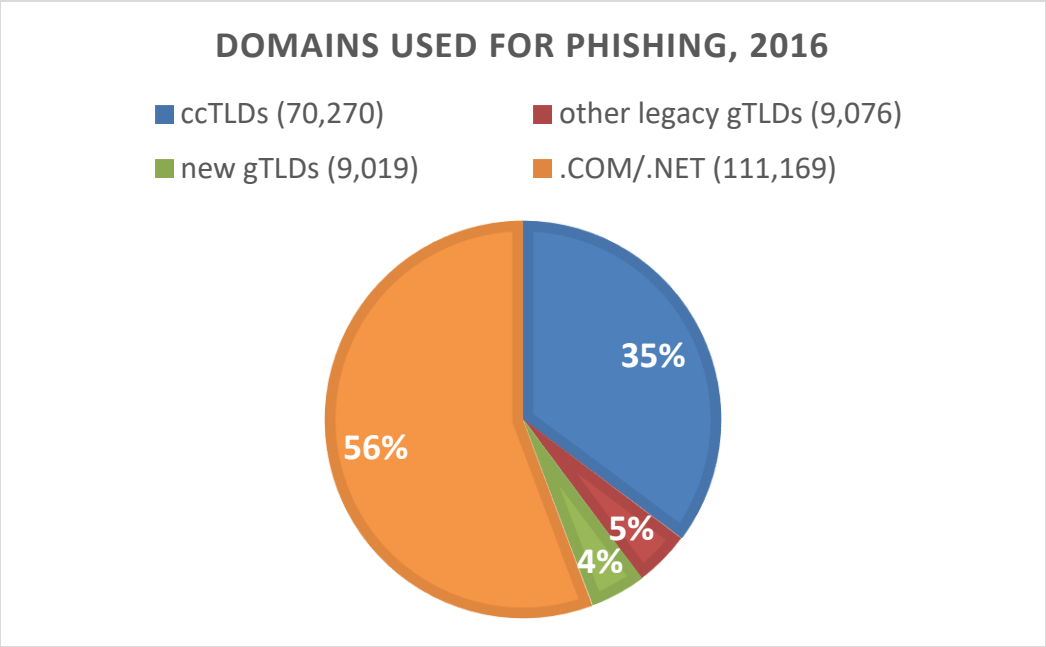
We analyzed the phishing domains and attacks to see how they were distributed among the TLDs. **Most phishing continues to be concentrated in just a few namespaces, with some TLDs having much more prevalent problems than others.**

As of December 2016, there were approximately 329 million domain names in the world's registries. That domain name space can be divided into four categories. The .COM and .NET registries are operated by Verisign and represented 43% of the domains in the world. Country-code domains (ccTLDs) represented another 43%. The legacy generic TLDs[4] introduced before 2013 represented 6%, and the new gTLDs (nTLDs) introduced from 2014 to the present were the remaining 8%:



However, the distribution of phishing does not parallel TLD market share:

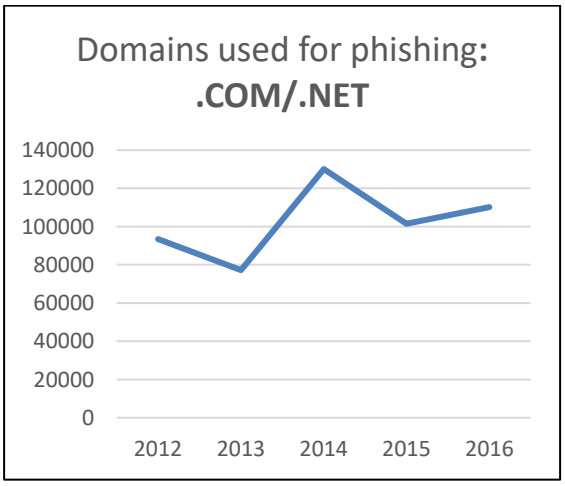
[4] The other "legacy" gTLDs are: .AERO, .ASIA, .BIZ, .CAT, .COOP, .INFO, .JOBS, .MOBI, .MUSEUM, .NAME, .ORG, .PRO, .POST, .TRAVEL, .TEL, and .XXX

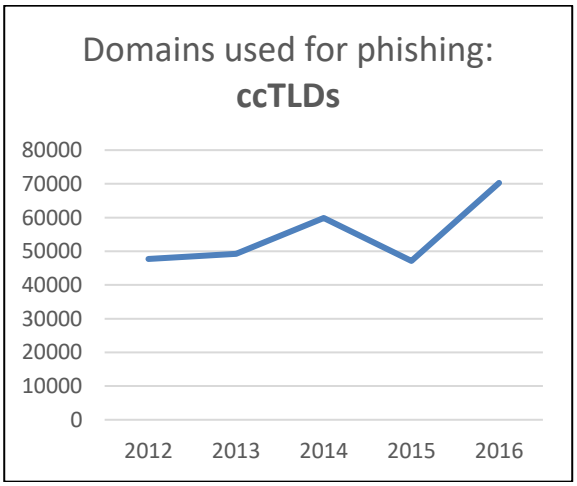


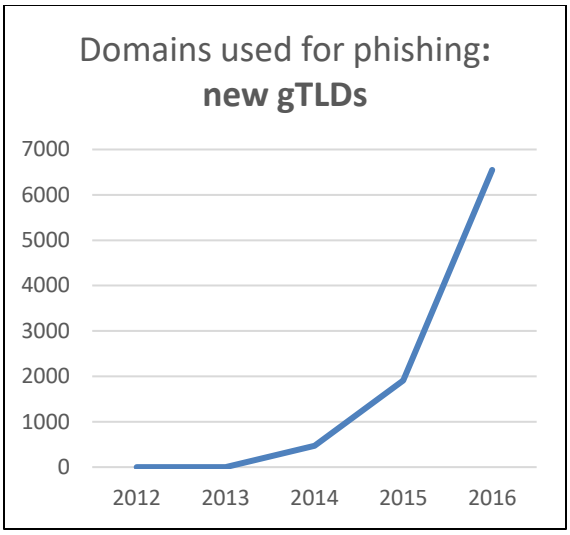
We see that 56% of the domains were in .COM and .NET. This happened for two reasons: there are many .COM web sites to hack and place phish on, and phishers also register large numbers of .COM domains. .COM's domains phishing score rose slightly, from 7.4 in 2015 to 7.9 in 2016.

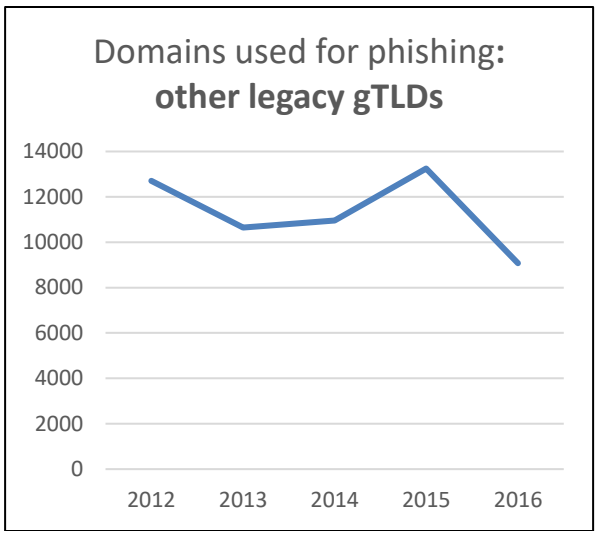
Phishers register smaller numbers of ccTLD domains. This may be because ccTLD domains generally tend to be more expensive than gTLD domains.

On the other hand, the new gTLDs have often been priced more cheaply than any other sector. Looking at the numbers for the past five years, we can see how the new gTLDs have recently contributed more phishing domains, while the legacy gTLDs contributed fewer:









For more about the new gTLDs, see pages 14-15.

To put the numbers in context and measure the prevalence of phishing in each TLD, we use the metrics "Phishing Domains per 10,000" and "Phishing Attacks per 10,000." "Phishing Domains per 10,000"[5] 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 domain and attack scores for each TLD. In 2016, looking at the TLDs that had at least one phishing domain:

- **The median phishing-domains-per-10,000 score was 3.7, and the average was 8.8.**
- **.COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 7.9.**

We therefore suggest that domains-per-10,000 scores between 3.7 and 7.9 occupy the middle ground, with scores above 8.0 indicating TLDs with increasingly prevalent phishing.[6] The top TLDs by score are:

---

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

[6] 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.
- 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, 2016

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

	TLD	TLD Location	# Unique Phishing attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016
1	.VE	Venezuela	1,206	1,045	77,555	134.7
2	.CC	Cocos (Keeling) Islands	13,708	13,061	1,750,000	74.6
3	.ML	Mali	1,448	1,434	220,000	65.2
4	.BD	Bangladesh	272	205	33,000	62.1
5	.KE	Kenya	260	207	50,000	41.4
6	.CENTER	new gTLD	136	135	32,809	41.1
7	.NG	Nigeria	307	267	65,000	41.1
8	.PW	Palau	2,782	2,702	675,000	40.0
9	.PK	Pakistan	301	227	62,000	36.6
10	.RU	Russia	4,340	2,433	735,000	33.1

.VE is the ccTLD of Venezuela. Almost all of the .VE domains noted above were registered by phishers. Similar issues plagued .VE domains nearly a decade ago, primarily due to a single phishing gang's use of a particular registrar. There are strong indications that we're seeing a similar pattern today.

.CC is a commercialized ccTLD; it is administered by Verisign through a subsidiary company, eNIC, which promotes it for generic use. Almost all of the .CC domains used for phishing were registered by Chinese phishers. This indicates a vulnerability in the distribution chain—one or a few registrars allowed repeated .CC registrations by phishers, and response by the registry is also a question. Malicious registrations in .CC have been high over the past three years. Given the damage caused by these campaigns, it would serve the industry players involved to address this long-standing issue.

.ML is the ccTLD of Mali. In 2013 it was repurposed commercially to offer free domains names, along with .CF (Central African Republic), and .GA (Gabon), which also had notable numbers of phishing domains in 2014 through 2016. These TLDs are operated by Freenom, which also operates the free .TK registry.[7] For more about these TLDs, please see "Compromised Domains versus Malicious Registrations" below.

.PW (Palau) is yet another commercialized ccTLD, operated by a company in the United Arab Emirates. In 2014 through 2016 .PW was plagued by Chinese phishers, who registered at least 2,318 domains in 2016 alone to attack Taobao.com, two major Chinese financial institutions, and a few other Chinese targets.

[7] Freenom declines to provide registration numbers, and so our domains-in-registry numbers are from DomainTools.

The New Top-Level Domains

Most new gTLDs (nTLDs) have now been out on the market for more than two years. What phishing is happening in them, and what trends are evident? **Our observations are:**

- **Phishing in the new top-level domains (nTLDS) is rising, but is not yet as pervasive as it is in the domain space as a whole.**
- **By the end of 2016, almost half of the nTLDs that were available for open registration had phishing in them.**
- **The nTLDs are also a place where phishers are purchasing domain names for themselves.**

Beginning in January 2014, the first of the new generic top-level domains (gTLDs) began rolling out. As of December 2016, 1,215 new gTLDs had entered the root, the result of a multi-year process run by the Internet Corporation for Assigned Names and Numbers (ICANN), which coordinates the top level of the Internet. The complete tables are presented in the Appendix, including the domain and attack scores for each TLD.

The number of nTLDs that contain phishing is rising steadily, with phishing occurring in 228 of the nTLDs in 2016:

- 2013: 0
- 2014: 72
- 2015: 120
- 2016: 228

Two-hundred and twenty-eight is almost half of the approximately 498 nTLDs that are available for open registration by any party. Around 720 other nTLDs have restrictions and can be registered only by their registry operators or by qualified entities, and therefore are resistant to malicious registrations. Only 500 nTLDs (open or not) had 100 or more domains in them, and almost half of the nTLDs have less than 10 domains in their registries.[8]

Phishing rates in the new gTLDs are growing, but have not yet reached the world average. In 2016, the median phishing score for all TLDs that had phishing was 3.7, and the average was 8.8. For nTLDs that had phishing, the median score was 2.2 and the average score was 4.0. Sixty-four nTLDs had scores above the world median. Overall nTLD scores may be lower because a smaller percentage of nTLD domains are in consequential use when compared to other TLDs, and there are therefore fewer nTLD domains to compromise. According to ntldstats.com, 59% of new gTLD domains were "parked" in early 2016—they resolved to generic holding and pay-per-click pages, they redirected, or did not resolve at all.[9] This left a pool of only 11.8 million nTLD domains for traditional hacking via website vulnerabilities and other methods. The parking rate for other kinds of TLDs is lower, perhaps 40% according to some historical studies.

