△| ARCHITELOS

The NᴀᴍᴇSᴇɴᴛʀʏ℠ Aʙᴜꜱᴇ Rᴇᴘᴏʀᴛ
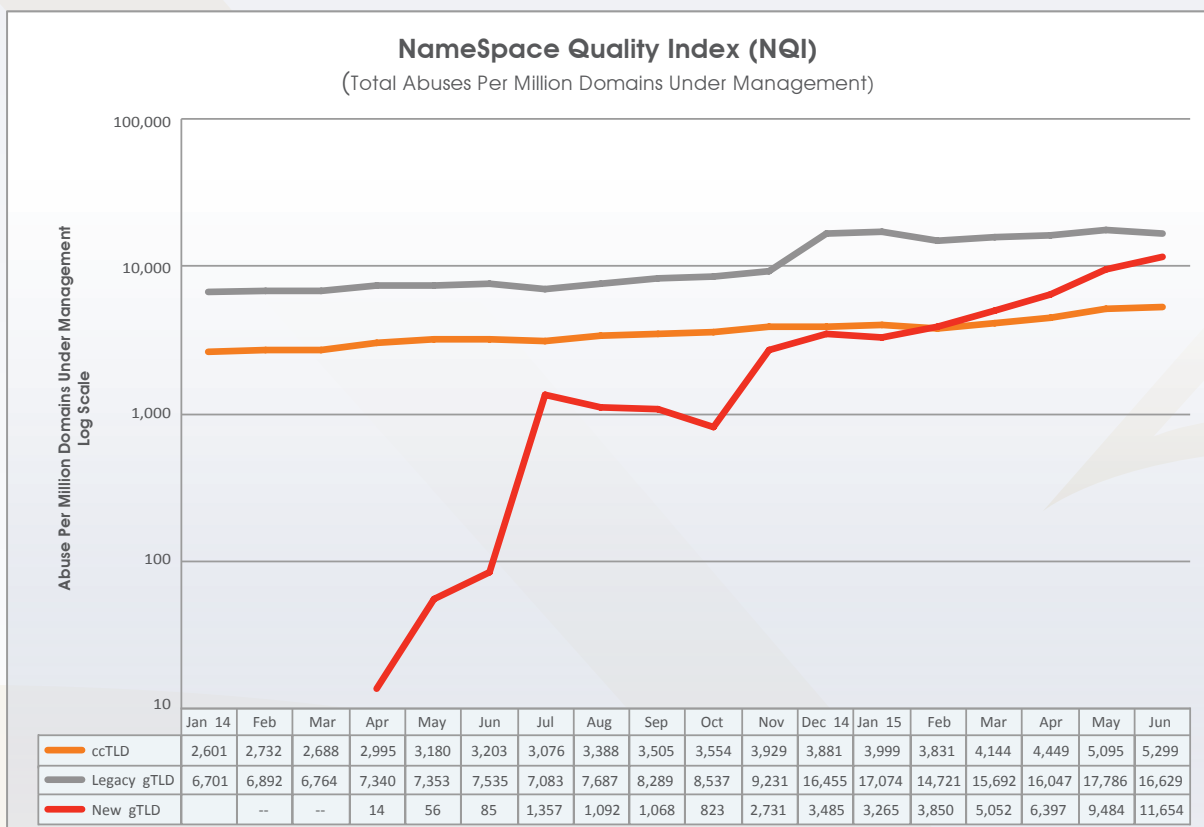Abuse Detection and Mitigation Service

New gTLD State of Abuse - 2015

The Architelos NameSentry℠ domain abuse monitoring, detection and mitigation service tracks abuse (phishing, malware, botnet C&C command-and-control, and spam) across all top-level domains (TLDs). The Internet now has almost 300 million domain names across more than 900 TLDs. In order to compare the different types of TLDs, we normalize the abuse data into the Architelos Namespace Quality Index (NQI). The NQI score is measured as abusive domains that are on our NameSentry℠ subscribed blocklists per million domains in each registry. This allows us to compare abuse consistently across TLDs. This following graph shows the NQI score for the collective categories of country code Top Level Domains (ccTLDs), Legacy gTLDs, and New gTLDs (nTLDs). The top grey line is the NQI score for the aggregate of the 22 legacy gTLDs (.com, .net, .org, .biz, etc). The orange line is the NQI score for the aggregate of all 280+ ccTLDs. Finally, the red line is the NQI score for the aggregate of the 500+ new nTLDs. What is clear is that over the past 16 months abuse has found the new gTLDs and has grown in proportion to exceed that of ccTLDs and is approaching the levels of Legacy gTLDs. Within new gTLDs, spam comprises 99% of all reported abuses as compared to approximately 90% in ccTLDs and Legacy gTLDs. Therefore phishing, malware and botnet C&C activity in new gTLDs is ten-fold less than in ccTLD and Legacy gTLDs on proportion of domains under management.

