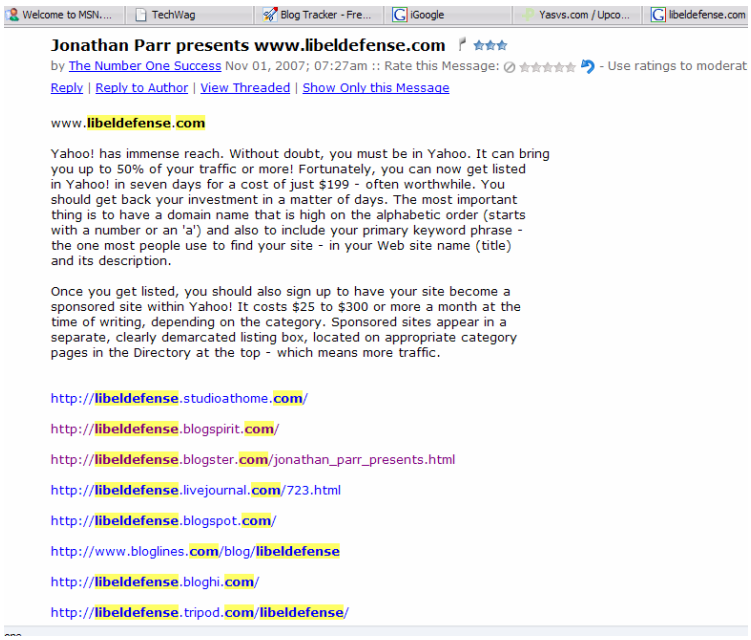
Social Networking Site Shut Down

Dan Morrill October 2007

A small web 2.0 web site named yasvs (yet another social voting site) was taken off the wire because their web site was referenced in a spam message that was focused on selling the services of Libel defense.

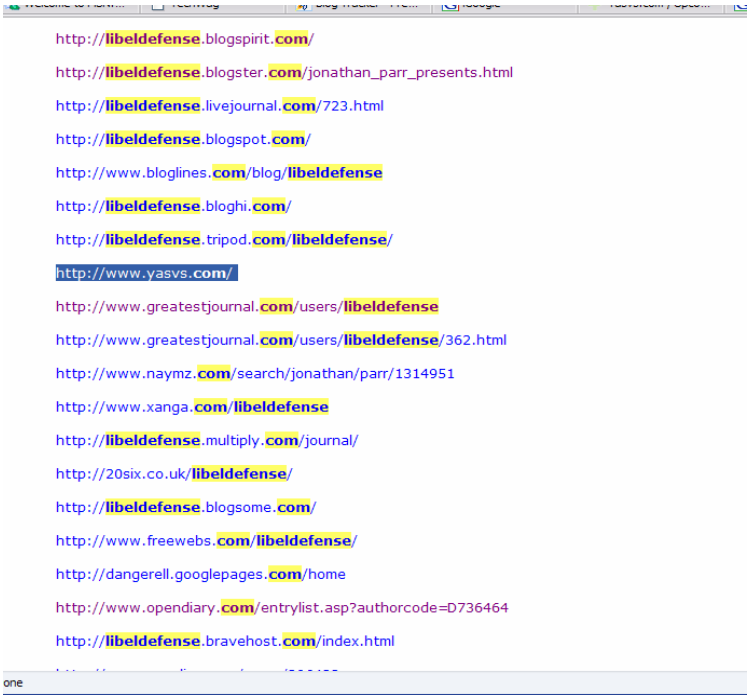


The process entailed sending thousands of messages much like the one to the above[1], to gain Google page links to increase their page rank, and of course, drive customers to their web site. This is a common way of getting links back to a site, and is not a good way of getting attention on your web site. While the initial pay off might be there, in the longer run this causes problems for the web sites involved.

It does matter to the ISP or the Hosting Company that the site in question is a live site with real people and real data behind it, or a spam site that is built on automation with no one at the wheel of the sites. The problem is that the ISP is going to get complaints, and they will take action, this action is usually to take the web site down.

