ITU WSIS Thematic Meeting on Cybersecurity

Steve Linford
Chief Executive Officer, Spamhaus

Geneva, Switzerland
28 June2005

About Spamhaus

- Spamhaus is an international non-profit organization which does a number of things. We have a team of 18 investigators based in 10 countries researching spam and spammers, we run the largest spam blocking system on the Internet, called the Spamhaus Block List, which now protects over 480M mailboxes, and our blocking system reject approximately 8 Billion spams every day.
- We manage a database called ROKSO which tracks the Internet's Spam Gangs, collating evidence on each gang.
- We work with Law Enforcement Agencies, mainly the FBI, the FTC, and a number of European agencies to identify and shut down illegal spam operations.
- And we lobby governments for effective anti-spam legislation (we're not so successful with that one).

Spam & Cybersecurity

- The reason we are talking about spam in the context of cybersecurity is that Spam is of course the delivery mechanism for all email security threats: phishing, endless permutations of scams, advance fee fraud, and viruses. Spam is therefore central to the cybersecurity issue.

The Proxies Problem

- The main exploit used by spammers is the hijacking of millions of private computers, by infecting them with viruses, worms or trojans, turning each infected machine into an anonymous proxy under the control of the spammer.
- Since early in 2003 almost all viruses have been created and sent out by spammers in order to build giant networks of hijacked machines through which to send their spam.
- Nowadays over 70% of spam is being sent from hijacked computers
- We have over 4 million infected machines on our lists, so the problem is huge.

- We estimate they are infecting new computers at the rate of bbetween 60,000 to 100,000 every week.

DDOS

- The other prime activity that hijacked proxies are used for is for conducting Distributed Denial Of Service attacks (DDOS).
- At around the same time as the first spam viruses such as Sobig were released, the main spam-blocking systems started coming under heavy DDOS attacks. Throughout 2003 there was wave after wave of DDOS attacks against spam-blocking systems, and the spammers succeeded in putting 2 of them out of business.
- Spamhaus was the most heavily hit. From April to December 2003 the spammers threw everything they had at us, with wave after wave of DDOS attacks, many of which were up to 500MB per second.
- At the time we had a 2MB line, it wasn't that our computers couldn't handle DDOS, it was simply that a 500MB per second attack instantly overwhelms anything less than a 500MB line.
- So we realized quickly that we had to get organized to survive DDOS attacks. We put our web site onto a 1GB line, and behind large unix boxes whose job was to filter out the attack traffic and let only legitimate traffic trough.
- For the rest of the year the spammers continued to launch wave after wave of attacks, but never suceeded in taking us down again. By November 2003 they got so desperate that they released a virus called MIMAIL E to increase the DDOS. MIMAIL E infected millions of computers and instructed each one to begin attacking the Spamhaus website.
- On a number of days in November 2003 we were being attacked on 3 fronts, we were under DDOS attack by two different gangs, one a Russian gang and one an American gang based in Ohio, and at the same time were under a massive attack from the MIMAIL virus.
- The spamers finally gave up when it became evident we had the ability to keep our systems up and defeat DDOS attacks.
- We never had a DDOS attack again. However, very few companies can afford a 1GB line and high-level technicians with the know-how to filter DDOS traffic, who work for us as volunteers.
- Normal Ecommerce infrastructure is at serious threat from DDOS attacks. We think that most governments do not realize how large the threat is. The groups behind these attacks are very highly organized and very criminal minded, and they are growing very fast.

