DAR II

Desenvolvimentos Avançados de Rede II - Segurança

COMBATE AO SPAM NA RCTS

FCCN Fundação para a Computação Científica Nacional

POS_Conhecimento Programa Operacional Sociedade do Conhecimento

RCTS Rede Ciência, Tecnologia e Sociedade

União Europeia FEDER

CERT.PT

Controlo de versões

Versão	Data	Estado	Autor
1	19-Fev-2007		João Pagaime

Aviso de confidencialidade

A quem se destina este documento

Gestores da Informática e Comunicações das Instituições ligadas à RCTS.

Índice

Índice de gráficos

Siglas / Acrónimos

BD – Base de Dados

DB - Database

DNS – Domain Name System

DoS – Denial of Service

FQDN – Full Qualified Domain Name

IETF - Internet Engineering Task Force

ISP – Internet Service Provider

MAPS RBL - Mail Abuse Protection System RBL

MTA - Mail Transfer Agent

MUA – Mail User Agent

NREN- National Research and Education Network

RBL - Real-time Black Lists

RCTS – Rede Ciência Tecnologia e Sociedade

SASL - Simple Authentication and Security Layer

SMTP – Simple Mail Transfer Protocol

SPF – Sender Policy Framework

SRS - Sender Rewriting Scheme

TLD – Top Level Domain

UBE - Unsolicited Bulk E-mail

UCE - Unsolicited Commercial E-mail

VPN – Virtual Private Network

1 Introdução

Uma fracção importante da quantidade de email que circula na Internet é spam, também designado de correio electrónico não solicitado, UCE, ou UBE.

O spam provoca gastos de tempo dos utilizadores para o eliminarem das suas caixas de correio, desperdiça largura de banda dos circuitos de ligação da Internet, e obriga a capacidades acrescidas em equipamentos e recursos humanos para manter os sistemas de email a funcionar em boas condições.

É habitual que os endereços de correio electrónicos com vários anos de existência ou que tenham sido publicados em páginas de Internet, recebam centenas de emails de spam por dia. Nestas condições é difícil lidar com tais endereços sem ajudas tecnológicas que tratem o spam automaticamente. Infelizmente tais medidas não são imunes a problemas de falsos positivos, em que um email legítimo é erroneamente classificado de spam e por isso não é lido pelo destinatário. Neste contexto o sistema email da Internet que outrora era considerado fiável, em que as mensagens eram entregues, ou então, se isso não fosse possível tecnicamente, o remetente receberia uma notificação de não-entrega, deixou de ser fiável. O sistema de email da Internet está progressivamente a perder fiabilidade, e consequentemente os utilizadores tenderão a perder confiança no sistema.

Não se vislumbra uma solução para o problema de spam, apesar de existirem várias propostas técnicas ou de outra natureza. O problema do spam, não podendo ser resolvido, pode ser mitigado através de uma gestão cuidadosa.

A FCCN tem promovido medidas para controlar o spam na RCTS, desde o controlo de relays-SMTP vulneráveis na rede, até à promoção da tecnologia SPF, entre outras medidas.

O problema do spam atingiu proporções tais que tem motivado o surgimento de medidas a níveis Nacional e Internacional, algumas das quais serão resumidas neste documento.

Serão também apresentado um levantamento de situação relativamente às outras NRENs Europeias.

Através das medidas técnicas apresentadas neste documento, a instalar em sistemas realizados de raiz ou comprados no mercado, é possível chegar a um sistema que filtre a maior parte do spam.

2 Iniciativas de combate ao spam na RCTS

Desde pelo menos o ano 2003 que o problema do spam tem merecido medidas de controlo especiais na RCTS. Actualmente o combate é realizado nas seguintes frentes:

- Atendimento de incidentes de segurança através do serviço CERT.PT. O CERT.PT trata incidentes de segurança relativos à RCTS, o que inclui queixas de spam.
- Controlo de relays-SMTP mal configurados. Uma das funções dos servidores de email é recebem email dos utilizadores e enviam-no para a Internet. Devem fazê-lo apenas para utilizadores controlados e não para qualquer cliente da Internet. Devido a problemas de configuração, alguns servidores fazem-no para qualquer cliente da Internet, o que pode ser explorado pelos spammers. A FCCN introduziu a política transcrita no "ANEXO I - Política Anti-spam na RCTS" para controlar estas situações.
- Promoção da adopção do SPF. O SPF é uma tecnologia que pretende legitimar se o computador que envia os emails está ou não autorizado a fazê-lo para um determinado endereço remetente.
- Realização de reuniões com ISPs Nacionais com vista a adopção de medidas anti-spam.

Actualmente a existência de relays-SMTP abertos já não se coloca como um problema grave, tendo vindo a ser resolvido à medida que os relays abertos foram tratados, e também pelo maior cuidado que os fabricantes de software MTA tem nas configurações por omissão que vem de fábrica.

3 SPF – Sender Policy Framework

Os domínios utilizam registos públicos (DNS) para direccionar pedidos de diferentes serviços (web, email, etc.) para as máquinas que prestam esses serviços. Os domínios já publicam registos para email (MX) que dizem ao mundo quais as máquinas que recebem mail para esse domínio.

O SPF funciona através da publicação de "reverses de MX" que dizem ao mundo quais as máquinas que enviam mail desse domínio. Quando recebe uma mensagem de um dado domínio, o receptor pode verificar esses registos para se assegurar de que o email provém de fonte "certificada".