NameSpace Quality Index (NQI)
(Total Abuses Per Million Domains Under Management)

	Jan 14	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec 14	Jan 15	Feb	Mar	Apr	May	Jun
ccTLD	2,601	2,732	2,688	2,995	3,180	3,203	3,076	3,388	3,505	3,554	3,929	3,881	3,999	3,831	4,144	4,449	5,095	5,299
Legacy gTLD	6,701	6,892	6,764	7,340	7,353	7,535	7,083	7,687	8,289	8,537	9,231	16,455	17,074	14,721	15,692	16,047	17,786	16,629
New gTLD		--	--	14	56	85	1,357	1,092	1,068	823	2,731	3,485	3,265	3,850	5,052	6,397	9,484	11,654

Graph 1 - NameSpace Quality Index Comparison for ccTLD, gTLDs and new gTLDs from Jan 2014 to May 2015.

△ | ARCHITELOS

The NameSentry℠ Abuse Report
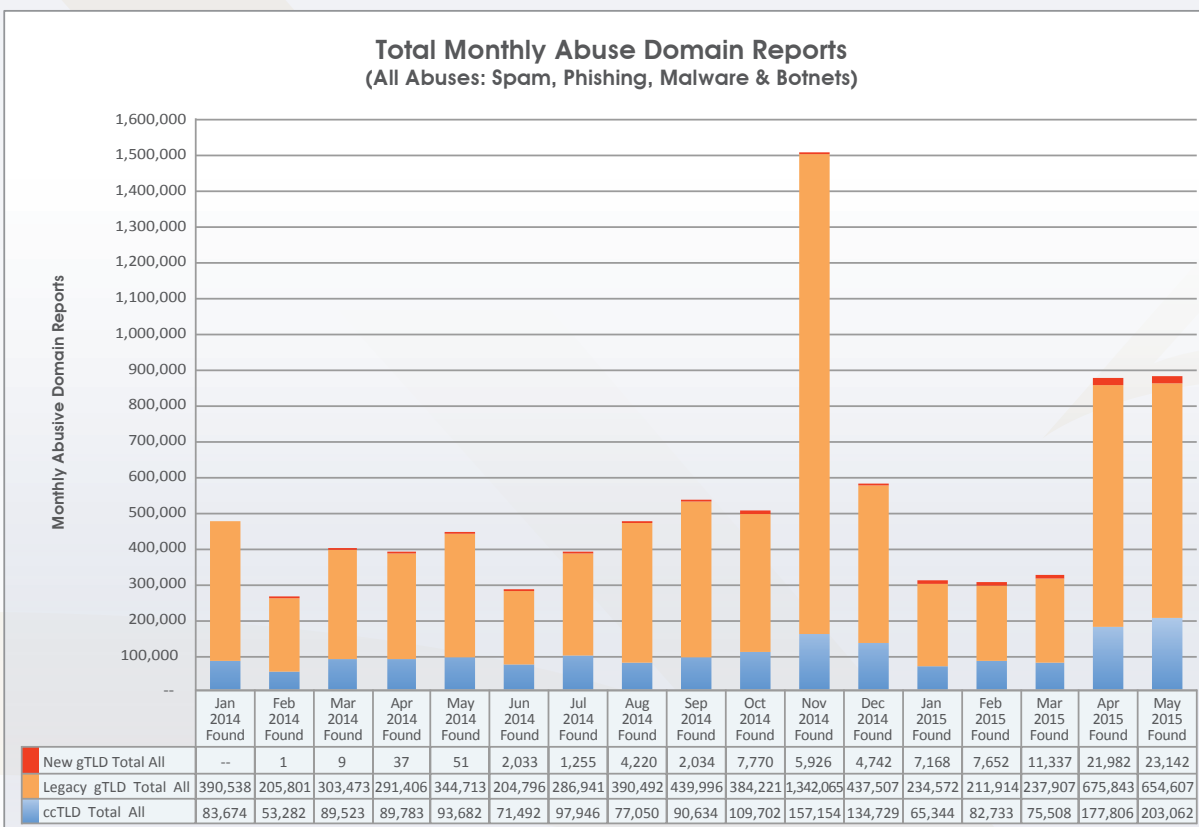Abuse Detection and Mitigation Service

Internet State of Abuse - 2015 - continued

The May 2015 NQI score for all ccTLDs was 5,299 abusive domains per million domains under management. The new gTLD NQI score in May was 11,654 per million domains under management, or over 100% greater than the ccTLDs. The NQI score for the legacy gTLDs is approximately 16,500 per million over the past several months. This is over three times the average level of aggregate abuse in ccTLDs.

Abuses per Million DUM	NQI Rating	% of Abuse	% Clean
less than 100	Excellent	< 0.01%	> 99.9%
101 - 1,000	Good	0.01 – 0.1%	99.8% – 99.9%
1,001 - 10,000	Caution	.1 – 1.0%	99.0% - 99.8%
over 10,001	At Risk	Over 1%	< 99.0%

A Focus on Detection of Abuse

The following graph presents abuses found or detected each month broken out by type of TLD: ccTLD, legacy gTLD, and New gTLD. The table at the bottom shows the timeline of abuse growth in the overall new gTLD program. The first abuse was detected in February 2014 and has grown to over 23,000 abusive domains in May 2015.