Instead, the problem in the nTLDs are malicious registrations, made for the purpose of phishing. Of the 6,549 domains used for phishing in the 228 nTLDs, 86% (5,633) were registered maliciously. (See Compromised Domains vs. Malicious Registrations below.)

[8] https://ntldstats.com/tld
[9] https://ntldstats.com/parking/tld , as of April 2017.

71% of those malicious registrations were found in just ten nTLDs:

	TLD	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains, 2016
1	.TOP	1,687	4,780,500	3.5
2	.XYZ	938	6,743,803	1.3
3	.ONLINE	566	564,822	9.6
4	.WIN	478	1,264,500	3.6
5	.SITE	221	600,244	3.6
6	.LINK	190	381,404	5.0
7	.CLUB	164	910,091	1.8
8	.WEBSITE	142	230,105	6.2
9	.CENTER	135	32,809	41.1
10	.TRADE	115	160,204	7.2

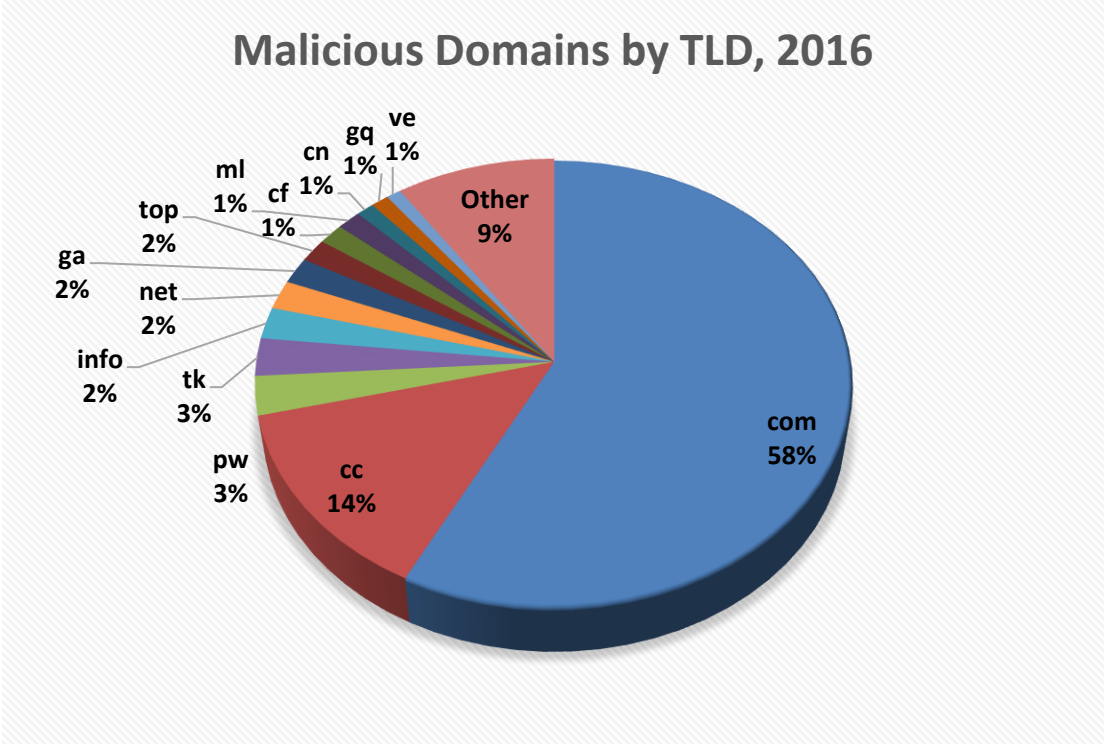
The TLD market is now more crowded and competitive than at any time in history, and some nTLD registries have been competing aggressively on price. **Low prices and sometimes lax practices are allowing nTLD domains to be used abusively in startling numbers by spammers. In April 2017, SURBL alone listed one million new gTLD domains on its spam/phishing/malware blocklist.**

Malicious Registrations vs. Compromised Domains

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 **195,475 domains used for phishing in 2016**, **we identified 95,424 that we believe were registered maliciously, by phishers – nearly half of all domains used for phishing. This is an all-time high, and almost three times as many as the 34,102 we found in 2015**.

The other 100,051 domains were almost all hacked or compromised on vulnerable Web hosting.

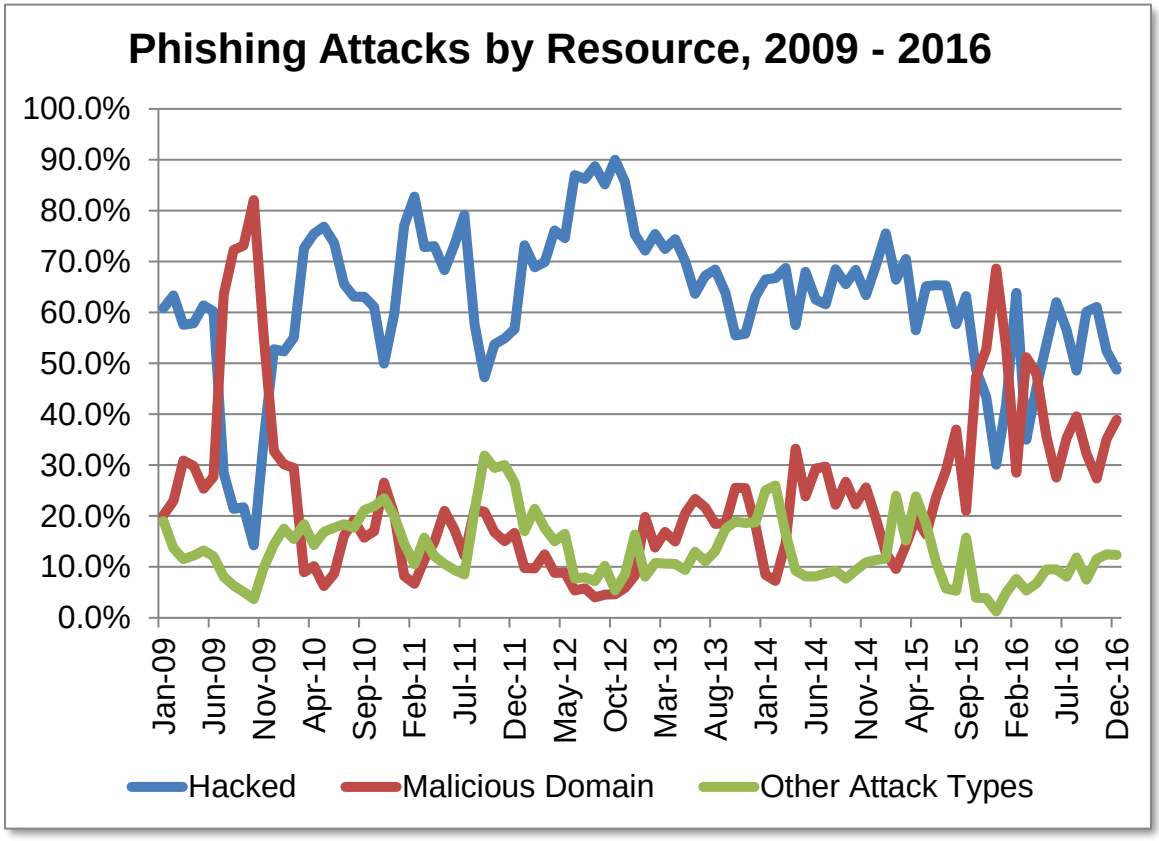


Seventy-five percent of the malicious domain registrations were made in just four TLDs: .COM, .CC, .PW, and .TK. More than 90% of malicious domains were found in just 14 TLDs, the top four plus .INFO, .NET, .GA, .TOP, .CF, .ML, .CN, .GQ, and .VE.

Of the 95,424 malicious domain registrations, 52,385 (55%) were registered to phish Chinese targets—services and sites in China that serve a primarily Chinese customer base.[10] Chinese phishers have always preferred to register domains, relying upon hacked domains and compromised Web servers less often than phishers elsewhere. We found this again in 2016, with about 83% of phishing attacks targeting Chinese brands being launched via maliciously registered domains. We continue to see phishers registering .CN domains in large numbers – 1,010 .CN domains in 2016. However, this is below numbers seen a few years ago, and represents a much smaller percentage of the malicious domains we saw overall.

However, it appears that some non-Chinese phishing groups are also registering malicious domains in increasing numbers. There was a huge rise in malicious domains used to target non-Chinese targets. In previous years around 80% of malicious domains targeted Chinese brands, but that dropped to just above 50% in 2016.

Observers outside of China did not detect most of the phish that CNNIC/APAC did inside of China, possibly because they are not parsing Chinese-language emails effectively, are not seeing instant-messenger and SMS lures, or do not have enough Chinese customers to justify setting up in-country honeypots. Whatever the case, the phishing takes advantage of registration, hosting, and payment infrastructures in different countries.



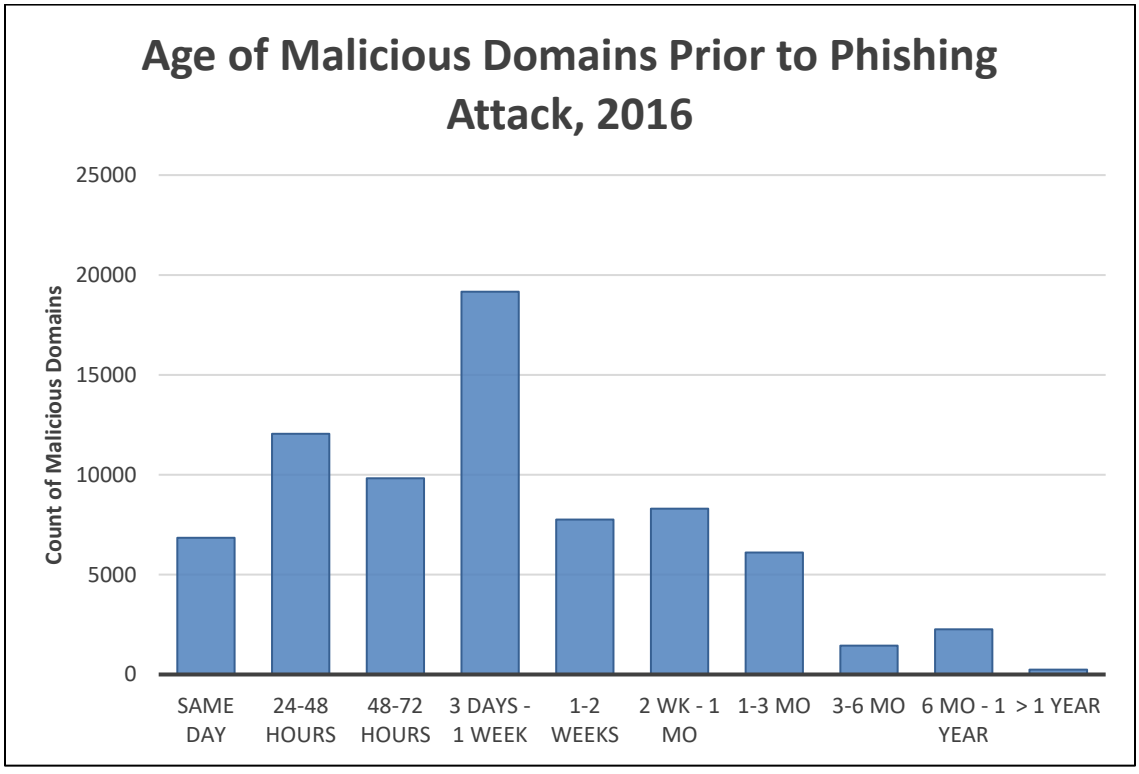
[10] These phishing attacks were advertised via e-mail lures written in Chinese, via SMS messages in Chinese sent to mobile phone customers in China, and via instant message clients popular in China such as Tencent QQ. Many of the domain registrations made by these phishers are made at Chinese registrars. Other factors about these attacks also point to perpetrators in China as well.

Domain Aging

It has been conventional wisdom that phishers use their domains soon after they register them. The theory has been that phishers want to attack on these domains quickly, because the domains might be recognized for what they are, or the associated credit card purchases might be flagged as suspicious (especially if the card numbers are stolen). **But our data shows that some phishers are aging the domains they register, sometimes waiting weeks or months before using them.** This may make sense because recently registered domains receive low reputation scores from security and anti-spam companies.

Less than 10% of maliciously registered domains were used for attacks on the same day they were registered. It takes nearly a week for the median maliciously registered domain to start hosting a phishing site. And a quarter of all domains registered for phishing are used only after two or more weeks have elapsed since registration.

