Subject: [Ext] Compliance complaint: [redacted]: Privacy/Proxy complaint re: [redacted] closed
Date: Tuesday, June 19, 2018 at 12:20:55 PM Pacific Daylight Time
From: Derek Smythe
To: ICANN Complaints Office
CC: Fakebanks
Attachments: public[redacted].pdf, sensitive[redacted].pdf

Dear ICANN Complaints Office

Please find a complaint closed by ICANN Compliance (see below included email).

While this complaint was closed by ICANN compliance, the issues highlighted to ICANN Compliance where this proxy was in violation of the ICANN RAA 2013, still remains. This is part of an ongoing pattern on serious issues reported to ICANN Compliance over a period of time and being closed, seeing the same lack of compliance enforcement. This is also not the first time a proxy issue was addressed in a similar way, in turn leading to much consumer harm. It is of concern that a registrar can deliberately lie, and despite evidence to the contrary, this is blindly accepted and the complaint closed. In turn this leads to harm.

This complaint was lodged as the reseller managing this proxy has a renown reputation in terms of malicious domain registrations. Where the proxy is not used, the visible registration details do not pass muster and begs the question as to whether any registration details are in fact verified as required in the ICANN RAA 2013. In turn this leads to mass DNS abuse and has a knock on effect in terms of fraud and other malicious activities.

Most recently, during the ICANN GDPR discussions, "Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation", "#5.3.3. Accuracy of Registration Data" (https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf [icann.org]), the conclusion was reached that domain registrations are verified as per the ICANN RAA and as such "The GDPR therefore does not require the introduction of a new verification or validation requirements.". As such much reliance was placed on ICANN and Registrars to uphold the terms of RAA. In fact this conclusion was flawed. This complaint and an associated sibling complaint illustrates the basis for saying that the public discussion conclusion is flawed.

It is an established fact that this is not happening at this reseller and upstream ICANN Accredited Registrar. This also led to a previous ICANN Compliance complaint [redacted] in 2016 which was closed, similarly resolved, with the issue never really resolved. The long ongoing sibling complaint [redacted] against the upstream Registrar is in fact a continuation of [redacted] (and incidentally the same bad actors and registration issues are used to conclusively prove weak compliance). This bigger issue saw the [redacted] spoofed more than a hundred times with clear and patently fake registration details [redacted] - a small example). In the same linked issue, other banks such as [redacted], [redacted] etc are spoofed, international commerce is massively spoofed, lawyers are spoofed - or have their websites stolen and republished - all this in ongoing 419 fraud with the registrar and reseller consistently allowing such abuse. What is more disturbing, domains are suspended, leading interested anti-mitigation parties to believe the issue is resolved, to only find the domain has been un-suspended with the same fake registration details and abuse still ongoing (example: [redacted] spoofing [redacted] and where job applicants are asked to submit their personal details for jobs, [redacted] spoofing [redacted] in Romance and like scams). Issues such as this led to this registrar and downstream reseller being the second most abused registrar for long-lived domains abused in organized cyber fraud emanating from West Africa. To be clear, these are not merely content issues, the abuse starts off during registration when fake details are supplied. Some of these domains have no content, but we even find [redacted] spoofed in procurement scams [redacted]). How can this be anything but DNS abuse? These domains have no legitimate purpose. While this may harm business, the concern of Artists Against 419 is that the consumer with no real protection in vast areas of abuse, with no overlap with commercial interests, and where

consumers are hardly acknowledged as a third party in any agreements. These are the parties loosing their privacy and livelihoods in fraud, undermining their rights. We see cancer sufferers become victims to fraud. We see victims commit suicide.

While it's easy making malicious behavior out to be purely a law enforcement issue, this is a buck passing exercise. Law enforcement engages after the fact of harm done, and only if in their jurisdiction and they have the capacity to address such, also if the financial loss is above a certain amount typically. By then it is too late for victims and the harm is already done. Restitution, if ever, is minimal. It's a published fact that the [redacted] Action Fraud system is only flagging for investigation if a loss is above a certain amount. Additionally we see only 1% of cyber-crime is prosecuted. Yet even those statistics are flawed as a very low percentage of victims report such crimes due to social factors. The enforcement efforts elsewhere may be better or worse, but the fact remains the authorities are overwhelmed with cyber crime, with much of this crime starting off with domain registrations - DNS abuse. Consumer and business losses are at an all time high and reported on regularly. DNS abuse forms much of the underlying infrastructure needed by criminal elements.

As such, having tickets with valid concerns illustrating the consumer harm done, incidentally also violating trademarks with impunity, closed with poor ICANN Compliance enforcement, is of extreme concern. Registrars are hiding WHOIS details in an effort at meeting GDPR compliance. Yet while the GDPR is meant to protect consumer privacy, weak registrar compliance at certain registrars and more to the point, ICANN Compliance not addressing these issues, undermines and perverts any GDPR efforts by turning privacy for malicious registrants into a tool to massively deprive innocent consumers not only of privacy, but to also defraud them and undermine their rights. Even now we are finding rogue proxies hidden behind a GDPR cloud. Only by looking at historic WHOIS and registration dates can we determine these are reseller proxies. We may even have a situation where a proxy is hidden behind a proxy in at least one case - all in an unaccountable fashion.