O spam está numa escalada exponencial. Uma significativa maioria do spam é forjado. O SPF permite aos servidores de mail destinguir facilmente emails forjados dos verdadeiros. Saliente-se que o SPF funicona antes do corpo da mensagem ser transmitido, poupando largura de banda e tempo de CPU para filtrá-la.

3.1 Funcionamento

Suponhamos que um spammer forja um endereço de hotmail.com e tenta enviar spam.

Ele liga-se de um lugar não pertencente a hotmail.com. Quando ele envia a sua mensagem, ver-se-á na ligação SMTP:

MAIL FROM: <endereco_forjado@hotmail.com>

Mas não é necessário acreditar na sua "palavra". Pode-se perguntar ao Hotmail se o endereço IP é proveniente da sua rede. Se o Hotmail publicar um registo SPF, esse registo dirá ao sistema receptor se a máquina que enviou a mensagem está autorizada a fazê-lo em nome de hotmail.com.

Se o Hotmail diz reconhecer a máquina, a verificação é bem sucedida e o sistema receptor pode acreditar que a mensagem provém de onde diz. Se a mensagem falha o teste do SPF, é uma falsificação e esse poderá ser um forte indicador de se tratar de spam.

O SPF foi concebido para proteger o "envelope sender". Isto refere-se ao return-path que aparece no "MAIL FROM" e, em menor medida, ao argumento de HELO, que se supõe ser um FQDN.

A vasta maioria das implementações de SPF hoje em dia utilizam o return-path como objecto de autenticação e não se envolvem com o cabeçalho "From:"

3.2 Estratégia Geral de Implementação

Para que o esquema de SPF funciona, é necessário trabalho em duas frentes:

- publicação do registo de SPF no DNS;
- adaptação dos MTAs para verificarem registos SPF e agirem em conformidade com uma dada configuração, mediante a resposta.

Uma primeira aproximação de implementação de "apenas publicação do registo" num ISP levará, previsivelmente, apenas algumas horas; requererá coordenação entre os administradores dos serviços de email e os administradores do DNS. Note-se que não há, à partida, qualquer desvantagem na publicação deste registo, uma vez que a sua resposta "por omissão" pode ser configurada como "neutra" (não repudiante).

Depois, há que considerar o problema mais imediato (caso não esteja à partida resolvido) – utilizadores genuínos não conseguirão enviar email directamente a partir de localizações remotas. Por exemplo, um teletrabalhador pode querer enviar email de trabalho a partir de casa, através do servidor de email do seu ISP. Se o registo de SPF da sua empresa não contemplar esse servidor, tais mensagens genuínas poderão ser rejeitadas. A configuração de uma VPN seria uma solução algo "pesada" e complicada para o normal utilizador e, para o propósito em análise, parece "overkill".

Parece bastante mais aceitável configurar um servidor de SMTP para lidar com mail proveniente de fora da sua rede, ao qual os utilizadores se ligariam através de SASL com usernames e passwords atribuídos para autenticação, evitando assim a possibilidade de abusos.

Durante uma primeira fase, seria dado tempo aos utilizadores para mudarem para SASL SMTP e para se adaptarem à ideia de aumento de segurança. À medida que os ISPs fossem publicando registos de SPF, a detecção de spam aumentaria. Neste período de adaptação, dever-se-á configurar a resposta por defeito do sistema como "neutral" ou "softfail", para evitar provável exclusão de mensagens provenientes de utilizadores que ainda não estejam em conformidade com o sistema. Estes podem ser identificados através do próprio mecanismo de SPF, com a directiva "exists" – os logs de DNS detectarão "quem" tentou enviar um email e a partir de "onde", indevidamente.

Uma vez que todos os utilizadores tenham configurado algum tipo de mecanismo de envio com autenticação (SASL), pode-se anunciar o fim do período de transição para uma determinada data. Nesta data, a configuração "por omissão" do sistema passaria para "fail": tal protegerá o domínio de ser forjado e será respeitado pelos clientes utilizadores de SPF.

3.3 Problemas

O SPF "quebra" o mail forwarding, utilizado por alguns mail providers ou por utilizadores que simplesmente criam um ficheiro '.forward' num sistema Unix para reenviar correio de uma conta para outra. O problema é que o email reencaminhado não provém do domínio de origem – o do remetente – e é, por isso, ilegitimamente rejeitado pela verificação SPF.

A solução apresentada é o Sender Rewriting Scheme (SRS). Isto consiste num método de reescrever os headers da mensagem por forma a passar a verificação SPF, mantendo o endereço do remetente original de modo a que as respostas à mensagem sejam encaminhadas apropriadamente . Note-se que a questão de implementação de SRS apenas se põe para "mail forwarding providers".

O SPF não impede um spammer de comprar um domínio, criar um registo SPF para ele, utilizá-lo para enviar mensagens e depois descartá-lo assim que figurar nas "blacklists". Para se contrariar isto, podem ser montados mecanismos de "reputation management". Administradores de mail podem registar a percentagem de mensagens que são rejeitadas, provenientes de um determinado domínio. Outro critério pode ser a antiguidade do domínio – um domínio registado há poucas horas não deve ter motivos legítimos para enviar um vasto volume de mensagens.

Mas, mais importante que tudo isto: se os spammers forem obrigados a comprar domínios para "usar e deitar fora", já haverá um impacto no seu modelo de negócio. Além disto, os dados de registo dos domínios serão elementos adicionais para rastrear a sua real identidade.

