Recommendations and Appreciation Letters from the Security Community

1. FBI Brussels Invite
2. Mariposa Botnet Takedown
3. IM Botnet Takedown
4. LegitScript - for rogue pharmacy
5. PhishLabs - for phishing and malware scams.
6. AA419.prg - 419 Fraud
Hi Bhavin,

The Law Enforcement Community (FBI, European Commission, UK SOCA, Europol and others) and the Registrars (both ccTLD and gTLD) and Registries, will be having a meeting in Brussels, Belgium on February 24-25, 2011. The goal of this meeting is to find better ways to prevent criminals from obtaining domain names and being able to trace and track criminals across international frontiers using DNS resources.

It has been brought to our attention that DirectI is one of the shining stars of the registrar community in eliminating fraud, exercising due diligence and having a good reputation. We believe our meeting in Brussels would be an excellent platform for you to highlight the success story of DirectI. We are very interested to hear your methods.

Below please find the invitation sent out a few weeks ago. We sincerely hope you can attend!!

Sincerely,

SSA Bobby Flaim

FBI/Operational Technology Division

Work: +1-703-985-2555

Cell: +1-571-437-3728
To: 'Bobby Flaim' <rflaim@stas.fbi.gov>  
Cc: Radomir.JANSKY@ec.europa.eu <Radomir.JANSKY@ec.europa.eu>; 'Gary Kibbey' <gary.kibbey@soca.x.gsi.gov.uk>  
Sent: Sun Jan 30 21:29:44 2011  
Subject: RE: Brussels LE/Registrar/Registry Meeting -February 24-25, 2011

Hi Bobby / Radomir

Thank you for your kind invite. Our team is actually attending the Parallels Summit at Florida around the same time and hence it will be difficult for me to attend this meeting.

I am happy to have someone share our methods with you as a case study in the form of a powerpoint if it is possible for someone at your end to present the same in our absence.

Thanks and have a great event

Warm Regards
Bhavin Turakhia
Founder & CEO
Directi

From: Flaim, Robert [mailto:Robert.Flaim@ic.fbi.gov]  
Sent: Monday, January 31, 2011 8:22 AM  
To: 'bhavin.t@directi.com'; 'rflaim@stas.fbi.gov'  
Cc: 'radomir.jansky@ec.europa.eu'; 'gary.kibbey@soca.x.gsi.gov.uk'  
Subject: Re: Brussels LE/Registrar/Registry Meeting -February 24-25, 2011

Hi Bhavin,

Thank you very much for you response. While we are very sorry to hear you cannot join, I think we will take you up your offer for a presentation.

As we indicated earlier, we have heard your registrar did a fantastic job in cutting fraud, keeping track of your resellers and being successful. We would love to learn how you did it, what we the costs involved and how long it took to see results.

Thank you again!!

Bobby
2. Mariposa Botnet Takedown

> -----Original Message-----
> From: Chris Davis [mailto:chris@defintel.com]
> Sent: Thursday, July 22, 2010 11:56 PM
> To: Directi Abuse Desk
> Cc: bhavin.t@directi.com
> Subject: Re: new DIRECTI
>
> Hi Imran
>
> Thank you very much for your clarity regarding my questions. I would
> like to again thank you and your team again for all the great work you
> do to help us stop these criminals.
>
> Directi is BY FAR THE BEST registrar we have ever worked with at
> taking down criminal domains in a timely, efficient and professional
> manner.
>
> Your team was absolutely key to the Mariposa Working Group taking down
> one of the largest Botnet in the history of the Internet. You and your
> team should be VERY proud of that :)
>
> Bhavin; David Dagon from Georgia Tech/ICAAN/IANA/MAAWG and I were
> thinking of making a special trip to India in the hopes we could meet
> with you for an hour or two. Could you please let me know if you might
> be interested in meeting with us, and if so, what dates might work for
> you?
>
> Thanks Again!
>
> Cheers!
>
> Christopher Davis
> CEO
> Defence Intelligence
> 180 Preston St. 3rd Floor
> Ottawa, Ontario, Canada.
> 1.877.331.6835
> cdcavias@defintel.com
Hello Team,

Thank you for your exceptional coordination with our team and the other providers this morning during the simultaneous shutdown. We wanted to follow up with you and let you know that despite the last minute unanticipated scramble, the takedown was a success and the botnet has been shutdown.

To confirm, the conference call is canceled for 7/1/2011 at 12:00 UTC. Again, thank you for accommodating our requests leading up to and during the shutdown and being integral in reaching our goal.