Yasvs, a Web 2.0 social networking site was referenced in a spam message that was sent at least 400 some odd times to various groups and boards around the world. The ISP of the hosting company got a number of complaints about the spam message, and when the ISP looked at the message made the determination to cut the web site Yasvs off the internet, leading to an interesting network search for the owner of Libel defense and how to keep this from happening in the future.

[1] http://www.nabble.com/Jonathan-Parr-presents-www.libeldefense.com-t4731737.html



The internet is still largely unregulated, and when someone does something that causes damage to the reputation or operation of another web site, the ability to find the person who did the damage becomes difficult, as well as remedy in making a web site whole again is also going to be problematic. The other problem is that with the wide distribution of spamming tools, the message can end up everywhere in a short period of time, including reputable security boards, forums, e-mail, and blogs long before anyone can push some kind of containment policy on the message[2].

The Notification

Initially the owner of the web site had to find out what was wrong when the web site suddenly no longer worked. The response back from the ISP was:

> We were notified by our ISP to disable your site this afternoon. This was due to complaints of unwanted e-mails that refer to your site. This is the email and it referenced your website. I have not pasted all of the e-mail but at the bottom were links to sites and as stated before yours was one of them.
>
> Subj: Jonathan Parr presents www.libeldefense.com
>
> www.libeldefense.com

Suddenly, a web 2.0 social book marking site was off the wire, no access to the data that the system stored, all functions taken down, and DNS dead. From there hunting down the

[2] http://www.google.com/search?hl=en&safe=off&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&q=libeldefense.com&btnG=Search

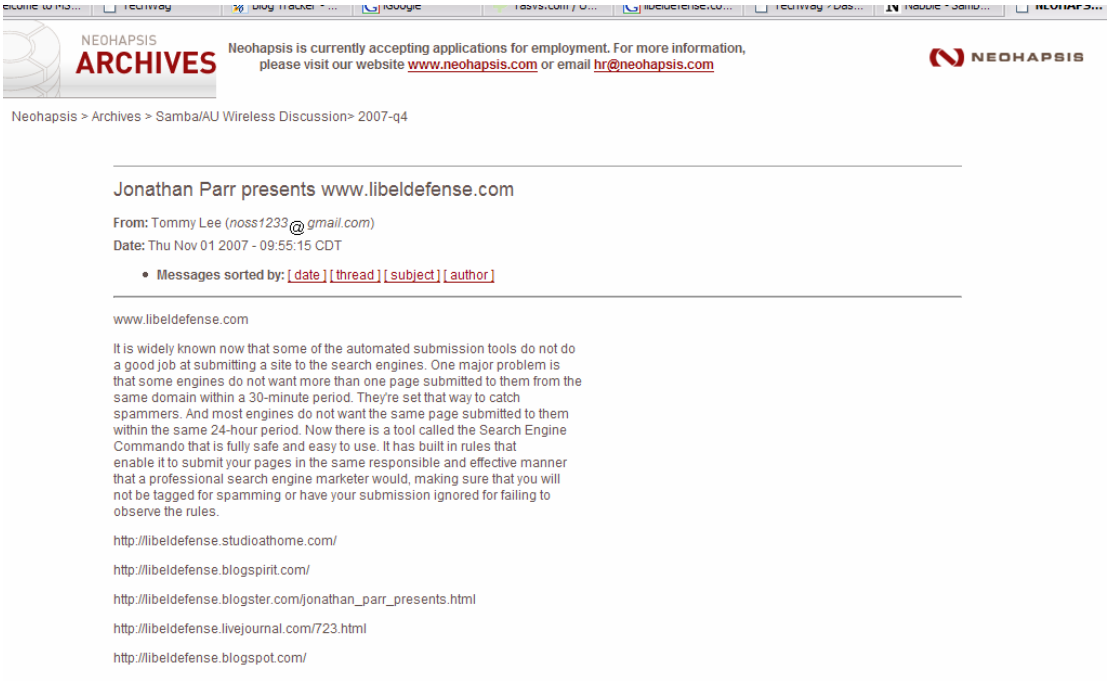
spammer became very important to prove the idea that the web site that was taken down was not involved in the spam itself, but was an innocent reference used in a spam message sent by someone else.