Much of the information I can share may be made publicly available, but certain information or keywords are sensitive.

Looking specifically at this ticket:
I pointed out exactly where the reseller is violating the ICANN RAA 2013. The reseller simply made one single change to their website at [redacted] by placing a titled and link on this page:

> Please note the following rules from ICANN
> ICANN Registrant Rights and Responsibilities

The last line then links to the ICANN RAA 2013's section on this at https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#registrant [icann.org]

However, this same document, the ICANN RAA 2013, also contains the requirements for a proxy:
https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#privacy-proxy [icann.org]

As pointed out in the complaint to ICANN Compliance, the terms of Section 2 of the RAA 2013 is not met. This situation has not been remedied.

Nowhere on the website, do we find the word proxy. Nor the name of the upstream sponsoring Registrar. As such we can't presume on the Registrar's pages.

As also stated to ICANN Compliance, the upstream Registrar has a separate and distinctly different proxy which is not this proxy.

It simply defies logic that this ticket has been closed. It also makes all the community efforts, time and money spent of reaching the Proxy Specifications as recorded in the ICANN RAA 2013 wasted and a joke, trivially ignored.

In the meantime, the harm to both consumer and commerce is ongoing. Even now again, we see ongoing abuse and harm, with the relevant terms not being in place:
- [redacted] is being spoofed with these domains -

[redacted]
- A fake courier [redacted], with the claimed address actually being that of [redacted], used in consumer attacks undermining privacy and enabling fraud.
etc ...

How can ICANN deny any responsibility for the harm done with malicious domains if ICANN Compliance is not enforcing the ICANN RAA or the public engagement processes that led to it becoming policy?

I request this issue be investigated as a matter of urgency in the public interest and in a transparent fashion. This complaint will be published in a week's time on the Artists Against 419 website. In the meantime I request the reseller's website is scrutinized to validate the legitimacy of the statements made in the relevant complaint. I myself will also seek two credible parties validate what is/is not available on the reseller's website.

Any of the incidents I refer to and which more information is required on, can be shared. Some of it may be sensitive and will be shared as both a confidential and a public version with just certain details redacted. Both versions of the detailed ICANN complaint submitted is attached hereto and marked as such.

Thank you.

Kind regards,

Derek Smythe
Artists Against 419
[redacted]

-------- Forwarded Message --------
Subject:[redacted]]: Privacy/Proxy complaint re: [redacted] closed
Date: Fri, 25 May 2018 23:29:00 +0000
From: Compliance Tickets [redacted]
Reply-To [redacted]
To [redacted]

Dear Derek Smythe,

Thank you for subm tt ng a Pr vacy/Proxy comp a nt [redacted]

[redacted] Proxy

ICANN Compliance complaint [redacted]

Derek Smythe

Artists Against 419

2018-03-17

Contents

[redacted]

[redacted] is a hosting provider, a domain name reseller and also a proxy provider for some domains registered via them.

Their website is at [redacted]

Their general privacy policy is at [redacted]

Of importance on this page and right at the bottom, is their address details and specifically the email address:

[redacted]

[redacted] *as Domain Name Reseller*

[redacted] is currently a [redacted] reseller under the ICANN registrar channel. We find many domains also labelled as such, showing a formal recognition of this relationship by the registrar:

Domain Name: [redacted]
Registry Domain ID: [redacted]
Registrar WHOIS Server: [redacted]
Registrar URL: [redacted]
Updated Date: 2018-02-08T07:00:00Z
Creation Date: 2017-04-04T07:00:00Z
Registrar Registration Expiration Date: 2018-04-04T07:00:00Z
Registrar: [redacted]
Registrar IANA ID: [redacted]
Registrar Abuse Contact Email: [redacted]
Registrar Abuse Contact Phone: [redacted]
Reseller: [redacted]

The ICANN RAA 2013 defines a reseller as:

> *1.24 A "Reseller" is a person or entity that participates in Registrar's distribution channel for domain name registrations (a) pursuant to an agreement, arrangement or understanding with Registrar or (b) with Registrar's actual knowledge, provides some or all Registrar Services, including collecting registration data about Registered Name Holders, submitting that data to Registrar, or facilitating the entry of the registration agreement between the Registrar and the Registered Name Holder.*

Considering [redacted] own registry entries attests to this relationship, this reseller is an official reseller of theirs. Additionally [redacted] offers full domain registration and management services on their own website.

[redacted] *as a Proxy*

We find a history of domains registered to the email address [redacted]. This is the exact same email address also used for the [redacted] privacy policy shown at the start. Further we also find email address [redacted] used for the same purpose.

