The NameSentry® Report 2013

The Internet has become a common tool and a daily necessity. In order of importance, humans need air, water, and food to live. Love and the Internet may be tied for 4th.

The problem is – how safe is the Internet that we rely on every day?

ABOUT our data

The NameSentry® Abuse Monitoring Service incorporates data from Internet Identity, SURBL, Spamhaus, MalwareURL, Malware Domain List, Zeus Tracker, Spyeye Tracker, and Palevo Tracker, and that aggregated data was used in this report's analysis. Our data providers were not involved in the creation of this report.
NameSentry mines additional data unique to each reported abuse. Domains under management numbers are taken directly from ccTLD registry and ICANN web sites.

Benchmarking the Current State

Over the next few years, more than 1,000 new top-level domains (TLDs) will be added to the Internet's existing TLDs such as .com, .net, and .uk. These new TLDs will include terms like .music, .web, and .doctor, and brands like .youtube, .amazon, and .alibaba. For the past few years, a debate has raged about the potential impacts of these new TLDs on the safety and security of the Internet.

- Will the new TLDs provide virgin real estate for phishers, spammers, and malware-wielding criminals?
- Will the introduction of new TLDs automatically translate into a more dangerous Internet for the average user?

These questions will be difficult to answer without a firm grasp on the level of abuse on the Internet today. Without benchmarking the "current state," it will be hard to determine the level of change, and the debate could easily evolve into a conceptual one, with opinions based on ideological positions instead of facts.

Before the massive change to the Domain Name System (DNS) occurs, we at Architelos decided to create a baseline for the levels of abuse – phishing, malware, spam, and related abuses, across all TLDs around the world. The analysis is built on data in the Architelos' patent-pending NameSentry® Abuse Detection and Mitigation Service. Since its introduction in November 2012, NameSentry has been tracking and analyzing abusive domain activity across the Internet.

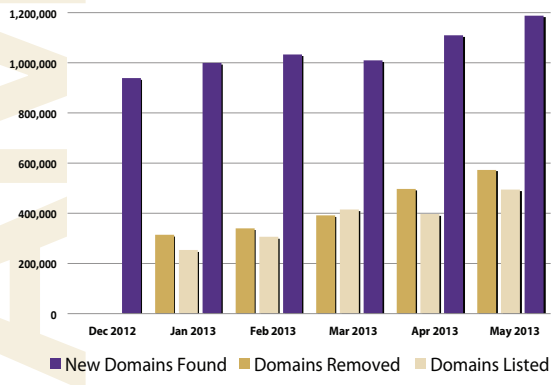
NAMESENTRY®
Abuse Detection and Mitigation Service

The NameSentry® Report 2013

HOW
bad is it?

The total number of active abusive domains increased 25% from December 2012 to May 2013. More abusive domains are being found than removed. As a result the namespace quality of the Internet is decreasing. Within the first five months of 2013, across all TLDs, more than 400,000 new abusive domains were found and added to blocklists on a monthly basis. On any given day, there are more than 1,000,000 domains on the blocklists tracked by NameSentry®. Large numbers of domains are added to the lists while "used" domains are cycled off after abuse takes place. With over 250 million domain names on the Internet, that translates to an NQI of 0.4% or roughly 4,000 abusive domains per million. The "Safety Level" for the entire Internet is "Exercise Caution."

Total Abusive Domains Increased over 25% from Dec 2012 to May 2013



Namespace Quality Index (NQI)

NQI measures the relative concentration of abusive domain names in any given namespace, thus providing a comparative measure of safety. Specifically, the NQI measures the number of reported abusive domain names per million Domains Under Management (DUM). The types of abuse include domains used for phishing, malware, botnet command-and-control, and domains advertised via spam sent from botnets and by other abusive means. NameSentry® uses data from trusted sources including Internet Identity, SURBL, Spamhaus, MalwareURL, ZeusTracker, SpyeyeTracker, and Malware Domain List. A large majority of the domains on these blocklists were registered for the purpose of perpetrating abuse, with a small minority consisting of domains that have been compromised by criminals. The NQI will be used not only to measure and communicate how safe or unsafe a particular namespace may be, but also to benchmark the industry's performance prior to the introduction of the new gTLDs. Once the current level of domain name abuse is benchmarked, it will be far easier to measure the impact of new gTLDs on the safety and security of the Internet.

NameSentry Index (NQI) Values	Levels of Abuse Concern	Colors	Results
Range is Abuses per million domain names	The namespace quality conditions are	As symbolized by this color	Percent Abuse
less than 1000	Excellent	Green	0% -0.01%
100 - 1,000	Good	Yellow	0.01% - 0.1%
1,000 - 10,000	Exercise Caution	Orange	0.1% - 1%
over 10,000	Surf at your Own Risk	Red	Over 1%

NAMESENTRY®
Abuse Detection and Mitigation Service

OUR
analysis shows

That 90% of listed domains were found when they were advertised in spam, with 6% involved in spreading malware. Phishing involves above 150,000 unique domains per year. Botnet command-and-control domains are relatively rare, but have a disproportionate importance.