This also hints at how phishers are paying for their domain names. Either the domains are paid for with legitimate means, or they are not purchased with stolen cards (because the fraud might be caught within the days immediately after purchase), or any payment fraud that did take place was never caught. Phishers may also be using alternate payment forms that make payment fraud difficult to detect.



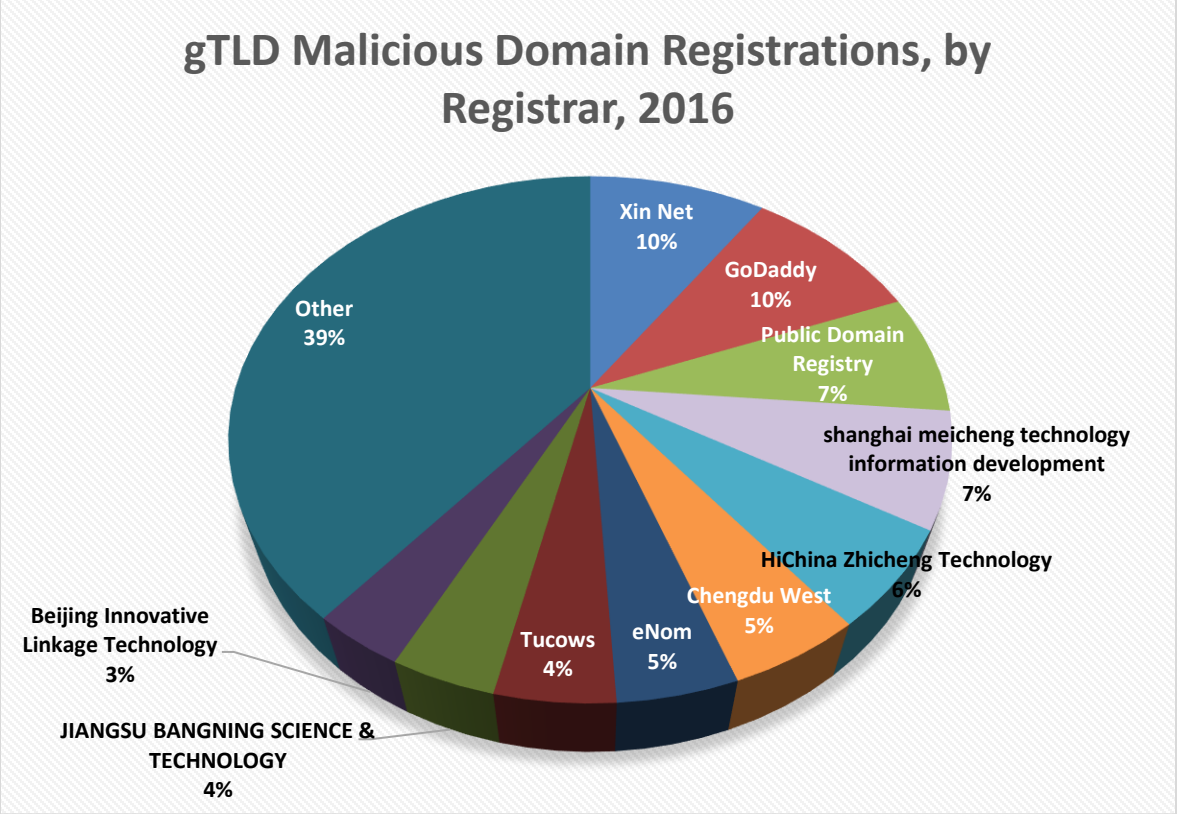
We found more than 2,500 domains in 2016 that were aged at least six months before they were used, well past the timeframe most anti-fraud reputation systems would score a domain as "new". A few domains (such as appleid-uk.com) were aged well past a year.

Registrars Used for Malicious Domain Registrations

Phishers (especially Chinese phishers) registered malicious domain names at record rates in 2016. Where are the phishers registering these domains? The following analysis looks at generic top-level domain (gTLD) registrations and not ccTLDs.[11]

We identified 1,701 registrars who had at least one gTLD domain used for phishing. Though we worked hard to consolidate this number down from the raw data, this probably represents an over-count, since some registrars have different names in different registries' systems. Some registrars own several other registrars and handle their operations, but keep the brands and accreditations separate for various reasons. Of the 1,701 registrars we identified, only 412 had at least one maliciously registered domain (24% of identified registrars).

A bit more than half of those malicious gTLD registrations were made by Chinese phishers. Six of the top ten registrars for abusive domains were located in China, and have primarily Chinese customers.



This year we looked into a new metric to understand which registrars are experiencing far more than their expected share or malicious domain registrations – the ratio of malicious

[11] ICANN makes public how many gTLD domains each of its registrars sponsors, but ccTLD registration numbers by registrar are not generally available.

vs. compromised domains handled by that registrar. All things equal, a registrar should experience a similar rate of malicious registrations vs. registrant websites or services being compromised by phishers. For 2016, the average rate of compromised vs. malicious registrations was 49%. The median number of malicious domains found at all registrars with at least one maliciously registered domain was five, meaning most registrars only had a handful of malicious phishing domains. The largest registrar, GoDaddy, had a ratio of just 25%, indicating that GoDaddy may be implementing some controls that effectively prevent fraudulent registrations.

We saw however that several registrars had a very large percentage of malicious registrations, which raises red flags. There were several large registrars whoi had aratio of malicious domains to compromised well over 90%:

Registrars with 100 malicious domain registrations + 75% malicious ratio overall

Registrar	Phishing Domains	Malicious Domains	Ratio
HANGZHOU DIANSHANG INTERNET TECHNOLOGY	364	364	100%
Webair Internet Development	115	115	100%
Shanghai meicheng technology information development	5518	5487	99%
JIANGSU BANGNING SCIENCE & TECHNOLOGY	3128	3083	99%
22NET	1174	1157	99%
Alibaba Cloud Computing	687	674	98%
Chengdu Fly	264	259	98%
Chengdu West	4033	3950	98%
West263	1100	1076	98%
Hangzhou Aiming Network	765	747	98%
Eranet Inernational	308	300	97%
Beijing Innovative Linkage Technology	2801	2723	97%
Xin Net	7653	7422	97%
BIZCN	2675	2576	96%
Xiamen Nawang technology	275	261	95%
OpenTLD	117	111	95%
Todaynic	147	137	93%
35 Technology	510	469	92%
HiChina Zhicheng Technology	5167	4657	90%
Google	761	680	89%
Alpnames	416	367	88%
WEBCC	1969	1693	86%
1API	1391	1168	84%
REG.RU	455	370	81%
Internet BS	2106	1701	81%
Namecheap	1483	1129	76%

The Rise of Domain Shadowing for Phishing

We saw the use of a new technique called "domain shadowing," a hybrid attack that uses the domains name system (DNS) to perpetrate phishing in a novel way.

"Domain Shadowing" is a hybrid attack in which a phisher compromises a legitimate domain name's DNS control in order to set up new subdomains; the new subdomains then point to the phisher's malicious content. What one sees in the DNS looks like this:

www.legitdomain.tld → Real website
mail.legitdomain.tld → Real e-mail service
stringthebadguysetup.legitdomain.tld → phishing site
phishedbrand.legitdomain.tld → phishing site

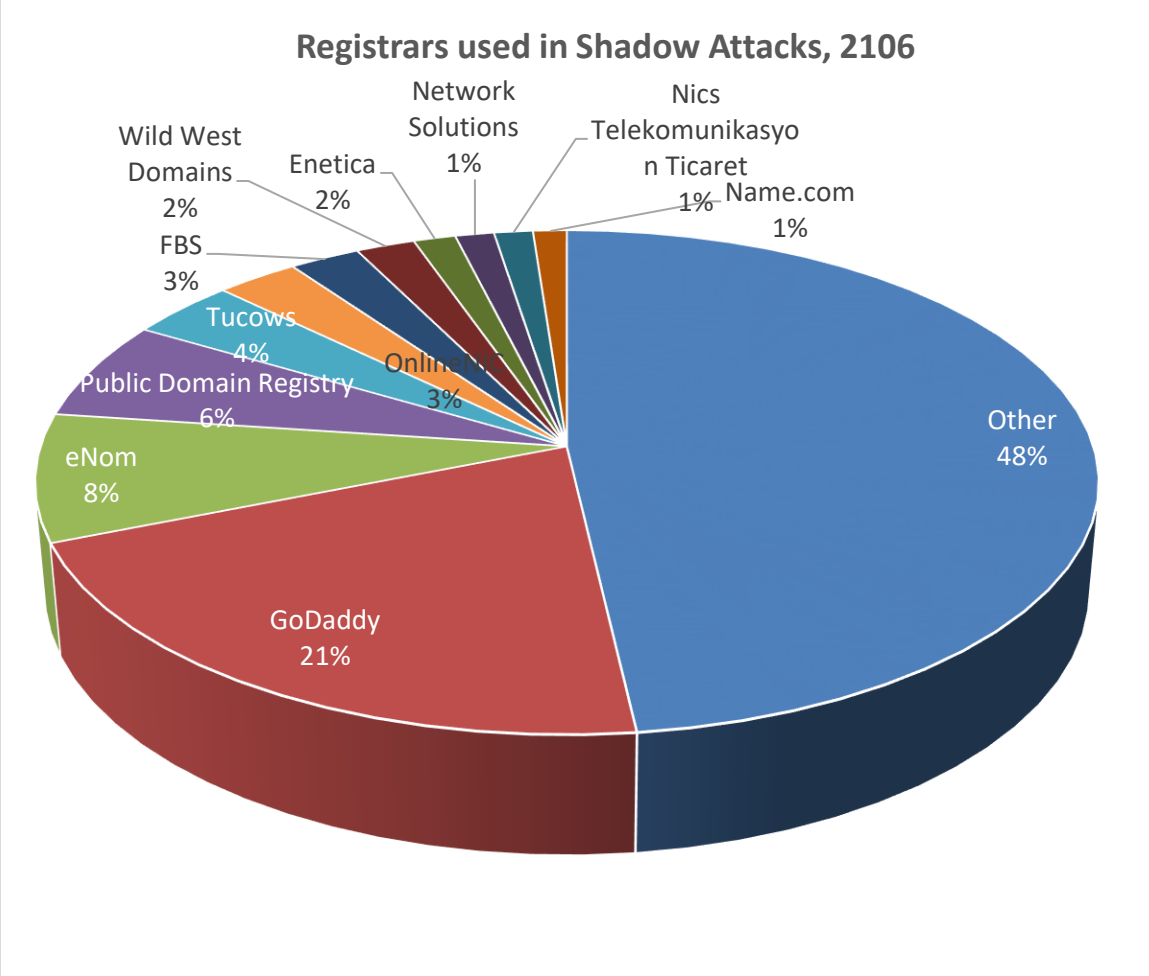
This technique was used for at least 1% of all phishing attacks in 2016. We are examining it since we've seen this method used heavily in other types of abuse, primarily the delivery of "exploit kits."

A domain shadowing attack is carried out in this way:

1) The phisher phishes domain name owners pretending to be their registrar or getting their registrar access credentials via some other common means.
2) Phisher logs into the domain owner's registrar or DNS management account.
3) Phisher adds new DNS "A" records, pointing various subdomains (hostnames) at IP addresses under the miscreant's control. The phisher may set up MX (Mail eXchange) records as well to create new hostnames that can be used for e-mail.
4) Phisher leaves any pre-defined addresses and DNS records alone, so no one is aware that the domain has been compromised. The main domain name continues to function normally.
5) Phisher spams or induces victims to come to the new hostnames he has created.

So why go through this complicated exercise? The main reason is to work under the umbrella of a "known" domain and take advantage of its good reputation in order to get malicious links, e-mails lures, and other related resources past traditional anti-abuse tools that are based on domain name reputation. A further benefit is that it its more difficult to shut down of these bogus hostnames -- that requires the careful cooperation of the registrar and/or DNS operator in order to cull the bad hostnames and shut off back-door access without affecting the legitimate domain that has been compromised.

We have seen hackers concentrate on specific registrars that have robust APIs and other tools for managing customers' domains. This allows the phishers to gain control over lots of domains that they can then easily manipulate via those handy tools. Typical shadow campaigns incorporate thousands of customized hostnames per domain.



We saw domain shadowing events at 122 registrars, but over 50% of these attacks occurred at just 11 registrars, each of which had at least 20 domains hacked for shadow campaigns. Looking at the main registrars affected by domain shadowing, we see highly automated and feature-rich North American registrars dominating the list.

