REGISTRYOFFICE

RegistryOffice Abuse Monitor Industry Review & Solicitation For Feedback

How New gTLD registries can efficiently & cost effectively fight domain abuse & promote a safer & better Internet

Cybercriminals increasingly prefer to register, rather than hack, domain names and some new gTLDs have become a magnet for malicious actors.

- Maciej Korczyński, Ph.D.

Grenoble Institute of Technology [1]

Outlining the Need for New Tools to Detect, Monitor and Report Domain Abuse

Starting in October 2013, hundreds of new generic top-level domains (gTLDs) entered into the Internet's root zone. This “New TLD” program[2] included top-level domains in both ASCII characters and in different scripts such as Arabic, Chinese, Cyrillic and Devanagari. This has been the largest historical root domain expansion in the history of the Internet.

These new gTLDs have brought new opportunities and new challenges.

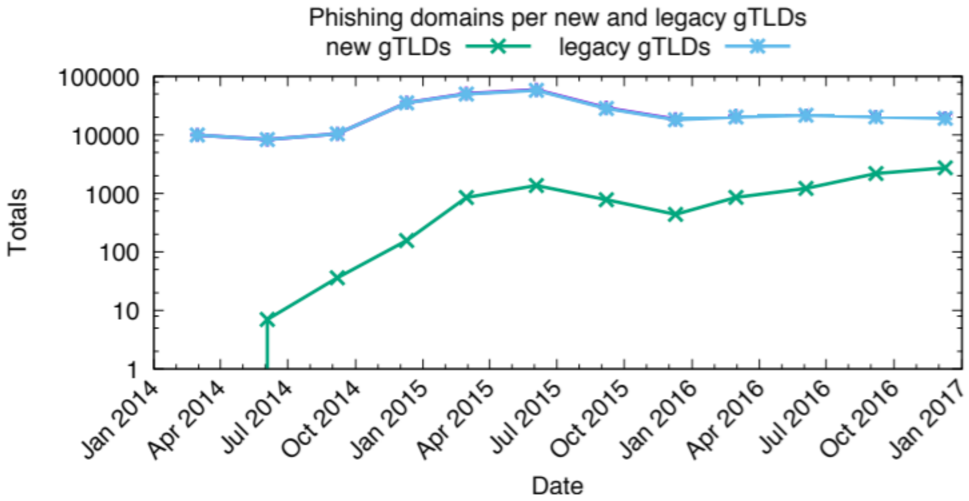
The new gTLDs have helped to enhance innovation, competition and consumer choice within the domain industry, but it has also added further opportunities for exploitation by criminals. An academic study on gTLD abuse found higher relative concentrations of compromised domains in legacy gTLDs, but miscreants frequently choose to maliciously register domain names using one of the new gTLDs.[3] Registrars of new gTLDs must therefore keep their registries clean of fraud before they become known as havens of criminal activity.

With the introduction of New gTLD registries combined with a growing cybercrime industry estimated to be worth more than $400 billion per year,[4] there has also been new requirements around "technical analysis" of their domains to detect and stop malicious use. Specification 11 (3) (b) of the ICANN New gTLD Registry Agreement[5] lays out the responsibilities to perform "technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets."

When such activity is discovered, the registry should enforce consequences for such activities that may include suspension of the domain name.

The registry must also maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks.

Those claiming to be harmed by a registry's lack of oversight have their concerns dealt with through the Public Interest Commitment Dispute Resolution Procedure (PICDRP) which can result in the termination of the Registry Agreement.[6]



Above Chart: Time series of counts of phishing domains in legacy gTLDs, and new gTLDs based on the Anti-Phishing Working Group feed (2014-2016) (Source: https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf)

How Domain Blacklists Threaten New gTLDs

Registrars of new gTLDs not only have a moral obligation to monitor their networks for various malicious activity, but gTLD domains associated with crime and fraud could be at higher risk of being put on blacklists.

Blacklists are typically created based on a scoring system that detects suspicious activity, and finding the associated URLs[7] (often IP addresses or domain names).