Há aspectos deste protocolo que podem ser explorados por alguém de intenções maliciosas no sentido de minar a validade da verificação SPF:

- A avaliação depende largamente do DNS. Um atacante malicioso poderia envenenar a cache do DNS de um alvo com dados forjados e fazer com que a verificação retornasse valores incorrectos.
- O endereço IP é presumido como sendo genuíno e correcto. Um atacante malicioso poderia forjar sequencias TCP para fazer com que um email parecesse provir de uma máquina autorizada, pela qual o atacante se faz passar.
- Tal como em muitos aspectos do email, há várias maneiras de entidades maliciosas utilizarem este protocolo como mecanismo de causa de ataques de negação de serviço distribuídos (DDoS):
- Como as implementações das verificações SPF necessitam de uma limitação no número de "includes" e "redirects" e/ou verificação de "loops", domínios maliciosos podem publicar registos que excedam esses limites numa tentativa de desperdiçar esforço computacional por parte dos seus alvos, ao receberem mail.
- Entidades maliciosas podem enviar grandes volumes de email, fazendo-o passar como provindo de um pretendido alvo, para uma grande variedade de servidores de

email legítimos. Estes servidores, então, exerceriam grande carga no DNS do alvo, ao efectuarem as verficações nos respectivos registos SPF.

3.4 Indicadores de utilização, depuração e registos

Para efeitos de indicadores de utilização, depuração (debug) e registos (logs) e possível configurar o SPF de tal forma que as consultas SPF fiquem registadas.

Isso permite saber que endereços IP tentaram enviar email por um determinado domínio e falharam. Isso pode ser útil para diagnosticar eventuais problemas com servidores legítimos, mas que, por esquecimento ou desconhecimento inicial, não foram registados no DNS.

Na caixa abaixo está transcrito um registo SPF onde a possibilidade de registo das consultas SPF foi actividade. Note-se as letras reforçadas.

```
cert.pt.                14400   IN      TXT     "v=spf1 ip4:193.136.2.194
ip4:193.137.198.36 ip4:193.137.198.37 ip4:193.137.198.38 ip4:193.137.198.39
+exists:%{i}._.%{h}._.%{s}._.%{r}.spflog.cert.pt -all"
```

A primitivas que estão a letra reforçada na caixa acima obrigam a que o sistema que faça a consulta SPF, realize uma pergunta ao sistema DNS com parâmetros especiais. Através do funcionamento normal do DNS, pergunta ficará registada no servidor DNS responsável pelo domínio "spflog.cert.pt". Os parâmetros especiais, ou macros, "%{i}", "%{h}", "%{s}" e "%{r}", são substituídos pelo sistema que faz a consulta SPF antes de realizar a pergunta DNS.

3.5 Ponto de situação

O SPF está publicado como RFC experimental "4408" desde Abril de 2006. Ao mesmo tempo foi publicada outra proposta alternativa da Microsoft:

- RFC 4405 – SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message - proposta da Microsoft;
- RFC 4406 – Sender ID: Authenticating E-Mail - proposta da Microsoft;
- RFC 4407 - Purported Responsible Address in E-Mail Messages - proposta da Microsoft.

O IETF não apoia uma das abordagens em detrimento da outra, e convida a comunidade a observar os resultados durante dois anos após publicação dos RFCSs, no sentido de, finalizado esse tempo, se ter chegado a um consenso.

Publicação SPF nos domínios de .PT

Fez-se um estudo da utilização do SPF nos domínios em .PT, com os resultados apresentados em seguida.

Dos 82.143 domínios delegados em .PT, 3.510, ou seja 4,3%, apresentaram registos SPF. Desses, a acção por omissão está expressa no gráfico de barras seguinte.

Dos registos SPF, 102 eram do tipo "spf2", ou seja, do tipo "sender-id".

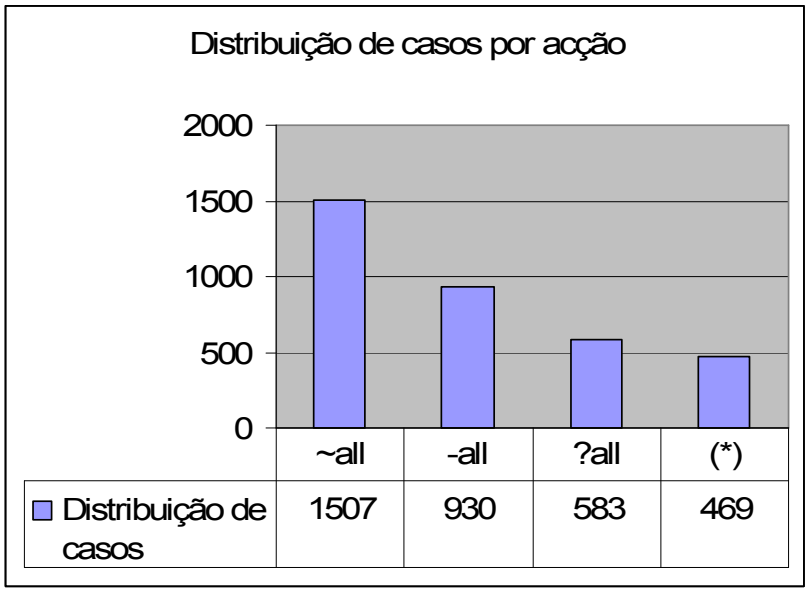

Gráfico 1- SPF - distribuição de casos

Os casos "~all", "-all", "?all" correspondem à acção a tomar pelo MTA que recepciona o email, quando concluiu que o enviador do email não está autorizado pelo SPF a enviar email pelo domínio em análise.

Os casos, ou acções a tomar, são:

- "~all" – softfail – os MTA não devem rejeitar email com base somente com esta indicação, podendo fazer mais verificações ao email;
- "-all" – fail - os MTA devem rejeitar este email;
- "?all" – Neutro – a mesma coisa do que passar no teste (existe apenas para efeitos informativos).
- "(*)" – não tem cláusula "all", não tendo portanto uma acção definida para sistemas não especificados no restante registo SPF.

Negações SPF no Megamail

O gráfico abaixo representa o número de emais por dia descartados à entrada do sistema Megamail nos últimos 75 dias.

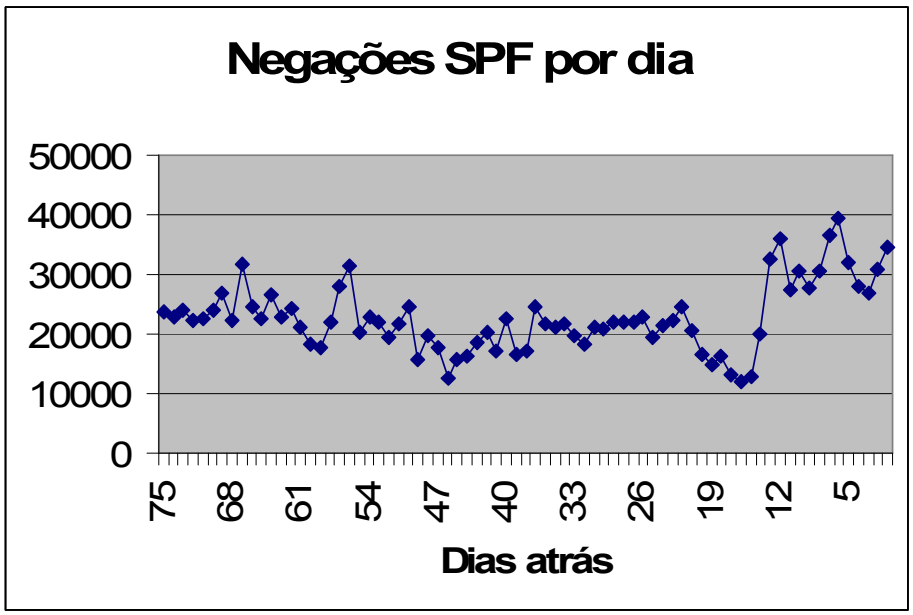

Gráfico 2 - Negações SPF por dia no Megamail

São descartados por dia cerca de 22.700 emails devido a verificações SPF. Como o sistema Megamail recebe cerca de 200.000 emails por dia, concluí-se que as rejeições SPF já chegam a um número não desprezável de mais de 10%.

3.6 Recomendações da FCCN/CERT.PT

A FCCN/CERT.PT recomenda às instituições utilizadoras da RCTS a utilização do SPF, quer na publicação DNS quer na consulta ao SPF, prestando suporte técnico via contactos do CERT.PT.

3.7 Resumo

A adopção em larga escala do SPF tornaria difícil a proliferação do spam, já que obrigaria à utilização e posterior descarte de domínios, o que teria custos importantes para o spammer.

A descrição técnica do SPF, vertida em RFC, encontra-se em fase experimental pelo menos por mais dois anos, havendo duas soluções técnicas concorrentes. Há ainda desafios

técnicos a resolver sobretudo com o reecaminhamento de emails, que, por causa do SPF, precisa de ser mais elaborado para passar nas verificações.

A adopção do SPF ainda não está massificada, mas já permite o descarte de um número expressivo de spam em sistemas de alto volume, como por exemplo o Megamail.

4 Iniciativas de âmbito Nacional e Europeu

Observa-se que as iniciativas de génese governamental tem sido mais de cariz legislativo e de tentativa de despertar o público e organizações responsáveis para este problema. Por "organizações responsáveis" entenda-se as organizações que possam ter um papel central como os ISPs ou reguladores de telecomunicações.

A União Europeia emitiu uma directiva no sentido de que o envio de correio comercial seja feito apenas quando há consentimento prévio para esse envio (sistema de opt-in). Portugal adoptou essa directiva, mas isso tem efeitos práticos limitados já que a natureza do spam é trans-Europeia, e, por vezes, avessa ao cumprimento das leis. Existe na Internet concentração da informação anti-spam debaixo da "European Contact Network of Spam Enforcement Authorities (CNSA)".

Em Portugal o problema do spam é das competências da ANACOM. De acordo com o Decreto-Lei n.º 7/2004, de 7 de Janeiro, relativo ao comércio electrónico, a ANACOM foi designada entidade de supervisão central, com competências sobre todos os domínios regulados neste diploma, incluindo a matéria das comunicações não solicitadas, ou spam, salvo nas matérias em que lei especial atribua competência sectorial a outra entidade.

No ano de 2005 foi lançada uma iniciativa anti-spam Nacional que pretende congregar os ISPs numa plataforma técnica única. O projecto encontra-se numa fase de estabelecimento de acordos entre os intervenientes.

4.1 Plataforma Nacional anti-spam

A plataforma Nacional anti-spam pretende vir a ser um sistema capaz de ajudar os operadores de email de grande volume a identificar e rejeitar spam.

A ideia centra-se em disponibilizar uma base de dados com aquilo que foi considerado spam por uma base alargada de utilizadores. O spam tende a ser um fenómeno local, sendo portanto útil tal BD a nível Nacional.

As instituições aderentes poderiam então, quando recebessem um email, consultar a plataforma no sentido de obter uma indicação sobre esse email em análise, ou seja, se seria ou não spam.

Actualmente os operadores de email, normalmente associados a ISPs, já tem mecanismos para o utilizador reportar spam. Tipicamente isso passa por ter um botão no Mail User Agent, ou então ter uma caixa de correio especial para o utilizador ir depositando o spam recebido. Havendo estes mecanismos, não é difícil alterá-los para enviar o spam, ou um resumo deste, para uma plataforma central.

A consulta à plataforma poderia ser feita através do DNS, ou seja, seriam criadas zonas DNS cujas respostas dariam indicação da classificação de spam de endereços IP ou mesmo de emails. A consulta estritamente por endereço IP dá a reputação desse endereço. Se no passado tiver sido enviado spam desse endereço, então este terá uma má reputação. Este mecanismo de consulta via DNS está bem suportado nos sistemas Mail Transfer Agent.

Informações mais detalhadas pode ser encontradas no "ANEXO II - Plataforma Nacional anti-spam".

5 Ponto de situação nas NRENs

O quadro abaixo resume o apuramento do sistemas de tratamento de spam nas NRENs Europeias, congéneres da FCCN, ligadas ao GEANT2.

NREN	Serviços de tratamento spam
 [off-site] ACOnet Website of ACOnet - Austrian NREN	Serviços de tratamento spam não encontrados
 [off-site] ARNES Website of ARNES - Slovenian NREN	Serviços de tratamento spam não encontrados
 [off-site] BELNET Website of BELNET - Belgian NREN	Serviços de tratamento spam não encontrados
 [off-site] CARNet Website of CARNet - Croatian NREN	Serviços de tratamento spam centrais não encontrados. Tem serviços de email: *E-mail addresses - possibility of using the e-mail service.*
 [off-site] CESNET Website of CESNET - Czech NREN	Serviços de tratamento spam não encontrados. Encontrado o seguinte documento técnico: *(Overview and recommendations for anti-spam tools). Technical report number 14/2005, CESNET, 2005 http://www.cesnet.cz/doc/techzpravy/2005/antispam/*
 [off-site] CYNET Website of CYNET - Cypriot NREN	Dificil procurar
 [off-site] DFN Website of DFN - German NREN	Parece haver uma arquitectura, mas não foi possível encontrar descrição de serviço

[off-site] EENet Website of EENET - Estonian NREN	Serviços de tratamento spam centrais não encontrados. Tem serviços de email: *E-mailboxes in EENet`s server*
[off-site] GARR Website of GARR - Italian NREN	Serviços de tratamento spam não encontrados
[off-site] GRNET Website of GRNET - Greek NREN	Backup Mailing Exchanger Service. Descrição de service: *When the Backup Mail Exchanger service is provided to a domain mail server, a backup space is provided in order to temporarily store e-mails directed to this domain in case of mail server connectivity failure. The service* ***is combined with antispam filtering techniques****, as black lists (RBL filtering), and it is provided to the E-Mail domains which are associated with the GRNET clients and the GRNET projects.*
[off-site] HEAnet Website of HEAnet - Irish NREN	*Anti Spam Service – MAPS RBL+*
[off-site] ISTF Website of ISTF - Bulgarian NREN	Serviços de tratamento spam centrais não encontrados. Tem webmail.
[off-site] IUCC Website of IUCC - Israeli NREN	Dificil procurar
[off-site] JSCC Website of JSCC - Russian NREN	Dificil procurar

[off-site] LATNET Website of LATNET - Latvian NREN	Parece haver alusões a filtragem de spam – "spam filtr□šana".
[off-site] LITNET Website of LITNET - Lithuanian NREN	Dificil procurar
[off-site] NIIF Website of NIIF - Hungarian NREN	Dificil procurar
[off-site] NORDUnet Website of NORDUnet - Nordic NREN	Não parece ter. Afiliadas não verificadas
[off-site] PSNC Website of PSNC - Polish NREN	Dificil procurar
[off-site] RedIRIS Website of RedIRIS - Spanish NREN	Descrição: Servicio de Correo Electrónico en la Comunidad RedIRIS: IRIS-MAIL • REd de Sensores de Antivirus de la Comunidad Académica Servicio MailBackup • Tiempo máximo de almacenamiento: 10 dias. • Intentos de reenvio: 10 horas. • SpamHausp Block List. • Open Relay DataBase
[off-site] RENATER Website of RENATER - French NREN	Serviços de tratamento spam não encontrados
[off-site] RESTENA Website of RESTENA - The Luxembourg NREN	WEBMAIL L'interface Webmail permet aux utilisateurs de lire leurs messages directement sur le web dans un environnement convivial et sécurisé.