Use of Subdomain Services for Phishing

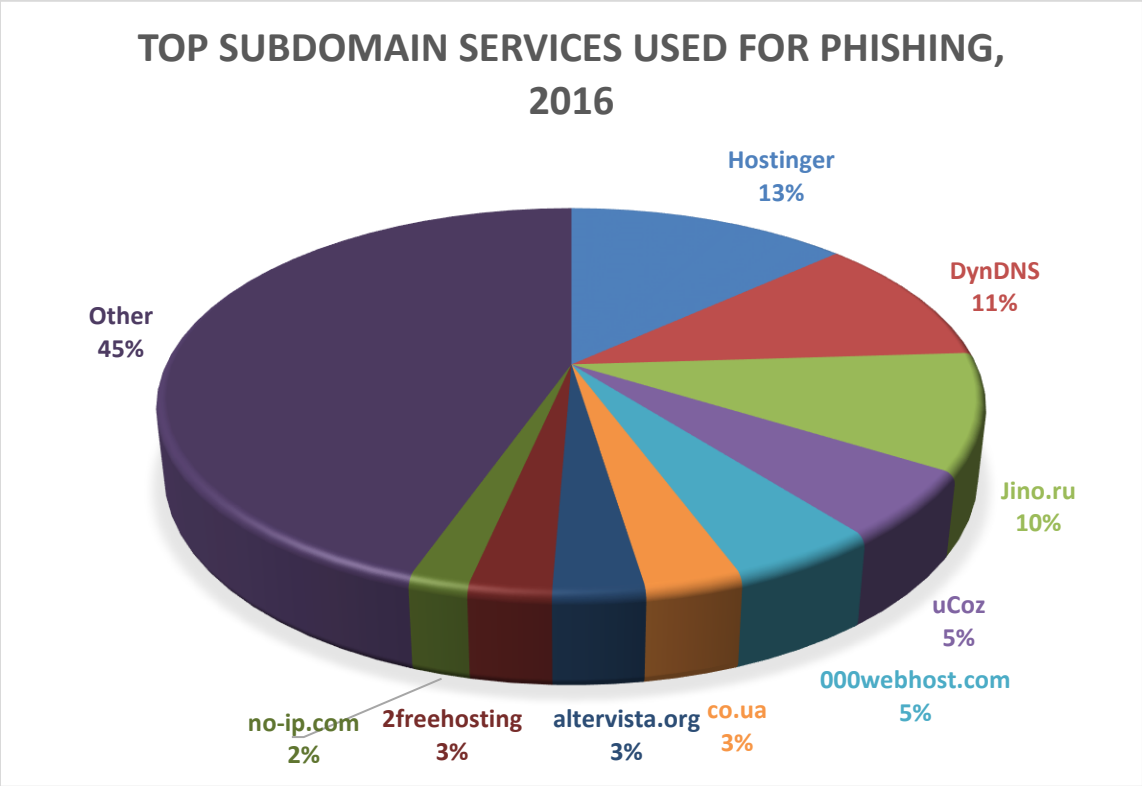
We saw the use of subdomain registrations for phishing decline again significantly in 2016, with only 13,590 attacks. However, subdomain registrations still represent 5.3% of all phishing attacks, so 1 in 20 attacks still involves a subdomain registration.

"Subdomain registration services" are providers that give customers subdomain "hosting accounts" beneath a domain name that the provider owns. These services are effectively domain registries of their own, and offer users a "domain name" -- their own DNS space -- and often offer free DNS management. 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 know of more than 900 subdomain providers. Use of subdomain services continues to be a challenge because many of the services are free, offer anonymous registration, and

only the subdomain providers themselves can effectively mitigate these phish.[12] Some are responsive to complaints, but many lack proactive measures to keep criminals from abusing their services.



Use of subdomain services remained an important but lesser-used avenue for phishing attacks. Continuing the trend since 2014, Subdomain resellers accounted for about 1 in 20 phishing at 13,590 attacks on subdomains in 2016 (5.3% of all attacks). The number of domains used for malicious subdomains remained close to historical values with 766 domains involved in 2016. For a change, no one provider dominated the statistics, with over 80 providers seeing at least 20 attacks and the top subdomain provider only seeing 1799 phishing attacks. In an interesting development, we saw very few Chinese targets like Taobao.com hit with phishing from subdomains which had normally been the case for many years. A vast majority attacked online services including eBay, Facebook, Google, Yahoo, Hotmail, and PayPal.

Only three subdomain resellers ended up with over 10% of the phishing attacks. Two of those (Hostinger and DynDNS) were very large providers with a long history of dealing with abuse – usually successfully, but scale still remains a challenge. The new provider on the list, debuting at Number 3 is the Russian web hosting company jino.ru. The company's domains were used in many attacks against western brands.

[12] 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.

Top Subdomain Services Used for Phishing, 2016

Rank	Attacks	Provider
1	1799	Hostinger
2	1462	DynDNS
3	1336	Jino.ru
4	764	uCoz
5	667	000webhost.com
6	440	co.ua
7	412	altervista.org
8	373	2freehosting
9	272	no-ip.com
10	250	runhosting.com
11	237	websitewelcome.com
12	221	smarterasp.net
	5357	All Others

Use of Internationalized Domain Names (IDNs)

Data continues to show that the unique characteristics of Internationalized Domain Names (IDNs) are not being used to facilitate phishing in meaningful numbers.

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 be composed of characters from non-Latin scripts such as Arabic, Chinese, Cyrillic, or Hindi. Over the past ten years, IDNs have been available at the second and third levels in many domain name registries. IDN TLDs allow the entire domain name to be in non-Latin characters, including the TLD extension.

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, thereby allowing the phisher to spoof a brand domain name. From January 2007 to December 2014 we found only nine true homographic phishing attacks.

In 2015 we saw one homographic attack:

- xn--paypl-680b.com → paypạl.com

In 2016, one hundred and eighty-five IDN domain names were used for phishing. Two were true homographic attacks:

- xn--fcbook-wta9d.com → fâcêbook.com
- xn--arbnb-b4a.com → ạjrbnb.com

Several more domains were used to display deceptive names in Chinese characters, or in a mix of Latin and Chinese characters. The domain strings themselves were misleading, but did not attempt to exactly copy domain names owned by the targets:

- xn--apple-uj8l559d.com → apple客服.com = "Apple customer service.com"
- xn--iphone-gj7k537u.com → iphone官网.com = "iphone official website.com"
- xn--wfrr5djviml2ak75a.cc → 商家办理部.cc = "merchant processing department.cc"

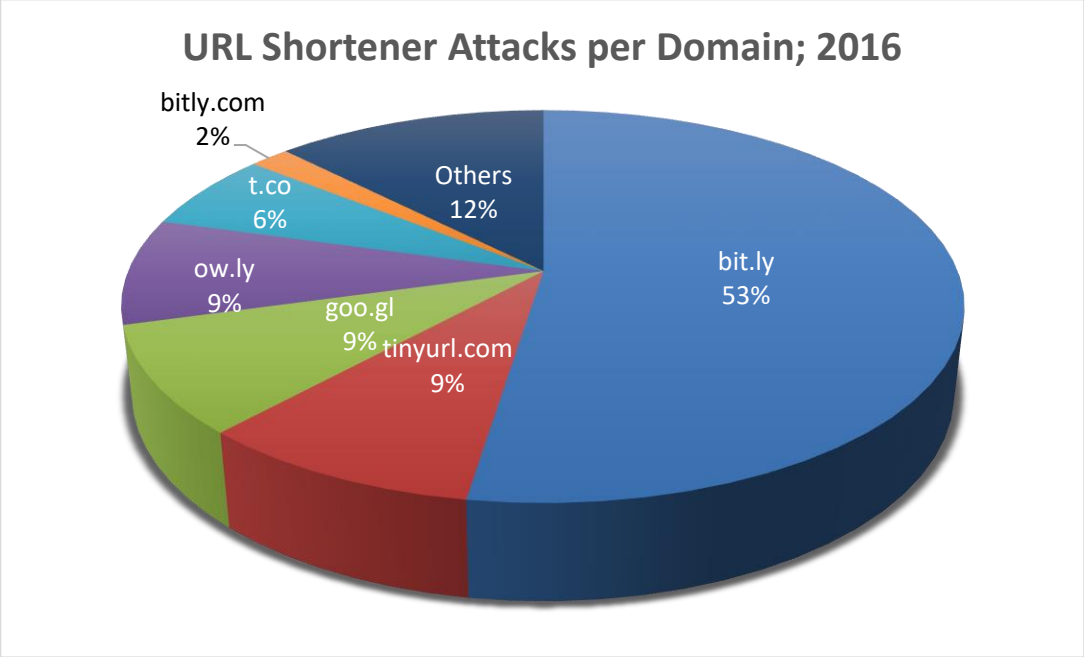
Given that IDNs have been widely available for years, why haven't phishers utilized IDN homographic attacks more often?

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 usually can't see homographic attacks.

Use of URL Shorteners for Phishing

Phishers their use of "URL shortening" services to obfuscate phishing URLs. Users of those services can obtain a very short URL to put in their limited-space posts or Tweets, which automatically redirects the visitor to a much longer "hidden" URL. Phishers continued to use shorterners at around the same rate in 2016 as they have over the past 3 years. This still only represents 2.5% of all phishing attacks, but prior work in this space had nearly eliminated such attacks. This may just represent a "steady state" of service providers employing countermeasures and phishers adapting to them.

In 2016, more than half of all URL shortener phish occurred on the very popular bit.ly and bitly.com domains, with 3,282 attacks. The other domains abused over 100 times by phishers included many of the most popular shortener services: tinyurl.com, goo.gl, ow.ly, and t.co.



Most of the major URL shortener providers have put screening mechanisms for malicious forwarding destinations in place, and have made it easier and more efficient to report abuse than in years past. In an emerging best practice, many shortener services provide tools for investigators to quickly determine forwarding destinations for specific URLs, and automated abuse reporting functions. We encourage all URL shortener providers to implement similar tactics and continue to improve them.

As we have pointed out in years past, blocklist provider SURBL (http://www.surbl.org) provides free information on abusive use of shortener services, and all URL shortener services should consider signing up for this feed of malicious URLs in order to mitigate abuse on their services. Large numbers of shortened URLs are still being seen in conjunction with malware exploit kit sites, pharma spam, and other abusive behavior, and while outside the scope of this report shows that this problem is not truly "solved" at this point, but abuse seems to remain stable.

Appendix: Phishing Statistics by TLD

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
ac	ccTLD	3	3	1,800	16.7	16.7	0	11	8	18,000	4.4	6.1	0
academy	new gTLD	6	5	22,500	2.2	2.7	0	4	4	19,576	2.0	2.0	1
accountant	new gTLD	9	9	56,920	1.6	1.6	7	0	0				
actor	new gTLD	1	1	1,714	5.8	5.8	0	0	0				
ad	ccTLD	0	0				0	3	1	1,750	5.7	17.1	0
ae	ccTLD	142	101	100,569	10.0	14.1	0	126	82	115,000	7.1	11.0	0
aero	new gTLD	1	1	10,287	1.0	1.0	0	5	5	9,916	5.0	5.0	0
af	ccTLD	10	9	6,001	15.0	16.7	1	5	2	4,100	4.9	12.2	0
ag	ccTLD	4	4	18,379	2.2	2.2	1	7	6	18,250	3.3	3.8	0
agency	new gTLD	11	10	28,756	3.5	3.8	1	5	5	23,980	2.1	2.1	4
ai	ccTLD	28	2	15,002	1.3	18.7	0	9	2	6,750	3.0	13.3	0
al	ccTLD	43	37	16,500	22.4	26.1	1	23	15	15,200	9.9	15.1	1
am	ccTLD	68	20	37,761	5.3	18.0	0	78	27	28,000	9.6	27.9	2
ao	ccTLD	3	3	4,050	7.4	7.4	0	1	1	3,550	2.8	2.8	0
aq	ccTLD	1	1	100	100.0	100.0	0	0	0				
ar	ccTLD	931	703	517,365	13.6	18.0	1	783	546	437,555	12.5	17.9	5
army	new gTLD	2	2	1,384	14.5	14.5	1	0	0				
as	ccTLD	4	4	14,100	2.8	2.8	0	7	4	14,000	2.9	5.0	0
asia	legacy gTLD	100	86	233,360	3.7	4.3	42	171	147	236,783	6.2	7.2	20

