A Case Study in Enforcing AntiSpam Legislation

spamMATTERS

We are at war. On one side, billions of dollars are being spent by consumers, enterprises and security companies to filter and block the rising flood of spam emails. On the other side, spammers (the enemy) bombard users with millions of e-mail messages per day, often using a host of automated spamming tools.

Over the past few years, both the percentage of e-mail represented by spam and, more importantly, the actual volume of **spam has continued to increase dramatically**. As soon as companies upgrade their Antispam defense, spammers find new ways to circumvent these, and as soon as users adapt to one threat, such as 'not opening attachments', another method emerges, such as 'phishing'. The merging in 2004 of spam, virus and Trojan horses coincided with a rampant increase in phishing, money laundering and 'key-logging' (now commonly referred to as spyware) attacks.

Despite significant advances in AntiSpam technology to fight the enemy, currently "spammers are winning the war"[1]. While most enterprise users are protected against spam by filtering technologies, the problem of spam has simply been pushed farther back in the network – e-mail administrators, network operators, ISPs and others who manage e-mail traffic still face enormous problems dealing with spam.

The problems associated with spam cannot be overestimated – spam inundates unprotected users' mailboxes; it has forced individual users, enterprises, ISPs and network operators to invest hundreds of millions of dollars in filtering tools, storage systems, additional servers and network bandwidth; it reduces corporate productivity; **it forces up the cost of doing business** for ISPs and network operators who then pass these costs along to consumers; and it creates a number of other problems from server crashes to slower message delivery.

the problem
is societal
not technical

Spammers clearly cannot be stopped by technology alone – spam filters, for example, lessen the symptoms of spam, but do not address the underlying problem of network overload and harassment by the enormous and growing volume of unwanted content generated by spammers. Consequently, on one level **the problem is societal not technical**. Recently, governments across the world started to realize this, and have begun to intervene in the spam war. As a result, there has been an emergence of laws in many nations to protect the 'Internet commons' and the sovereignty of the end-user's e-mail 'inbox'. However, new products and techniques are required to help enforce these new spam laws – the laws themselves will simply not be effective in addressing the spam problem.

The SpamMATTERS solution is currently the only product on the market that focuses on forensic technology to help enforcement agencies track, monitor and gather evidence against the people behind spam; a technology that is sorely needed to make laws against spam as effective as possible. The following case study illustrates how the SpamMATTERS solution was deployed by the Australian Communications Authority (ACA) in enforcing the Australian spam law and thereby dramatically reducing the volume of spam sent from Australian sources relative to other spam sources around the world.

[1] Radicati Group – Sept 2004

Why spam laws alone cannot stop spam

Legal intervention in the 'spam-war' is not new. The state of Nevada in the USA introduced a law as early as 1997, long before spam became a serious problem. The intention of all such laws has been to empower action against spammers in order to stop the problem at its source and, thereby, to substantially reduce the amount of spam clogging networks and irritating corporate users and consumers. As the volume of spam increased in recent years, so did the number of spam laws across the world. However, while the laws proposed to combat spam were put forth with good intentions they are not actually addressing the problem in a substantive way.

In 2003 alone, 23 new state-based anti-spam laws were laid down in the USA, and on January 1, 2004 the 'Controlling the Assault of Non-Solicited Pornography and Marketing' or 'CAN-SPAM' Act took effect. CAN-SPAM was widely criticized for its relative weakness compared, for example, to the California anti-spam law that it superseded, and few truly believed it would end spam. History has confirmed the pessimism that many initially expressed about CAN-SPAM – the law has failed spectacularly. Compliance with CAN-SPAM, even in good months, is well below 10 percent and sometimes under one percent.

Since the law went into effect in January 2004, we still face the same problem: "Spam volumes are on the rise"[2]. At the publication date of this document, CAN-SPAM has achieved a small number of high-profile convictions, but these cases were costly to mount. As a criminal law, the burden of proof is high and only a few parties, such as the Federal Trade Commission (FTC), State Attorneys General and ISPs, are permitted to prosecute spammers under the Act.

As governments across the world will pass their own spam legislation, they unfortunately all face the same problem that CAN-SPAM has encountered – finding an economically practical way to enforce these laws. The problem will become more pronounced as tightening budgets and higher government priorities, such as combatting terrorism, compete for limited taxpayer funds.