	webmail.restena.lu PROTECTION ANTI-spam / ANTI-VIRUS La protection anti-spam / anti-virus comporte un système de filtrage qui protège les boîtes aux lettres des utilisateurs contre les spam et les virus. Le système permet la détection et le marquage des messages de spam. Les pièces jointes aux courriers électroniques entrants sont également analysées. POUR LES INSTITUTIONS COMPTES E-MAIL EN LIGNE Le service comprend la mise à disposition aux institutions d'un outil simple, complet et convivial permettant la gestion des comptes e-mail centralisés en ligne. Les création, modification, suppression et redirection des adresses sont gérées par le service administratif de l'institution en question à travers une interface web. **ANTI-spam/ANTI-VIRUS CENTRALISÉ** Le service anti-spam/anti-virus centralisé est basé sur un serveur relais de courrier électronique qui fonctionne comme station intermédiaire entre l'extérieur (Internet) et le serveur mail propre de l'institution. Cette passerelle garantit ainsi la protection de la messagerie interne de l'institution.
RoEduNet [off-site] RoEduNet Website of RoEduNet - Romanian NREN	Serviços de tratamento spam não encontrados. Terá serviço de backup-MX
sanet. [off-site] SANET Website of SANET - Slovakian NREN	Serviços de tratamento spam não encontrados. Terá serviço *Mail hosting (access through POP3 or UUCP)*
SURFnet [off-site] SURFnet	Serviço encontrado: *The Mail Filter can be used to*

Website of SURFnet - NREN in the Netherlands	*check and filter email messages on viruses and spam before they are delivered to the institutions mail server.*
[off-site] SWITCH Website of SWITCH - Swiss NREN	Serviços de tratamento spam não encontrados
[off-site] UKERNA Website of UKERNA/JANET - United Kingdom NREN	Serviço encontrado: *The JANET Mailer Shield service helps make an organisation's mail facilities more secure and robust, particularly where the organisation is small or its resources for managing e-mail are limited.*
[off-site] ULAKBIM Website of ULAKBIM - Turkish NREN	Dificil procurar
[off-site] University of Malta	Serviços de tratamento spam não encontrados

O gráfico seguinte resume a distribuição de casos por NREN.

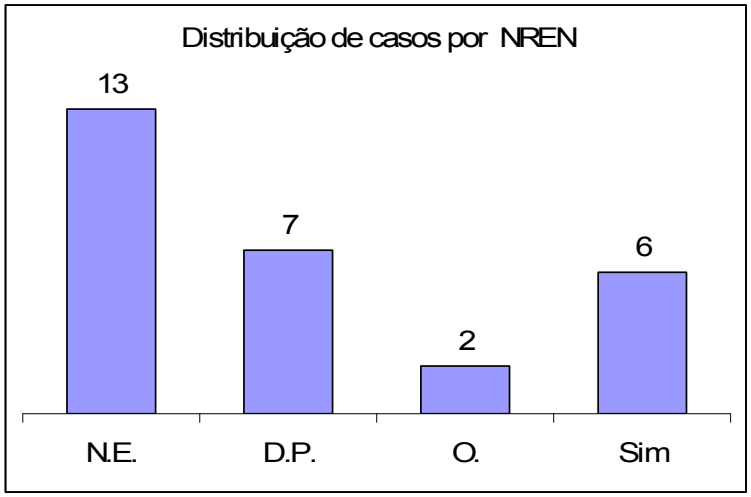

Gráfico 3- Distribuição de casos por NREN

LEGENDA:

- "N.E." - Não foi encontrada a existência de filtragem anti-spam;
- "D.P." – Difícil procurar por dificuldades linguísticas;
- "O." – Outro caso;
- "Sim" – Tem filtragem anti-spam;

5.1 Descrição dos casos de interesse

Descrição do caso "GRNET - Grécia"

A NREN disponibiliza o service de Backup Mail Exchanger para os domínios das Instituições utilizadoras. O serviço é combinado com técnicas anti-spam como filtragem black-lists - RBL.

Descrição do caso "HEAnet – Irlanda"

Em associação com o MAPS LLC oferece service anti-spam aos seus utilizadores sem custos adicionais.

O serviço Mail Abuse Prevention Realtime Blackhole List ou RBL+ é conhecido como um método de reduzir o volume de mensagens indesejadas, reconhecendo sítios da Internet que foram origem de spam no passado.

Pode ser mantida uma white-list pelas organizações utilizadoras para ultrapassarem a política de filtragem geral.

Como aderir ao serviço:

1. Enviar email de pedido com detalhes do software;
2. Assinatura dos termos de utilização;
3. Envio dos detalhes de configuração – nem todos os servidores são compatíveis;
4. Após configuração o email começa a ser filtrado.

Mais informação pode ser encontrada no endereço http://www.heanet.ie/downloads/AntiSpam.pdf.

Descrição do caso "RedIRIS - Espanha"

A NREN disponibiliza o service de Backup Mail para os domínios das Instituições utilizadoras.

O serviço é combinado com técnicas anti-spam:

- SpamHausp Block List. - http://www.spamhaus.org/
- Open Relay DataBase (http://www.ordb.org/ - este serviço terá sido desactivado em Dezembro de 2006)

Tem anti-vírus para vírus de alta-difusão.

O quadro abaixo dá um exemplo de configuração por parte de uma instituição utilizadora, que tivesse o domínio "org.es".

```
org.es     IN    MX    10  estafeta1.org.es.
```

```
        IN    MX   20  estafeta2.org.es.

        IN    MX   30  mail.rediris.es.
```

Nota-se que este exemplo de configuração não é eficaz contra spam, já que o spam será filtrado pelo serviço "Backup Mail" apenas se os dois servidores de maior prioridades estiverem indisponíveis.

Descrição do caso "RESTENA – Luxemburgo"

Com serviço centralizado ANTI-spam/ANTI-VIRUS, provavelmente com configuração via relay-SMTP.