Total Monthly Abuse Domain Reports
(All Abuses: Spam, Phishing, Malware & Botnets)

	Jan 2014 Found	Feb 2014 Found	Mar 2014 Found	Apr 2014 Found	May 2014 Found	Jun 2014 Found	Jul 2014 Found	Aug 2014 Found	Sep 2014 Found	Oct 2014 Found	Nov 2014 Found	Dec 2014 Found	Jan 2015 Found	Feb 2015 Found	Mar 2015 Found	Apr 2015 Found	May 2015 Found
New gTLD Total All	--	1	9	37	51	2,033	1,255	4,220	2,034	7,770	5,926	4,742	7,168	7,652	11,337	21,982	23,142
Legacy gTLD Total All	390,538	205,801	303,473	291,406	344,713	204,796	286,941	390,492	439,996	384,221	1,342,065	437,507	234,572	211,914	237,907	675,843	654,607
ccTLD Total All	83,674	53,282	89,523	89,783	93,682	71,492	97,946	77,050	90,634	109,702	157,154	134,729	65,344	82,733	75,508	177,806	203,062

Graph 2 - Comparison of Abuse by Type for new gTLDs, Legacy gTLDs and ccTLDs from Jan 2014 to May 2015.
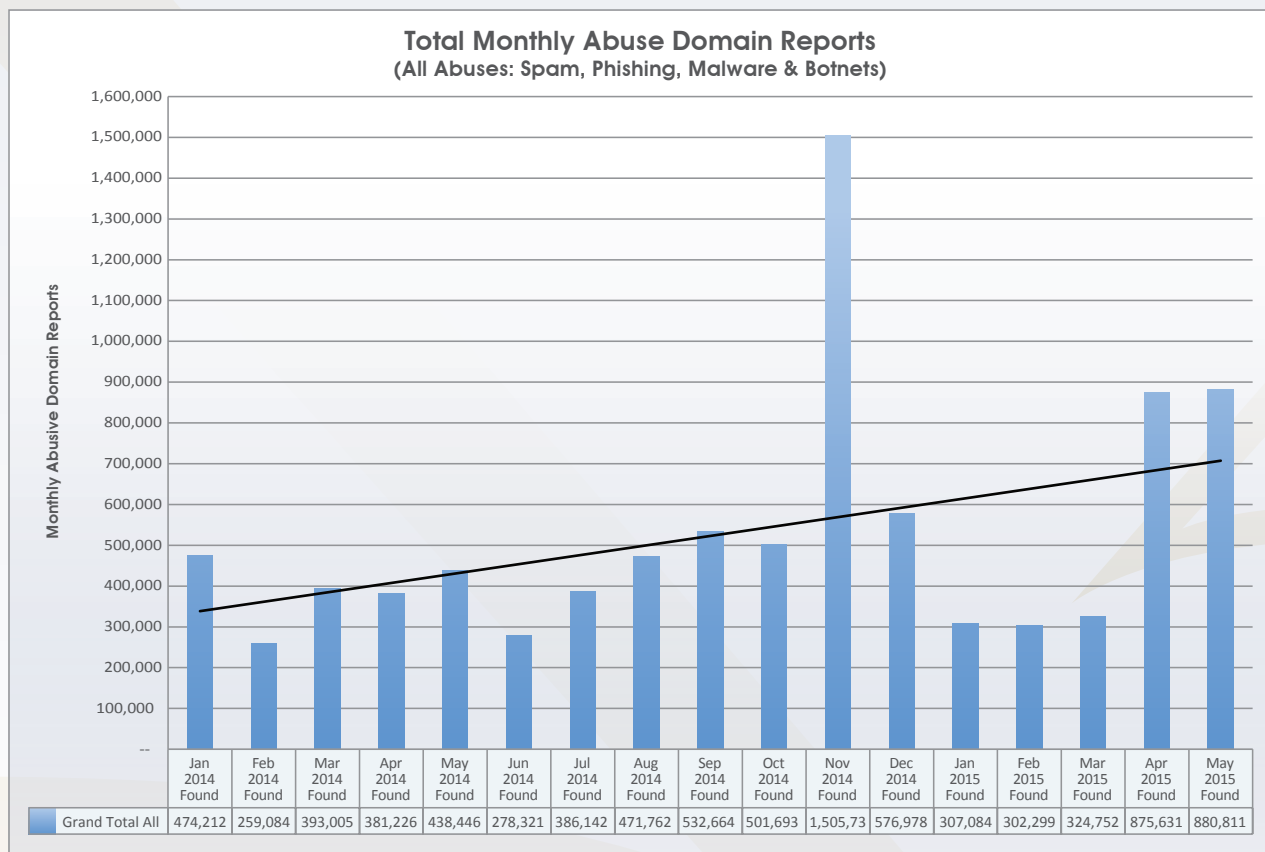
ARCHITELOS