A particular new gTLD associated with a high level of fraudulent activity could make individual domains using it more likely to be put on a blacklist. Security researcher John Bambenek has observed a double-standard between legacy and new domains. He notes, "If, for instance, 2 million new .com malicious domains were registered, the registrar/TLD (or reseller) may be completely blameless for that event. Nonetheless, that event and pattern is useful data to drive someone to ask, 'why did the criminal ecosystem make that decision?'"[8] Enterprises can simply decide to block the entire new gTLD if the threats they face from those domains seem sufficiently harmful.

Having a new gTLD associated with crime and fraud makes it far less appealing to consumers who, for instance, don't want their emails to be caught in spam filters or their websites blocked on corporate networks.

New gTLDs have been gaining traction for phishing - some new gTLDs are cheap to register, and they can often register many common words and brand names, helping them appear to be more legitimate.

Web users have since become more aware that a name like nike.pizza may not be operated by Nike. Since there's also a perception risk when people see a new gTLD they consider suspicious in an email or web address, consumers could treat new gTLDs with some suspicion.

It comes down to this: Domain reputation equals domain value.

It's essential for registries to to protect their domain reputation among security researchers, and, importantly, among consumers.

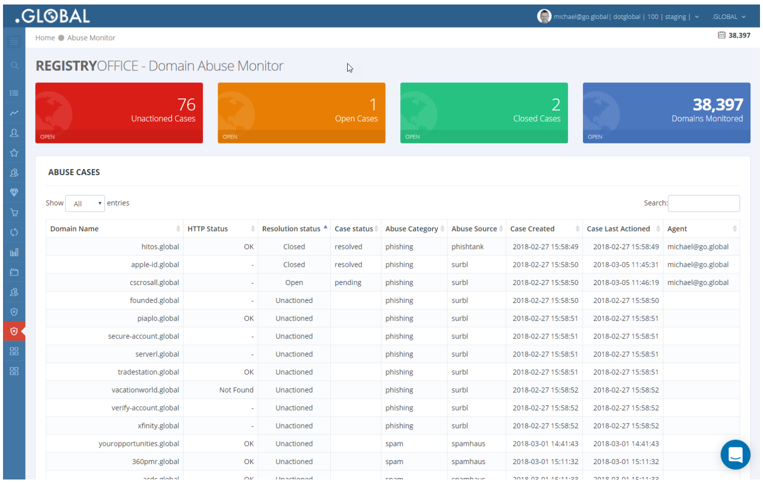
Proactive Abuse Monitoring

The RegistryOffice Abuse Monitor sets out to provide a service to improve anti-abuse efforts, reduce costs, and prevent cybercrime by combining cutting-edge monitoring with case management and ICANN-compliant reporting.

The Abuse Monitor uses domain information feeds from industry-leading researchers such as Spamhaus and SURBL to present users with actionable data.[10]

This also means registries are proactively finding malicious users before they're reported to ICANN and before they've done any damage. For instance, domains in the Add Grace Period will be labeled "already registered", indicating the domain that was just registered has already been reported, making it very likely the domain was registered in bad faith.

The Abuse Monitor shows suspicious domains as they occur, letting the registry team quickly take action.



REGISTRYOFFICE - Domain Abuse Monitor

76 Unactioned Cases — OPEN
1 Open Cases — OPEN
2 Closed Cases — OPEN
38,397 Domains Monitored — OPEN

ABUSE CASES

Show All entries   Search:

Domain Name	HTTP Status	Resolution status	Case status	Abuse Category	Abuse Source	Case Created	Case Last Actioned	Agent
hitos.global	OK	Closed	resolved	phishing	phishtank	2018-02-27 15:58:49	2018-02-27 15:58:49	michael@go.global
apple-id.global	-	Closed	resolved	phishing	surbl	2018-02-27 15:58:50	2018-03-05 11:45:31	michael@go.global
cscrosall.global	-	Open	pending	phishing	surbl	2018-02-27 15:58:50	2018-03-05 11:46:19	michael@go.global
founded.global	-	Unactioned		phishing	surbl	2018-02-27 15:58:50	2018-02-27 15:58:50	
piaplo.global	OK	Unactioned		phishing	surbl	2018-02-27 15:58:51	2018-02-27 15:58:51	
secure-account.global	-	Unactioned		phishing	surbl	2018-02-27 15:58:51	2018-02-27 15:58:51	
serverl.global	-	Unactioned		phishing	surbl	2018-02-27 15:58:51	2018-02-27 15:58:51	
tradestation.global	OK	Unactioned		phishing	surbl	2018-02-27 15:58:51	2018-02-27 15:58:51	
vacationworld.global	Not Found	Unactioned		phishing	surbl	2018-02-27 15:58:52	2018-02-27 15:58:52	
verify-account.global	-	Unactioned		phishing	surbl	2018-02-27 15:58:52	2018-02-27 15:58:52	
xfinity.global	-	Unactioned		phishing	surbl	2018-02-27 15:58:52	2018-02-27 15:58:52	
youropportunities.global	OK	Unactioned		spam	spamhaus	2018-03-01 14:41:43	2018-03-01 14:41:43	
360pmr.global	OK	Unactioned		spam	spamhaus	2018-03-01 15:11:32	2018-03-01 15:11:32	
acdc.global	OK	Unactioned		spam	spamhaus	2018-03-01 15:11:33	2018-03-01 15:11:33	

The RegistryOffice Abuse Monitor dashboard shows unactioned cases, open cases, closed cases, and the total number of domains monitored.

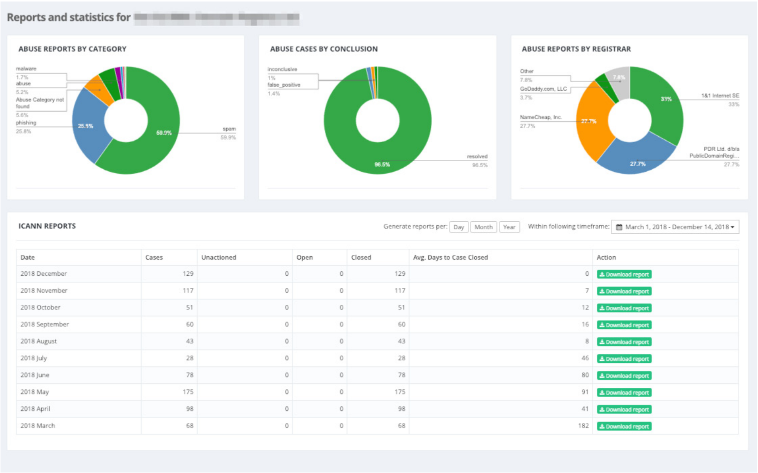
ICANN-Compliant Reporting

ICANN can request an abuse audit checking that the Registry Operator is in compliance with Spec 11(3)(b) of the Registry Agreement.

In accordance with this specification, RegistryOffice Abuse Monitor provides ICANN-compliant statistical reports on the number of security threats identified and the actions taken.

Abuse Monitor also provides a standard suite of reports to give registries further insight into abuse within their zone so they can, for instance, take preemptive action against criminals before they purchase a domain.

There are unlimited user accounts per client with secure two-factor authentication, and staff can monitor domains, user accounts . Plus the user reporting features in user management



Reports and statistics for [redacted]

ICANN REPORTS

Generate reports per: Day Month Year   Within following timeframe: March 1, 2018 - December 14, 2018

Date	Cases	Unactioned	Open	Closed	Avg. Days to Case Closed	Action
2018 December	129	0	0	129	0	Download report
2018 November	117	0	0	117	7	Download report
2018 October	51	0	0	51	12	Download report
2018 September	60	0	0	60	16	Download report
2018 August	43	0	0	43	8	Download report
2018 July	28	0	0	28	46	Download report
2018 June	78	0	0	78	80	Download report
2018 May	175	0	0	175	91	Download report
2018 April	98	0	0	98	41	Download report
2018 March	68	0	0	68	182	Download report