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
at	ccTLD	180	142	1,271,868	1.1	1.4	7	263	209	1,269,326	1.6	2.1	3
attorney	new gTLD	1	1	7,771	1.3	1.3	0	0	0				
au	ccTLD	3,475	2,510	3,070,000	8.2	11.3	3	2,812	2,172	3,000,364	7.2	9.4	27
auction	new gTLD	1	1	3,173	3.2	3.2	1	0	0				
ax	ccTLD	1	1	2,600	3.8	3.8	0	3	3	2,000	15.0	15.0	0
az	ccTLD	32	25	25,014	10.0	12.8	0	23	17	18,500	9.2	12.4	0
ba	ccTLD	40	30	19,500	15.4	20.5	0	62	48	17,977	26.7	34.5	1
band	new gTLD	1	1	9,482	1.1	1.1	0	0	0				
bb	ccTLD	3	3	2,800	10.7	10.7	0	2	2	2,600	7.7	7.7	0
bd	ccTLD	272	205	33,000	62.1	82.4	0	85	6	31,500	1.9	27.0	0
be	ccTLD	490	379	1,544,745	2.5	3.2	35	539	398	1,533,750	2.6	3.5	5
berlin	new gTLD	1	1	58,593	0.2	0.2	0	72	72	58,486	12.3	12.3	0
bet	new gTLD	2	2	28,215	0.7	0.7	1	0	0				
bf	ccTLD	1	1	1,300	7.7	7.7	0	2	2	1,200	16.7	16.7	0
bg	ccTLD	62	41	53,000	7.7	11.7	0	56	43	48,500	8.9	11.5	1
bi	ccTLD	5	3	2,100	14.3	23.8	0	2	1	2,400	4.2	8.3	0
bid	new gTLD	103	95	607,743	1.6	1.7	90	1	1	100,853	0.1	0.1	1
bike	new gTLD	1	1	14,432	0.7	0.7	0	3	2	14,112	1.4	2.1	0
bio	new gTLD	3	2	14,651	1.4	2.0	0	0	0				
biz	legacy gTLD	659	534	2,370,871	2.3	2.8	156	1,063	786	2,447,835	3.2	4.3	47
bj	ccTLD	0	0				0	1	1	700	14.3	14.3	0
black	new gTLD	3	3	23,803	1.3	1.3	2	0	0				
bm	ccTLD	0	0				0	2	2	8,150	2.5	2.5	0
bn	ccTLD	1	1	1,400	7.1	7.1	0	0	0				

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
bo	ccTLD	39	25	11,000	22.7	35.5	0	17	13	10,250	12.7	16.6	0
boutique	new gTLD	1	1	8,268	1.2	1.2	0	0	0				
br	ccTLD	8,871	6,706	3,890,000	17.2	22.8	114	5,326	3,735	3,848,070	9.7	13.8	31
brussels	new gTLD	1	1	6,973	1.4	1.4	1	0	0				
bs	ccTLD	1	1	2,600	3.8	3.8	0	1	1	2,500	4.0	4.0	0
bt	ccTLD	2	2	1,900	10.5	10.5	0	10	10	1,700	58.8	58.8	0
build	new gTLD	3	3	4,014	7.5	7.5	1	0	0				
business	new gTLD	6	6	14,209	4.2	4.2	3	0	0				
buzz	new gTLD	2	2	1,900	10.5	10.5	2	0	0				
bw	ccTLD	2	2	7,950	2.5	2.5	0	4	4	7,150	5.6	5.6	0
by	ccTLD	250	176	118,000	14.9	21.2	0	220	158	30,974	51.0	71.0	1
bz	ccTLD	40	28	34,000	8.2	11.8	3	41	22	33,500	6.6	12.2	2
bzh	new gTLD	1	1	6,555	1.5	1.5	0	1	1	5,823	1.7	1.7	1
ca	ccTLD	1,196	947	2,550,000	3.7	4.7	9	1,430	1,106	2,466,136	4.5	5.8	12
cab	new gTLD	1	1	3,951	2.5	2.5	1	0	0				
cafe	new gTLD	2	1	8,393	1.2	2.4	0	0	0				
capetown	new gTLD	3	3	4,633	6.5	6.5	0	0	0				
capital	new gTLD	3	3	5,766	5.2	5.2	1	0	0				
cards	new gTLD	5	5	5,553	9.0	9.0	5	3	3	5,233	5.7	5.7	2
care	new gTLD	7	6	13,665	4.4	5.1	3	3	3	11,222	2.7	2.7	2
careers	new gTLD	2	2	7,013	2.9	2.9	0	0	0				
casa	new gTLD	4	4	18,833	2.1	2.1	0	0	0				
cash	new gTLD	2	2	5,962	3.4	3.4	2	0	0				
cat	legacy gTLD	44	36	110,922	3.2	4.0	0	57	40	97,130	4.1	5.9	0
catering	new gTLD	1	1	3,317	3.0	3.0	0	1	1	3,075	3.3	3.3	0
cc	ccTLD	13,708	13,061	1,750,000	74.6	78.3	13,003	4,011	3,119	2,550,500	12.2	15.7	2,618

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
cd	ccTLD	15	9	2,600	34.6	57.7	0	7	5	2,600	19.2	26.9	1
center	new gTLD	136	135	32,809	41.1	41.5	134	9	8	31,163	2.6	2.9	4
cf	ccTLD	1,494	1,474	725,000	20.3	20.6	1,431	933	802	325,000	24.7	28.7	176
ch	ccTLD	589	449	2,034,509	2.2	2.9	54	366	292	1,981,948	1.5	1.8	5
chat	new gTLD	1	1	8,943	1.1	1.1	1	0	0				
cheap	new gTLD	0	0				0	1	1	3,609	2.8	2.8	0
christmas	new gTLD	1	1	3,793	2.6	2.6	0	0	0				
church	new gTLD	4	4	15,868	2.5	2.5	0	2	1	12,828	0.8	1.6	0
ci	ccTLD	10	9	8,500	10.6	11.8	0	14	11	7,000	15.7	20.0	0
city	new gTLD	3	3	32,867	0.9	0.9	2	0	0				
ck	ccTLD	1	1	1,300	7.7	7.7	0	0	0				
cl	ccTLD	1,208	913	524,420	17.4	23.0	2	1,667	1,086	502,011	21.6	33.2	9
cleaning	new gTLD	0	0				0	2	2	2,457	8.1	8.1	0
click	new gTLD	57	56	222,091	2.5	2.6	50	4	3	177,156	0.2	0.2	3
clinic	new gTLD	3	3	5,998	5.0	5.0	0	0	0				
clothing	new gTLD	4	2	13,628	1.5	2.9	0	0	0				
cloud	new gTLD	85	78	89,009	8.8	9.5	75	0	0				
club	new gTLD	182	164	910,091	1.8	2.0	99	102	86	552,875	1.6	1.8	40
cm	ccTLD	25	22	35,000	6.3	7.1	3	47	16	61,732	2.6	7.6	3
cn	ccTLD	1,895	1,739	20,608,428	0.8	0.9	1,010	2,066	1,837	16,363,594	1.1	1.3	631
co	ccTLD	1,665	978	2,110,000	4.6	7.9	370	1,332	643	1,999,500	3.2	6.7	132
coffee	new gTLD	1	1	11,917	0.8	0.8	0	0	0				
com	legacy gTLD	125,249	104,181	131,817,167	7.9	9.5	54,931	127,708	94,338	126,645,118	7.4	10.1	25,020
community	new gTLD	2	2	10,610	1.9	1.9	0	3	2	8,913	2.2	3.4	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
company	new gTLD	15	15	49,766	3.0	3.0	12	6	5	44,303	1.1	1.4	1
computer	new gTLD	2	2	4,848	4.1	4.1	1	0	0				
construction	new gTLD	0	0				0	1	1	6,512	1.5	1.5	0
consulting	new gTLD	5	5	19,000	2.6	2.6	3	0	0				
cool	new gTLD	1	1	13,788	0.7	0.7	1	3	2	11,109	1.8	2.7	0
coop	legacy gTLD	2	2	9,828	2.0	2.0	0	6	6	8,847	6.8	6.8	0
country	new gTLD	2	2	1,560	12.8	12.8	2	0	0				
cr	ccTLD	17	14	19,000	7.4	8.9	0	44	22	15,500	14.2	28.4	0
credit	new gTLD	0	0				0	1	1	2,181	4.6	4.6	0
creditcard	new gTLD	1	1	760	13.2	13.2	1	0	0				
cricket	new gTLD	9	7	26,686	2.6	3.4	7	0	0				
cruises	new gTLD	1	1	2,166	4.6	4.6	1	1	1	2,250	4.4	4.4	0
cu	ccTLD	0	0				0	1	1	1,500	6.7	6.7	0
cv	ccTLD	0	0				0	3	3	1,300	23.1	23.1	0
cx	ccTLD	10	5	20,000	2.5	5.0	1	21	11	42,500	2.6	4.9	0
cy	ccTLD	13	8	15,000	5.3	8.7	0	22	16				0
cz	ccTLD	284	211	1,280,916	1.6	2.2	3	470	267	1,230,330	2.2	3.8	3
dance	new gTLD	0	0				0	3	2	4,775	4.2	6.3	0
date	new gTLD	50	48	153,884	3.1	3.2	46	33	30	109,692	2.7	3.0	30
de	ccTLD	1,548	1,189	16,114,000	0.7	1.0	313	1,763	1,241	16,009,814	0.8	1.1	32
dental	new gTLD	0	0				0	1	1	6,076	1.6	1.6	0
design	new gTLD	9	7	54,169	1.3	1.7	1	0	0				
diamonds	new gTLD	0	0				0	1	1	3,291	3.0	3.0	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
digital	new gTLD	4	4	18,676	2.1	2.1	2	0	0				
direct	new gTLD	7	7	9,633	7.3	7.3	6	1	1	8,289	1.2	1.2	0
directory	new gTLD	9	8	19,042	4.2	4.7	6	5	4	19,292	2.1	2.6	0
dj	ccTLD	0	0				0	4	3	6,500	4.6	6.2	0
dk	ccTLD	245	190	1,327,688	1.4	1.8	0	315	245	1,314,508	1.9	2.4	7
dm	ccTLD	0	0				0	1	1	2,250	4.4	4.4	0
do	ccTLD	107	28	20,000	14.0	53.5	0	194	42	25,212	16.7	76.9	0
dog	new gTLD	3	1	6,913	1.4	4.3	0	0	0				
domains	new gTLD	1	1	6,860	1.5	1.5	0	1	1	7,319	1.4	1.4	0
download	new gTLD	3	3	92,561	0.3	0.3	1	1	1	26,105	0.4	0.4	1
durban	new gTLD	1	1	2,437	4.1	4.1	0	0	0				
dz	ccTLD	7	6	6,400	9.4	10.9	0	7	7	7,734	9.1	9.1	0
ec	ccTLD	89	70	39,190	17.9	22.7	0	55	39	41,250	9.5	13.3	0
edu	special	46	39	7,466	52.2	61.6	0	40	34	7,512	45.3	53.2	0
education	new gTLD	3	3	19,819	1.5	1.5	0	2	2	17,642	1.1	1.1	1
ee	ccTLD	37	34	125,036	2.7	3.0	0	207	40	103,398	3.9	20.0	0
eg	ccTLD	21	15	9,800	15.3	21.4	0	28	16	9,500	16.8	29.5	0
email	new gTLD	71	69	62,268	11.1	11.4	68	14	11	54,388	2.0	2.6	8
engineering	new gTLD	1	1	4,168	2.4	2.4	1	0	0				
equipment	new gTLD	3	1	6,452	1.5	4.6	0	0	0				
es	ccTLD	1,605	513	1,838,066	2.8	8.7	26	2,222	532	1,795,017	3.0	12.4	8
estate	new gTLD	2	2	9,543	2.1	2.1	0	0	0				
et	ccTLD	0	0				0	1	1	2,200	4.5	4.5	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
eu	ccTLD	1028	863	3,760,695	2.3	2.7	296	1,165	875	3,862,467	2.3	3.0	25
eus	new gTLD	2	2	6,310	3.2	3.2	0	3	1	4,941	2.0	6.1	0
events	new gTLD	4	3	18,532	1.6	2.2	0	2	1	16,317	0.6	1.2	0
expert	new gTLD	6	6	28,956	2.1	2.1	4	11	11	29,629	3.7	3.7	1
exposed	new gTLD	1	1	2,494	4.0	4.0	1	0	0				
fail	new gTLD	2	2	2,645	7.6	7.6	2	0	0				
faith	new gTLD	12	12	47,465	2.5	2.5	12	4	4	40,316	1.0	1.0	4
family	new gTLD	1	1	12,266	0.8	0.8	1	0	0				
farm	new gTLD	3	1	10,100	1.0	3.0	0	0	0				
fashion	new gTLD	2	2	8,436	2.4	2.4	0	0	0				
fi	ccTLD	132	107	422,630	2.5	3.1	0	218	186	381,415	4.9	5.7	0
fishing	new gTLD	1	1	1,879	5.3	5.3	0	0	0				
fit	new gTLD	1	1	8,638	1.2	1.2	0	0	0				
fitness	new gTLD	1	1	8,248	1.2	1.2	0	0	0				
fj	ccTLD	6	6	2,550	23.5	23.5	0	2	1				0
flights	new gTLD	0	0				0	1	1	2,017	5.0	5.0	0
florist	new gTLD	1	1	2,654	3.8	3.8	0	0	0				
fm	ccTLD	15	12	18,000	6.7	8.3	0	11	10	18,750	5.3	5.9	0
fo	ccTLD	2	2	3,600	5.6	5.6	0	0	0				
foundation	new gTLD	1	1	7,719	1.3	1.3	1	1	1	6,398	1.6	1.6	0
fr	ccTLD	970	673	2,985,000	2.3	3.2	27	1,389	952	2,870,712	3.3	4.8	24
frl	new gTLD	2	2	14,261	1.4	1.4	1	0	0				
fund	new gTLD	1	1	8,423	1.2	1.2	1	0	0				
fyi	new gTLD	1	1	7,460	1.3	1.3	1	0	0				
ga	ccTLD	1,893	1,866	675,000	27.6	28.0	1,812	656	502	288,325	17.4	22.8	85

