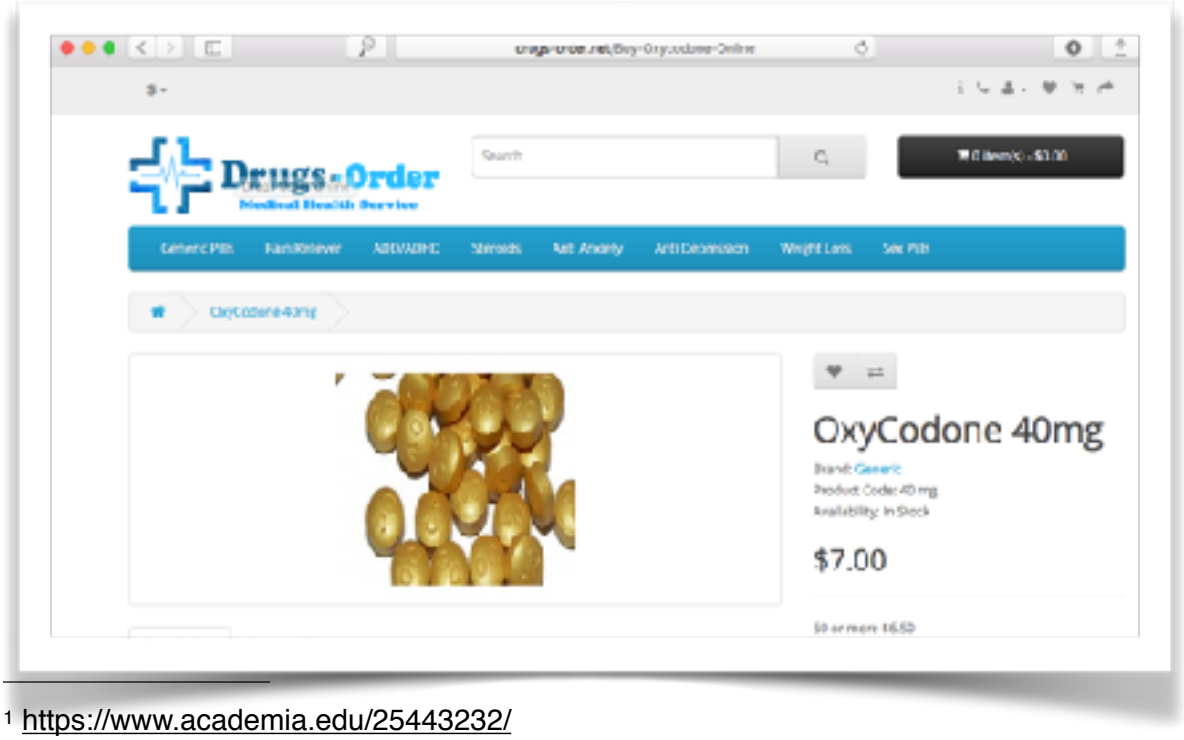
To: ALAC, At-Large Leadership & Greater Internet Community
From: Garth Bruen, KnujOn LLC/ALAC NARALO
Subject: Circumvention of ICANN Process by Criminal Domains
Date: 13 March 2017

Brief

This memo concerns a domain with false WHOIS (DRUGS-ORDER.NET) reported through the ICANN WHOIS Data Reporting System (WDPRS). The domain is used as an illegal pharmacy which does not display a pharmacy license and sells controlled substances (opioids) without a prescription. Opioids are synthetic versions of heroin that are much more potent. Domains with uncorrected WHOIS are supposed to be suspended/deleted within 45 days. The information presented here will demonstrate: 1) a loophole exists in the ICANN WDPRS process which is easily exploited and 2) the WDPRS ticketing system does not adequately handle conditional changes during the complaint period. The domain in question has been registered at four (4) different registrars using (3) different sets of invalid WHOIS data over an 8-month period.

Facts

In June 2016 the domain DRUGS-ORDER.NET was featured as a case study within an extensive report concerned with online opioids[1]. The domain is continues to be used as an illegal pharmacy selling controlled substances without a prescription without presenting a pharmacy license. A content sample is provided below.



[1] https://www.academia.edu/25443232/Online_Opioids_Report_Concerning_Ease_of_Access_Highlighting_Potential_Solutions_Using_Existing_Laws_and_Technology

The focus of the information in this memo is on the handling of WDPRS tickets, but additional interactions are provided for context. Internet users who find gTLD domains with inaccurate WHOIS records may file a WDPRS complaint with ICANN.[2] The ICANN WDRPS process can take up to 45 days and sometimes slightly longer depending on the circumstances. If the registrant does not comply with the request to update the WHOIS data, the domain should be suspended or canceled.[3] If the registrar fails to comply with the process the registrar may be in breach of their contract with ICANN.[4] The details cover a 214 day period involving a series of complaints and interactions and are grouped chronologically for clarity.