Enforcing Spam Laws is a costly process

The cost of gathering spam data, extracting the attributes that are illegal in the jurisdiction and conversion to evidence is extremely high and very labor intensive. In the case of OptinRealBig.com, Microsoft and the New York's attorney general Eliot Spitzer settled with the defendant Scott Richter for US$40,000 after spending seven months in investigation, discovery and the courts after initially seeking US$20 million.

Most law enforcement agencies are not equipped to gather evidence against spammers cost-effectively. Obfuscation and randomization techniques, combined with users tainting data during the complaint process, exacerbate the challenge. Law enforcement faces common problems when attempting to prosecute spammers:

*" Spam volumes are on the rise, say several recent surveys. In early August, the nonprofit group Consumers Union reported that in a survey of 2000 e-mail users, **47 percent said spam had increased** since the federal antispam law took effect in January. "*

Source:
http://www.pcworld.com/news/article/0,aid,117464,00.asp

*"It's (CAN-SPAM Act) definitely a **failure** ….The term 'toothless tiger' comes to mind."*

Source:
CEO of New York Research firm Basex

*"**Practically all spam is spoofed**—that is if you were to hit the reply button, your message wouldn't reach the person who actually sent it. The reason is that they don't want you to write them back, and they don't want to be found."*

Source:
http://www.forbes.com/technology/2004/02/27/cx_ah_0227tentech.html

[2] Source: http://www.pcworld.com/news/article/0,aid,117464,00.asp

- Spammers attempt to operate in anonymity
- Spammers use exploited hosts to deliver bulk messages, such as compromised home computers with a broadband connection (so-called ‘zombies’), hiding their true identities
- Spammers can implement a solution for very low cost, exploiting the low barrier to entry for web-based business
- Spammers can increase the volume of their messages by an order of magnitude while incurring very little incremental cost
- Spammers can deliver their payload, profit from the result and disappear in days (or even in hours). The window of opportunity is decreasing.
- Spammers can be in any location around the globe, even in jurisdictions where no spam laws have been formulated or tested.

If Spam Laws are to be successful, they must therefore be accompanied by new tools that help to enforce these laws.

> *”In a January 2005 survey, Osterman Research found that 44% of e-mail and Web users had reduced their use of these technologies over the past year as a result of spam, spyware and related problems.”*
>
> *Osterman Research*

The need for a spam forensic solution

The key challenge for enforcement of spam laws is the speed and cost-effectiveness with which evidence is gathered against spammers.

SpamMATTERS addresses this problem by creating a symbiotic system between end-users (the public), governments, legal investigators and enforcement agencies:

- SpamMATTERS allows end-users (the public) to easily submit evidence against spammers, either via a website or an Outlook plug-in
- SpamMATTERS allows governments to collect data (evidence) from a variety of sources, including the public and other third-party vendors (e.g. AntiSpam Firms)
- SpamMATTERS allows legal investigators to easily analyze the data and trace spam back to it’s source
- SpamMATTERS empowers enforcement agencies to cost-effectively gather the necessary legal evidence against spammers, in order to prosecute them in the courts.

SpamMATTERS cost effectively speeds up the process of gathering evidence against spammers and broadens the number of participating enforcement agencies. This enables governments to focus more heavily on the prosecution of spammers rather than to focus on the data-collection and filtering processes.

In order to explain how this is achieved, a case study with the Australian Communications Authority (ACA) will be used to guide the reader through the SpamMATTERS solution.

> *”In a 2004 survey of US households, 92 percent of consumers said they were reluctant to share personal information online because the risks outweighed the benefits.*
>
> *61 percent had reduced confidence in disclosing credit card information online.”*
>
> *Forrester Research*

> *”There is much to be done in the fight against spam by [regulators] cooperating with each other.”*
>
> *Richard Thomas*
> *UK Information Commissioner*

Case Study

Australian Communications Authority (ACA)

The Australian Communications Authority (ACA) is responsible for implementing the Spam Act 2003, which commenced on 10 April 2004. To achieve this goal, the ACA sought a solution to make it easier for the public to submit high-quality forensic evidence and for the ACA to analyse the large number of submissions.