Note: *A registrar standards complaint was also filed via ICANN compliance a day prior to this complaint. A reply was received today:* [redacted]*. This forms part of the issues and other we see and why this complaint was lodged.*

[redacted] *is a primary source of malicious domains using* [redacted] *as sponsoring registrar. In an analysis, over 60% of domain names with Registrar* [redacted]*, showed* [redacted] *as the reseller. This is* [redacted] *TLD domain which for some reason does not show the reseller tag, so this figure is higher.* [redacted] *themselves are the second most abused registrar in terms of advance fee fraud domains, malicious domains deliberately registered for advance fee purposes. Typically these domains are registered with deliberately supplied inaccurate registration details. The registration details will not pass the most basic of scrutiny or checks.*

The registrar [redacted] *see themselves as "only a registrar" as per their website, yet do not enforce the mandated registrant requirements or check validity leading to gross abuse. They never respond to enquiries either via email or via their website form which they insist a complainant need to use. Their website form has no flow control system and supplies the complainant with no automatic receipt or like response code. This has been mentioned before in complaints to ICANN on this registrar. In the past the registrar has replied to ICANN they never received any such complaints. This situation continues, thereby making a mockery of the ICANN RAA requirements and any accountability metrics like retaining abuse reports. In turn this is leading to mass unlawful usage of their services to target consumers in fraud. We also see a migration of malicious actors, away from other registrars that are not fraud tolerant, to them.*

As such, to see [redacted] having a proxy, knowing the continuous invalid registrations we see where upstream registrar [redacted] does not check such details and knowing the primary source of these domains are [redacted], we shudder to think what hides behind this proxy.

But the reason for this complaint is that [redacted] has none of the proxy terms mentioned in the SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS of the ICANN RAA 2013 (which the sponsoring Registrar [redacted] has signed). Yet [redacted] should have abided by these terms.

In this case, as per definitions in Section 1, [redacted] is "P/P Provider" or "Service Provider" providing a "Proxy Service" to their "P/P Customer"s.

The associated responsibility of providing such a proxy service is also defined in Section 3.7.7.3 of the RAA 2013 and previous iterations, where the "P/P Customer" is the "licensee" and the "P/P Provider" or "Service Provider" is called the "Registered Name Holder".

Looking at Section 2 states:

> *2 Obligations of Registrar. For any Proxy Service or Privacy Service offered by the Registrar or its Affiliates, including any of Registrar's or its Affiliates' P/P services distributed through Resellers, and used in connection with Registered Names Sponsored by the Registrar, the Registrar and its Affiliates must require all P/P Providers to follow the requirements described in this Specification and to abide by the terms and procedures published pursuant to this Specification.*

As per the definitions and this description, this applies [redacted] and the below terms should be applicable.

> *2.1 Disclosure of Service Terms. P/P Provider shall publish the terms and conditions of its service (including pricing), on its website and/or Registrar's website.*
>
> *2.2 Abuse/Infringement Point of Contact. P/P Provider shall publish a point of contact for third parties wishing to report abuse or infringement of trademarks (or other rights).*
>
> *2.3 Disclosure of Identity of P/P Provider. P/P Provider shall publish its business contact information on its website and/or Registrar's website.*
>
> *2.4 Terms of service and description of procedures. The P/P Provider shall publish on its website and/or Registrar's website a copy of the P/P Provider service agreement and description of P/P Provider's procedures for handling the following:*
>
> *2.4.1 The process or facilities to report abuse of a domain name registration managed by the P/P Provider;*
>
> *2.4.2 The process or facilities to report infringement of trademarks or other rights of third parties;*
>
> *2.4.3 The circumstances under which the P/P Provider will relay communications from third parties to the P/P Customer;*
>
> *2.4.4 The circumstances under which the P/P Provider will terminate service to the P/P Customer;*
>
> *2.4.5 The circumstances under which the P/P Provider will reveal and/or publish in the Registration Data Service (Whois) or equivalent service the P/P Customer's identity and/or contact data; and*
>
> *2.4.6 A description of the support services offered by P/P Providers to P/P Customers, and how to access these services*

To be clear here and to avoid confusion, the sponsoring Registrar [redacted] has it's own affiliated proxy service [redacted] and webpage at [redacted] that has nothing to do with the services this compliance complaint relates to. The contact details are completely different and clearly identified as such in domain registrations.

No terms or costs linked to this proxy are found on [redacted] website. The only portion or web content relating to proxy services is at [redacted]. This is merely some marketing

material and not the required content we are looking for. **As such none of the mandated terms are available!**

Registrant Details Used

The domains using the [redacted] proxy uses the following registration details:

Registrant Name: [redacted]
Registrant Organization: [redacted]
Registrant Street: [redacted]
Registrant City: [redacted]
Registrant State/Province: [redacted]
Registrant Postal Code: [redacted]
Registrant Country: [redacted]
Registrant Phone: [redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: [redacted]

For some domains we see (apparently newer?):

Registrant Name: [redacted]
Registrant Organization: [redacted]
Registrant Street: [redacted]
Registrant City: [redacted]
Registrant State/Province: [redacted]
Registrant Postal Code: [redacted]
Registrant Country: [redacted]
Registrant Phone: [redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: [redacted]

Using an online domain email lookup tool such as [redacted], we see widespread usage of this proxy with over 2,300 domains having been recorded thus far:

[redacted]

[redacted]

Reverse Whois » EMAIL [redacted] { 2,362 domain names }

NUM	DOMAIN NAME	REGISTRAR	CREATED	UPDATED	EXPIRY
1	[redacted]		12 Mar 2018	13 Mar 2018	12 Mar 2019
2	[redacted]		12 Mar 2018	13 Mar 2018	12 Mar 2019
3	[redacted]		11 Mar 2018	12 Mar 2018	11 Mar 2019
4	[redacted]		13 Mar 2018	13 Mar 2018	13 Mar 2019
5	[redacted]		11 Mar 2018	12 Mar 2018	11 Mar 2019
6	[redacted]		28 Feb 2018	7 Mar 2018	28 Feb 2019

We also see a variation of this proxy registration using email address [redacted]. While this email is not solely used for proxy registrations, many are *(It also yields some extremely interesting and invalid domain registrations such as [redacted])*. Some of these registrations also appear to be "Privacy Service" registrations as per the RAA proxy definitions used before.