In today's environment, there is little recourse that a web site has when complaints are registered against it, and the ISP enforces the ban on the web site.

Hunting down the Spammer.

While we can not directly label Libel Defense as a spammer, it is a point of fact that multiple messages were posted all over the internet that featured the subject Jonathan Parr presents Libel defense. While this is circumstantial, the results of the network and e-mail analysis shows that the whole process was relatively buried in the internet, with various covers, e-mail addresses, and IP addresses around the globe that were involved in this process. In many ways this is a typical spam process, what makes this unique was the reaction of the ISP system in relationship to the complaints generated by the process. While Yasvs was only taken off the internet for three days, and is on probation to ensure that something like this does not happen again, and if it does, yasvs goes down permanently, in most ways, this is a typical spam scenario, only with a penalty for a web site caught up in the spam message.

The Network/ISP/Hosting Company level search



Even more than a week after the initial outbreak, some 400+ of these messages selling Libeldefense.com are still available via Google, meaning a lot of Google juice has been

created for libel defense, while in the longer run; the web sites mentioned in the e-mail have been taken down.

The web site Libel defense[3] is still on line, days after the spam message. There is a reason for this. The way that Libel defense has been set up on the internet makes it near impossible to shut down, as the trail ends four layers deep in the internet.

The interesting part about Libel defense is that they have no way of contacting them. Even though they have a contact page, the page itself is blank, with nothing to fill in, no e-mail address, and is essentially useless for anyone trying to get hold of the company. While they sell a damage repair service according to them, with no way to contact them, they have no way of generating any business what so ever[4].

[3] http://libeldefense.com/
[4] http://libeldefense.com/contact.html

The whois information for Libel Defense is[5]:

Registrant:
Domains by Proxy, Inc.

Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
Domain Name: LIBELDEFENSE.COM

Domain servers in listed order:
NS477.PAIR.COM
NS5.NS0.COM

The problem with the registration information because it obfuscates the path to the company.

Registrant:
Domains by Proxy, Inc.

DomainsByProxy.com
15111 N. Hayden Rd., Ste 160, PMB 353
Scottsdale, Arizona 85260
United States

[5] http://who.godaddy.com/WhoIsVerify.aspx?domain=libeldefense.com&prog_id=godaddy

Registered through: GoDaddy.com, Inc. (http://www.godaddy.com)
Domain Name: LIBELDEFENSE.COM
Created on: 04-Apr-07
Expires on: 05-Apr-08
Last Updated on: 20-Sep-07

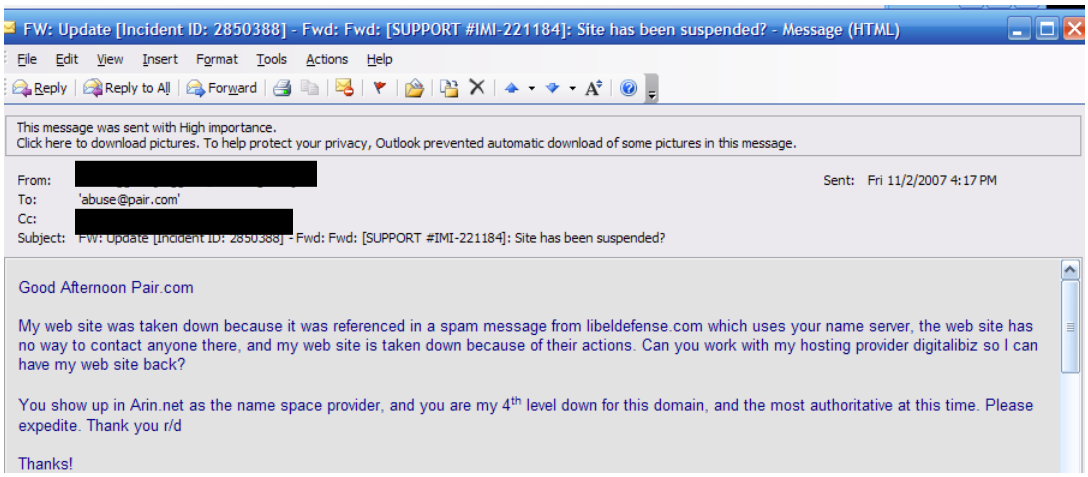
Administrative Contact:
Private, Registration LIBELDEFENSE.COM@domainsbyproxy.com
Domains by Proxy, Inc.
DomainsByProxy.com
15111 N. Hayden Rd., Ste 160, PMB 353
Scottsdale, Arizona 85260
United States
(480) 624-2599 Fax -- (480) 624-2599