Descrição do caso "SURFnet – Holanda"

Nome do serviço: MailFilter. Pode ser usado para verificar e filtrar mensagens por vírus e spam antes de serem entregues ao servidor de email da Instituição.

As propriedades do filtro podem ser configuradas com requisitos locais através de interface web.

Descrição do caso "UKERNA/JANET – Reino Unido"

Serviço de MAPS RBL+ na JANET.

Subscrição do serviço Mail Abuse Prevention System LLC (MAPS, agora parte da "Trend Micro") em benefício de todas as Instituições utilizadoras.

Serviço Mailer Shield

Website of UKERNA/JANET - United Kingdom NREN Serviço encontrado: *The JANET Mailer Shield service helps make an organisation's mail facilities more secure and robust, particularly where the organisation is small or its resources for managing e-mail are limited.*

5.2 Resumo

Ao nível das NRENs assiste-se sobretudo a ausência de serviços centrais de filtragem de spam. As que tem tais serviços disponibilizam sistemas de filtragem básicos,

presumivelmente de baixa interactividade e integração com os utilizadores finais e seus sistemas envolventes, e com baixa probabilidade de falsos positivos. Evita-se a análise do conteúdo dos emails.

Os sistemas de filtragem de spam mais eficazes precisam de estar integrados com os utilizadores finais, e de analisar o conteúdo das mensagens. A integração com o sistema dos utilizadores permite

- Que a filtragem beneficie de aprendizagem por classificação local realizada pelos utilizadores;
- Que se possa configurar uma caixa de correio de spam, onde os emails classificados como spam são depositados e fiquem acessíveis aos utilizadores.

A utilização de caixas de correio para spam, consultáveis pelos utilizadores, permite que se adoptem métodos de classificação automática de spam mais agressivos, e portanto com maior risco de falsos positivos, numa perspectiva de que o utilizador verifique regularmente a caixa de correio para spam salvar alguns casos de falsos positivos.

6 Contra medidas técnicas

Não existe solução definitiva para o spam, nem a abordagem para mitigar o problema deve ser unicamente técnica. As contra medidas devem ser também de natureza regulatória, de educação e cooperação.

Porém com medidas unicamente técnicas é possível rejeitar uma elevada quantidade de spam. As medidas descritas tendem a desactualizar-se com o tempo já que os spammers adaptam-se às condições, havendo portanto um circulo de adaptações entre a actividade de spamming e remédios aplicáveis.

As contra medidas técnicas são mais eficazes se forem usadas várias, de tipos diferentes, em conjunto e num equilíbrio continuamente regulado ao longo do tempo. No processo de recepção de email, pode-se por exemplo fazer um conjunto de verificações básicas nos

passos iniciais da ligação SMTP, e depois, se o email passar essas verificações, aplicar um sistema de classificação heurística.

Também é usual atribuir pontuação aos emails com base em critérios variados, e no fim do processo de verificações dar um destino ao email consoante a pontuação final. O destino pode ser, por exemplo, o descarte do email, deixar passar sem alterações, ou colocar o email numa caixa de correio especial.

6.1 Quadro resumo

Medidas que não precisam de analisar o conteúdo do email

Nome	**Descrição**	**Onde**	**Riscos/problemas**
SPF e/ou Sender-ID	Informa a Internet dos sistemas autorizados a enviar email por um determinado domínio (dificulta a usurpação de domínios)	• Publicação DNS • Verificação no MTA	Baixo risco de falsos positivos; Possíveis problemas com re-direcção de email
Existência de domínio do emissor	Rejeitar email se o domínio de origem não existe. Refinamento: rejeitar se domínio origem não tiver MX-record	Verificação no MTA	Baixo risco de falso positivos
Greylisting	Dar um erro de recepção temporário quando surgem endereços IP novos a tentar enviar email	No MTA	Baixo risco de falso positivos
Blacklist/whitelist	Consultar listas para saber da reputação do endereço IP que estão a tentar enviar email	Verificação no MTA	Qualidade das listas variam muito. Assiste-se na prática a falsos positivos. É necessário ter uma whitelist para contrariar entradas indesejadas na blacklist

Existência de registo PTR	Rejeitar email se o endereço IP não tiver resolução do endereço para um nome	Verificação no MTA	Assiste-se na prática a falsos positivos
DKIM ou META	Validação via sistema criptográfico. Baixa utilização	Verificação no MTA	-

Medidas que precisam de analisar o conteúdo do email

Nome	**Descrição**	**Onde**	**Riscos/problemas**
Filtragem por palavras chave	Descartar email com determinadas palavras chave.	• No MTA • No MUA (software do utilizador)	Facilmente contornável pelos spammers e muito sujeito a falsos positivos
Resumo (fingerprint) de mensagens	Resume-se os emails considerados spam num fingerprint. Emails seguintes com o mesmo resumo (fingerprint) ficam eleitos para serem descartados	• No MTA • Teoricamente no MUA	Precisa de uma boa base de dados de spam; O algoritmo de resumo pode precisar de constantes melhoramentos à medida que os spammers se adaptam
Filtragem heurística	Classificação com base na forma do email – tem ou não HTML, etc. Tem um processo de aprendizagem.	• No MTA • Teoricamente no MUA	Precisa de uma boa base de dados de spam; Sujeito a falsos positivos

