SPAMHAUS

November 5, 2017

Good morning, my name is Chris Lewis, Chief Scientist at SpamhausTechnology, which is one of the most well-respected sources of anti-spam and malware filtering information in the world. While many of you may not have heard of us, more than half of all Internet users world-wide are protected by our data in one way or another, whether branded as “Spamhaus” or not.

Unlike most (all?) of the people speaking to you on the subject of the Canadian Anti-Spam Law, I work deep inside anti-spam technology. To me, this is a 7x24 effort, deep in the trenches seeing what is happening - several billion spams are "seen" by our technology daily. To me this is a vocation, as I have spent over 23 years fighting this blight on the Internet, over 17 as an unpaid volunteer.

I worked in Ottawa first as Senior Security Architect at Bell Northern Research, later Nortel from 1991 through to 2012. During this time, it became obvious that email spam was becoming a war that **must not** be lost, and I did a great deal of unpaid work working on solutions. Nortel deployed it just in time for the first great spam/malware attacks of 1997/8.

In 2003 I developed a new technology that greatly increased the effectiveness of the filtering. This required vast amounts of sensor data from all over the Internet, analysis of the data, and by way of return, I published the results for free for all to use. Late 2012, Nortel downsized to the point at which they had to let me go, and I transferred to Spamhaus the next day.

I am a the founding members (recently Treasurer) of the Coalition Against Unsolicited Commercial Email (CAUCE), invited to speak at the Federal Trade Commission Spam panel, advised on the about-to-be-passed US CANSPAM Act, a founding member of the NCFTA/FBI "Slamspam Project", won an award from the FBI for my efforts in helping secure US Government networks, and was invited to be a Senior Technical Advisor for the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG), and belong to many technical working groups targetting specific forms of spam and malware.

I have trained and assisted in cases with many law enforcement/regulatory groups around the world. Participated in discussions on what is now CASL with Industry Canada dating back to 2005 with the Federal Anti-Spam Task Force, and was consulted on early drafts of CASL. I have onsulted with CRTC over the years in training, investigations, and personally brought in cases from our datasets for the CRTC to successfully prosecute under CASL against Canadian entities. I arranged for Spamhaus to supply Public Safety/Canadian Cyber Incident Response Centre (CCIRC), entirely without charge, with 10s of millions of spams per day and related security information, from which they supply infection alerts to Canadian industry and assist with prosecutions under CASL and other laws.

I speak here only on spam, rather than other forms of online abuse, but the issues are just as dire (if not more) in abuse areas other than spam, such as malware, fraud and phishing.

Of particular interest here is that much of my time as an advisor with M3AAWG was spent helping the email sender community (marketing and other industry groups) and drafted several parts of the Sender Best Common Practises (BCPs) that are in use today throughout the industry about prior permission requirements, unsubscription and so on.

Which begs the question - if most of the industry, including the largest marketers in the world are already complying with these BCPs (and thus CASL) and doing quite well, why are some Canadian companies so concerned with compliance with CASL?

Other specific facts and details:

Spamhaus operates “email sensors” that monitor billions of emails per day via arrangements with their providers. Spamhaus itself also operates mail servers for systems that contain only long-dead or never existing email addresses - which means that essentially all of it is spam, with no valid email. Over the past 7 years, there was a peak in 2011 of 10 billion per month (peaks to 750 million per day) in our own servers. Most of this was the Rustock botnet, infamous for high volume of fake pills and fake brandname watches.

For a few years after that, the volume averaged around 3 billion/month. Over the past year, the volume has climbed almost all the way back to 10 billion/month, and instead of fake pills and watches, it's ransomware from the Necurs botnet which is even more destructive than we hear about on the news. Yet, within that volume, there is are still very high volumes of affiliate spam advertising legitimate, semi-legitimate, and outright fraudulent companies and products from people who have no concept of privacy, hackers stealing and selling email addresses (along with other personal information), phishing, and so on.

Industry leaders, such as Senderbase/Talos, have long been sources of reliable "on the wire" real statistics on spam volumes, and they generally tend to agree with our numbers. We don’t expect exact matches in numbers, every sampling of spam is different, but our trends match.

I've had the opportunity to be able to monitor the volume of email and spam received by some of Nortel's old email domains for almost 20 years. I built and ran the email servers that handled them when they were in use by real people, and for the 18 years they were defunct.

By 1997, Nortel chose to decommission these domains, and moved all users to the main email domain. In 1997, there 3 million emails per month, of which 40% was spam. By 2001, 4 million, all o which were spam. By 2003, 7 million spam, and of April 2016, 150 million. It is 350 million today.

At most, that portion of Nortel had 8,000 users. If it wasn't for the filters, today, each would have to manually delete about 1500 emails per day. Volumes like that are not sustainable now even with filtering (which is never 100%), and certainly not into the future.

This is a 350-fold increase in spam over 20 years. I'm sure you'll look at each other and say "my spam hasn't gone up that much!". And the answer is, that it hasn't, ONLY because industry - your ISPs and the providers of spam filtering data/solutions such as us, have through ever-stronger efforts managed to filter it before it hit your mailbox.

The volume keeps growing, the spammers “game” our systems, and technical solutions are becoming more and more difficult and expensive to keep it at bay.

Some of those spreading fear and uncertainty about CASL might well be saying now that “this is just the criminal spam outside of Canada”. But on the contrary, those numbers contain significant amounts of perfectly legitimate advertising that no user could possibly have requested. It contains significant amounts that is advertising Canadian products or services, or is done by Canadians acting as affiliates for foreign afflliliate marketing programs. In fact, some of the spam is soliciting people for these programs. Secondly, even if we didn’t contribute much to the problem, we are still bound to do our part, for the problem and threat is global in nature.

Over the past several years, a new issue has arisen – Canadian hosting/facilitation of foreign spammed content. CASL is an important tool in getting these shut down. Without CASL, Canada becomes known as a “safe” or “bullet-proof” for spammers (and other online abuse), and as experience shows, whether by company or country, the volumes and local problems skyrocket to everyone's detriment.

CASL is well suited to handle such issues, with adequate escape clauses for when it is a mistake or oversight, as well as authorization to work with foreign regulators and law enforcement – just as the CRTC does now. Our legitimate marketers are protected from frivolous claims, yet, have the guidance they need to develop appropriate due-diligence.

A colleague of mine had his own domain mail server, on which only he and his wife used email. "Something" happened back in the early 2000s, and the volumes of spam quickly jumped to millions per day. This was so much traffic he couldn't even reject the incoming connections without having to pay bandwidth surcharges, so he turned it over to us and now we use it for spam research.

There are laws that would allow him to take action, entirely aside from CASL. But the legal system is such that it would cost at least $10,000 or more just to put a lawyer on retainer. This wouldn't match the CASL requirements for complaints because it only affects him.

This is the sort of thing where CASL Private Right of Action (PRA) is so important - giving the individual or small organization a chance to deal with problems that the regulatory bodies cannot due to lack of resources or not qualifying for CASL intervention. CASL already has checks and balances to ensure that PRA is not abused.

PRA is currently suspended, and I urge this panel to make sure that it is not lost and comes into force as soon as possible.

In the end spam is not a technical problem, it has always been a human problem that us technical personnel can't solve well enough to sustain into the future. It's past time for governments and regulators to step in and put on the brakes before it becomes a problem that cannot be solved by technology that further erodes our citizen's trust in the technology and damages the Canadian economy.

The EU is now adopting privacy laws that will require much the same, if not stronger, regulation than Canada's CASL. EU law is already far stronger than the US CAN SPAM Act.

Australia's laws are almost as strong as ours (but not quite as broad a coverage), and as industry studies have shown, the stricter a country's laws are about opt-in, the more successful email marketing is.

CASL is the envy of much of the rest of the world. The emphasis must be on supporting and enforcing CASL and bringing PRA into force, rather than taking half-measures or reversing course.

Thank you for allowing me to present. I am available to assist in any way, please don't hesitate to contact me by email.

Chris Lewis

Chief Scientist
Spamhaus Technology