Technical Contact:
Private, Registration LIBELDEFENSE.COM@domainsbyproxy.com
Domains by Proxy, Inc.
DomainsByProxy.com
15111 N. Hayden Rd., Ste 160, PMB 353
Scottsdale, Arizona 85260
United States
(480) 624-2599 Fax -- (480) 624-2599

Domain servers in listed order:
NS477.PAIR.COM
NS5.NS0.COM

One might think that the site is hosted by GoDaddy or Domains by Proxy, but the real telling information is in the domain servers in listed order, they might have bought the domain from Domains by Proxy, who resells for GoDaddy, but they are actually hosted by Pair.com. contacting Domains by Proxy or GoDaddy immediately got a response from their abuse teams, to go to pair.com.

Pair.com never responded to the abuse complaint, so getting pair.com to take action was impossible. The original abuse complaint to pair was.



Because this abuse complaint never responded in any form of answer to Pair.com the trail ends there in hunting the person through the internet. The hosting company may or may not ever respond to the message, technically as the informal investigation trail stops here, the legal trail can start here. This is the important part, if engaging a lawyer, they will need to have as much information as possible, including all e-mails, trace records and IP addresses that were used to sign up for the account, or otherwise fraudulently use resources for purposes other than they were intended for.

Legally the only way to see if Pair will do anything is to get a lawyer to issue a quick discovery subpoena to Pair, and see if they will respond to that. Pair is not under any obligation to do anything, but this is also not the first time that Pair has been involved in some form of spam or virus relay. The picture below shows that there is a discoverable history in pair not responding to abuse complaints[67].

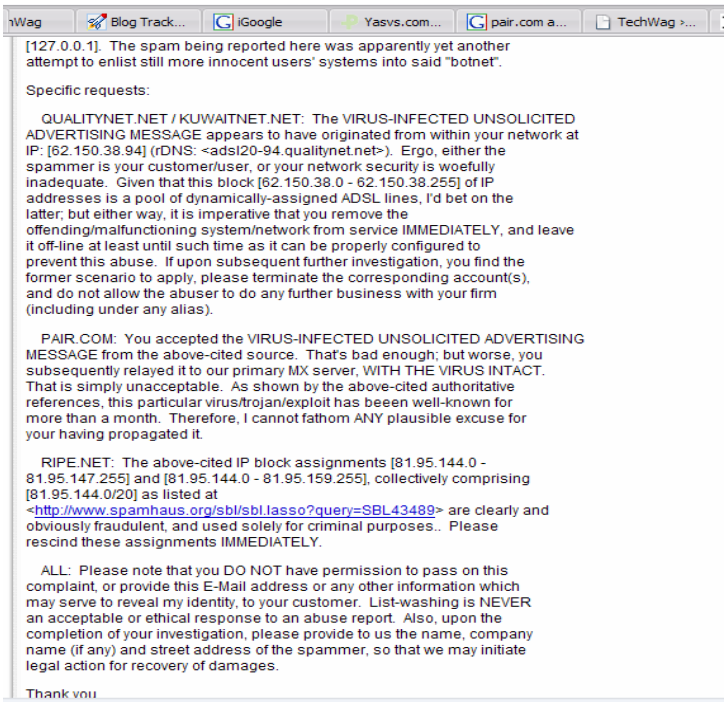
Pair though does have a spam or abuse policy, however, without being able to get them to respond to a message sent to the abuse desk, and no abuse contact on the Pair.com abuse page[8] the reality about getting abuse to effectively do anything is slim to none without enlisting legal support.