NameSentry NQI Levels

NQI Level	PCT	TLDs
Excellent	21%	15
Good	50%	36
Caution	19%	14
At Risk	10%	7
All TLDs > 100,000 Domains		72

Fifteen TLDs achieve an "Excellent" NQI rating, while thirty-six TLDs receive a "Good" NQI level. Fourteen TLDs fall into the "Exercise Caution" level, and seven TLDs are labeled "Surf at your own Risk."

Recognizing Abuse

Classifying the abusive use of domains, and measuring the relative concentration of each, is another method to evaluate safety and security. Some domains can be classified reliably in automated fashion, especially those harboring malware. Domains advertised in spam are highly reliable pointers to various kinds of abuse and these e-mails are harvested from "spam traps" set up to receive unsolicited e-mail. Spam is the main way that criminals advertise their schemes. Most spam emails direct recipients to drive-by malware downloaders, phishing pages, counterfeit drug sales, financial fraud sites, and other criminal enterprises. In addition, spam messages are often sent from illegal botnets, further feeding the Internet's thriving criminal underground.

Our analysis shows that 90% of listed domains were found when they were advertised in spam, with 6% involved in spreading malware. Phishing involves above 150,000 unique domains per year. Botnet command-and-control domains are relatively rare, but have a disproportionate importance.

NAMESENTRY®
Abuse Detection and Mitigation Service

Not all TLDs are Equal

TLD registries can be distinguished by how resistant they are to abusive registrations, and how active or passive the registry is in detecting and mitigating abuse. Low prices, ineffectual registrars, and a lack of compliance and enforcement tend to attract abusive registrations, whereas restrictive registration policies and higher prices tend to deter abusive domain registrations. The charts below apply the NQI to TLDs that have more than 100,000 domains under management. These TLDs account for over 257 million domain names – over 99% of the total domains in the world's registries.

NameSpace Quality Index

Excellent

TLD	APM
tel	0
no	17
xxx	27
ie	33
nz	39
cz	46
ch	48
dk	53
sk	62
au	66
fi	81
lt	82
hu	83
si	92
pt	93

Date: as of May 31, 2013
Source: www.namesentry.com

Good

TLD	APM	TLD	APM
hk	102	id	250
tw	108	nu	260
gr	111	mx	264
sg	114	ro	266
nl	116	de	270
kr	132	cl	297
il	139	ir	301
ae	140	lv	303
ve	149	cc	316
se	151	tr	419
vn	156	es	449
co	172	br	451
my	198	PO	462
za	198	jp	556
ca	206	tv	600
ws	222	pl	660
tk	224	name	958
it	239	fr	980

Exercise Caution

TLD	APM
me	1,011
at	1,066
eu	1,309
uk	1,451
ua	1,947
be	2,235
ar	2,362
org	2,596
com	4,260
su	7,010
net	7,121
biz	7,495
pro	7,941
mobi	9,349

All TLDs > 100,000 domains

At Risk

TLD	APM
info	12,085
us	14,932
ru	25,079
asia	25,327
in	27,111
pw	30,151
cn	30,406

NameSentry Index (NSI)

Scale	APM
Excellent	less than 100
Good	100 - 1,000
Caution	1,000 - 10,000
At Risk	over 10,000

APM - Abuse per million domains

NAMESENTRY®
Abuse Detection and Mitigation Service

FOR more information

or to be added to the NameSentry Report mailing list Architelos will publish these statistics on no less than a quarterly basis to measure the quality of the total Internet namespace and identify notable trends.

If you would like additional information about the report, please contact us at namesentry@architelos.com. If you'd like to automatically receive the next installment of the NameSentry® Report, please sign up here.

About Architelos Inc.

Architelos, Inc. provides SaaS based TLD managed services solutions, and strategic consulting for clients in the Domain Name (DNS) Industry. NameSentry® a patent pending abuse detection and mitigation service, is the second SaaS based service launched by the company. Architelos is unique in having over 30 years of experience in building, launching and managing multi-million name gTLDs. Clients include new as well as existing generic Top Level Domain (gTLD) and Country Code (ccTLD) registries. Architelos has locations in Leesburg (VA), Los Angeles, (CA), Toronto (Canada) and Dublin (Ireland), as well as data centers in Toronto and Los Angeles. For more information follow us @architelos on Twitter or join us on Facebook.

NAMESENTRY®
Abuse Detection and Mitigation Service