The NameSentry℠ Abuse Report
Abuse Detection and Mitigation Service

A Focus on Detection of Abuse - continued

The chart below depicts total domain abuse newly found each month from January 2014 through May 2015. The found data is a subset of the total active abuses used in the NQI scoring in the prior graph. Using a linear trend line, new abuse reports have increased 100% over that time, from approximately 350,000 per month in January 2014 to more than 700,000 per month in May 2015. The profile indicates seasonal variations along with a substantial spike of spam abuse in late November into early December coinciding with the holiday season. For the first quarter of 2015 newly found abuse reports fell to about 300,000 per month. However, in April and May the abuse reports (mostly spam) increased substantially to over 850,000 per month. This represents a 100% increase over the same months in 2014 and is consistent with the overall trend of increasing abuse.

We have seen very slow growth in the overall domain market, and some legacy TLDs are flat or contracting. To spur growth some TLDs are providing aggressive discounting for the first time.
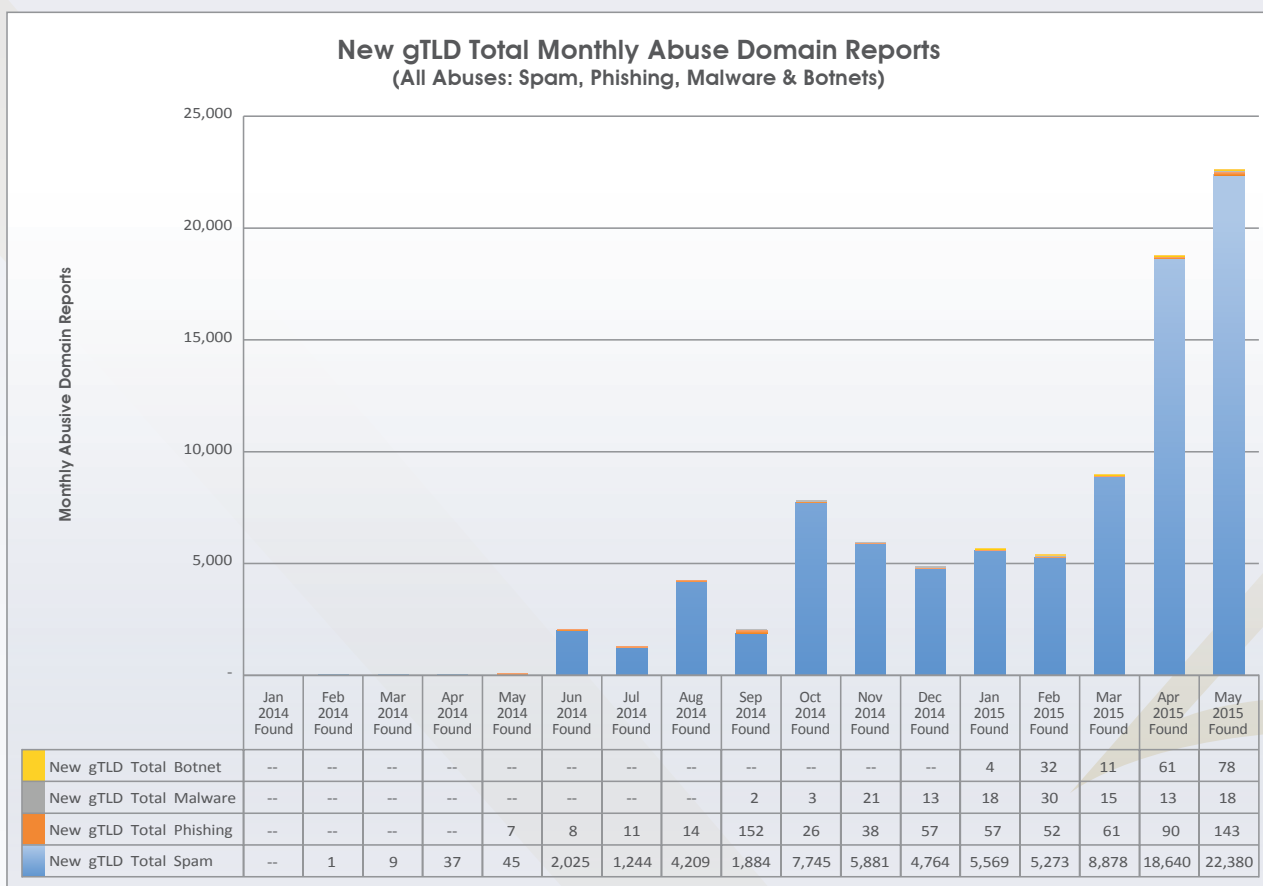
Total Monthly Abuse Domain Reports
(All Abuses: Spam, Phishing, Malware & Botnets)

	Jan 2014 Found	Feb 2014 Found	Mar 2014 Found	Apr 2014 Found	May 2014 Found	Jun 2014 Found	Jul 2014 Found	Aug 2014 Found	Sep 2014 Found	Oct 2014 Found	Nov 2014 Found	Dec 2014 Found	Jan 2015 Found	Feb 2015 Found	Mar 2015 Found	Apr 2015 Found	May 2015 Found
Grand Total All	474,212	259,084	393,005	381,226	438,446	278,321	386,142	471,762	532,664	501,693	1,505,73	576,978	307,084	302,299	324,752	875,631	880,811

Graph 3 - Total Monthly Abuse across all TLDs from Jan 2014 to May 2015.