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
gal	new gTLD	1	1	3,483	2.9	2.9	1	0	0				
gallery	new gTLD	0	0				0	1	1	17,372	0.6	0.6	0
gd	ccTLD	89	7	2,700	25.9	329.6	0	548	7	3,400	20.6	1611.8	0
gdn	new gTLD	4	4	310,464	0.1	0.1	4	0	0				
ge	ccTLD	104	80	29,500	27.1	35.3	0	69	54	26,789	20.2	25.8	1
gf	ccTLD	2	1	700	14.3	28.6	0	1	1	650	15.4	15.4	0
gg	ccTLD	16	2	25,000	0.8	6.4	1	16	13	57,950	2.2	2.8	0
gh	ccTLD	7	5	3,400	14.7	20.6	0	1	1	3,350	3.0	3.0	0
gi	ccTLD	0	0				0	2	1	2,200	4.5	9.1	0
gift	new gTLD	1	1	24,611	0.4	0.4	1	0	0				
gifts	new gTLD	1	1	3,645	2.7	2.7	1	0	0				
gl	ccTLD	556	2	5,050	4.0	1101.0	0	418	6	6,200	9.7	674.2	1
global	new gTLD	13	12	28,058	4.3	4.6	7	0	0				
gm	ccTLD	3	2	1,500	13.3	20.0	0	17	3	1,450	20.7	117.2	0
gn	ccTLD	2	2	300	66.7	66.7	0	0	0				
gop	new gTLD	0	0				0	1	1	2,004	5.0	5.0	1
gov	special	8	5	5,613	8.9	14.3	0	6	4	5,610	7.1	10.7	0
gp	ccTLD	0	0				0	60	30	2,300	130.4	260.9	0
gq	ccTLD	1,059	1,052	350,000	30.1	30.3	1,001	444	379	175,000	21.7	25.4	88
gr	ccTLD	575	459	390,000	11.8	14.7	0	556	415	375,782	11.0	14.8	2
graphics	new gTLD	3	3	7,684	3.9	3.9	0	1	1	8,059	1.2	1.2	0
gratis	new gTLD	3	3	2,987	10.0	10.0	2	0	0				
gs	ccTLD	19	5	25,000	2.0	7.6	0	28	7	78,834	0.9	3.6	0
gt	ccTLD	24	21	16,000	13.1	15.0	0	21	14	16,000	8.8	13.1	1

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
guide	new gTLD	6	4	13,976	2.9	4.3	1	0	0				
guitars	new gTLD	1	1	1,903	5.3	5.3	0	0	0				
guru	new gTLD	6	6	62,685	1.0	1.0	1	14	14	67,097	2.1	2.1	3
gy	ccTLD	4	4	3,500	11.4	11.4	0	22	5	3,900	12.8	56.4	0
haus	new gTLD	1	1	4,526	2.2	2.2	1	0	0				
help	new gTLD	48	45	43,510	10.3	11.0	45	17	15	35,962	4.2	4.7	13
hk	ccTLD	171	126	146,997	8.6	11.6	10	144	105	160,407	6.5	9.0	3
hm	ccTLD	0	0				0	3	3	42,156	0.7	0.7	0
hn	ccTLD	5	5	11,901	4.2	4.2	0	29	23	11,000	20.9	26.4	0
holdings	new gTLD	0	0				0	1	1	5,432	1.8	1.8	0
holiday	new gTLD	2	2	5,116	3.9	3.9	2	0	0				
host	new gTLD	55	44	50,848	8.7	10.8	35	13	5	5,887	8.5	22.1	0
hosting	new gTLD	10	1	6,157	1.6	16.2	0	0	0				
house	new gTLD	3	2	14,863	1.3	2.0	1	0	0				
how	new gTLD	1	1	2,481	4.0	4.0	0	0	0				
hr	ccTLD	111	90	97,261	9.3	11.4	0	134	110	87,567	12.6	15.3	0
ht	ccTLD	7	4	2,800	14.3	25.0	1	48	8	2,700	29.6	177.8	0
hu	ccTLD	720	333	699,608	4.8	10.3	0	570	377	655,391	5.8	8.7	1
id	ccTLD	951	729	234,194	31.1	40.6	63	436	270	172,982	15.6	25.2	5
ie	ccTLD	220	171	225,471	7.6	9.8	0	198	152	212,297	7.2	9.3	0
il	ccTLD	242	181	221,789	8.2	10.9	0	342	217	225,500	9.6	15.2	8
im	ccTLD	83	18	29,098	6.2	28.5	3	269	21	34,100	6.2	78.9	0
immo	new gTLD	2	1	12,940	0.8	1.5	1	0	0				
immobilien	new gTLD	1	1	7,576	1.3	1.3	0	0	0				
in	ccTLD	2,834	2,139	2,225,223	9.6	12.7	305	2,092	1,506	2,018,562	7.5	10.4	45

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
info	legacy gTLD	3,643	3,205	5,786,794	5.5	6.3	2,168	2,878	2,311	5,062,589	4.6	5.7	452
ink	new gTLD	11	4	24,768	1.6	4.4	2	3	3	9,515	3.2	3.2	3
institute	new gTLD	2	2	8,379	2.4	2.4	0	1	1	7,483	1.3	1.3	0
insure	new gTLD	1	1	4,045	2.5	2.5	1	0	0				
int	special	3	3	264	113.6	113.6	0	0	0				
international	new gTLD	5	3	20,633	1.5	2.4	1	3	2	18,742	1.1	1.6	1
io	ccTLD	188	39	232,000	1.7	8.1	2	29	17	170,200	1.0	1.7	0
iq	ccTLD	3	3	283,872	0.1	0.1	0	3	3	1,200	25.0	25.0	0
ir	ccTLD	501	392	836,026	4.7	6.0	0	504	345	583,900	5.9	8.6	15
is	ccTLD	41	32	16,825	19.0	24.4	0	51	41	53,800	7.6	9.5	1
istanbul	new gTLD	2	2	16,825	1.2	1.2	0	0	0				
it	ccTLD	1,452	1,145	3,001,885	3.8	4.8	225	1,312	989	2,869,010	3.4	4.6	13
je	ccTLD	2	2	4,790	4.2	4.2	0	23	8	5,400	14.8	42.6	0
jm	ccTLD	2	2	6,800	2.9	2.9	0	2	1				0
jo	ccTLD	7	5	4,200	11.9	16.7	0	16	9	4,200	21.4	38.1	0
jobs	legacy gTLD	1	1	3,404	2.9	2.9	0	1	1	46,119	0.2	0.2	0
joburg	new gTLD	2	2	3,393	5.9	5.9	0	0	0				
jp	ccTLD	177	123	1,454,636	0.8	1.2	2	213	164	1,410,247	1.2	1.5	0
ke	ccTLD	260	207	50,000	41.4	52.0	0	172	5				0
kg	ccTLD	6	6	10,200	5.9	5.9	0	19	14	9,900	14.1	19.2	0
kh	ccTLD	16	11	3,200	34.4	50.0	0	12	3				0
ki	ccTLD	0	0				0	5	3	500	60.0	100.0	0
kim	new gTLD	14	14	119,599	1.2	1.2	13	1	1	38,428	0.3	0.3	0
kitchen	new gTLD	2	1	6,176	1.6	3.2	0	0	0				
kiwi	new gTLD	0	0				0	1	1	10,333	1.0	1.0	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
kn	ccTLD	0	0				0	2	2	1,750	11.4	11.4	0
koeln	new gTLD	1	1	25,271	0.4	0.4	1	0	0				
kr	ccTLD	125	81	1,086,000	0.7	1.2	0	229	156	1,033,152	1.5	2.2	1
kw	ccTLD	4	3	4,200	7.1	9.5	0	4	2				0
ky	ccTLD	0	0				0	6	4	6,250	6.4	9.6	0
kz	ccTLD	183	148	126,214	11.7	14.5	1	222	164	121,900	13.5	18.2	3
la	ccTLD	30	20	40,000	5.0	7.5	8	25	13	62,400	2.1	4.0	0
land	new gTLD	1	1	14,245	0.7	0.7	0	2	2	14,620	1.4	1.4	0
lat	new gTLD	1	1	2,543	3.9	3.9	0	0	0				
lb	ccTLD	6	4	3,900	10.3	15.4	0	6	4	3,750	10.7	16.0	0
lc	ccTLD	3	2	4,500	4.4	6.7	1	61	22	6,500	33.8	93.8	0
lease	new gTLD	1	1	1,705	5.9	5.9	1	0	0				
li	ccTLD	25	18	50,477	3.6	5.0	4	41	17	63,241	2.7	6.5	1
life	new gTLD	7	7	50,710	1.4	1.4	1	0	0				
lighting	new gTLD	1	1	6,185	1.6	1.6	0	0	0				
limited	new gTLD	60	59	4,861	121.4	123.4	58	26	24	2,990	80.3	87.0	13
link	new gTLD	198	190	381,404	5.0	5.2	174	62	52	183,903	2.8	3.4	36
live	new gTLD	13	13	76,506	1.7	1.7	13	1	1	13,953	0.7	0.7	1
lk	ccTLD	109	78	180,833	4.3	6.0	0	61	45	50,225	9.0	12.1	0
loan	new gTLD	36	35	1,880,182	0.2	0.2	33	0	0				
lol	new gTLD	1	1	79,565	0.1	0.1	1	0	0				
london	new gTLD	3	3	57,884	0.5	0.5	1	3	3	62,331	0.5	0.5	0
love	new gTLD	2	1	16,871	0.6	1.2	0	0	0				
lr	ccTLD	2	1	350	28.6	57.1	0	0	0				
ls	ccTLD	0	0				0	1	1	1,100	9.1	9.1	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
lt	ccTLD	256	74	159,000	4.7	16.1	1	287	94	173,970	5.4	16.5	2
ltd	new gTLD	6	5	43,581	1.1	1.4	5	0	0				
lu	ccTLD	33	20	90,000	2.2	3.7	0	47	28	87,798	3.2	5.4	0
luxury	new gTLD	3	1	991	10.1	30.3	0	0	0				
lv	ccTLD	67	54	105,200	5.1	6.4	0	97	77	117,000	6.6	8.3	2
ly	ccTLD	3,904	15	12,600	11.9	3098.4	0	2,066	22	88,798	2.5	232.7	1
ma	ccTLD	74	50	60,300	8.3	12.3	0	138	106	59,500	17.8	23.2	1
management	new gTLD	2	2	9,878	2.0	2.0	2	0	0				
market	new gTLD	3	3	11,508	2.6	2.6	0	4	3	8,995	3.3	4.4	1
marketing	new gTLD	3	3	16,339	1.8	1.8	1	9	8	14,622	5.5	6.2	0
mc	ccTLD	0	0				0	3	2	3,300	6.1	9.1	0
md	ccTLD	29	23	20,900	11.0	13.9	1	54	39	23,000	17.0	23.5	0
me	ccTLD	754	567	994,000	5.7	7.6	369	601	339	993,500	3.4	6.0	49
media	new gTLD	7	7	29,773	2.4	2.4	2	0	0				
melbourne	new gTLD	7	2	9,958	2.0	7.0	0	0	0				
men	new gTLD	1	1	95,247	0.1	0.1	1	0	0				
menu	new gTLD	3	3	6,398	4.7	4.7	1	0	0				
mg	ccTLD	8	5	27,100	1.8	3.0	0	17	11	4,100	26.8	41.5	0
mk	ccTLD	52	38	25,000	15.2	20.8	0	42	34	25,000	13.6	16.8	1
ml	ccTLD	1,448	1,434	220,000	65.2	65.8	1,366	424	351	195,000	18.0	21.7	80
mm	ccTLD	7	4	4,200	9.5	16.7	0	0	0				
mn	ccTLD	38	24	16,500	14.5	23.0	0	36	32	15,800	20.3	22.8	1
mo	ccTLD	0	0				0	4	2	2,750	7.3	14.5	0
mobi	legacy gTLD	174	114	688,396	1.7	2.5	75	426	207	710,066	2.9	6.0	44
moda	new gTLD	1	1	2,641	3.8	3.8	1	0	0				