The Spam Industry

- The reason spam is growing at such phenomenal rates, is because there is a thriving industry based around spam.
- There is a well-organized industry of mostly Russians and East Europeans writing and releasing viruses and trojans, and then collecting and selling the lists of machines infected by them. There is an industry in writing and selling the specialist hijacking software needed for spamming. There is an industry in collecting and selling addresses, and an industry in buying and selling spam jobs. There is big business in arraging the hosting for the spam websites, normallly in China, and therefore there are spam agents who take care of bribing the local ISPs and installing the servers.
- These industries come together in the many "secret" spam clubs, literally Spam Supermarkets, where spammers can buy lists of freshly infected machines directly from the spam gangs who writeand send out the viruses. In these Spam Supermarkets spammers canbuy the specialist software they need for spamming anonymously, software such as Send-Safe and DMS designed specifically toinstruct hijacked computers to send out millions of spasm anonyously.
- This activity is done boldly, in the open.
- If you go into any of these spammer clubs, such as www.SpamForum.biz <http://www.SpamForum.biz/> or www.Specialham.com <http://www.Specialham.com/>, you can come out with 10,000 proxies and everything you need to begin phishing today. By tonight you can have collected 1000 bank accounts and VISA cards. So then you think, if I can see this, law enforcemment can see this too. Therefore, why can I still see this?
- Often you hear that spammers are impossible to track down, nobody knows where they are or how many there are... but with the vast majority of spam that is not the case...
- The major players in the Spam Industry are well known and have been listed in our ROKSO database for a long time. We know their names, their locations, addresses, and in many cases even their social security numbers.
- We have for a long time named two Russians as the two people most likely to have been behind the Sobig virus. Both of them make their money by selling proxy spamware, software specifically designed for hijacking virus-infected computers, and selling lists of freshly infected machines to the rest of the spammers. Their businesses depend entirely on gathering as many infected computers as possible. One of them in particular is able to release new versions of his software (called "Send Safe") at the same time that new worms, varints of the original Sobig code, are released into the wild. And by coincidence new versions of the Send

Safe proxy hijacker contain new features already programmed to take advantage of new hijacking features coded into the new viruses just released. Their names are Alexey Panov and Ruslan Ibragimov.

- Both have been listed in our ROKSO database for years. Both believe themselves to be out of the reach of law enforcement, and as both have been doing this activity for a few years now despite tons of evidence on them available to law enforcement agencies worldwide, both appear so far to be correct that they will not be caught.
- Problem Spam Service Locations

CHINA

- For the last 4 years China has been the preferred country for spammers to operate through. From their home countries, mostly the US and Russia, spammers buy hosting from Chinese networks on which to host viagra websites, porn, scams, and of course the ever present spam clubs, the spam supermarkets. For many years the Chinese authorities and networks simply ignored the problem. Milllions of users around the world sent millions of complaints to the Chinese networks hosting the spammers, the Chinese networks simply binned all complaints. More than two thirds of the spammers listed in our ROKSO
database use Chinese hosting for their spam operations.
- 70% of websites advertized in spam are physically located in China.
- The problem has been very difficult to crack because of the way the Chinese networks are managed and the language barrier. Still today the big spam supermarkets are still hosted in China, as are the majority of the spammed illegal drugs websites and pornography sites. Almost all the websites are operated by American and Russian spammers, many of which employ tricks to keep the web sites up - for example, since all of the spam is targetted at Westerners, the spammers often set their chinese web servers up so that their Chinese ISPs can't see the sites. Often we ask a Chinese network to take a site down and they respond that they can't see any site on the IP address. So we have now built a proxy server to allow Chinese ISPs to see 'back' into their own networks from outside China to see the spammers' websites located on their networks.
- We think we have finally turned the tide in China, as nowadays almost all Chinese networks are in contact with us. In fact we now have better communication and collaboration with most Chinese networks than with some giant American networks.

RUSSIA

- Russian spam gangs are heavily involved in the proliferation of proxies, computers hijacked by viruses or trojans.
- The type of spammers we encounter in Russia are far more criminal in nature than even the worst of the American spammers. The Russian gangs often tend to be involved in all areas of cybercrime, their main occupations are spamming, card fraud, ddos for hire.