The NAMESENTRY℠ Abuse Report
Abuse Detection and Mitigation Service

The Progression of New gTLD Abuse

The following chart provides a breakout of the new gTLD abuses between phishing, malware, botnet C&C command-and-control domains, and spam. Spam has accounted for 99% of all new gTLD abuse reports since the inception of the program. The first spam report in a new gTLD was found in February 2014 followed by the first phishing in May and first malware detected in September 2014. We began tracking Botnet C&C abuse in January 2015. In ccTLD and legacy gTLDs spam comprises approximately 90% of all reported domains therefore the new gTLD program currently has substantially less phishing and malware than the mature legacy and ccTLD markets.
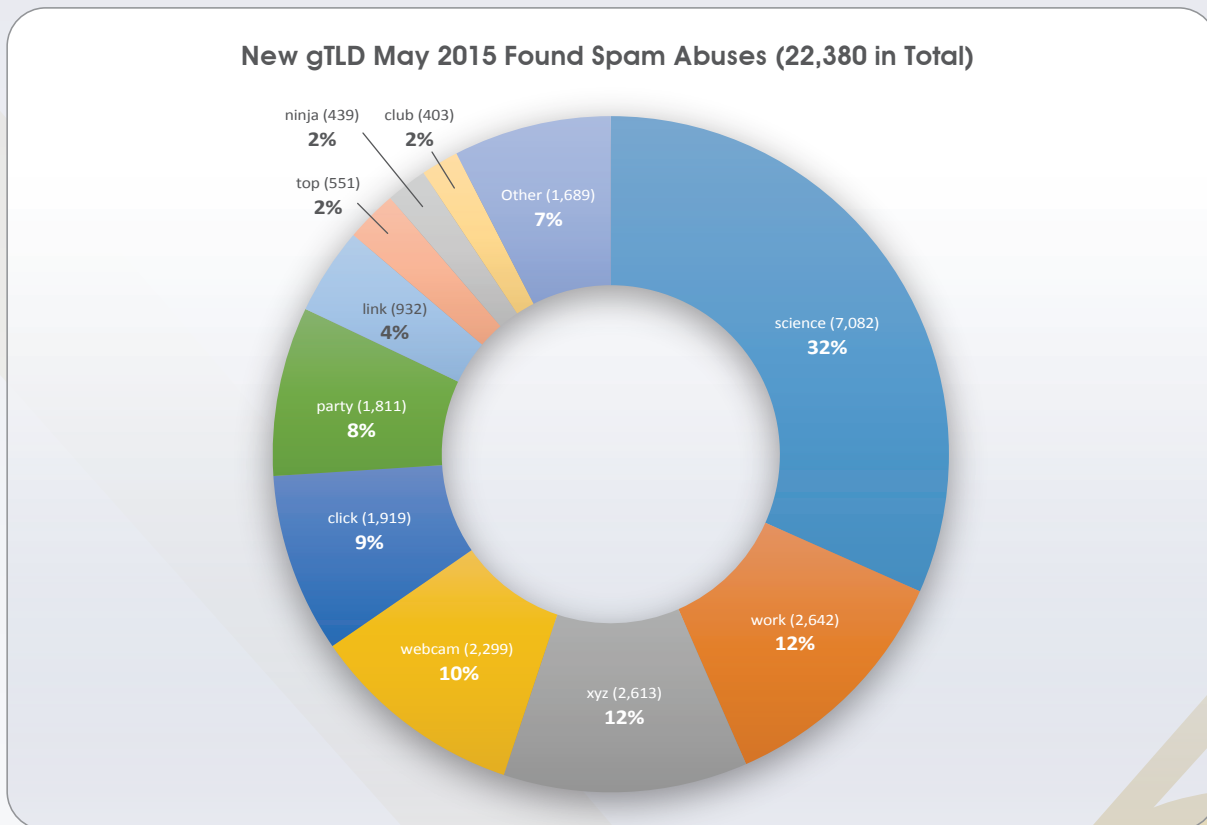
New gTLD Total Monthly Abuse Domain Reports
(All Abuses: Spam, Phishing, Malware & Botnets)

	Jan 2014 Found	Feb 2014 Found	Mar 2014 Found	Apr 2014 Found	May 2014 Found	Jun 2014 Found	Jul 2014 Found	Aug 2014 Found	Sep 2014 Found	Oct 2014 Found	Nov 2014 Found	Dec 2014 Found	Jan 2015 Found	Feb 2015 Found	Mar 2015 Found	Apr 2015 Found	May 2015 Found
New gTLD Total Botnet	--	--	--	--	--	--	--	--	--	--	--	--	4	32	11	61	78
New gTLD Total Malware	--	--	--	--	--	--	--	--	2	3	21	13	18	30	15	13	18
New gTLD Total Phishing	--	--	--	--	7	8	11	14	152	26	38	57	57	52	61	90	143
New gTLD Total Spam	--	1	9	37	45	2,025	1,244	4,209	1,884	7,745	5,881	4,764	5,569	5,273	8,878	18,640	22,380

Graph 4 - new gTLDs with the most SPAM Abuses Reported in May 2015.