AUGUST 2016 (First Complaint(s))

Following the publishing of the Online Opioids[5] report, a review of the details of each domain in the report was commenced and various complaints were filed about all the featured domains. The WHOIS record for the domain DRUGS-ORDER.NET indicated that it was registered in the United Arab Emirates but the address details were either inconsistent or non-existent in the UAE. A WDPRS was filed with ICANN on 4 August 2016 and given the ticket number LZU-874-15728. On 5 August complaints were also sent sent directly to the registrar (Moniker), the registry (Verisign) and a DNS proxy service (CloudFlare).

On 9 August Moniker reported they were investigating the issue. Following that note, the domain appeared to be briefly suspended. However, on 16 August the domain was still active and this status was reported back to Moniker. Moniker responded on 17 August that the domain only had a “parking” page. However this was a scripting trick that denied displaying the opioids shop to certain IP addresses (apparently including Moniker’s IPs). This was explained in detail to tMoniker which stated the case had been reopened in response.

Moniker reported on 19 August that the domain had been transferred and was no longer their problem. Since the domain had been transferred to a new registrar (Shinjiru[6]) a fresh WDPRS complaint (XWD-417-62113) was filed with ICANN which was immediately rejected by ICANN because they already had an on open complaint about the domain.

Since the contract requires the registrar to respond to WDPRS reports within 15 days ICANN compliance was asked on 22 August to confirm that the registrar had acknowledged the complaint. ICANN Compliance did not respond.

---

[2] https://forms.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form

[3] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

[4] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

[5] https://www.academia.edu/25443232/Online_Opioids_Report_Concerning_Ease_of_Access_Highlighting_Potential_Solutions_Using_Existing_Laws_and_Technology

[6] https://www.internic.net/registrars/registrar-1741.html

On 25 August Verisign acknowledged the original report but stated they would take no action and the issue should be referred to the registrar. CloudFare removed the DNS proxy service but the owners of DRUGS-ORDER.NET immediately found a new DNS proxy.

SEPTEMBER 2016 (DRUGS-ORDER.NET at second registrar)

On 7 September ICANN compliance closed the original complaint (LZU-874-15728) because the *"complaint is about something not consistent with the current Whois data",* likely referring to the fact that the domain was at new registrar with different data. The WHOIS data for DRUGS-ORDER.NET had been changed from its original invalid data to new invalid data. The record now claimed a non-specific address in Pakistan at an open market. The space referred to in the record is a space that does not have permanent structures.

A new WDPRS complaint (ZBD-527-74371) was filed with ICANN on 27 September which was immediately rejected by ICANN because *"A complaint regarding the same domain name or top-level domain is currently being processed"*, however the previous complaint (LZU-874-15728) was closed according to ICANN's September 7 statement and the supplemental complaint (XWD-417-62113) was also closed. This may refer to a fourth complaint (XPS-621-83556) for which there is no additional information because ICANN did not issue a confirmation of this complaint. The problem here is that more recent complaints would be accurate to the current data and should be considered, outstanding complaints would not be consistent.

Compliance reported on 30 September that "*it was determined that tickets LZU-874-15728, XWD-417-62113, XPS-621-83556, and ZBD-527-74371 were improperly closed*" and *"ICANN will follow up with the registrar per process and provide you an update with its findings."* However, there was no update after nearly one month.

OCTOBER 2016 (DRUGS-ORDER.NET at Third registrar)

Because there had been no direct communication from ICANN, the domain was still online, and the WHOIS was again invalid a new WDPRS complaint (EIY-801-13281) was submitted on 27 October. Additionally the domain had been transferred to a third registrar (GuangDong[7]). The domain record professed a new non-existent address in the United States. The complaint was immediately rejected by ICANN because *"A complaint regarding the same domain name or top-level domain is currently being processed".* It is completely unclear if the still-open referenced complaint was one of the ones re-opened by ICANN on 30 September.

NOVEMBER 2016 - FEBRUARY 2017 (More process, lack of communication)

Due to the back-and-forth with no observable action an update was requested of ICANN on 10 November. On 14 November ICANN responded that the issue was still being investigated. By 19 November ICANN reported that "I*CANN determined that tickets EIY-801-13281, XBS-245-51640 and FXG-731-63835 were improperly closed. For your reference, ticket FXG-731-63835 has been re-opened and ICANN will follow up with the new registrar per*

[7] https://www.internic.net/registrars/registrar-1619.html

process and provide you an update with its findings. Please note, ICANN is continuing to process ticket LZU-874-15728"

There was no apparent action or further communication from ICANN during this period. At different points in time the domain appears to be offline for a time but would eventually resurface as explained in the next section.