- Unless there is serious DDOS involved targetting banks, Russian spam gangs are not stopped by law enforcement.
- Few russian networks make any effort to keep spammers off. The largest Russian network - Rostelecom - claims that Russian law prevents them from terminating any customer and therefore they can not take action to stop hardcore spam gangs operating from their network.
- While China is now working to get rid of spammers, Russia is making no effort and is now the most attractive country for cyber crime.

Legislation

- Spammers are seeing that spam laws are doing nothing to stop them, in fact the penalties of most existing spam laws are so low as to be of no consequence to spammers. Even if they are finally tracked down and caught, in most of the cases we've seen they are simply given a slap on the wrist and allowed to keep the proceeds of their spamming.
- Everyone asks the question, "why isn't spamming banned?" The problem with legislation is that the government departments responsible for putting the legislation together have so far only sought advice from the direct marketing industry. IOW, they ask the group whose business depends on sending junk, whether the sending of junk outght to be banned. Predictably, they get told that everyone loves receiving junk. Hence the US have the disastrous CAN-SPAM Act which has caused spam volumes to skyrocket.
- On introduction of CAN-SPAM spam levels shot up by 10% and are increasing now more rapidly than ever.
- In Britain we have'nt faired much better, we have a law which permits spamming and has almost no penalty, so there have been no procesuctions of British spammers.
- In stark contrast, in Australia, the Australian Direct Marketing Association helped push Australia's Spam Act through.
- Australia is the one success story. The Australian anti-spam law is working, because it's a good law, with very high penalty (too much for spammers to risk), and because the Australian Communications Authority are enforcing it. Since the introduction of the Autralian spam law Spamhaus has seen a dramatic decline in activity from Australian spammers.

- Spamhaus has asked the European Comission to adopt the Australian spam law, as a template, and implement it across Europe as quickly as possible.

Consumer Confidence

- Consumer confidence in Ecommerce is being eroded very fast now. Consumers are being innundated with scams, trojans, key-loggers. Each phishing operation brings in thousands of fresh credit card and bank account numbers. The spammers have developed skills in social engineering that make emails not just appear to be clearly from your bank, but also employ highly believable reasons for why you shoud trust this email and click the link.
- The majority of banks are not reacting fast enough to the problem.
- Most banks are doing little beyond advising customers not to click links in emails. Instead they're telling customers to key the bank's website address into their browsers. Meanwhile the phishers have moved to infecting the user's DNS so that now when the user keys in www.paypal.com <http://www.paypal.com/> their browser is taking them to an IP address which is under the control of the phisher.
- My bank, HSBC, only alllows customers to use online banking if they have Microsoft Windows PCs, HSBC's Apple Macintosh and Linux users are told to go out and buy PCs if they want to use online banking.

Enforcement

- The spammers are moving at a sprint, while most law enforcement agencies are moving at snails pace, with their arms tied behind their backs by lack of resources. The miniscule percentage of spammers that are caught, are let off by courts with barely a slap on the wrist, and immediately resume their activities. We are not wining this war at all, but it's not through lack of trying, we simply do not have enough resources to stop it.
- The problem is that currently, spamming pays. We need to turn this around fast, to make spamming not pay.

Conclusion

- Spam is a cancer, it is fast killing the ability to use the Internet for commercial transactions. It is killing trust in the internet. The costs of spam including the costs of dealing with it, and of dealing with what spam delivers, such as phishing and endless financial scams, is costing the world an amount we are no longer able to calculate. The cost to the financial industry alone, and to consumers, is now staggering.

- Everyone is looking for the silver bullet to kill the problem. Although one single bullet doesn't exist, there are enough smaller bullets available to fill a silver gun anyway:
- Implement proper legislation quickly that actually bans spamming instead of trying to regulate it. Like CAN-SPAM, all legislation that tries to regulate spamming immediately fails, because you can't regulate spam, you can only ban it.
- Allocate proper funding to the law enforcement agencies so they can train a hundred times more agents for cybercrime investigations.
- Implement penalties for Internet Service Providers who knowingly host spam operations, to put an end to some well known

Number of words: 2484