Once again, using [redacted], we see widespread usage of this proxy with over 600 such domains recorded: [redacted]

[redacted]

Reverse Whois » EMAIL [redacted] { 676 domain names }

NUM	DOMAIN NAME	REGISTRAR	CREATED	UPDATED	EXPIRY
1	[redacted]		20 Jun 2014	15 Feb 2018	20 Jun 2018
2	[redacted]		13 Feb 2015	13 Feb 2018	13 Feb 2018
3	[redacted]		23 Nov 2001	13 Feb 2018	23 Nov 2018
4	[redacted]		3 Jun 2014	9 Feb 2018	3 Jun 2018
5	[redacted]		31 Oct 2017	7 Feb 2018	31 Oct 2018
6	[redacted]		13 Jun 2015	5 Feb 2018	13 Jun 2018
7	[redacted]		23 Dec 2017	5 Feb 2018	23 Dec 2018
8	[redacted]		7 Jan 2001	5 Feb 2018	7 Jan 2023
9	[redacted]		2 Feb 2016	2 Feb 2018	2 Feb 2018

This email was first observed as far back as 2015 with domain [redacted] where it was spoofing [redacted]: [redacted]

Two registrant names are used, [redacted] and [redacted] with company name [redacted]. The company name is self-explanatory, it is [redacted].

The name [redacted] can be commonly found linked to QHoster, also in their network information and address as seen in the proxy registrations. Example [redacted]:

```
....
OrgName:      [redacted]
OrgId:        [redacted]
Address:      [redacted]
City:         [redacted]
StateProv:
PostalCode:   [redacted]
Country:      [redacted]
RegDate:      [redacted]
Updated:      [redacted]
Ref:          [redacted]

OrgAbuseHandle: [redacted]
OrgAbuseName:   [redacted]
OrgAbusePhone:  [redacted]
OrgAbuseEmail:  abuse@[redacted]
OrgAbuseRef:    [redacted]

OrgTechHandle: [redacted]
OrgTechName:   [redacted]
OrgTechPhone:  [redacted]
OrgTechEmail:  abuse@[redacted]
OrgTechRef:    [redacted]
....
```

The [redacted] address is actually the address of a company specializing the formation of offshore companies: [redacted]

Email address [redacted] is also found on [redacted] own web pages on their privacy page as shown earlier.

As such there can be no confusion or doubt that the details shown in the domain registrations are those of [redacted].

As such it is proven that reseller [redacted] is providing proxy services.

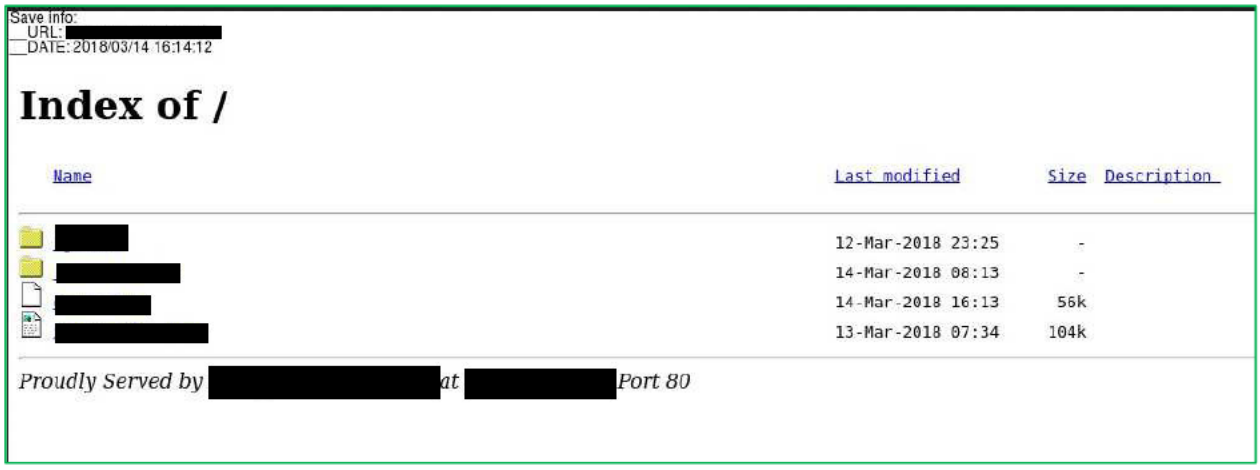
Continuous Malicious Domains

While preparing this document, a check on the link to [redacted] mentioned earlier, showed a new domain [redacted] has just been registered and using this proxy registration:

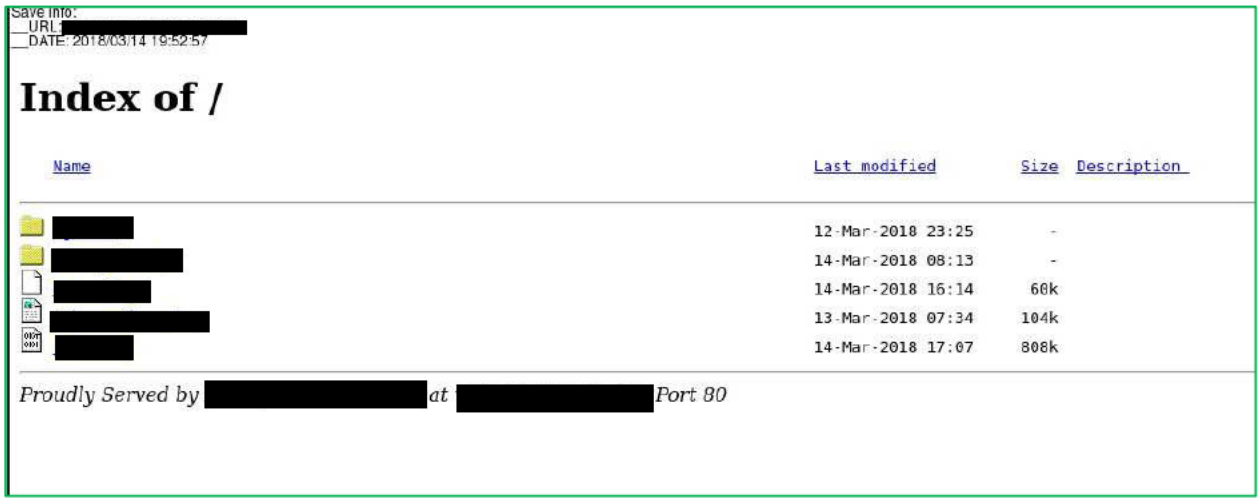
Domain Name: [redacted]
Registry Domain ID: [redacted]
Registrar WHOIS Server: [redacted]
Registrar URL: [redacted]
Updated Date: 2018-03-13T07:00:00Z
Creation Date: 2018-03-12T07:00:00Z
Registrar Registration Expiration Date: 2019-03-12T07:00:00Z
Registrar: [redacted]
Registrar IANA ID: [redacted]
Registrar Abuse Contact Email: [redacted]
Registrar Abuse Contact Phone: [redacted]
Reseller: [redacted]
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: [redacted]
Registrant Street: [redacted]
Registrant City: [redacted]
Registrant State/Province: [redacted]
Registrant Postal Code: [redacted]
Registrant Country: [redacted]
Registrant Phone: [redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: [redacted]
….
Name Server: [redacted]
Name Server: [redacted]
Name Server: [redacted]
Name Server: [redacted]
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
Last update of WHOIS database: 2018-03-14T07:00:00Z

A quick check on the usage shows a few things; we already have a [redacted] spoof (419 related, not phishing) at the associated website, and a PHP mailer form commonly used in 419 fraud. As such this domain and spoof was recorded: [redacted]

Since recording it, the responsible party has now also placed more malicious content on the associated website. An attack is in progress of being set while writing this report.



Versus three hours later:



An analysis of the new file, [redacted]

As such this website and associated domain is clearly under malicious control.

This is not surprising and par for the course, as we have been seeing many such malicious activities and have recorded them.

We also find UDRP's against this proxy where typically the respondent never replies; a $10 domain causing at least a $2,500 loss to the applicant to just defend his rights. It begs the question as to why the result of a violation of policies is wrapped in extensive and expensive processes for the victims which will have no lasting effect or relief (refer [redacted] which was included in the [redacted] standards complaint to ICANN).

[redacted] -

Respondent is [redacted] */* [redacted] *('Respondent'),* [redacted]

[redacted] - [redacted] &

[redacted]

Respondents are [redacted], *and* [redacted]

[redacted]

This is not surprising in our experience. Yet this does not acknowledge the consumer harm done in the process. The evidence of malicious abuse is extensive.

While we could try twisting this into "content issues", we need to consider other usage. Consider: [redacted] being abused to spoof [redacted] with no website, only in email:

From: [redacted]
Date: 2017-09-22 14:20 GMT+02:00
Subject: [redacted] *Procurement Contract Agreement*
To: [redacted]

Attn: [redacted]

Good day to you.

I wish to inform you that your mail with REF number was well received for the supply of the [redacted] *chemical from* [redacted]*. I have attached your contract agreement and I wish to inform you that you should study the agreement before signing the RED seal in the attached agreement.*

You are advised to print out the copies of the agreement and sign page one to four any where at the bottom of each copy and in page five you are to fill in your name, address and sign the red seal. In Page four, you are to fill in your bank details in CAP letters.

After signing the contract agreement, you are to scan and send all scanned copy from page one to page five back to me, only then your contract approval letter can be sent to you along with your contract certificate,your license buyer certificate, your Power of attorney (POA) and the [redacted] *Company details then you can contact the* [redacted] *company for purchase of the one liter sample of the* [redacted] *chemical for approval of the 10,000 liters of the* [redacted] *chemical.*

If you have any difficulties, you can always ask and I will be glad to make understanding to you.

[redacted]
Email: [redacted]

```
Delivered-To: (removed)@gmail.com
Received: by [redacted] with SMTP id [redacted];
Fri, 22 Sep 2017 05:20:24 -0700 (PDT)
```

[redacted]

Simple reality is there is no way to mitigate malicious domain abuse at hosting level.