MARCH 2017 (Closure and re-launch of DRUGS-ORDER.NET at fourth registrar)

On 6 March ICANN compliance reported that it closed all the complaints related to DRUGS-ORDER.NET because "*The registrar demonstrated that it took reasonable steps to investigate the Whois inaccuracy claim by suspending, deleting, cancelling or otherwise deactivating the domain name."* However, it is also noted that *"Further, the domain has been transferred to a different registrar."* The domain is currently active selling opioids registered at its fourth registrar (GRANSY[8]) using a proxy WHOIS server.

Registrar-Specific Timeline

For simplicity the registration history for DRUGS-ORDER.NET is outlined below

Moniker: 15 November 2016 - 19 August 2016, registered with false Arab Emirates address

Shinjiru: 19 August 2016 - 27 October 2016, registered with false Pakistani address

Guangdong: 27 October 2016 - 27 February 2017, registered with false U.S. address

Gransy: 27 February 2017 - Present, proxied registration WHOIS

[8] https://www.internic.net/registrars/registrar-1505.html

Analysis

* Domains may escape suspension through transfer to another registrar

* Domain transfers can apparently occur without correcting false WHOIS data first

* Transferred domains with known false data may be re-registered with new false WHOIS data

* There is no apparent limit to the number of times a domain may be transferred nor a limit to the number of times false WHOIS data may be used

* WDPRS is clearly designed to exclude duplicate complaints, however the only duplication in the complaints was the domain name, the discrete complaint data changed

* The WDPRS ticketing system does not appear to consider the changing status of a domain during the open complaint period

* The WDPRS ticketing system does not appear to accept new data, in this case a valid ticket concerning new invalid record data

* The rate of a registrant's ability to change the WHOIS data and/or transfer a domain is not concurrent with the ability of the WDRPS to manage complaints about the data

* ICANN staff did recognize that tickets were closed improperly but this is assumed to be a manual process

* While ICANN staff acknowledges improper closing of complaints, exactly what was improper is not relayed back to the submitter

* Complaint submitters have very little insight into the overall process

* ICANN Compliance appears to equate ticket closure with issue resolution

* The WDRPS cycle from complaint to closure is supposed to be 45 days but the total timeline of the final ticket was 116 days

* The number of days between the re-opening of the tickets and final closure was 107 days

* ICANN Compliance did not appear to adhere to its own time policy in the enforcement/ investigation of the final complaint

* The ICANN Compliance process does not seem to consider case-related factors, specifically intentional or serial WHOIS fraud for the purposes of facilitating criminal activity

Conclusions

The original purpose of the WDPRS is to either correct or remove domains with false WHOIS records. Maintaining an accurate record is a condition of the domain registrant agreement. If a WHOIS inaccuracy is not cured the registrar is obligated to suspend/delete the domain within 45 days. This system has been defeated.

The ICANN WDPRS system fails to understand criminal intent. The ways in which the DNS is used by criminals for their own purposes is not considered. Conversely, criminals have a detailed understanding of the DNS and its policy to the extent that it is easily manipulated.

By and large, the involved registrars apparently complied with the contract yet the domain escaped deletion. This suggests a problem with the ICANN process and not necessarily with registrar response. Contractual sanctions are are aimed at registrars, but if the registrars comply yet violating domains endure we clearly have more complex problems. Even if the registrars follow the process there is no real end.

There are two base problems: 1) the contract(RAA) and 2) the process(WDPRS). The process is an extension of the contract and has its own specific problems, but the contract needs to be fixed first. The contractual problem is that “willful” abuse of the domain system has no clear definition or limit. Willfully entering false data and then replacing false WHOIS records with other false records is not compliance. Allowing a domain with a false record to be transferred with a new false record to a new registrar is not compliance. Allowing a false record to be replaced with a proxy record is not an reasonable response. A proxy registration begs trust. A domain with criminal intent and three prior false records should not be trusted. We must ask whether or not it is reasonable that a domain with three proven false address in three different countries can be allowed to transfer a fourth time and then use a proxy registration.

Any registrant engaged illicit commerce may create a domain for an illegal purpose and simply transfer it to one of the other nearly 3000 accredited registrars. There is no limit to the number of times, even at the current rate of transfers related to DRUGS-ORDER.NET it would take hundreds of years to run out potential transfers.

In terms of process, WDPRS complaints do not have a contextual element and the process cannot handle complex data. WDPRS is inflexible. This problem can be addressed without a contract change. They system needs revision with an understanding of how the system itself is manipulated with criminal intent by detecting status changes and considering the full registration history of the domain.

Additional Issues

Beyond the WDPRS issues there are some more specifics in dealing with the various providers: 1) Concerning the original complaint the domain was not suspended by Moniker in the sense intended by the contract, rather a false parking page was placed making it appear suspended, a true suspension would have involved a registry-lock status removing it from the DNS; 2) The registration/transfer of a domain with bad WHOIS data would appear to violate the WHOIS Accuracy Program Specification[9].

---

[9] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy