

KnújOn (nûj-ôn)



Policy Failure Enables Mass Malware: Part II (SECURETABS.NET, OnlineNIC and ICANN)

A Report by KnújOn.com, LLC

September 29, 2010

Abstract: This report details a series of compromised websites that redirect to illicit online pharmacies. Complaints filed about one domain in particular (SECURETABS.NET) were ignored and then rejected by ICANN.

Brief

The following memo details the history of a malware redirect intrusion on several university websites which load the illicit pharmacy SECURETABS.NET. KnujOn.com filed a WHOIS inaccuracy complaint against this site first on July 18, 2010 and then again on September 16, 2010 because the complaint went unaddressed, the WHOIS record uncorrected, and the domain undeleted. Additionally, KnujOn filed a REGISTRAR complaint following ICANN's instructions because OnLineNIC has violated RAA 3.7.8 and 3.7.5.3, but our complaint was summarily REJECTED by ICANN September 20, 2010. We are requesting a full explanation of (A) why our Registrar complaint was rejected, (B) what steps OnLineNIC took to investigate and correct the reported inaccuracy as specified in the April 2003 "Registrar Advisory Concerning the 15-day Period in Whois Accuracy Requirements" and the May 2002 "Registrar Advisory Concerning Whois Data Accuracy", and (C) why the domain SECURETABS.NET has not yet been suspended while multiple intrusions and malware force Internet browsers to this URL after the failure to correct the WHOIS record beyond the 45 day complaint cycle.

Timeline

July 18, 2010 – KnujOn.com discovers malicious redirection on a university website and attempt to contact the owner of the unlicensed pharmacy. Finding that the contact details are false, KnujOn files an ICANN WDPRS inaccuracy complaint against SECURETABS.NET

August 2, 2010 – 15 Days pass without the record being corrected

September 2, 2010 – 45 Day WDPRS complaint cycle ends without record being corrected or the domain being deleted

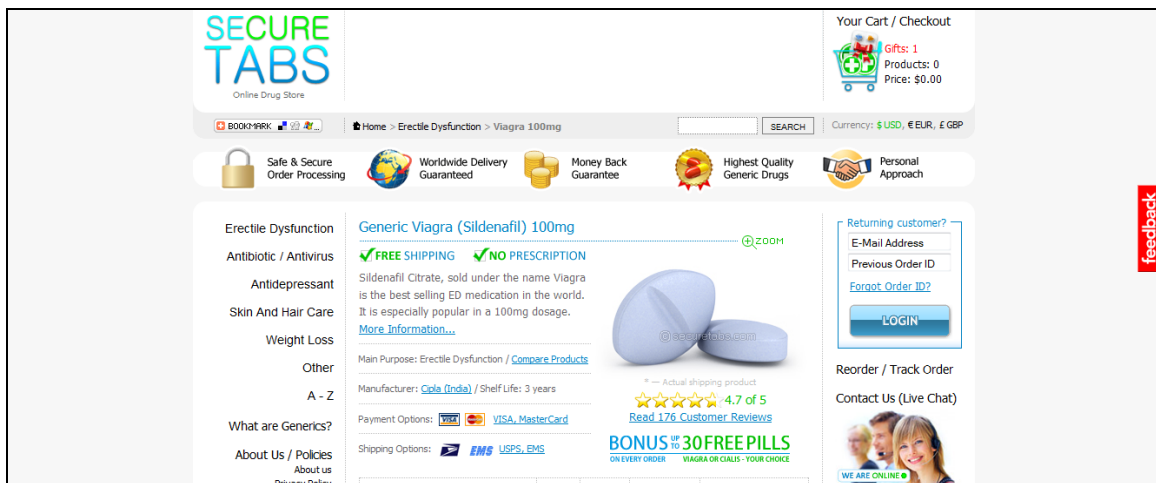
September 16, 2010 – KnujOn.com re-files SECURETABS.NET inaccuracy complaint and files a Registrar complaint because OnlineNIC has violated RAA

September 20, 2010 – ICANN Rejects KnujOn's Registrar complaint claiming we filled out the wrong form.

Initial Issue: Malware Redirection to SECURETABS.NET

The following URLs are malicious samples that redirected to SECURETABS.NET. They may have been corrected as we have been notifying the victims.

bands.illinois.edu/content/university-band
bands.illinois.edu/content/general-audition-information
bands.illinois.edu/content/summer-band
bands.illinois.edu/content/basketball-bands-audition-information
bands.illinois.edu/content/wind-orchestra
bands.illinois.edu/content/harding-symphonic-band-fall-2010-syllabus
ankn.uaf.edu/IEW/africa.html
www.bands.uiuc.edu/content/2009-winners
bts.earlham.edu/admissions/student_life
ankn.uaf.edu/IKS/rights.html
it.udel.edu/ats/node/540
alumni.tfc.edu/news/memorials/gregorydowell
lfccworkforce.com/certifications-licensures/what-is-certification-/



The screenshot displays the SECURETABS Online Drug Store website. The header includes the logo, navigation menu, and a shopping cart showing 1 gift and 0 products for \$0.00. The main content area features a product listing for Generic Viagra (Sildenafil) 100mg, highlighting benefits like free shipping and no prescription. The page also includes a sidebar with navigation links, a login section for returning customers, and a feedback button on the right side.

The code actually loads a site called pharm-tracker[DOT]com which in turn sequentially loads one of four illicit pharmacy domains: generictab[DOT]com, securetabs[DOT]net, cheapdrugsnorx[DOT]com, bestgenericpharma[DOT]com.

Once this malicious activity was found in July we attempted to notify all parties including the registrant of SECURETABS.NET but our email to the Registrant was rejected. An email to OnlineNIC abuse also went unanswered.

<sergeymironov@ymail.com>:
74.6.136.65 failed after I sent the message.
Remote host said: 554 delivery error: dd Sorry your message to sergeymironov@ymail.com cannot be delivered. This account has been disabled or discontinued [#102]. - mta1065.mail.sk1.yahoo.com

The rest of the WHOIS information is false as well, the “address” given is:

Zvenigorodkaya st. 26-17, Moscow Moscow AF 125482

The postal code “125482” does not match anything relevant in Russia or anywhere else. The country code given as “AF” is for Afghanistan which does not match the “Moscow Moscow” portion of the record. The street “Zvenigorodkaya St.” does not exist, the only closest approximation would be *Zvenigorodskaya Ulitsa* which does not have a 26.

Accordingly, we filed a WDPRS complaint on July 18, 2010. On August 2, 2010, 15 Days pass without the record being corrected. September 2, 2010 – 45 Day WDPRS complaint cycle ends without record being corrected or the domain being deleted. On September 16, 2010 – KnjOn.com re-files SECURETABS.NET inaccuracy complaint and files a Registrar complaint because OnlineNIC has violated RAA. On Mon September 20, 2010 ICANN rejected our Registrar complaint.

ICANN Accepts then Rejects Registrar Complaint against OnlineNIC

Following the instructions on the InterNIC website we selected the link: “Have a Problem with a Registrar?”



InterNIC

Home [Registrars](#) [Whois](#) [FAQ](#)

InterNIC—Public Information Regarding Internet Domain Name Registration Services

Do you have a complaint or dispute?

Your Registrar or Domain Name:

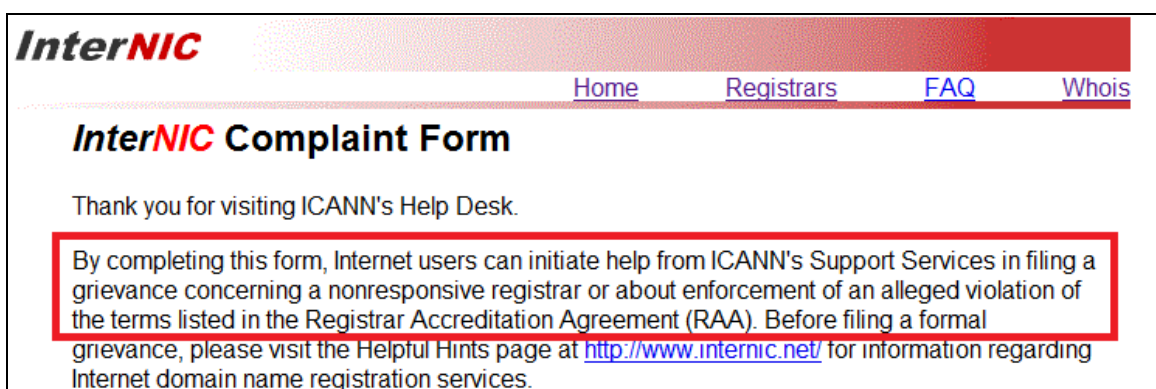
- [Domain Name Transfer Dispute](#)
- [Unsolicited Renewal or Transfer Solicitation](#)
- [Your Registrar is Not on the Accredited List](#)
- [Unauthorized Transfer of Your Domain Name](#)
- [Trademark Infringement](#)
- [Registrar Services Dispute](#)

Information about Registrars

- [Search Accredited Registrar Directory](#)
 - [Alphabetical List](#)
 - [List by Location](#)
 - [List by Language Supported](#)
- [Have a Problem with a Registrar?](#)
 - [Complaint Form](#)
 - [Helpful Hints](#)

Further instructions:

“Internet users can initiate help from ICANN's Support Services in filing a grievance concerning a nonresponsive registrar or about enforcement of an alleged violation of the terms listed in the Registrar Accreditation Agreement (RAA)”



InterNIC

Home [Registrars](#) [FAQ](#) [Whois](#)

InterNIC Complaint Form

Thank you for visiting ICANN's Help Desk.

By completing this form, Internet users can initiate help from ICANN's Support Services in filing a grievance concerning a nonresponsive registrar or about enforcement of an alleged violation of the terms listed in the Registrar Accreditation Agreement (RAA). Before filing a formal grievance, please visit the Helpful Hints page at <http://www.internic.net/> for information regarding Internet domain name registration services.

One of the selections built into the form is: “Whois - Inaccurate Whois Hidden Whois”

- Whois - Inaccurate Whois Hidden Whois

In response we received this email:

“We appreciate you taking the time to complete a InterNic Complaint Report. Your complaint, however, references inaccurate Whois data, which is handled through a separate complaint system. These complaints are not handled through the InterNic Complaint System and do not get referred.”

We are completely confused by this response and lack of action.

“Although ICANN's limited technical mission does not include resolving individual customer-service complaints, ICANN does collect and monitor such complaints to discern trends. If you would like to submit a complaint about a registrar for ICANN's records, please use the Registrar Problem Report Form located at the InterNIC website. As a courtesy, ICANN will forward your complaint to the registrar for review and further handling”

Also: **“These complaints are not handled through the InterNic Complaint System and do not get referred.”**

Contradicts information on the Compliance Website: **“ICANN will forward your complaint to the registrar for review and further handling”**

This is a serious organizational issue that has allowed an illicit, malware/hacking-promoted, false WHOIS domain to go undetected. This process is the definition of a bureaucratic “Runaround.”

Problems with OnlineNIC

OnlineNIC claims to be in the United States but it has been known for some time that their professed address of ---- is fake. In the article "Visiting OnlineNIC's Non-Office" by Andrew Naylor (<http://dotsnews.com/domain-name-news/184>) it is shown to be an empty lot. This false address has been used in OnlineNIC's own domain registration (onlinenic.com) for years. The email contact address for Onlinenic.com is also false:

```
<kitty@onlinenic.com>:  
218.104.139.233 does not like recipient.  
Remote host said: 550 RC:LD The email account that you tried to reach does no  
exists.  
Giving up on 218.104.139.233.
```

We have filed numerous complaints about OnlineNIC's false address with ICANN to no avail.

OnlineNIC, Inc. (onlinenic.com) is allegedly located in the Oakland area of California but various investigations reveal it is actually in China and its U.S. locations are fraudulent. Most of this became apparent during trademark lawsuits against OnlineNIC by Microsoft and Verizon (http://www.theregister.co.uk/2009/08/27/onlinenic_verizon_ruling_upheld/; <http://www.thedomains.com/2009/03/12/onlinenic-settles-with-microsoft-appeals-verizon-decision/>). OnlineNIC sponsors thousands of unlicensed pharmacy domains in violation of U.S. and California law. They have been notified multiple times about these sites. OnlineNIC actually has several alleged addresses. The address given in the InterNIC directory and in their WHOIS record is 351 Embarcadero E. Oakland CA 94606. This address was revealed to be an empty lot in an article by Andrew Naylor called "Visiting OnlineNIC's Non-Office"¹ over a year ago. We have filed inaccuracy complaints about this address but Onlinenic.com endures. Their second address, 2315 26th Avenue, San Francisco, CA, is related to a California business registration that has been suspended by the Secretary of State.

