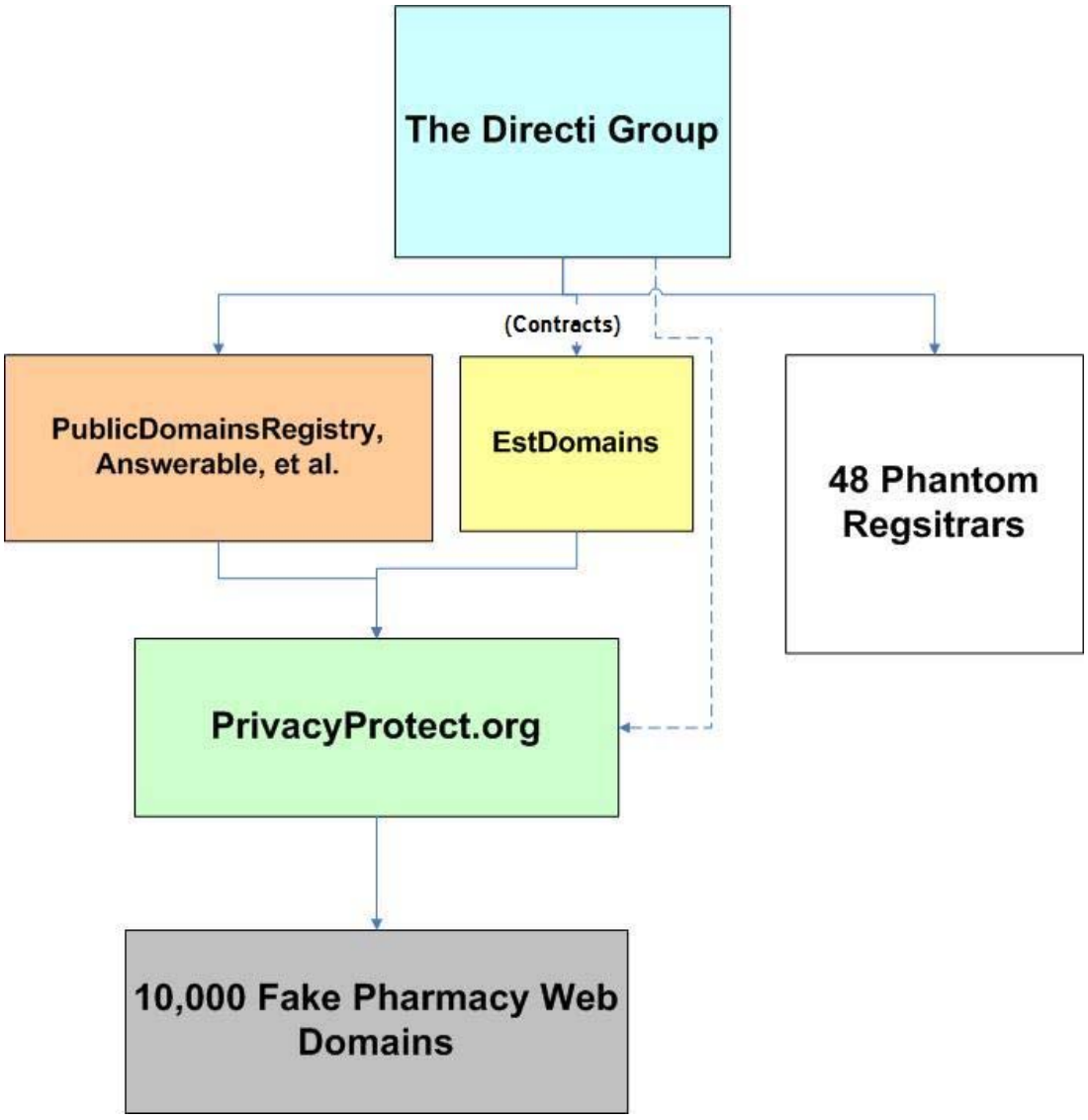
Phantom Registrars, Fake Pharmacies, and the Secret Infrastructure



A report from KnujOn.com detailing the Directi Group's control of 48 Phantom Registrars, the proliferation of unlicensed pharmacy domains at Directi affiliates, and their use of the anonymously owned PrivacyProtect.org to shield ownership of illicit websites

Prepared by Garth Bruen at KnujOn.com and Dr. Robert Bruen at Coldrain.net PO Box 404 - Wilmington VT 05363 - United States
August 28, 2008

About KnujOn

KnujOn.com collects spam email freely from the public and processes it through the KnujOn Policy Enforcement Engine. This engine is a rules-based interface that gathers data on illicit websites and attempts to determine what the best path for proper enforcement is. The engine also collects feedback from the existing Internet policy structure to uncover bottlenecks, breakpoints and general failures. This system also generates reports made available to our clients, industry and government.

Introduction

In our continuing effort to shed light on the dark corners of the Internet we have produced this report on the Directi Group, a fairly large player in the Registrar world. We have highlighted their use of the controversial service PrivacyProtect.org, their association with EstDomains, their continued sponsorship of fake pharmacy domains, and their apparent ability to get Registrar accreditations for 48 Phantom Companies.

48 Phantom Registrars

KnujOn has found at least 48 ICANN-accredited Registrars that do not seem to exist. All of the Registrars in question are affiliated with the Directi Group (Directi, PublicDomainsRegistry, Answerable, LogicBoxes). Our attention was first brought to them when we released our report of the Ten Worst Registrars for illicit domains, spam, and false registrations (http://www.knujon.com/registrars/). At the time, in some records Directi's address was listed as: "14525 SW Millikan #48732 Beaverton Oregon". Directi has since denied this and now disclosed its address as being in Mumbai, India. This prompted us to take a closer look at all the Registrars in Internic's (ICANN) directory (http://www.internic.org/origin.html) affiliated with Directi and presenting themselves as being located in the United States. 8 Directi–affiliated Registrars list their address on the Internic Registrar Directory as: 14525 SW Millikan #48732 Beaverton Oregon.

In examining the directory for the other 40 Direct-affiliated Registrars, we find an even more confusing address:

15 West 47th Street New York, NY 10036 Oregon
United States
+1-650-331-0716

The first line is obviously ambiguous with "Oregon" on the end of a New York address. An additional layer of confusion is added by the fact that "650-331-0716" is a San Mateo, California phone number. So, where are these companies? New York, Oregon, California or Mumbai? There is nothing wrong with having multiple business locations, but this fact is not disclosed on any their websites or at Internic.

Next, we set out to verify if any of these companies were real. Because of the confusing addresses we researched the New York, Oregon, California and India business registries. None of the Directi-affiliated companies listed in the Internic Registrar Directory are real licensed companies:

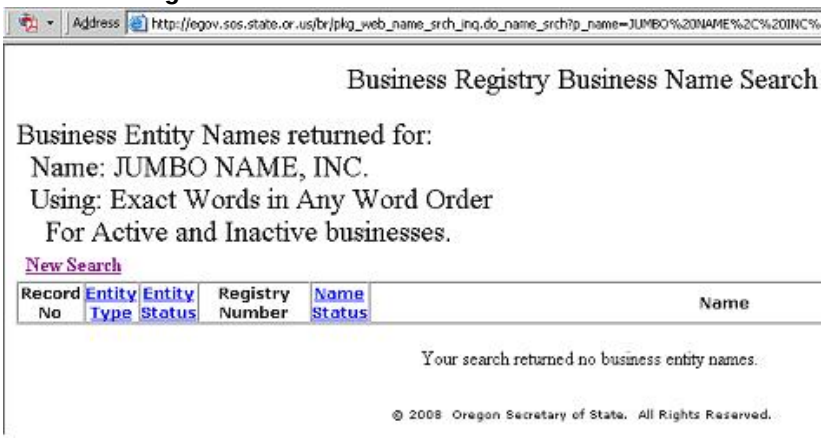
Jumbo Name, Inc.
Your Domain King, Inc.
Fenominal, Inc.
Game For Names, Inc.
Ever Ready Names, Inc.
Find Good Domains, Inc.
Go Full House, Inc.
Instinct Solutions, Inc.
Name Perfections, Inc.
Need Servers, Inc.
Network Savior, Inc.
Power Carrier, Inc.
Power Namers, Inc.
Super Name World, Inc.
Tech Tyrants, Inc.
The Registrar Service, Inc.
Trade Starter, Inc.
Unpower, Inc.
Venus Domains, Inc.
Yellow Start, Inc.
Zone Casting, Inc.
Extend Names, Inc.
Extremely Wild Key Registrar, Inc.
Magic Friday, Inc.
Name To Fame, Inc.
Net Juggler, Inc.
Unified Servers, Inc.
Names Bond, Inc.
Specific Name, Inc.
Genuine Names, Inc.
Best Site Names, Inc.
Get Real Names, Inc.
Global Names Online, Inc.
Naming Associate, Inc.
The Names Registration, Inc.
Cool Ocean, Inc.
Names Real, Inc.
Big Domain Shop, Inc.
Colossal Names, Inc.
Click Registrar, Inc.
Cotton Water, Inc.
Crystal Coal, Inc.
Curious Net, Inc.
Domain Band, Inc.
Domain Mantra, Inc.
Platinum Registrar, Inc.

There is an expression that a company can “exist only on paper”, but in this case we don’t even have that.

Internic Says Jumbo Name is U.S. based

Directi's Whois records say India

But the point is moot since Jumbo Name, Inc. does not seem to exist...
Not in Oregon



Not in New York

Not in India

The Fake Pharmacies

We have collected content and data for the 19,000 plus domains using the PrivacyProtect.org service that have been advertised through spam and narrowed the analysis down to 9,156 domains that are currently active.

What has been found is very interesting and helps explain how a rogue Registrar can play a big role in supporting massive fake pharmacy networks.

Directi Sponsored airbestmedications.com

Directi Sponsored yourworldtrustpharmacy.com

Starting with a list of 1,820 fake pharmacy domains all using PrivacyProtect.org and all registered through Directi/PublicDomainsRegistry we find these sites are all served from 132.206.106.15, an IP at the McGill University (likely a compromised

machine, maybe even that of a student). Half of the content for the sites is served from an IP in Austria, the other half from an IP in the UK. (Full lists of all referenced domains and IP addresses available at KnujOn.com)

We could call McGill today and get this IP closed but it would only be a temporary obstacle for the criminals. In fact, since KnujOn collected this data the sites have already moved to 61.153.209.98, which is Donghai University in China. These networks are very nimble, the content is highly portable and deployed by scripted kits. This is where the Registrar comes in. They have to make the sites resolve at a new location quickly. The IP addresses of the fake pharmacies change, but the Registrar and proxy registration service are constants. The nameservers for these sites are all at Directi/PublicDomainsRegistry and also shielded by PrivacyProtect.org.

Their subtle misdirection provides cover. If a consumer complains to Directi/PublicDomainsRegistry about these sites they simply direct them to the ISP host that serves the content. If and when the site content is closed by the ISP host, Directi/PublicDomainsRegistry just helps them set up at a new IP. The true owners are of course shielded by PrivacyProtect.org. It’s a cycle they have adapted to, so the fake online pharmacy business continues with minimal interruptions.

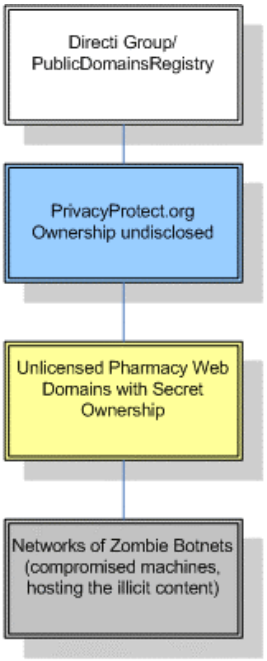
Secret Infrastructure

The service that shields ownership of the unlicensed pharmacies, PrivacyProtect.org, is itself a phantom with undisclosed ownership. It was revealed in a Washington Post article that the Directi Group actually owns PrivacyProtect.org, a fact they did not deny when they responded to the article (http://voices.washingtonpost.com/securityfix/2008/06/anonymous_domain_sales_a_spamm_1.html).

In summary, we have thousands of illicit domains cloaked by a company which is also anonymously owned. The domains are all sponsored by the Directi Group which is affiliated with 48 Registrars that cannot be proven to be real entities. Clearly there are serious problems with oversight, due diligence, and accountability. How can the consumer be protected under these conditions?

While Directi claims they will suspend illicit domains, KnujOn has found on many occasions Directi sponsored domains being removed temporarily only to be restored after a brief period with the same content (http://www.knujon.com/news.html#08052008). The sheer volume of fake pharmacies at Directi is daunting, and given the fact that they can all be traced to one source: PrivacyProtect.org, would it not be time for Directi to reconsider its relationship with PrivacyProtect.org if they are serious about solving the problem?

As for ICANN, how is it possible that so many companies can be granted accreditation with unverified credentials?



In this scheme there is only one real responsible party with control over the illicit websites

Examining the Role of Registrars in Illicit Activity

In examining what is driving and enabling Internet criminality KnujOn has taken a critical look at the Registrar community. Some have wondered why, noting that a Registrar simply holds domains names and resolves them to IP addresses. But that is the simple point. Registrars have been given an enormous public trust. KnujOn has noted serious flaws in the system that is supposed to monitor Registrar compliance and the failure of the industry to police itself.

It is entirely possible that Directi is a victim here and has no knowledge of the rampant abuse occurring in their space. In defense of the Registrars it is difficult to monitor the content and use of all the domains held by a Registrar. However, KnujOn has noted Registrars refusing to terminate illicit domains even after receiving detailed information about the illegal nature of these sites (http://www.darkreading.com/document.asp?doc_id=161511&WT.svl=news2_1).

Even more telling we have two recent cases of Registrars being directly involved in fraud, spamming and other questionable activities.

In 2002 Peter Kuryliw pleaded guilty to fraud in a Canadian court and was fined $30,000 for targeting over 40,000 business with fake invoices (http://www.competitionbureau.gc.ca/epic/site/cb-bc.nsf/en/00405e.html). Mr. Kuryliw was granted accreditation for an Internet Registration business by ICANN (namejuice.com) and may have part ownership in several other Internet companies. And it continues, in 2003 a court ordered a Kuryliw-affiliated Registrar to stop using deceptive emails (http://www.ftc.gov/opa/2003/12/domainreg.shtm). Namejuice.com is still operating.

Example two. Scott Richter paid $7 million to Microsoft in 2006 in a settlement arising out of a lawsuit alleging illegal spam activities (http://www.microsoft.com/presspass/press/2003/dec03/12-18NYSAGandMicrosoftPR.mspx). He also settled another spam case with New York Attorney General for $50,000 in 2004. In 2008 MySpace was awarded $ 4.8 million in damages and $ 1.2 million in attorney's fees in a judgment against Richter’s company for sending spam to MySpace members through compromised MySpace accounts (http://www.toptechnews.com/news/MySpace-Takes-On-the--Spam-King-/story.xhtml?story_id=11300ADUSD8F). Scott Richter owns Registrar Dynamic Dolphin, which until recently was the largest user of the PrivacyProtect.org service.

Registrars will often refer spam victims to the "upstream ISP" or website operators to file abuse complaints. However, when the content is hosted on zombie botnets and the owners are anonymously hidden by PrivacyProtect.org, there is no one else to direct a complaint to but the Registrar. And it is the Registrar who has ultimate control over terminating a domain.

EstDomains and Directi

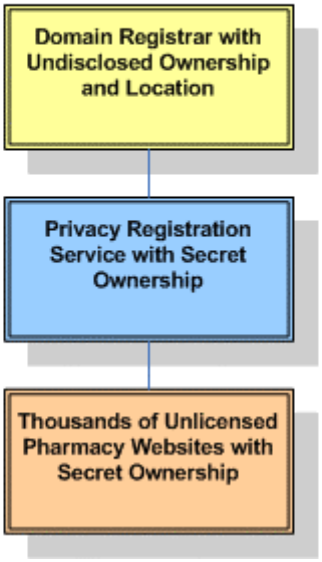
EstDomains is a Registrar that also makes heavy use of the PrivacyProtect.org service for masking the ownership of fake pharmacy domains. EstDomains is incorporated in Delaware. For those not familiar with U.S. geography, Delaware is a tiny state that earns its keep by being very business-friendly. Typically, any business incorporated in Delaware is not actually there. This means there are scant details publicly available for who owns EstDomains.

EstDomains Sponsored fastcanadianpharmacy.com

It is also important to note that this site claims it is "FDA Approved" and "Trusted by VeriSign." The depth of misrepresentation at these sites is profound and seems to exist with absolute impunity.

So, we have an ICANN Registrar with undisclosed ownership who sponsors unlicensed Internet pharmacy domains (advertised with spam from zombie botnets) with anonymous ownership through an anonymously owned privacy registration service. How is the consumer being protected?

Where is the accountability?



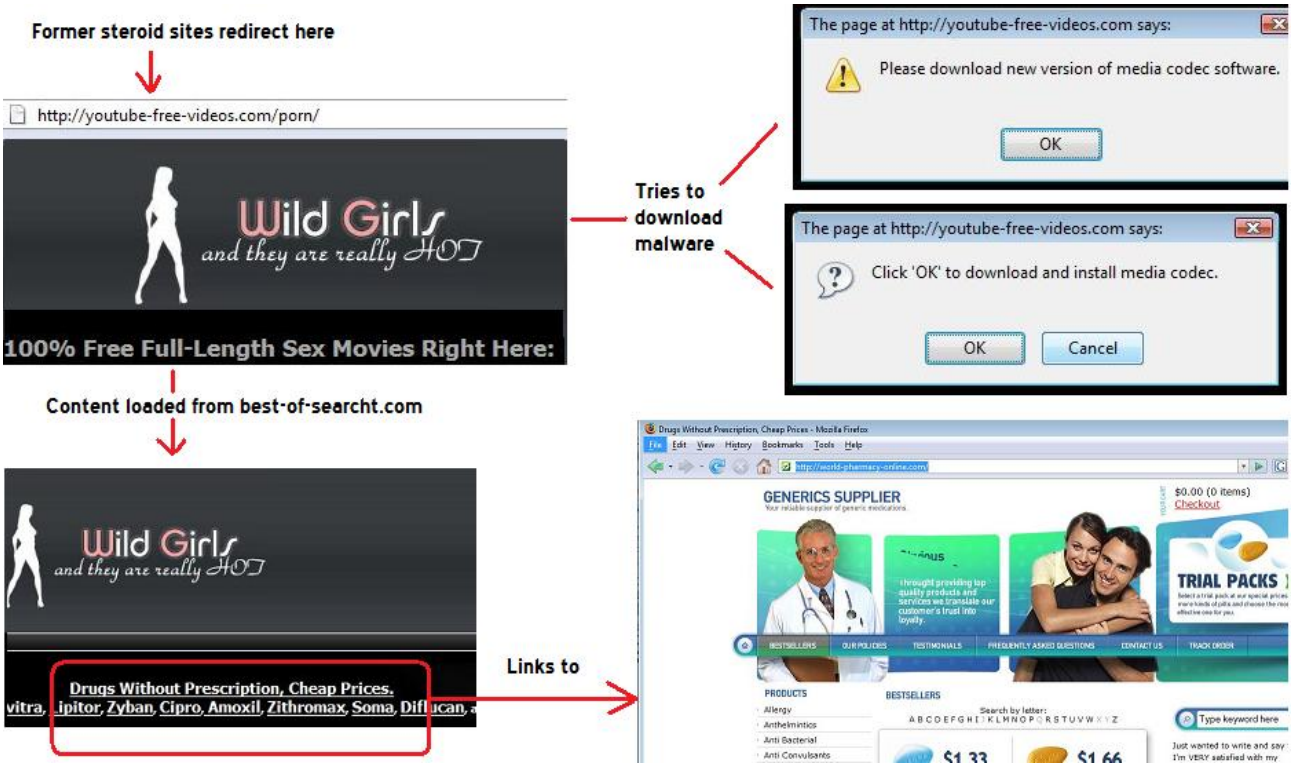
Brandjacking

All of these websites contain trademark and/or copyright infringements. Some of the domain names themselves are brandjacked. The example below incorporates both Pfizer and Lilly in one domain name.

Directi Sponsored, PrivacProtect sheilded pfizerlillymedicals.com

Drugs, Pornography, and Malware

Using pornography to lure unsuspecting Internet users into unknowingly downloading malware is an old trick, but one that continues to work. However, KnujOn has found an array of EstDomains sponsored, PrivacyProtect.org sheilded domains that combine drugs, porn and malware. Several former steroids EstDomains sites have metadata that appears to offer Schedule 3 substances like Morphine, Testosterone, and Vicodin but redirects the user's browser to youtube-free-videos.com (also sponsored by EstDomains), a porn site that attempts download malware in the guise of a "player update." The scripting vigorously prevents the user from navigating away from the page or closing it. The content of youtube-free-videos.com is served from best-of-searcht.com (also sponsored by EstDomains), another porn site that has links to another fake pharmacy: world-pharmacy-online.com (also sponsored by EstDomains).



This EstDomains sponsored and PrivacyProtected domain asiangirlporn.net rotates different sites the user is redirected to. One site, movlabs.com, seems to feature films that depict rape scenes as well as attempting to download malware from aviupdate.com (also sponsored by EstDomains).

EstDomains Sponsored movlabs.com

Another redirect landing launched from asiangirlporn.net links to fake virus/spyware scan site: security-scan-pc.com. This particular fake security software is actually one of the most insidious PC infections to date. It blocks access to the Control Panel, Registry Editor, hard drive, removable media, Task Manager, Run, and just about any utility someone might use to fix their PC or remove the malware. It also blocks installation and running of legitimate anti-virus packages. Once infected your PC can only be used as a botnet node or a doorstop.

Directi Sponsored security-scan-pc.com

It is unclear whether this simply an attempt to expand the botnets or a trap for anyone trying to investigate these sites.

Phishing

Among the lists of Directi sponsored, PrivacyProtect.org shielded domains we found defunct sites that were possibly used for phishing:

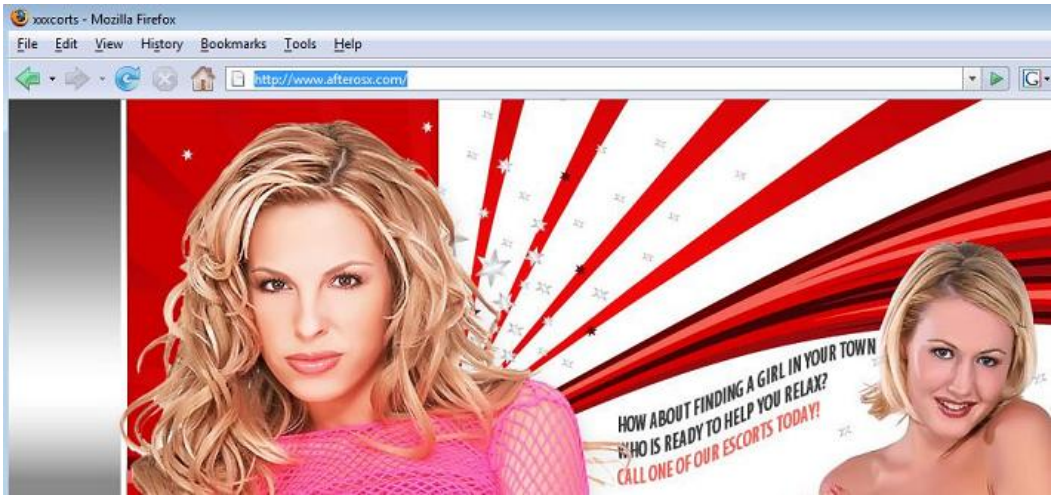
onlinewachoviaaccountupdate.com
wachoviamembersaccountupdate.com
wachoviaonlineaccountsmembersupdates.com

Other Illicit Sites

PrivacyProtect.org is used to register domains that offer pirated software and counterfeit consumer goods.

Prostitution?

KnujOn has also found a number of Directi sponsored, PrivacyProtect.org shielded sites that offer "escorts"



Conclusion

The buck hasn't been passed, it's been flushed. Directi and other Registrars have seemingly been able to carve out an infrastructure within the infrastructure with its own rules and standards of conduct where the players are secret and there is no accountability.

Critical questions need to be answered: How much money to Registrars make from fake pharmacy domains? What would it take to prevent the constant, mass population of fake pharmacy sites? What resources does law enforcement need to move drug interdiction from the street to the web?

In addition to a detailed investigation into the nebulous world of fake Internet pharmacies, a serious policy review is required to figure out how it go this bad. The system needs to be fixed to prevent further degradation of global communication. Care and oversight of the Internet is a public trust. Dozens of nonexistent companies being given Registrar accreditations violates this trust. Allowing illicit sites to operate with secret ownership violates this trust.

Directi has a real opportunity at this moment to be a leader in the Registrar community by dumping all of these illicit domains, blocking criminal customers from registering new sites, and cutting its ties with PrivacyProtect.org. We challenge to Directi to take the responsible steps that will help rebuild public trust.

Prepared by Garth Bruen at KnujOn.com and Dr. Robert Bruen at Coldrain.net PO Box 404 - Wilmington VT 05363 - United States
August 28, 2008