Some of the high-level requirements from the ACA were defined as:

1. **Public Submissions Interfaces** - Provision of secure methods to collect spam-emails, both from the public and other available sources, such as bulk spam emails from honeypots.
2. **System Load and Scalability** – The system must be capable of processing one million e-mail messages per day.
3. **Generic System Outputs** – The system must be capable of grouping spam messages into categories based on requirements of the ACA, and support all common character encodings for e-mail messages.
4. **Forensic Extraction** – The system must be able to cross-correlate spam messages and find the source (spammer). Several detailed requirements were listed including the ability to detect forged headers.
5. **Jurisdiction specific Forensic Extraction** – Each jurisdiction states specific 'illegal actions' in the definition of Spam. For example:
   - Falsifications of headers
   - Falsification of sender and/or domain
   - Absence of (working) unsubscribe link
   - Missing tags on subject line or deliberately misleading subjects.

   Each of these jurisdiction-specific attributes need to be verified in validating evidence for spam.
6. **ACA Access** – ACA staff must be able to access the system securely from remote locations
7. **Reporting** – Provision of reports on apparent Australian spammers, phishing attacks against Australians (wherever from), spam linked to child abuse material (wherever from), lists of compromised computers and general information on spam being reported by Australians
8. **"Court Ready" Evidence** – capture, collection, collation, storage and retention of data in a tamper-proof and confirmed veracity

The ACA also defined key criteria of concern to their investigative team. These were to prioritize submissions in the following manner:

- Identify spam with an "Australian Link" (as defined by the Australian Spam Law 2003)
- Identify Australian phishing events
- Select a subset of the largest spam campaigns globally
- Create "Campaigns" of the above criteria
- Identify and extract information on compromised hosts and spammers resources (such as mail server, web hosts, domain and name server information)
- Identify the responsible ISP and Country/Jurisdiction for compromised hosts
- Ability to review submissions from a particular submitter (or group) who may have initiated a formal enquiry

"California-based Postini processed more than four billion messages in January (2005). It found that approximately four in five was spam."

Source: http://news.bbc.co.uk/2/hi/technology/3465307.stm

"Last year daily global e-mail traffic via the Internet amounted to 56.7 billion messages per day. Of that, the firm says, 25.5 billion messages were spam, or about 45%."

Source: http://www.forbes.com/technology/2004/02/27/cx_ah_0227tentech.html

"Spam is ripe for organised crime, as the majority of spam relates to the vice and drugs industry…"

Source: http://www2.vnunet.com/News/1151421

After evaluation of Internet Security and Antispam technology, the ACA selected SpamMATTERS as the solution to meet their stated requirements. "No other vendor offered an end-to-end forensic solution like SpamMATTERS", says John Haydon (Executive Manager Consumer and Universal Services Obligation Australian Communications Authority).

> *"…As it stands, spammers are winning the war. If the trend continues, Radicati researchers suggest, some 70% of all e-mail will be spam within three years."*
>
> *Source:*
> *http://www.forbes.com/technology/2004/02/27/cx_ah_0227tentech.html*

Deployment of SpamMatters Solution

SpamMATTERS was rapidly deployed for the ACA within four weeks of project go-ahead. Most of the time was spent on customizing wording of user interfaces for the Australian public and ensuring privacy issues were addressed rigorously.