The NAMESENTRY℠ Abuse Report
Abuse Detection and Mitigation Service

The Progression of New gTLD Abuse - continued

Spam abuse reports from March to April increased over 100% from under 9,000 to over 18,000. This increase was sustained in May with spam reports growing another 20% to over 22,000 spam reports. The graph below depicts the distribution of the new May spam reports by new gTLD.
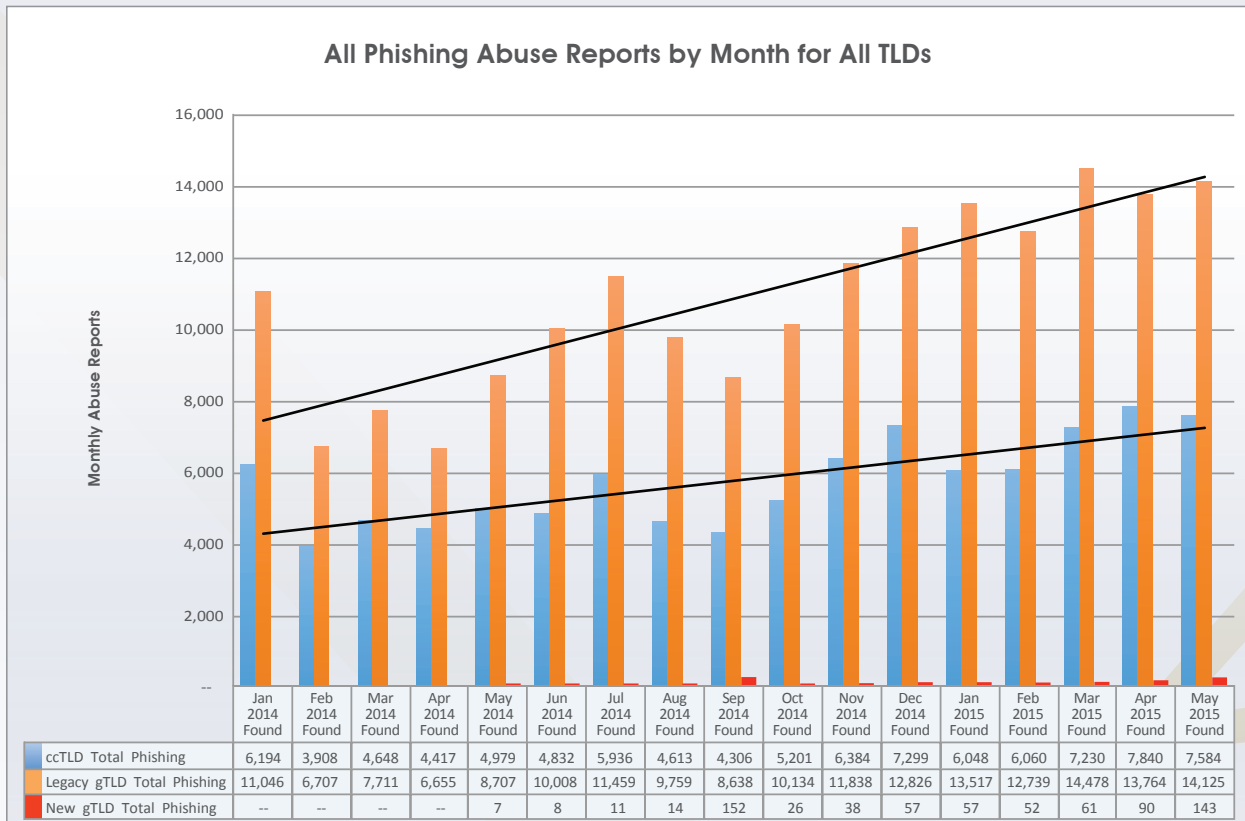
New gTLD May 2015 Found Spam Abuses (22,380 in Total)

ninja (439) **2%**
club (403) **2%**
top (551) **2%**
Other (1,689) **7%**
link (932) **4%**
science (7,082) **32%**
party (1,811) **8%**
click (1,919) **9%**
webcam (2,299) **10%**
xyz (2,613) **12%**
work (2,642) **12%**

Graph 5 - New gTLDs with the most SPAM Abuses Reported in May 2015.