Below is a list of some domain names found, the claimed business name, comments, a link to the database entry indicated as “DB” and a snapshot marked “Snap” - recorded at the time of entering into the Artists Against 419 database:

1	Spoofing: Active DB: Snap:
2	Content stolen from: Currently host suspended. DB: Snap:
3	Spoofing: Active and content hidden at

	DB: [redacted] Snap: [redacted]
4	[redacted] Spoofing: [redacted] Content hidden at [redacted] DB [redacted] Snap: [redacted]
5	[redacted] Content stolen from: [redacted] Content hidden in a sub-domain at [redacted] DB: [redacted] Snap: [redacted]
6	[redacted] Spoofing: [redacted] Content hidden at [redacted] DB: [redacted] Snap: [redacted]
7	[redacted] Spoofing: [redacted] Currently host suspended. DB: [redacted]
8	[redacted] Spoofing: [redacted] Content hidden in a sub-domain at [redacted] DB: [redacted]
9	[redacted] Spoofing: [redacted] Content in a sub-domain at [redacted] DB: [redacted] Snap: [redacted]
10	[redacted] Content stolen from: [redacted] Content hidden in a sub-domain at [redacted] DB: [redacted] Snap: [redacted] Also see: [redacted]
11	[redacted] Spoofing: [redacted] Status unknown. Content was hidden at [redacted] and found after victim report. Ref: [redacted] DB: [redacted]

	Snap: [redacted]
12	[redacted] Spoofing: [redacted] **ClientHold** Was hidden at [redacted] behind a fake 404 page DB: [redacted] Snap: [redacted]
13	[redacted] Spoofing: [redacted] SMTP (email) usage only, no web content. DB: [redacted] Email: [redacted]
14	[redacted] Fraud type illegal internationally: Classical Black Money Scam Status currently unknown DB: [redacted] Snap: [redacted]
15	[redacted] Fraud type illegal internationally: Classical Black Money Scam Active DB: [redacted] Snap: [redacted]
16	[redacted] Fraud type illegal internationally: Classical Black Money Scam Active DB: [redacted] Snap: [redacted]
17	[redacted] Fraud type illegal internationally: Classical Black Money Scam Status currently unknown DB: [redacted] Snap: [redacted]
18	[redacted] Fraud type: Bogus courier **Expired** DB: [redacted] Snap: [redacted] Note: Found after victim report in a loan scam and researching. Was exposing victim personal information onto the net!
19	[redacted] Fraud type: Loan fraud (linked to previous domain [redacted]) **Clienthold** DB: [redacted] Snap: [redacted]

20	[redacted] [redacted] Courier fraud ([redacted] syndicate) with content and logo stolen from [redacted] Re-hosts upon hoster suspension Active DB: [redacted] Snap: [redacted] This is a common template used many times (also in seen in the [redacted] issue). Also see: [redacted] ([redacted]) [redacted]
21	[redacted] [redacted] Procurement fraud [redacted] syndicate), company profile stolen from [redacted], director images stolen. Active DB: [redacted] Snap: [redacted] Profile: [redacted] Stolen directors: [redacted] [redacted]
22	[redacted] [redacted] Spoofing: [redacted] Active, hidden at [redacted] DB: [redacted] Snap: [redacted]

Any violation of trademarks and/or copyright issues is merely incidental. The consumer has no rights to such claims, yet they are the very reason why these websites exist. This needs to be made clear.

None of the above banks are phishing. They were verified to be 419 in nature as is explained at [redacted]

[redacted] *Knowledge of the Proxy Service*

The ICANN RAA: SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS portion on proxies, makes provision for savings by which the registrar will not be responsible for a proxy he is not aware of:

3 Exemptions. Registrar is under no obligation to comply with the requirements of this specification if it can be shown that:

3.1 Registered Name Holder employed the services of a P/P Provider that is not provided by Registrar, or any of its Affiliates;

3.2 Registered Name Holder licensed a Registered Name to another party (i.e., is acting as a Proxy Service) without Registrar's knowledge; or

3.3 Registered Name Holder has used P/P Provider contact data without subscribing to the service or accepting the P/P Provider terms and conditions.

3.1 & 3.3: We have already established that [redacted] is a [redacted] reseller. As per the RAA definitions; "*1.3 "Affiliate" means a person or entity that, directly or indirectly, through one or more intermediaries, Controls, is controlled by, or is under common control with, the person or entity specified."* As such reseller [redacted] is an affiliate of [redacted] and 3.1 does not apply. 3.3 would be impossible, and even if it were, reseller and registrar were both notified as these domains are sponsored by them. As such 3.3 does not apply either.

3.2: [redacted] has been made aware of this proxy on more than one occasion. Much of the evidence cannot be produced for the simple reason of [redacted] insisting on complainant use a website form which does not send any acknowledgement and thus allows for no proof or accountability in terms of ICANN compliance metrics. This issue has been raised before, mentioned earlier and will be addressed fully with evidence in the relevant compliance ticket lodged as mentioned earlier. But at least two such emails do exist where both [redacted] and [redacted] were copied on malicious domains using this proxy.