---

6 http://www.google.com/search?q=pair.com+abuse+reporting&btnG=Search&hl=en&safe=off&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial

7 http://groups.google.com/group/news.admin.net-abuse.sightings/browse_thread/thread/11a767a65ff06ac2

8 http://pair.com/policies/abuse.html



With that investigative channel shut down because of a hosting company, the next step is to go after the logged IP addresses that were registered when the spammer made an account on the web site.

E-Mail and Forum entries analysis

Essentially the spammer used the e-mail of Blank@blank.com, or other e-mail addresses that point back to publicly hosted systems like Gmail and yahoo. This is a very common way of getting around needing an e-mail address or anything near a valid e-mail address when the person creates the account on a web site[9].

The best way to get around the use of Blank@blank.com is the common use of sending the password to a customer via e-mail to ensure that a valid e-mail address was entered when the user signs up is to send an auto-generated password when they make a registration. The base software that was used for the social networking site has no such provision. That is a flaw in the social networking site software that must be repaired by the company who is developing the software.

The software though did register a number of IP addresses when the person registered, that pointed to a service provider in Amsterdam, and a service provider in Corpus Christie Texas. Going back through those essentially ended up in a dead end. The IP addresses were either not registered, or were a home ADSL system, which raises the

[9] http://www.google.com/search?hl=en&safe=off&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=yfD&q=blank%40blank.com&btnG=Search

potential that the person has access to a SpamNet or SpamBot to do their work rather than doing anything manually or in smaller increments.

The e-mail headers from the spam messages sent through forums also contained little usable information.

The site used Google as shown below

Subject: Jonathan Parr presents www.libeldefense.com
From: Tommy Lee <noss1233 (at) gmail.com>
Message-id: dea2eb130711010752y71c6401evae126d11f2dd3fe9 (at) mail.gmail.com
Date: 2007-11-01 15:52:08[10]

As well as using Yahoo shown below

Jonathan Parr libeldefense at yahoo.com
Wed Oct 31 14:28:34 CET 2007[11]

The problem with dead ends is a common issue when it comes down to hunting someone through the internet. Given the level of propagation of the messages (with 400 known messages) there are some assumptions made about how we went about this, which is tie into multiple e-mail systems, and then send his messages that way. Using yahoo, Gmail or any other public mail system is not a surprise here either. It is just one other way to cover the tracks of a spammer. Essentially the forum and e-mail headers will end up being another dead end in the process of finding this person.

Use of Reputational Systems

The other part of this was logging the name Jonathan Parr as a trusted resource or person on the internet by using a number of social networking systems. Additionally, as with any search for a person, there is more than one Google ganger (or person with the same name) in the system. The key to finding the right person is to tie the name to the spam message header to see how the use of people search and reputation systems can be used to the best benefit of the spammer.

The name in relation to libel defense does not turn up any real information that can be used[12], but it does turn up an interesting story about another swindle that was being run about a work at home scheme using the same name[13].

One good hit though was found at one of the smaller reputation systems, naymz that also featured the whole libel defense system.

---

[10] http://archive.netbsd.se/?ml=samba-technical&a=2007-11&m=5575986
[11] http://mailman.fsfeurope.org/pipermail/discussion/2007-October/007246.html
[12] http://www.google.com/search?hl=en&safe=off&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=XSE&q=%22jonathan+parr%22+libeldefense.com&btnG=Search
[13] http://friendsinbusiness.com/board1/archive3/index.cgi?read=106992

The name Jonathan Parr[14] was also used as a reference point in determining more about the spammer, which did not lead to many references outside of the smaller web sites. But it was interesting to see the use of Web 2.0 based reputational systems also being used by the spammer to send the message.

Results

The results of this kind of work, to show that the web site that had been taken down went a long way in getting the web site restored three days after it had been taken down by the ISP. The message from the hosting company was:

> We do understand that you have not violated anything. We've noted the account. Unfortunately this kind of situation does happen and is unfortunate. We're doing everything we can to get your site back up and running.

What was interesting was the level of detail that the Hosting company had to go to, to convince the ISP that the site was not a spam site. And that it was simply misused by a user who had no real intent of using the social book marking site as it had been intended to be used.

While the web site was brought back up by being able to show that there was a lot of evidence that implicated libeldefense.com in the spam and not the social book marking

[14] http://www.naymz.com/search/jonathan/parr/1314951

site, it took this level of effort to get the site back on line, and to reduce the liability of the ISP from reputational damage.

What is also relevant was the advice from two lawyers who while did not represent the web site, chimed in stating that there was realistically very little that could be done by the web site that had been taken down. The odds that the spammer if and when fully found having the money to pay for the reputational damage and downtime were slim at best. Given the extensive use of proxies, spam tools, and other ways of obfuscating information, and no way to contact the owner of the web site, there is a certain level of plausible denial on the part of the web site owner. While the circumstantial evidence is there, the actual evidence is inferred, meaning there is no real way to prove anything, there is no real legal recourse for this, and that the best advice is to move to a different hosting provider if it happens again.

Recommendations

Lessons Learned are the important part of anything that happens on the internet, especially when it influences the operation of a web site. In the Web 2.0 world, we rely on user generated content to help flesh out our web sites, and bring in the “wisdom of crowds” process to ensure that we are engaging, entertaining, and relevant to the users who use the system.

Have a solid spam and Terms of Service Policy – these are the only ways of setting a financial burden on people who use the web site for purposes other than intended. If they use the site, they agree to the TOS and policies, if they violate them, then there is a better legal leg to stand on if the choice of prosecution is the only way to find a remedy for the situation.

Keep in mind what is important here, it is getting your web site back up and running, the network forensics and hunting them down can wait. As we were told, and as we agree, people are fickle, and your property could go out of mind overnight.

Just because you used a captcha, does not mean that you are still dealing with a human, some bots can get around captcha’s.

If you have a social networking site, there is always someone who is going to do something radically stupid, it will not cost him or her, it will cost you. Spammers are not the only people out there who can have a site taken down, or otherwise screw up a wonderfully running web site.

If you have a social networking site, make sure that people are using the site, if they have only posted one article; odds are most likely they are spam, and you will want to delete them

If you do not have a plan in place on how to plan around a disaster with your social networking site, make sure you have backups, make sure you have a way to completely recover the site if you get taken down for what ever reason.

Make sure you have an alternative hosting plan available if you have to go that route. This will be the quickest and most expedient way of returning to operations.

This is not new, but rarely ever published, the abuse of social networks is more involved when the site is small, has limited resources, and limited money to go along with it.

If you end up with your site compromised because of a spammer, and like we have done here, do not identify them, it only feeds them and gives them more street cred and Google juice. The last thing you want to do is feed their ego, or their spammy mother ship along the way.

You will find that these spammers have been identified in the past, Google search all your new users, and make sure that they are not associated or affiliated with spam operations in the past. We found that when we googled the spammers web site and name, that the spammer has been identified with fraud and spam since 2004.

While these are some hard lessons learned by our social networking site, and us as owners and operators of that site, we do hope that if anyone has a site lost to a spammer, that they can see what we did, what we didn't do, and why we arrived at the decision to move the site to another hosting solution.

Spam is everywhere, and it can seriously cost you if you do not have a plan on how to deal with it, especially when your shiny new web 2.0 web site is up and running. Spammers and people who will misuse your site are going to find it, and do things that in the longer run could cost you dearly.

Summary

There is little that a company can do when they have been involved in any form of spam message. The normal reaction of the ISP or the Hosting company is to pull the site off the internet. For the web site that was pulled that is not a spam site, this can cause a lot of problems down the road in establishing back their reputation, and they need to be ready and have the ability to show that they are an innocent victim of someone else's spam message. If this proof can not be obtained, it can be difficult if not impossible to get your web site back, or the data off your web site if the hosting company decides to permanently remove it.