The NameSentry℠ Abuse Report
Abuse Detection and Mitigation Service

A Focus On Phishing

Seeing the overall trend of a 100% increase in abuses found from Jan 2014 to May 2015 we wanted to focus on phishing to see if similar trends occurred. The following graph depicts new phishing abuses found broken out by category of TLD. Legacy gTLD phishing reports have also increased by almost 100% based upon the linear trend line going from approximately 7,300 to over 14,000 over the 17 month period. The May 2015 increase over May 2014 for legacy gTLDs was 62%. The ccTLD phishing has increased from approximately 4,100 to 7,100 or a 75% increase on a linear trend line. The May 2015 increase over May 2014 for ccTLDs was 52%. Phishing in New gTLDs increased from seven found in May 2014 to 143 in May 2015 or a twenty-fold increase.
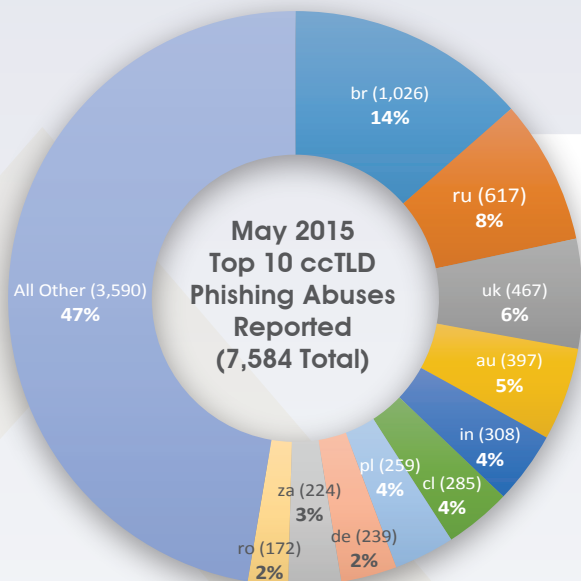
All Phishing Abuse Reports by Month for All TLDs

	Jan 2014 Found	Feb 2014 Found	Mar 2014 Found	Apr 2014 Found	May 2014 Found	Jun 2014 Found	Jul 2014 Found	Aug 2014 Found	Sep 2014 Found	Oct 2014 Found	Nov 2014 Found	Dec 2014 Found	Jan 2015 Found	Feb 2015 Found	Mar 2015 Found	Apr 2015 Found	May 2015 Found
ccTLD Total Phishing	6,194	3,908	4,648	4,417	4,979	4,832	5,936	4,613	4,306	5,201	6,384	7,299	6,048	6,060	7,230	7,840	7,584
Legacy gTLD Total Phishing	11,046	6,707	7,711	6,655	8,707	10,008	11,459	9,759	8,638	10,134	11,838	12,826	13,517	12,739	14,478	13,764	14,125
New gTLD Total Phishing	--	--	--	--	7	8	11	14	152	26	38	57	57	52	61	90	143

Graph 6 - Comparison of Phishing Trends between ccTLDs, Legacy gTLDs, and new gTLDs for Jan 2014 to May 2015.

The NAMESENTRY℠ Abuse Report
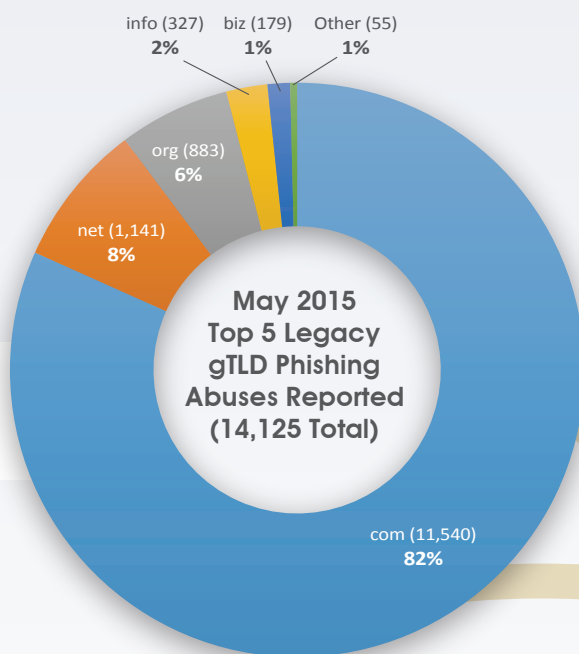Abuse Detection and Mitigation Service

A Focus On Phishing - continued

The following graphs show the TLDs by type (ccTLD, Legacy gTLD, New gTLD) with the highest number of phishing abuse listings in the month of May 2015.
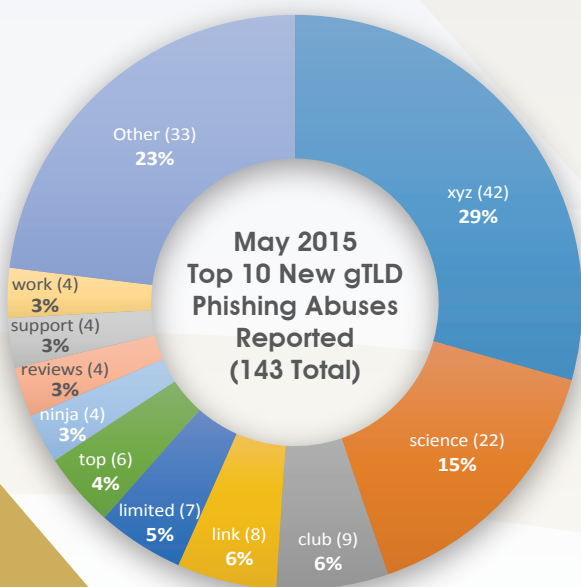