In the first the relevant bank being spoofed was also copied:

Subject: [redacted] *Spoof and proxy protection:* [redacted]
Date: Wed, 17 Jan 2018 00:27:11 +0200
From: Derek Smythe [redacted]
Reply-To: [redacted]
Organization: aa419.org
To: abuse@[redacted]*, abuse@*[redacted]
CC: [redacted]

Hello [redacted] */* [redacted]

Re: [redacted]

This domain has been registered with [redacted] *as a domain proxy provider and is spoofing the real* [redacted] *in the the USA.*

Content is found hidden here:
[redacted]

This domain is spoofing the legitimate at [redacted]

We also see this from the source code of
[redacted]
> <!-- Mirrored from [redacted] *by HTTrack Website Copier/3.x [XR&CO'2014], Thu, 12 May 2016 12:09:07 GMT -->*

The telephone number as found at
[redacted]
[redacted]

This is a [redacted] [redacted] *VOIP number, meaning the receiver of calls can be in any of over 200 counties.*

Verify at [redacted]

This is not on of the real [redacted] telephone numbers, which can be found here: [redacted]

The banking panel is not that of the real [redacted]. This is commonly seen in banks used for 419 fraud purposes.
Ref: [redacted]

The domain uses [redacted] as a proxy provider:
> Domain Name: [redacted]
> Registry Domain ID: [redacted]
> Registrar WHOIS Server: [redacted]
> Registrar URL: [redacted]
> Updated Date: 2018-01-11
> Creation Date: 2016-07-21
> Registrar Registration Expiration Date: 2018-07-21
> Registrar: [redacted]
> Registrar IANA ID: [redacted]
> Registrar Abuse Contact Email: [redacted]
> Registrar Abuse Contact Phone: [redacted]
> Reseller: [redacted]
> Status: clientTransferProhibited
> Registry Registrant ID:
> Registrant Name: [redacted]
> Registrant Organization: [redacted]
> Registrant Street: [redacted]
> Registrant City: [redacted]
> Registrant State/Province: [redacted]
> Registrant Postal Code: [redacted]
> Registrant Country: [redacted]
> Registrant Phone: [redacted]
> Registrant Phone Ext:
> Registrant Fax:
> Registrant Fax Ext:
> Registrant Email: [redacted]
> Registry Admin ID:
> Admin Name: [redacted]
> Admin Organization: [redacted]
> Admin Street: [redacted]
> Admin City: [redacted]
> Admin State/Province: [redacted]
> Admin Postal Code: [redacted]
> Admin Country: [redacted]
> Admin Phone: [redacted]
> Admin Phone Ext:
> Admin Fax:
> Admin Fax Ext:
> Admin Email: [redacted]
> Registry Tech ID:
> Tech Name: [redacted]
> Tech Organization: [redacted]

> Tech Street: [redacted]
> Tech City: [redacted]
> Tech State/Province: [redacted]
> Tech Postal Code: [redacted]
> Tech Country: [redacted]
> Tech Phone: [redacted]
> Tech Phone Ext:
> Tech Fax:
> Tech Fax Ext:
> Tech Email: [redacted]
> Name Server: [redacted]
> Name Server: [redacted]
> DNSSEC: unsigned
> URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
> Last update of WHOIS database: 2018-01-16 15:17:45

The hoster, [redacted]*, has been alerted numerous times to this abuse. They chose not to respond and/or address this obvious fraud.*

Since this domain is a malicious domain and is using [redacted] *as a domain proxy, this is as much a registrar issue as a hosting issue. Please suspend this domain for violations of the Registrant Agreement and your policies.*

Thank you.

Regards,

Derek Smythe
Artists Against 419
http://www.aa419.org

In this email, the details are also being asked as per ICANN RAA 3.7.7.3 while making both [redacted] and [redacted] aware that the mandated proxy details cannot be found.

Subject: ICANN RAA Mandated Proxy provisions?
Date: Sat, 28 Oct 2017 01:42:37 +0200
From: Derek Smythe [redacted]
Reply-To: [redacted]
Organization: aa419.org
To: info@[redacted]*, support@*[redacted]
CC: abuse@[redacted]

Hello [redacted]

cc [redacted] *- Sponsoring Registrar*

Re: [redacted] *proxy services*

We notice you are offering domain proxy protection services for domains using yourself as the proxy agent. Typically these details are shown:

> Registrant Organization: [redacted]
> Registrant Street: [redacted]
> Registrant City: [redacted]
> Registrant State/Province: [redacted]
> Registrant Postal Code: [redacted]
> Registrant Country: [redacted]
> Registrant Phone: [redacted]
> Registrant Phone Ext:
> Registrant Fax:
> Registrant Fax Ext:
> Registrant Email: [redacted]

This just became topical where we found a domain spoofing [redacted] *with these domain details, the domain being sourced from* [redacted] *with* [redacted] *as sponsoring Registrar.*

A closer look shows this to be a common occurrence, even spoofing banks, for example:

> Domain Name: [redacted]
> Registry Domain ID: [redacted]
> Registrar WHOIS Server: [redacted]
> Registrar URL: [redacted]
> Updated Date: 2017-10-26
> Creation Date: 2017-10-25
> Registrar Registration Expiration Date: 2018-10-25
> Registrar: [redacted]
> Registrar IANA ID: [redacted]
> Registrar Abuse Contact Email: [redacted]
> Registrar Abuse Contact Phone: [redacted]
> Reseller: [redacted]
> Status: clientTransferProhibited
> Registry Registrant ID:
> Registrant Name: [redacted]
> Registrant Organization: [redacted]
> Registrant Street: [redacted]
> Registrant City: [redacted]
> Registrant State/Province: [redacted]
> Registrant Postal Code [redacted]
> Registrant Country: [redacted]
> Registrant Phone: [redacted]
> Registrant Phone Ext:
> Registrant Fax:
> Registrant Fax Ext:
> Registrant Email: [redacted]