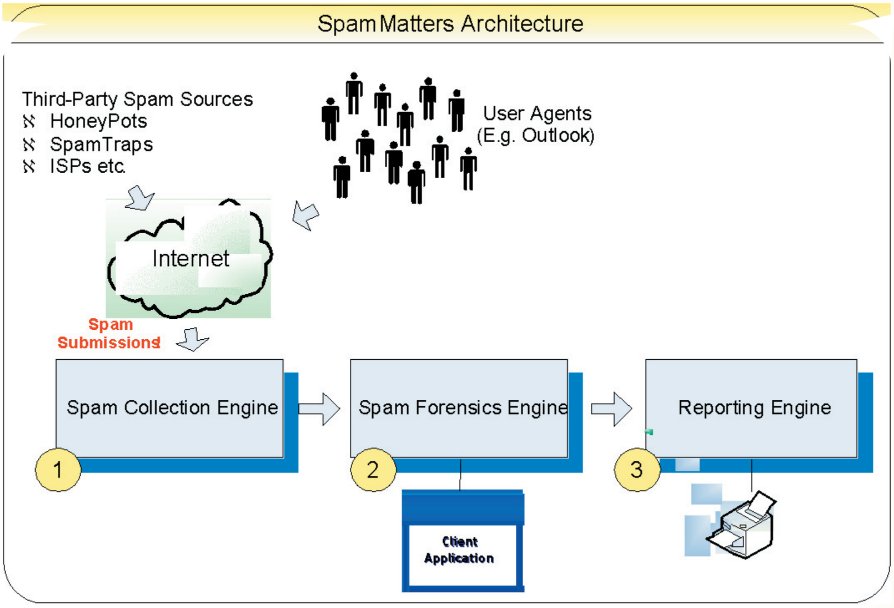


Figure 1: System Overview

SpamMATTERS provided the ACA with the required technical components that allowed the ACA to focus on spam enforcement and public concern issues – these components included:

- Hosting of Submission and Collation servers, in a secure co-location facility
- ACA branded submission clients for Outlook, Outlook Express, E-mail and Web Form
- SpamMATTERS forensic engine that analyzes and aggregates the e-mail data
- The SpamMATTERS Reporter Interface (Windows-based application) for ACA Investigators
- A secure encrypted link for ACA investigators to access forensic data.

The ACA provided:

- Web-based manuals that explained the new submissions systems to end-users
- Staff to provide support to end-users.

The SpamMatters Forensics Engine was custom configured for the ACA to look for particular types of spam and phishing emails, including:

- Spam and Phishing emails that originated from Australia
- Bursts of the biggest and worst spam globally every day (10 campaigns per day).

SpamMATTERS was easily customized for the specific detection requirements of the ACA. The SpamMATTERS 'Plugin' architecture allows new intelligence to be enhanced and evolved. For more information of this "Plugin" design, refer to the SpamMATTERS Deployment methodology white paper.

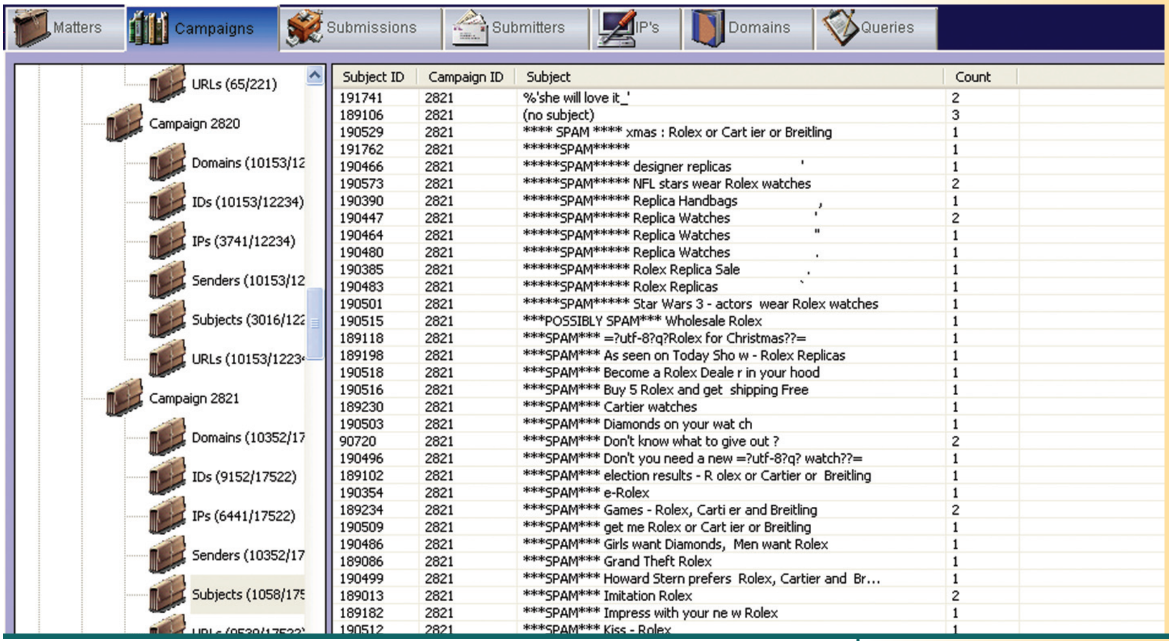
> *"No other vendor offered an end-to-end forensic solution like SpamMATTERS"*
>
> *John Haydon, Executive Manager.*
> *Consumer and Universal Services Obligation, ACA*

Results of the ACA Implementation

The SpamMATTERS system currently processes on average 50,000 e-mail submissions per day, with peaks of up to **200,000 messages per day**. Over the first four months of operation more than **3 million messages** have been submitted to the SpamMATTERS system. The growth in submissions is approximately 10% every month. The system architecture has been designed to perform extensive forensic analysis in volumes of potentially millions per day.

> *"SpamMATTERS' Collation Engine currently receives on average 50,000 e-mail submissions per day, with peaks of up to* ***200,000 messages per day****."*

Despite the volume of spam, the investigators can easily access information based on their needs. The SpamMATTERS Reporting engine extracts information and presents the forensic information in an easy-to-use Windows-based GUI (see Figure 2):



Subject ID	Campaign ID	Subject	Count
191741	2821	%'she will love it_'	2
189106	2821	(no subject)	3
190529	2821	**** SPAM **** xmas : Rolex or Cart ier or Breitling	1
191762	2821	*****SPAM*****	1
190466	2821	*****SPAM***** designer replicas '	1
190573	2821	*****SPAM***** NFL stars wear Rolex watches	2
190390	2821	*****SPAM***** Replica Handbags ,	1
190447	2821	*****SPAM***** Replica Watches '	2
190464	2821	*****SPAM***** Replica Watches "	1
190480	2821	*****SPAM***** Replica Watches .	1
190385	2821	*****SPAM***** Rolex Replica Sale .	1
190483	2821	*****SPAM***** Rolex Replicas `	1
190501	2821	*****SPAM***** Star Wars 3 - actors wear Rolex watches	1
190515	2821	***POSSIBLY SPAM*** Wholesale Rolex	1
189118	2821	***SPAM*** =?utf-8?q?Rolex for Christmas??=	1
189198	2821	***SPAM*** As seen on Today Sho w - Rolex Replicas	1
190518	2821	***SPAM*** Become a Rolex Deale r in your hood	1
190516	2821	***SPAM*** Buy 5 Rolex and get shipping Free	1
189230	2821	***SPAM*** Cartier watches	1
190503	2821	***SPAM*** Diamonds on your wat ch	1
90720	2821	***SPAM*** Don't know what to give out ?	2
190496	2821	***SPAM*** Don't you need a new =?utf-8?q? watch??=	1
189102	2821	***SPAM*** election results - R olex or Cartier or Breitling	1
190354	2821	***SPAM*** e-Rolex	1
189234	2821	***SPAM*** Games - Rolex, Carti er and Breitling	2
190509	2821	***SPAM*** get me Rolex or Cart ier or Breitling	1
190486	2821	***SPAM*** Girls want Diamonds, Men want Rolex	1
189086	2821	***SPAM*** Grand Theft Rolex	1
190499	2821	***SPAM*** Howard Stern prefers Rolex, Cartier and Br...	1
189013	2821	***SPAM*** Imitation Rolex	2
189182	2821	***SPAM*** Impress with your ne w Rolex	1
190512	2821	***SPAM*** Kiss - Rolex	1

Figure 2: SpamMATTERS Reporter

Public e-mail users can use a variety of methods to submit spam including the Outlook plug-in and the web-form. ACA's legal investigators then use the SpamMATTERS Reporter application to analyze and organise all the data and gather evidence against spammers.