May 2015 Top 10 ccTLD Phishing Abuses Reported (7,584 Total)

- br (1,026) 14%
- ru (617) 8%
- uk (467) 6%
- au (397) 5%
- in (308) 4%
- cl (285) 4%
- pl (259) 4%
- de (239) 2%
- za (224) 3%
- ro (172) 2%
- All Other (3,590) 47%

Graph 7 - ccTLDs with the most Phishing Abuses Reported in May 2015.

Ten ccTLDs comprised 53% of the 7,584 new phishing reports in May 2015. This equates to 56 phishing reports per million ccTLD domains under management. The .br TLD had the highest number of phishing reports with 1,026 followed by .ru with 617 and .uk with 467.

May 2015 Top 5 Legacy gTLD Phishing Abuses Reported (14,125 Total)

- info (327) 2%
- biz (179) 1%
- Other (55) 1%
- org (883) 6%
- net (1,141) 8%
- com (11,540) 82%

Graph 8 - Top 5 Legacy gTLDs with the most Phishing Abuses Reported in May 2015.

Three Legacy gTLDs comprised 94% of 14,125 new phishing reports in May 2015. This equates to 89 phishing reports per million Legacy gTLD domains under management. The .com TLD had the highest number of phishing reports with 11,540 followed by .net with 1,141 and .org with 883.

May 2015 Top 10 New gTLD Phishing Abuses Reported (143 Total)

- xyz (42) 29%
- science (22) 15%
- club (9) 6%
- link (8) 6%
- limited (7) 5%
- top (6) 4%
- ninja (4) 3%
- reviews (4) 3%
- support (4) 3%
- work (4) 3%
- Other (33) 23%

Graph 9 - Top 10 new gTLDs with the most Phishing Abuses Reported in May 2015.

Ten New gTLDs comprised 77% of the 143 new phishing reports in May 2015. This equates to 24 phishing reports per million new gTLD domains under management. The .xyz TLD had the highest number of phishing reports with 42 followed by .science with 22 and .club with 9.

The NameSentry℠ Abuse Report
Abuse Detection and Mitigation Service

Summary

In summary, overall newly found abuses (all types of spam, phishing, malware and botnet C&C) are increasing at 100% annually. Overall, aggregate ccTLDs have 33% (one third or 67% less) of the abuse levels detected in the aggregate of Legacy gTLDs. High levels of spam have been detected in New gTLDs that are twice that of ccTLDs when normalized for domains under management. New gTLDs are still very low on phishing, malware and botnet C&C abuse levels when compared to Legacy gTLDs and ccTLDs. However, as new gTLDs achieve greater adoption and awareness we expect the more malicious abuses to grow as well.

△
ARCHITELOS

Software

Well before the launch of the first new gTLD of the 2012 round, we saw the need for targeted tools that did not exist in the industry. NameSentry℠, a patented abuse detection and mitigation service, is an easy-to-use portal that allows you to monitor the overall health and reputation of your TLD or domain portfolio near real-time. Used by ICANN's Global Domains Division for abuse market intelligence and by over 45% of new gTLDs in the market to protect their users and enable compliance with Specification 11(3)b of the ICANN Registry Agreement, NameSentry℠ is the unequivocal industry standard.

Architelos has also developed a suite of financial software products for domain registries and registrars. The solution is based on a number of modules each of which have perform specific roles, or when combined, support the financial activities of domain businesses.
*   Folio Exchange℠ - a next generation billing & remittance system that integrates with the all the front and back-end systems needed to automate billing.
*   NumberSense℠ - a powerful tool that calculates deferred revenue & cost positions, accounting revenue & costs,and integrates seamlessly with both Folio Exchange and your general ledger.
*   Business Intelligence tools that provides insightful graphic-driven reports on the key business drivers of a registry. The user is faced with a series of high level graph dashboards which is constantly fed data from a range of sources (back-end, publically available industry macro data and external sources). The user can customise their views and drill down to more detailed layers of data in order to investigate discrepancies and understand business trends.

About Illumintel (Illumintel.com)

Greg Aaron is President of Illumintel and a co-creator of NameSentry℠. Greg is an expert in domain abuse detection and mitigation and works regularly with registries, registrars, and law enforcement to combat spam, malware, phishing, and other abuses. Greg is a member of ICANN's Security and Stability Advisory Committee (SSAC) and is co-chair of the Anti-Phishing Working Group's Internet Policy Committee.

For More Information

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 at http://architelos.com/contact-us/