We find a [redacted] *spoof here:*
[redacted]

What is even more disconcerting, is that we uncover an extremely well known login panel for bank spoofs massively abused by a certain party;
[redacted]

Since [redacted] is an official [redacted] reseller, the ICANN RAA 2013 SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS applies. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#privacy-proxy

This section makes it clear that this also applies to your as an official [redacted] reseller.

We closely checked your website for these terms. They could not be found. The closest we could find was this, which does not meet these terms:
[redacted]

As per sect 3 of this part:
> 3 Exemptions. Registrar is under no obligation to comply with the requirements of this specification if it can be shown that:
>
> 3.1 Registered Name Holder employed the services of a P/P Provider that is not provided by Registrar, or any of its Affiliates;
>
> 3.2 Registered Name Holder licensed a Registered Name to another party (i.e., is acting as a Proxy Service) without Registrar's knowledge; or
>
> 3.3 Registered Name Holder has used P/P Provider contact data without subscribing to the service or accepting the P/P Provider terms and conditions.

As per the ICANN RAA 2013 definitions, the Registered Name Holder is [redacted]

As per 3.1, [redacted] is an affilate.
As per 3.2, [redacted] is being copied on this email.
As per 3.3, [redacted] is clearly offering this service as 1309 recorded domain names indicates.

As per the ICANN RAA definitions:
> 1.13 "Illegal Activity" means conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law.

Spoofing [redacted], Banks and like to defraud consumers by registering domain names to host email services and furthering these malicious impersonation activities, meets this definition.

Also note that as per SECT 3.7.7.3 of the ICANN RAA:
> Any Registered Name Holder that intends to license use of a domain
> name to a third party is nonetheless the Registered Name Holder of
> record and is responsible for providing its own full contact
> information and for providing and updating accurate technical and
> administrative contact information adequate to facilitate timely
> resolution of any problems that arise in connection with the
> Registered Name. A Registered Name Holder licensing use of a
> Registered Name according to this provision shall accept liability for
> harm caused by wrongful use of the Registered Name, unless it

> discloses the current contact information provided by the licensee and
> the identity of the licensee within seven (7) days to a party
> providing the Registered Name Holder reasonable evidence of actionable
> harm.

This begs the question: Will you disclose the licensee information?

According to our database statistics, over 60% of all malicious 419-type domains sponsored via [redacted] *we recorded, originated at* [redacted]

We are noticing a trend by malicious parties that have their domains suspended at other registrars moving to the likes of [redacted] *and* [redacted]*. This creates a bullet-proof environment for malicious domains. To be clear, the malicious activity starts when the domain name is chosen to impersonate a party or match the fraud. This is not some innocent domain where the attached hosting services are compromised and abused.*

As such we wish to know where we can find these mandated the ICANN RAA 2013 SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS terms on the [redacted] *website?*

Also, please be as kind as to reveal the licensee details for [redacted] *as what has been illustrated to you at URL* [redacted] *is actionable harm.*

Thank you.

Derek Smythe
Artists Against 419
http://www.aa419.org

Return-Path: <pm_bounces@[redacted]
Delivered-To: [redacted]
Received: from [redacted]

[redacted]

Derek Smythe,

Thank you for contacting our support team. A support ticket has now been opened for your request. You will be notified when a response is made by email. The details of your ticket are shown below.

Subject: ICANN RAA Mandated Proxy provisions?
Priority: Medium
Status: Open

You can view the ticket at any time at
[redacted]

Regards,

[redacted]

Return-Path: [redacted]
Delivered-To: [redacted]
Received: from [redacted]

[redacted]

[redacted] *has been disabled.*

Let us know the rest active abusing domains so we can check them 1 by 1.

Ticket ID: [redacted]
Subject: ICANN RAA Mandated Proxy provisions?
Status: Answered
Ticket URL: [redacted]

Regards,

[redacted]

Subject: Re: [Ticket ID: [redacted] *ICANN RAA Mandated Proxy provisions?*
Date: Sun, 29 Oct 2017 23:30:55 +0200
From: Derek Smythe [redacted]
Reply-To: [redacted]
Organization: aa419.org
To: [redacted]
CC: [redacted]

Hello [redacted]
cc: [redacted] *Abuse*

Obviously you did not reply to the question being asked. You simply terminated one domain spoofing a bank that was given as an example of the actionable harm, yet not addressing the real underlying issue at hand causing harm and violating ICANN policies as per the RAA.

It is for this reason we will be lodging a compliance complaint.

Further we have no choice but to regard [redacted] *proxy as a Rogue Proxy, listing it as such:*

[redacted]

Derek Smythe
Artists Against 419
http://www.aa419.org

As such, despite the email subject being "*ICANN RAA Mandated Proxy provisions*", this question is never answered. Nor are the details ever supplied. Additionally [redacted] was cc'ed on these communications.

---ooo000ooo---