If you need anything further from us, please let us know.

Best Regards,
--
Lauren Lamp
Manager / Service Delivery

IID -- Actively Securing the Extended Enterprise

E-mail: lauren.lamp@internetidentity.com
Office: +1.253.590.9928 | Fax: +1.425.699.6597
24/7 Service Line: +1.253.590.4100 ext. 0 | 888.239.6932 ext. 0
February 22, 2012

Bhavin Turakhia  
Founder and CEO, Directi

Aman Masjide  
Manager, Compliance and Abuse Mitigation, Directi

Directiplex, Old Nagardas road, Andheri (East)  
Mumbai, MH 400069  
India

Dear Bhavin and Aman:

It is my great pleasure to write this letter commending Directi’s commitment to Internet safety, and specifically the fine work of Directi’s compliance and abuse mitigation team, many of whom we have had the opportunity to work with over the last four years.

As you know, “rogue” online pharmacies are a significant threat to human and animal health. There are literally hundreds upon hundreds of instances of hospitalization, overdose, and death resulting from the sale of counterfeit drugs, or prescription drugs sold without a valid prescription, via the Internet. LegitScript’s mission is to help make the Internet safer by identifying and, working with Registrars, disabling these fraudulent and dangerous websites.

When Registrars take a stand against rogue online pharmacies, they save lives. In 2008, Directi was the first Registrar to commit to a policy of disabling domain names used in furtherance of this illicit activity. In this respect, history has clearly shown Directi to be a leader: literally hundreds of Registrars have since followed suit, and today, the standard industry practice is for Domain Name Registrars to disable domain names that sell unregulated, dangerous pharmaceuticals and prescription drugs without a prescription.

This is all-the-more impressive given Directi’s prominence as one of the world’s leading “Top Ten” Registrars. Despite having a significant proportion of the domain name market, Directi has an extremely low percentage of rogue online pharmacies — and those are typically quickly disabled. In fact, as we monitor forums and bulletin boards frequented by cybercriminals, they often encourage each other to “avoid Directi,” having found out the hard way that they cannot use Directi’s platform as a safe haven to engage in criminal fraudulent activity.

At LegitScript, we realize that none of this happens without a day-to-day commitment from Directi’s staff, including the compliance and abuse mitigation team. Directi and its staff should be proud of their work in identifying and disabling websites engaged in the
sale of unsafe pharmaceuticals and drugs, which helps keep the Internet safe and saves lives.

LegitScript is pleased to commend Directi and its staff for their excellent work in fighting drug-related cybercrime, and we look forward to Directi's continued leadership in this important area.

Cordially,

John Horton
President and Founder, LegitScript
February 25, 2012

Mr. Aman Masjide
Directi
Directiplex
Next to Andheri Subway,
Old Nagardas Road,
Andheri (East),
Mumbai, Maharashtra 400069

Mr. Masjide:

I am writing to you to express my appreciation on behalf of PhishLabs for the contributions that Directi has made to securing the Internet.

Our company, PhishLabs, investigates over 20,000 attack incidents per year ranging from phishing attacks to malware incidents, and online job scams. We are grateful for our partnership with Directi, without which, there would certainly be more cybercrime on the Internet and more victims.

Our ability to report attacks involving malicious domain names to Directi and know that they will be promptly investigated and suspended once confirmed, gives us the confidence to recommend Directi’s services to our friends, partners and customers.

Please express our thanks and support to your management and especially your colleagues in the compliance and security departments.

Sincerely,

John LaCour, CISSP
CEO, PhishLabs
13th February 2012

To whom it may concern,

I am an administrator of http://aa419.org and I have been fighting internet crime for over 5 years.

During that time I, and other members of aa419, have dealt with many registrars and hosters including Directi.

Directi is one of the best, if not *the* best, registrar when it comes to dealing with abuse complaints. Their response time to abuse reports can be as quick as 5 minutes and very rarely longer than an hour. The abuse team always keeps in contact which means we are always aware of the action that has been taken.

In recent months Directi has been monitoring our database of domains that are used in internet scams. They investigate immediately an entry is made that relates to their services and they promptly take the appropriate action.

The Directi abuse team is also one of the most pro-active when it comes to internet fraud. They help to find and identify fraudsters abusing their services.

We commend Directi for their attitude and commitment to fighting internet fraud.

Lance Hull
Administrator - www.aa419.org