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
moe	new gTLD	12	6	6,078	9.9	19.7	0	0	0				
mom	new gTLD	10	10	51,121	2.0	2.0	9	0	0				
money	new gTLD	0	0				0	1	1	5,284	1.9	1.9	0
moscow	new gTLD	1	1	23,780	0.4	0.4	0	0	0				
mp	ccTLD	6	1	10,290	1.0	5.8	0	446	1	600	16.7	7433.3	0
mr	ccTLD	1	1	1,600	6.3	6.3	0	3	3	1,500	20.0	20.0	0
ms	ccTLD	2	2	9,300	2.2	2.2	0	5	4	8,950	4.5	5.6	0
mt	ccTLD	16	16	11,000	14.5	14.5	0	17	13	9,400	13.8	18.1	0
mu	ccTLD	33	13	8,100	16.0	40.7	0	318	8	9,350	8.6	340.1	0
mv	ccTLD	2	2	4,200	4.8	4.8	0	3	3	3,500	8.6	8.6	0
mw	ccTLD	3	2	10,100	2.0	3.0	0	2	2	2,600	7.7	7.7	0
mx	ccTLD	1,007	796	818,540	9.7	12.3	15	710	481	801,990	6.0	8.9	7
my	ccTLD	346	250	323,175	7.7	10.7	1	364	267	321,794	8.3	11.3	0
mz	ccTLD	11	9	4,700	19.1	23.4	0	12	3				0
na	ccTLD	6	4	3,900	10.3	15.4	0	8	5	3,700	13.5	21.6	0
name	legacy gTLD	55	53	162,374	3.3	3.4	31	38	28	171,980	1.6	2.2	2
nc	ccTLD	1	1	4,800	2.1	2.1	0	2	2	4,500	4.4	4.4	0
ne	ccTLD	1	1	450	22.2	22.2	0	2	1	400	25.0	50.0	0
net	legacy gTLD	11,403	6,018	16,285,470	3.7	7.0	1,990	12,686	7,124	16,174,960	4.4	7.8	680
network	new gTLD	3	2	18,425	1.1	1.6	1	0	0				
news	new gTLD	14	13	77,256	1.7	1.8	3	2	1	43,227	0.2	0.5	0
nf	ccTLD	79	3	1,200	25.0	658.3	0	114	7	1,200	58.3	950.0	0
ng	ccTLD	307	267	65,000	41.1	47.2	47	106	78	39,500	19.7	26.8	0
ni	ccTLD	4	4	6,200	6.5	6.5	0	6	4				0
ninja	new gTLD	1	1	38,214	0.3	0.3	0	12	7	53,806	1.3	2.2	1

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
nl	ccTLD	954	835	5,684,334	1.5	1.7	56	925	750	5,607,788	1.3	1.6	9
no	ccTLD	163	107	716,677	1.5	2.3	0	229	172	680,214	2.5	3.4	0
np	ccTLD	128	114	55,000	20.7	23.3	0	113	6				0
nr	ccTLD	0	0				0	30	2	300	66.7	1000.0	0
nu	ccTLD	42	33	325,000	1.0	1.3	0	262	71	302,992	2.3	8.6	0
nyc	new gTLD	2	2	75,057	0.3	0.3	0	2	2	78,791	0.3	0.3	0
nz	ccTLD	325	259	669,714	3.9	4.9	10	340	248	653,641	3.8	5.2	1
om	ccTLD	4	3	2,800	10.7	14.3	0	1	1	2,650	3.8	3.8	0
one	new gTLD	38	34	63,044	5.4	6.0	32	0	0				
online	new gTLD	566	545	564,822	9.6	10.0	513	10	7	123,071	0.6	0.8	6
ooo	new gTLD	0	0				0	1	1	17,685	0.6	0.6	0
org	legacy gTLD	7,101	4,874	11,230,268	4.3	6.3	762	8,518	6,029	10,893,296	5.5	7.8	170
ovh	new gTLD	4	4	57,228	0.7	0.7	0	0	0				
pa	ccTLD	7	6	18,500	3.2	3.8	0	14	11	18,500	5.9	7.6	0
paris	new gTLD	1	1	22,431	0.4	0.4	0	6	4	232,104	0.2	0.3	0
partners	new gTLD	1	1	5,087	2.0	2.0	1	0	0				
parts	new gTLD	2	1	5,249	1.9	3.8	0	0	0				
party	new gTLD	61	61	79,966	7.6	7.6	60	159	146	219,115	6.7	7.3	145
pe	ccTLD	214	164	99,000	16.6	21.6	3	206	156	92,750	16.8	22.2	0
pet	new gTLD	1	1	10,281	1.0	1.0	1	0	0				
pf	ccTLD	0	0				0	4	3	1,650	18.2	24.2	0
pg	ccTLD	4	4	2,000	20.0	20.0	0	2	1				0
ph	ccTLD	123	93	76,000	12.2	16.2	1	469	107	66,750	16.0	70.3	1
photo	new gTLD	5	4	27,913	1.4	1.8	1	2	1	24,290	0.4	0.8	1
photography	new gTLD	6	4	49,799	0.8	1.2	0	8	8	51,713	1.5	1.5	0
photos	new gTLD	1	1	19,145	0.5	0.5	1	5	5	19,210	2.6	2.6	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
physio	new gTLD	1	1	1,211	8.3	8.3	0	0	0				
pics	new gTLD	7	7	31,160	2.2	2.2	1	1	1	31,155	0.3	0.3	0
pictures	new gTLD	1	1	7,100	1.4	1.4	0	0	0				
pizza	new gTLD	4	1	4,383	2.3	9.1	0	0	0				
pk	ccTLD	301	227	62,000	36.6	48.5	0	245	170	57,530	29.5	42.6	0
pl	ccTLD	2,923	1,956	2,610,634	7.5	11.2	52	1,884	1,228	2,719,834	4.5	6.9	10
plus	new gTLD	2	2	6,710	3.0	3.0	1	0	0				
pm	ccTLD	14	12	7,220	16.6	19.4	9	6	3	7,250	4.1	8.3	1
pn	ccTLD	58	3	8,000	3.8	72.5	0	91	3	1,000	30.0	910.0	0
press	new gTLD	16	16	48,542	3.3	3.3	9	1	1	9,096	1.1	1.1	1
pro	legacy gTLD	238	94	431,368	2.2	5.5	35	70	52	128,853	4.0	5.4	0
productions	new gTLD	0	0				0	1	1	44,451	0.2	0.2	0
properties	new gTLD	2	2	10,590	1.9	1.9	0	1	1	10,881	0.9	0.9	0
property	new gTLD	2	2	13,204	1.5	1.5	2	0	0				
ps	ccTLD	34	27	7,300	37.0	46.6	0	38	23	8,792	26.2	43.2	0
pt	ccTLD	303	236	872,544	2.7	3.5	0	286	203	778,000	2.6	3.7	0
pub	new gTLD	7	7	66,395	1.1	1.1	7	5	4	43,010	0.9	1.2	1
pw	ccTLD	2,782	2,702	675,000	40.0	41.2	2,674	1,050	946	1,030,600	9.2	10.2	741
py	ccTLD	50	38	17,800	21.3	28.1	0	159	116	18,000	64.4	88.3	0
qa	ccTLD	5	4	17,000	2.4	2.9	0	10	6	16,100	3.7	6.2	0
quebec	new gTLD	1	1	9,431	1.1	1.1	0	0	0				
racing	new gTLD	4	4	140,300	0.3	0.3	1	9	7	27,376	2.6	3.3	2
re	ccTLD	23	16	24,750	6.5	9.3	5	18	12	27,500	4.4	6.5	1
recipes	new gTLD	0	0				0	1	1	4,388	2.3	2.3	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
red	new gTLD	4	4	319,564	0.1	0.1	3	3	3	70,034	0.4	0.4	0
ren	new gTLD	48	47	320,116	1.5	1.5	47	7	7	236,168	0.3	0.3	6
rent	new gTLD	3	3	8,127	3.7	3.7	3	0	0				
rentals	new gTLD	12	10	10,462	9.6	11.5	9	3	2	11,052	1.8	2.7	0
repair	new gTLD	4	4	6,134	6.5	6.5	2	1	1	6,336	1.6	1.6	1
report	new gTLD	9	9	5,148	17.5	17.5	8	2	2	4,445	4.5	4.5	0
restaurant	new gTLD	1	1	10,458	1.0	1.0	0	0	0				
review	new gTLD	80	77	75,017	10.3	10.7	74	2	1	64,636	0.2	0.3	1
reviews	new gTLD	25	25	16,515	15.1	15.1	23	32	27	17,254	15.6	18.5	18
ro	ccTLD	820	608	900,605	6.8	9.1	0	1,152	825	875,061	9.4	13.2	5
rocks	new gTLD	30	22	75,017	2.9	4.0	14	2	2	63,728	0.3	0.3	0
rs	ccTLD	336	297	16,535	179.6	203.2	0	154	112	84,300	13.3	18.3	1
ru	ccTLD	4,340	2,433	735,000	33.1	59.0	307	2,405	1,857	5,040,000	3.7	4.8	34
run	new gTLD	3	3	73,986	0.4	0.4	2	0	0				
rw	ccTLD	18	8	88,872	0.9	2.0	0	11	8	2,300	34.8	47.8	0
sa	ccTLD	57	48	5,420,000	0.1	0.1	0	66	52	41,000	12.7	16.1	0
sale	new gTLD	4	4	13,097	3.1	3.1	0	0	0				
sc	ccTLD	3	2	7,500	2.7	4.0	1	5	4	6,300	6.3	7.9	1
school	new gTLD	3	2	8,783	2.3	3.4	0	0	0				
science	new gTLD	79	75	232,164	3.2	3.4	72	252	214	339,053	6.3	7.4	211
scot	new gTLD	1	1	13,097	0.8	0.8	0	0	0				
sd	ccTLD	9	7	8,779	8.0	10.3	0	6	5	3,000	16.7	20.0	0
se	ccTLD	294	222	1,448,432	1.5	2.0	3	496	371	1,398,451	2.7	3.5	7
services	new gTLD	72	68	24,374	27.9	29.5	63	8	8	21,434	3.7	3.7	8