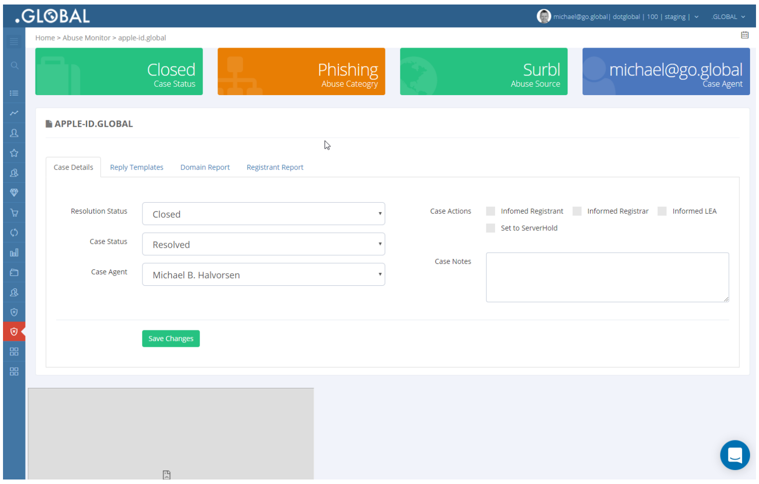
Example summary report

Abuse Case Management

RegistryOffice Abuse Monitor includes a Case Management System where you can professionally and efficiently manage your abuse cases. Abuse cases are automatically populated into a queue system, where they are categorized and accompanied with relevant information.

Abuse Monitor lets registries quickly send messages to the relevant party - whether it’s the registrant, a law enforcement agency, or the registrar who sold the domain. This system helps simplify and practically eliminate lengthy back-and-forth communication when domain name abuse stems from resellers.

Ultimately, it provides a structure and workflow for registries to manage abuse cases in line with ICANN’s guidelines.[11] As an option, expert security professionals at RegistryOffice can quickly suspend obvious violations and notify the relevant parties of the action. For more complex cases, the professional can launch an investigation and manage communications between parties on the registry operator’s behalf. This can free the registry operator to concentrate its scarce resources on other business matters and strategy.



Home > Abuse Monitor > apple-id.global

Closed
Case Status

Phishing
Abuse Cateogry

Surbl
Abuse Source

michael@go.global
Case Agent

APPLE-ID.GLOBAL

Resolution Status: Closed

Case Status: Resolved

Case Agent: Michael B. Halvorsen

Case Actions: □ Infomed Registrant □ Informed Registrar □ Informed LEA □ Set to ServerHold

Case Notes:

Example case report

User Management

Abuse Monitor has unlimited number of user accounts to be enabled by the Registry Operator. User management is handled by the client.

Two factor authentication (2FA) is included for safe and secure access to the system

Footnotes

[1] http://mkorczynski.com/asiaccs2018Korczynski.pdf

[2] TLDs are the letters found at the end of an Internet address, such as .com, .net, or .org. Any TLD that does not represent a country or a territory is known as a generic TLD, or gTLD.

[3] https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

[4] McAfee, Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies, June 2014, http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

[5] https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

[6] https://www.icann.org/resources/pages/picdrp-2014-01-09-en

[7] Universal Resource Identifiers or “URIs” are strings of characters that unambiguously identify a particular resource. For instance, the Uniform Resource Locator (URL) used to identify a web address is a common URI informally

[8] https://www.icann.org/en/system/files/files/bambenek-daar-validation-review-report-20jul18-en.pdf

[9] https://securedomain.org/Documents/SDF_Report1_June_2015.pdf

[10] Abuse Monitor do not validate the findings nor do a technical analysis.

[11] https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en

Conclusion

After looking at the data and studies on domain abuse, the RegistryOffice Abuse Monitor provides a system that we believe provides a proactive and efficient approach to abuse issues faced by all domain registries. We think that by developing the right tools, we can make it cheaper and easier than ever to build a better, safer Internet at the registry level.

We encourage you to provide your feedback and insights on the approach we've outlined in this whitepaper and keep an open discussion around what registries need to keep the Internet safe.

Contact us & Book a Demo

We invite you to provide direct feedback and get a personalized demo of RegistryOffice Abuse Monitor.

Please schedule a feedback session and demo with RegistryOffice Senior VP Marketing & Sales Pinky Brand:

pinky@registryoffice.global
+1.512.402.3095

REGISTRYOFFICE