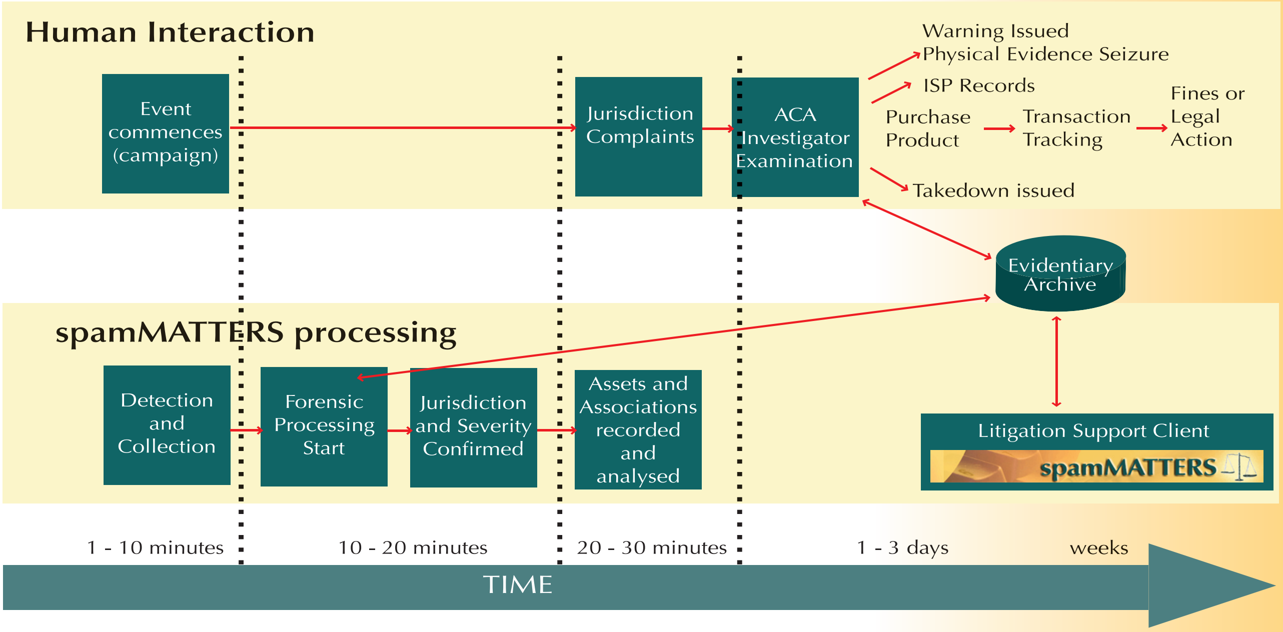


Figure 3: SpamMATTERS processes forensic data as spam is being sent

Forensic analysis is performed on submissions as the public, spamtraps or honeypots contributes them. As indicated in Figure 2, the detection of newly emerging spam campaigns is available within minutes of the event occurring:

- In the case of spam campaigns, this information can be used to identify the resources of the spammer that guide investigations.
- In the case of phishing, the data may be used to accelerate take-downs or to warn banking personnel.
- In the future, ACA will be using data to advise ISPs of compromised hosts in their networks.

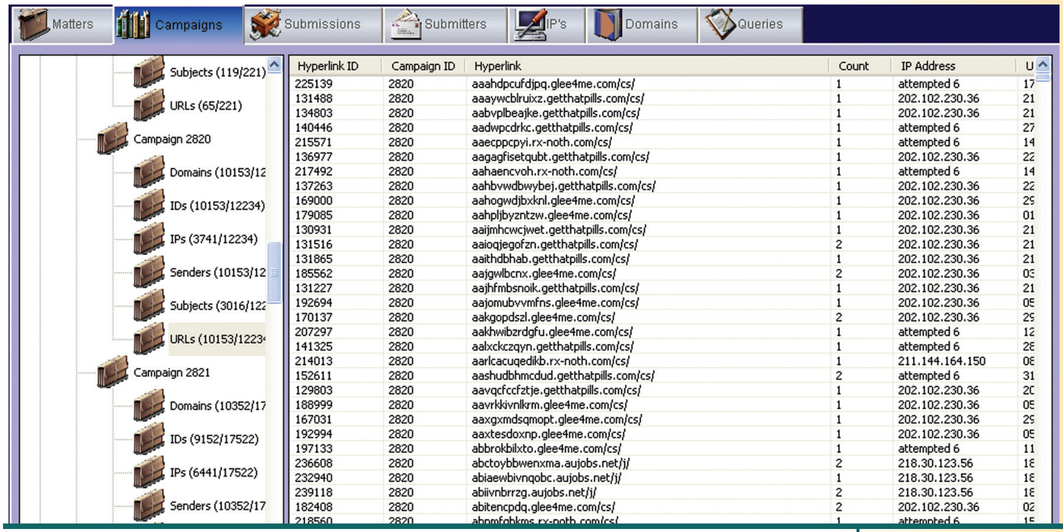
The SpamMATTERS implementation delivered on the key stated requirement from the ACA of empowering legal investigators:

i) Providing a method for collecting high-quality data and

ii) Enabling legal investigators to easily and cost-effectively collect evidence against spammers. This evidence can now be used in investigations or potentially court proceedings to prosecute spammers.