Business Entity Detail

Data is updated weekly and is current as of Friday, January 22, 2010. It is record of the entity.

Entity Name:	ONLINENIC
Entity Number:	C2151424
Date Filed:	12/03/1999
Status:	SUSPENDED
Jurisdiction:	CALIFORNIA
Entity Address:	2315 26TH AVENUE
Entity City, State, Zip:	SAN FRANCISCO CA 94116
Agent for Service of Process:	REX W LIU
Agent Address:	2315 26TH AVENUE
Agent City, State, Zip:	SAN FRANCISCO CA 94116

¹ <http://dotsnews.com/domain-name-news/184>

Their third address is a residential address which we will not reveal here because there is no evidence that the location is associated with OnlineNIC. The fourth address, 909 marina village pkwy #236 Alameda CA 94501, is a UPS mail box.

View Location Detail

The UPS Store 909 MARINA VILLAGE PKWY ALAMEDA, CA 94501-1048 Phone: (510)769-8221 Fax: (510)769-2187 E-mail The UPS Store #0578	Regular Hours of Operation: Monday 09:00 AM - 06:00 PM Tuesday 09:00 AM - 06:00 PM Wednesday 09:00 AM - 06:00 PM Thursday 09:00 AM - 06:00 PM Friday 09:00 AM - 06:00 PM Saturday 10:00 AM - 04:00 PM
---	--

Additional Information:
MARINA VILLAGE SHOPPING CENTER NEXT TO ROUND TABLE

Since the lawsuits their CA business has been re-registered by their U.S. lawyer, Perry J. Narancic.² Narancic represented them against MS and Verizon and negotiated the multi-million dollar settlement. OnlineNIC's real address is likely 7F International Trade Building, 388 South Hubin Road, Xiamen China that exists even in ICANN documents.³ It is time for this charade to end.

Absolutee Corp Ltd

Absolutee Corp Ltd is OnlineNIC's privacy protection service and it is doubtful that OnlineNIC and Absolutee are distinct entities. Furthermore, the Registrars China-Channel, 35.com and USA Intra Corp. are all likely part of the same organization. On April 19, 2010 the Malletier group, which owns Louis Vuitton, was issued a default judgment of \$960,000.00 against Absolutee for "knockoff" sales through OnlineNIC sponsored domains by by California Northern District Court Judge Maxine M. Chesney (<http://docs.justia.com/cases/federal/district-courts/california/candce/3:2009cv05612/222027/27/>). The Honorable Maxine Chesney also issued an injunction against Absolutee preventing them from any further violation of these trademarks (<http://docs.justia.com/cases/federal/district-courts/california/candce/3:2009cv05612/222027/26/>).

This is same Absolutee that WIPO decided against for registering "tiffanyline.com" (WIPO 2009_d2009-0430) and "buickopen.com" (WIPO 2007_d2007-0279). As seen in the above examples "The Respondent did not reply to the Complainant's contentions."

It would be useful at this point to provide some background on Absolutee:

- Absolutee has been flagged as supporting the Russian Business Network⁴
- Absolutee has been linked to a payment processing system for child pornography called Avalonpay⁵
- Absolutee was linked to a fake Fidelity Investments phishing site⁶

² http://www.nk-pc.com/index.php?option=com_content&view=article&id=47&Itemid=54

³ http://www.icann.org/en/tlds/pro1/pdf/rop_exhibit_a5.pdf

⁴ http://www.wired.com/images_blogs/dangerroom/files/iDefense_RBNUUpdated_20080303.doc

⁵ <http://www.matchent.com/wpress/?q=node/369>

⁶ <http://www.ecommerce-journal.com/node/1195>

- Absolutee was linked to malware distribution⁷
- The site “absolutee.com” has been known to appear as a download location in virus scan logs⁸

⁷ <http://www.dslreports.com/forum/remark.16686792>

⁸ <http://www.bleepingcomputer.com/forums/lofiversion/index.php/t111606.html>