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
sex	new gTLD	2	2	12,652	1.6	1.6	0	0	0				
sexy	new gTLD	3	3	18,883	1.6	1.6	2	6	6	24,197	2.5	2.5	2
sg	ccTLD	311	238	175,894	13.5	17.7	0	331	262	178,215	14.7	18.6	1
sh	ccTLD	2	2	7,500	2.7	2.7	1	6	5	7,100	7.0	8.5	0
show	new gTLD	2	2	4,642	4.3	4.3	1	0	0				
si	ccTLD	135	109	121,930	8.9	11.1	0	172	83	118,146	7.0	14.6	0
singles	new gTLD	1	1	4,522	2.2	2.2	0	0	0				
site	new gTLD	221	216	600,244	3.6	3.7	199	9	8	83,214	1.0	1.1	6
sk	ccTLD	134	102	353,708	2.9	3.8	0	230	132	341,368	3.9	6.7	0
sl	ccTLD	8	6	1,600	37.5	50.0	0	2	2	1,500	13.3	13.3	0
sm	ccTLD	1	1	2,200	4.5	4.5	0	1	1	2,250	4.4	4.4	0
sn	ccTLD	14	7	4,500	15.6	31.1	0	16	8	4,500	17.8	35.6	0
so	ccTLD	13	11	14,000	7.9	9.3	0	12	8	17,000	4.7	7.1	1
social	new gTLD	5	5	18,017	2.8	2.8	3	5	3	15,741	1.9	3.2	1
software	new gTLD	0	0				0	1	1	9,645	1.0	1.0	1
solar	new gTLD	3	1	6,741	1.5	4.5	0	3	1	6,185	1.6	4.9	0
solutions	new gTLD	65	61	57,444	10.6	11.3	53	18	10	44,194	2.3	4.1	3
space	new gTLD	110	109	214,916	5.1	5.1	95	12	10	106,723	0.9	1.1	8
sr	ccTLD	2	2	221,890	0.1	0.1	0	6	4	3,000	13.3	20.0	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
srl	new gTLD	1	1	3,412	2.9	2.9	0	0	0				
st	ccTLD	7	4	12,000	3.3	5.8	1	42	8	12,376	6.5	33.9	0
store	new gTLD	10	9	83,647	1.1	1.2	9	0	0				
stream	new gTLD	2	2	3,412	5.9	5.9	2	0	0				
su	ccTLD	249	116	83,568	13.9	29.8	73	116	66	118,780	5.6	9.8	14
supplies	new gTLD	1	1	3,052	3.3	3.3	0	0	0				
supply	new gTLD	0	0				0	1	1	3,315	3.0	3.0	0
support	new gTLD	89	85	118,910	7.1	7.5	83	15	13	16,118	8.1	9.3	11
sv	ccTLD	16	12	18,128	6.6	8.8	0	19	8	8,100	9.9	23.5	0
sx	ccTLD	0	0				0	1	1	4,310	2.3	2.3	1
sy	ccTLD	3	3	1,500	20.0	20.0	0	2	1	1,412	7.1	14.2	0
sydney	new gTLD	9	8	9,394	8.5	9.6	0	0	0				
systems	new gTLD	9	8	21,015	3.8	4.3	7	1	1	18,316	0.5	0.5	1
sz	ccTLD	2	2	1,600	12.5	12.5	0	1	1	1,500	6.7	6.7	0
tattoo	new gTLD	1	1	2,870	3.5	3.5	0	0	0				
tax	new gTLD	2	1	4,811	2.1	4.2	1	0	0				
taxi	new gTLD	1	1	9,385	1.1	1.1	0	0	0				
tc	ccTLD	2	2	20,982	1.0	1.0	0	12	8	7,900	10.1	15.2	0
team	new gTLD	1	1	9,442	1.1	1.1	1	0	0				
tech	new gTLD	97	89	314,216	2.8	3.1	80	1	1	27,703	0.4	0.4	1
technology	new gTLD	4	4	313,505	0.1	0.1	2	2	2	24,458	0.8	0.8	0
tf	ccTLD	3	3	3,100	9.7	9.7	0	56	9	3,000	30.0	186.7	0
tg	ccTLD	6	6	1,400	42.9	42.9	0	5	4	1,000	40.0	50.0	0
th	ccTLD	159	114	65,000	17.5	24.5	0	251	185	64,732	28.6	38.8	1
tips	new gTLD	14	8	33,932	2.4	4.1	4	5	5	24,958	2.0	2.0	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
tj	ccTLD	10	6	7,200	8.3	13.9	0	17	13	6,700	19.4	25.4	2
tk	ccTLD	2786	2,758	18,700,000	1.5	1.5	2,592	3,472	2,746	23,130,423	1.2	1.5	644
tl	ccTLD	16	4	1,800	22.2	88.9	0	32	12	1,900	63.2	168.4	0
tm	ccTLD	6	3	17,000	1.8	3.5	0	24	2	16,200	1.2	14.8	0
tn	ccTLD	62	44	36,139	12.2	17.2	1	46	31	32,288	9.6	14.2	0
to	ccTLD	89	24	18,500	13.0	48.1	3	146	33	17,500	18.9	83.4	0
today	new gTLD	36	35	60,558	5.8	5.9	30	7	7	48,288	1.4	1.4	1
tokyo	new gTLD	0	0				0	3	2	41,881	0.5	0.7	0
tools	new gTLD	5	3	7,883	3.8	6.3	1	0	0				
top	new gTLD	1,788	1,687	4,780,500	3.5	3.7	1,602	555	505	967,655	5.2	5.7	501
town	new gTLD	1	1	2,867	3.5	3.5	1	0	0				
tr	ccTLD	341	272	350,000	7.8	9.7	0	493	338	377,751	8.9	13.1	4
trade	new gTLD	115	115	160,204	7.2	7.2	109	22	21	31,032	6.8	7.1	0
training	new gTLD	1	1	17,401	0.6	0.6	0	1	1	16,301	0.6	0.6	0
travel	legacy gTLD	5	5	17,906	2.8	2.8	0	14	8	18,161	4.4	7.7	1
tt	ccTLD	6	2	4,950	4.0	12.1	0	7	4	4,900	8.2	14.3	0
tv	ccTLD	175	134	540,200	2.5	3.2	7	264	198	575,800	3.4	4.6	6
tw	ccTLD	247	198	329,884	6.0	7.5	0	184	124	330,100	3.8	5.6	0
tz	ccTLD	60	47	13,000	36.2	46.2	0	52	35	10,400	33.7	50.0	1
ua	ccTLD	1,371	449	560,345	8.0	24.5	5	598	446	552,956	8.1	10.8	3
ug	ccTLD	36	28	6,500	43.1	55.4	0	30	23	6,500	35.4	46.2	0
uk	ccTLD	3,458	2,753	10,592,882	2.6	3.3	313	3,930	3,052	10,637,764	2.9	3.7	287
university	new gTLD	1	1	4,989	2.0	2.0	0	0	0				
uno	new gTLD	2	2	17,588	1.1	1.1	1	1	1	20,994	0.5	0.5	0
us	ccTLD	1,179	1,030	2,019,000	5.1	5.8	631	1,173	817	1,678,479	4.9	7.0	195
uy	ccTLD	146	108	79,195	13.6	18.4	1	92	76	74,517	10.2	12.3	0
uz	ccTLD	15	14	30,310	4.6	4.9	0	20	14	26,800	5.2	7.5	0
va	ccTLD	1	1	318	31.4	31.4	0	0	0				
vacations	new gTLD	4	4	4,184	9.6	9.6	3	4	3	4,424	6.8	9.0	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
vc	ccTLD	50	6	46,215	1.3	10.8	1	94	12	39,600	3.0	23.7	0
ve	ccTLD	1,206	1,045	77,555	134.7	155.5	832	414	386	63,030	61.2	65.7	3
vegas	new gTLD	2	2	12,319	1.6	1.6	1	0	0				
ventures	new gTLD	2	2	7,857	2.5	2.5	0	1	1	7,514	1.3	1.3	0
vet	new gTLD	1	1	5,856	1.7	1.7	0	0	0				
vg	ccTLD	24	7	4,600	15.2	52.2	0	9	3	4,900	6.1	18.4	0
vi	ccTLD	0	0				0	1	1	1,600	6.3	6.3	0
villas	new gTLD	0	0				0	1	1	1,995	5.0	5.0	0
vip	new gTLD	39	39	569,414	0.7	0.7	38	0	0				
vision	new gTLD	0	0				0	2	2	4,338	4.6	4.6	0
vlaanderen	new gTLD	1	1	6,669	1.5	1.5	0	0	0				
vn	ccTLD	392	309	550,000	5.6	7.1	0	463	320	500,075	6.4	9.3	7
vu	ccTLD	176	6	1,600	37.5	1100.0	0	91	7	1,625	43.1	560.0	0
wales	new gTLD	1	1	12,355	0.8	0.8	0	0	0				
wang	new gTLD	14	14	987,414	0.1	0.1	14	10	10	601,120	0.2	0.2	9
watch	new gTLD	0	0				0	2	2	5,260	3.8	3.8	1
webcam	new gTLD	32	31	48,881	6.3	6.5	29	21	20	78,513	2.5	2.7	19
website	new gTLD	162	142	230,105	6.2	7.0	109	19	13	124,668	1.0	1.5	9
wf	ccTLD	4	1	1,995	5.0	20.1	0	0	0				
wien	new gTLD	1	1	14,981	0.7	0.7	0	0	0				
win	new gTLD	478	456	1,264,500	3.6	3.8	452	132	130	559,606	2.3	2.4	129
work	new gTLD	35	29	80,400	3.6	4.4	16	6	6	97,021	0.6	0.6	4
works	new gTLD	0	0				0	1	1	9,044	1.1	1.1	0
world	new gTLD	11	7	34,895	2.0	3.2	3	4	4	26,421	1.5	1.5	3
ws	ccTLD	59	39	151,000	2.6	3.9	9	200	90	157,000	5.7	12.7	10
wtf	new gTLD	1	1	7,909	1.3	1.3	0	1	1	7,119	1.4	1.4	0
xin	new gTLD	1	1	341,405	0.0	0.0	0	0	0				
xn--6frz82g (.移动)	new gTLD	0	0				0	1	1	3,419	2.9	2.9	0

TLD	TLD Type	# Unique Phishing Attacks 2016	Unique Domain Names used for phishing 2016	Domains in registry, Dec 2016	Score: Phishing domains per 10,000 domains 2016	Score: Attacks per 10,000 domains 2016	# Total Malicious Domains Registered 2016	# Unique Phishing Attacks 2015	Unique Domain Names used for phishing 2015	Domains in registry, Dec 2015	Score: Phishing domains per 10,000 domains 2015	Score: Attacks per 10,000 domains 2015	# Total Malicious Domains Registered 2015
xn--80adxhks (.МОСКВА)	new gTLD	1	1	20,358	0.5	0.5	0	0	0				
xn--czru2d (.商城)	new gTLD	1	1	7,571	1.3	1.3	0	0	0				
xn--p1ai (.РФ)	ccTLD	65	56	899,000	0.6	0.7	0	47	35	864,340	0.4	0.5	0
xxx	legacy gTLD	1	1	167,991	0.1	0.1	0	6	5	174,920	0.3	0.3	0
xyz	new gTLD	938	894	6,743,803	1.3	1.4	634	282	228	1,785,125	1.3	1.6	196
yoga	new gTLD	0	0	7,094	0.0	0.0	0	0	0				
yt	ccTLD	1	1	4,218	2.4	2.4	0	0	0				
za	ccTLD	1288	1,061	1,060,055	10.0	12.2	59	1,081	777	1,088,814	7.1	9.9	7
zm	ccTLD	14	12	4,300	27.9	32.6	0	14	9				0
zone	new gTLD	5	5	16,804	3.0	3.0	3	8	1	14,468	0.7	5.5	0
zw	ccTLD	34	31	25,500	12.2	13.3	0	31	2				0
	Host Based Attacks	**248,692**	**195,475**	**329,047,130**	5.8	7.3	**95,426**	**227,471**	**160,155**	**310,852,857**	5.2	6.1	34,102
	IP Address Attacks	**6,373**						**2,809**					
	ALL ATTACKS	**255,065**						**230,280**					

About the Authors & Acknowledgments

The authors wish to thank the following for their support: Peter Cassidy and Foy Shiver of the APWG; Guanggang Geng, Huan Lei, and Xiaodong Lee at CNNIC for the contribution of APAC phishing data for this report; and DomainTools for its contribution of WHOIS data to help identify trends in malicious registrations. 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.

Greg Aaron is Vice-President at iTheat Cyber Group, a cybersecurity firm that provides risk data and analysis to companies in a wide variety of industries, including consumer products, entertainment, and pharmaceuticals. Greg is an authority on the use of domain names for e-crime, and works with registrars, registries, law enforcement, and researchers to investigate phishing, malware, spam, botnet, and piracy cases. Greg serves as the APWG's Senior Research Fellow, and as Co-Chair of the APWG's Internet Policy Committee. He is a member of ICANN's Security and Stability Advisory Committee (SSAC), and was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG). Greg is also an expert on domain industry operations, and has overseen the launches and operations of the multiple top-level domains, He was the senior industry expert on the Ernst & Young team that evaluated over one thousand new TLD applications to ICANN in 2012-2013. He has significant experience with Internet governance and ICANN policy-making). Greg is a magna cum laude graduate of the University of Pennsylvania.

Rod Rasmussen is the Founder and Principle of R2 Cyber, a cybersecurity consulting practice focused on research and public policy. He is formerly President and CTO of Internet Identity and served as its technical leader since he co-founded the company in 2001 until its purchase by Infoblox in 2016. He then served as Infoblox's Vice President of Cybersecurity until 2017. He is widely recognized as a leading expert on the abuse of the domain name system by criminals. Rod is co-chair of the Anti-Phishing Working Group's (APWG) Internet Policy Committee. He is a member of ICANN's Security and Stability Advisory Committee (SSAC), a member of the Online Trust Alliance's (OTA) Steering Committee, and was appointed to the FCC's Communications Security, Reliability and Interoperability Council (FCC CSRIC) multiple times. He is also an active participant in the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG), and was IID's FIRST representative (Forum of Incident Response and Security Teams). He also is a regular participant in DNS-OARC meetings, the worldwide organization for major DNS operators, registries, and interested parties. Rasmussen earned an MBA from the Haas School of Business at UC-Berkeley and holds two bachelor's degrees, in Economics and Computer Science, from the University of Rochester.

#