iii) Proof of non-compliance with the Australian spam Law by extracting and highlighting spamming techniques as: sender falsification, header manipulation, absence of (working) unsubscribe, use of proxies or zombies to deliver spam.

> *"With the MoU*'s signed with USA, UK and Korea, this technology gives us the ability to cross-jurisdictionally act rapidly. As more countries come up to speed with spam enforcement we are technically ready to work with them"*
>
> *"The deployment meets the requirements for spam enforcement under the Australian law. It allows us to deal with massive volumes of spam, which means we have a true metric of the spam activity on any given day. At the same time we eliminate the repetitive work in organizing and extracting evidence"*
>
> *John Haydon*
>
> **Memorandum of Understanding*



Subjects (119/221)
URLs (65/221)
Campaign 2820
Domains (10153/12
IDs (10153/12234)
IPs (3741/12234)
Senders (10153/12
Subjects (3016/122
URLs (10153/1223
Campaign 2821
Domains (10352/17
IDs (9152/17522)
IPs (6441/17522)
Senders (10352/17

Hyperlink ID	Campaign ID	Hyperlink	Count	IP Address	U
225139	2820	aaahdpcufdjpq.glee4me.com/cs/	1	attempted 6	17
131488	2820	aaaywcblruixz.getthatpills.com/cs/	1	202.102.230.36	21
134803	2820	aabvplbeajke.getthatpills.com/cs/	1	202.102.230.36	21
140446	2820	aadwpcdrkc.getthatpills.com/cs/	1	attempted 6	27
215571	2820	aaecppcpyi.rx-noth.com/cs/	1	attempted 6	14
136977	2820	aagagfisetqubt.getthatpills.com/cs/	1	202.102.230.36	22
217492	2820	aahaencvoh.rx-noth.com/cs/	1	attempted 6	14
137263	2820	aahbvwdbwybej.getthatpills.com/cs/	1	202.102.230.36	22
169000	2820	aahogwdjbxknl.glee4me.com/cs/	1	202.102.230.36	29
179085	2820	aahpljbyzntzw.glee4me.com/cs/	1	202.102.230.36	01
130931	2820	aaijmhcwcjwet.getthatpills.com/cs/	1	202.102.230.36	21
131516	2820	aaioqjegofzn.getthatpills.com/cs/	2	202.102.230.36	21
131865	2820	aaithdbhab.getthatpills.com/cs/	1	202.102.230.36	21
185562	2820	aajgwlbcnx.glee4me.com/cs/	2	202.102.230.36	03
131227	2820	aajhfmbsnoik.getthatpills.com/cs/	1	202.102.230.36	21
192694	2820	aajomubvvmfns.glee4me.com/cs/	1	202.102.230.36	05
170137	2820	aakgopdszl.glee4me.com/cs/	2	202.102.230.36	29
207297	2820	aakhwibzrdgfu.glee4me.com/cs/	1	attempted 6	12
141325	2820	aalxckczqyn.getthatpills.com/cs/	1	attempted 6	28
214013	2820	aarlcacuqedikb.rx-noth.com/cs/	1	211.144.164.150	08
152611	2820	aashudbhmcdud.getthatpills.com/cs/	2	attempted 6	31
129803	2820	aavqcfccfztje.getthatpills.com/cs/	1	202.102.230.36	20
188999	2820	aavrkkivnlkrm.glee4me.com/cs/	1	202.102.230.36	05
167031	2820	aaxgxmdsqmopt.glee4me.com/cs/	1	202.102.230.36	29
192994	2820	aaxtesdoxnp.glee4me.com/cs/	1	202.102.230.36	05
197133	2820	abbrokbilxto.glee4me.com/cs/	1	attempted 6	11
236608	2820	abctoybbwenxma.aujobs.net/j/	2	218.30.123.56	18
232940	2820	abiaewbivnqobc.aujobs.net/j/	1	218.30.123.56	18
239118	2820	abiivnbrrzg.aujobs.net/j/	2	218.30.123.56	18
182408	2820	abitencpdq.glee4me.com/cs/	2	202.102.230.36	02
218560	2820	abpmfgbkms.rx-noth.com/cs/	1	attempted 6	15

Figure 4: Obfuscated URLs in spam campaigns

Today, the SpamMATTERS solution supports the ACA to:

- Issue penalties including heavy fines
- Share evidence with the Australian Federal Police and other enforcement agencies across the globe
- Issue warnings to identified spammers (newly emerging)
- Potential for court action
- Issue advice to accidental spammers or uneducated marketing organizations.

At the time of publication of this case study, Australia has disappeared from the list of Top 10 spamming nations (as reported by http://www.spamhaus.org/statistics.lasso). The top 3 currently are: US, China and Korea.

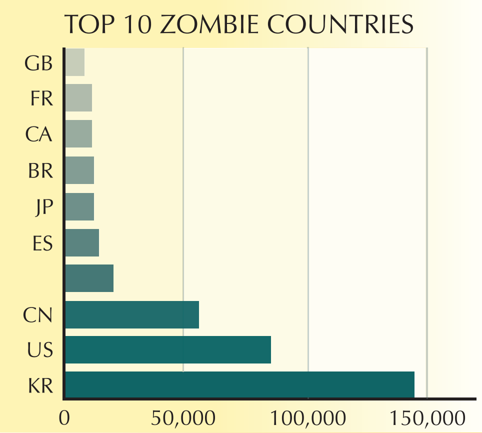


Figure 5: Tracking Zombie growth

Conclusion

Spammers are winning the spam war and are continuing to drive up the cost of e-mail for corporations, consumers, ISPs, network operators and others. Despite innovative AntiSpam solutions and new spam laws being implemented world-wide, the flood of spam emails continues to increase. A new type of forensic solution is required to enforce the growing number of spam laws, and attack the spammer with the full force of the law.

SpamMATTERS attempts to help fight the war on the legal battlefield, by empowering the courts to prosecute spammers. This is accomplished by providing a complete forensic solution that can:

i) Collect spam both from the public and third-party sources

ii) Perform forensic analysis on the data

iii) Package the evidence in a way that is acceptable to the courts.

SpamMATTERS' solution thereby stops the spam problem at its source. The ACA case study illustrates that the SpamMATTERS solution is quickly deployed and can be customized to country-specific requirements. The case study also demonstrates that laws, by themselves, will be largely ineffective in solving the spam problem, but that they can be made effective with appropriate enhancement tools.

The fight against spam also requires global collaboration that is rapid, efficient and effective. The SpamMATTERS system facilitates rapid data interchange between enforcement agencies across jurisdictions. This will accelerate takedowns, identify and disable spammers and present a credible threat to potential spam or phishers.

To better serve its customers, SpamMATTERS encourages close collaboration with Network Security and Antispam vendors. "Our focus is to deliver real-time enforcement solutions – by partnering with vendors the sharing of data will accelerate the resolution of emerging threats. Such a collaboration also sends a positive message to the community that there is a united team of specialists fighting spam, phishing and other threats", says David Jones, Founder & CEO of SpamMATTERS.

The combination of appropriate anti-spam technology and good forensics to support law enforcement against spammers is a potent combination in fighting spam – anti-spam technology focuses on fighting spam, while forensics in support of laws focuses on fighting spammers.

Authors' Biographies

Michael Osterman

Michael Osterman is the President and Founder of Osterman Research, a leading market research and analysis firm in the messaging industry. Osterman Research's recent report "*Spam in the Enterprise: Market Problems, Needs and Trends*" is one of the defining research reports regarding spam.

Roland Arlt

Roland Arlt is a Business Development Manager at Sensory Networks, the world's leading developer of OEM hardware acceleration technology for network security applications. Prior to Sensory Networks, Roland co-founded Cloudmark and Blue Tiger Networks, having begun his career at Goldman Sachs International.

spamMATTERS

USA 1 866 254 1530
Int'l +61 2 9412 3806
www.spammatters.com
info@spammatters.com