Bayesianos	Filtragem por vocabulário. Tem um processo de aprendizagem. Usa uma BD de referência que precisa de ser mantida actualizada. Tem alto potencial de filtragem quando mesmo quando usado isoladamente	• No MTA • Teoricamente no MUA	Precisa de uma boa base de dados de spam; Sujeito a falsos positivos; A parametrização deve ser feita em grupos que usem vocabulário comum

Outras Medidas

Nome	**Descrição**	**Onde**	**Riscos/problemas**
Filtragem comportamental	Limitar acesso ao serviço SMTP de sistemas que apresentem comportamentos desviados. Rate-limit. Mais usado para proteger o serviço SMTP na globalidade	• No MTA	Pode gerar acumulação de emails noutros pontos da Internet
Desafio/resposta	Aceitar email apenas depois do remetente ter respondido com sucesso a um desafio, como por exemplo a cópia de um palavra chave no desafio	• No MTA • Potencialmente no MUA	Não entrega de emails legitimos; Entrega de desafios (emails) a utilizadores inocentes; Potencial de dead-lock se o sistema não foi cuidadosamente codificado

HELO/CSV (Certified Server Validation)	Rascunho no IETF - draft-ietf-marid-csv-intro-02	No MTA	
Micropagamento	Criar um sistema de email em que cada mensagem seria paga – proposto pela Microsoft	Vários - Alterações profundas ao sistema de email	

6.2 Sem análise de conteúdo do email

As medida apresentadas de seguida baseam-se em testes simples, não examinando o conteúdo dos emails. São medidas com fraca probabilidade de ter falsos positivos.

SPF e/ou Sender-ID

As configurações a realizar são a dois níveis:

- Publicar os registos no DNS para protecção do domínio (por exemplo "instituicao.pt");
- Configurar os MTAs da instituição para fazer verificações SPF.

Recomenda-se a utilização de pelo menos do SPF. O SPF está descrito detalhadamente na secção "3" deste documento.

Existência de domínio do emissor

Por vezes os spammers usam um domínio inexistente para envio de spam. Recomenda-se que se façam validações do domínio de origem, ou seja, não aceitar o email se o domínio de origem não existir.

Um refinamento desta técnica consiste em não deixar passar o email se o domínio existir, mas não tiver um registo MX.

Greylisting

Actualmente grande parte do spam é enviado a partir de zoombies, ou seja, de computadores com a segurança comprometida e controlados pelos spammers. Os zoombies são maioritariamente computadores domésticos, cujo dono não se apercebe da situação.

Os motores de spam instalados nos zoombies tendem a ser simples e evitam o consumo elevado de recursos no computador para escapar à detecção do utilizador. Por causa disso os sistemas encarregues de enviar spam tipicamente não se dão ao trabalho de tentar repetir o envio se não conseguirem entregar o email na primeira tentativa.

Tirando partido disso, surgiu uma nova técnica de protecção que consiste em negar a recepção de email para endereços IP desconhecidos, retornando ao emissor um erro temporário. Se for um MTA legítimo a receber esse erro temporário, tentará reenviar o email passado poucos minutos (tipicamente cerca de 15 minutos), mas se for um motor de spam a receber o erro, provavelmente não tentará novamente. O MTA de recepção mantém memória dos sistemas que efectuaram nova tentativa de envio e passa-os para uma "whitelist", dispensando-os no futuro no futuro de terem que fazer a entrega em dois passos.

Se no futuro a adopção do greylist se tornar generalizada é de esperar que os spammers adaptem os seus motores e envio para fazerem múltiplas tentativas de envio.

Existência de registo PTR

Normalmente os servidores tem um registo DNS que dá o nome através do endereço IP. Tradicionalmente são os servidores que enviam email na Internet. Um computador que tente enviar email a partir de um endereço IP sem registo PTR é suspeito.

Não se recomenda a negação de emails só com base neste critério.

Blacklist/whitelist

Estas listas de IPs permitem aferir da reputação de um determinado endereço IP, e, concretamente, se terá ou não enviado spam no passado. Existe elevada variação da qualidade destas listas, importando por isso escolher cuidadosamente a lista que se configure no MTA. A gestão de blacklists, designadamente o atendimento a pedidos de remoção de endereços IP, é um processo consumidor de recursos, dai a variação de qualidade mencionada. Na prática observa-se que alguns endereços legítimos vão parar às blacklists, sendo portanto necessário operar também uma whitelist que valide determinados endereços, mesmo que estejam na blacklist.

Uma variação das blacklists são as listas de endereços IP que, por definição prévia, não devem enviar email. Exemplo disso são as gamas de endereços IP de clientes ADSL residenciais.

A consulta às listas faz-se normalmente através do DNS

DKIM ou META

Sistema que recorre a criptografia – assinatura de emails. Actualmente a sua utilização é muito baixa.

6.3 Com análise de conteúdo do email

A análise de conteúdo de email, também designado de filtragem, é a técnica mais comum anti-spam. Pode ter resultados espectaculares, filtrando a maioria do spam, mas verifica-se na prática que tem falsos positivos. Precisa de constante alimentação das base de dados de referência.

Filtragem por palavras chave

É uma filtragem simples por palavras chave presentes nos emails. São facilmente contornáveis pelos spammers, bastando para isso escrever as palavras com erros ortográficos, mas cujo sentido ainda seja perceptível para os humanos.

Resumo (fingerprint) de mensagens

Com esta técnica caracteriza-se resumidamente uma mensagem de spam, previamente classificada por utilizadores, guardando para referencia futura esse resumo. Novas mensagens são também resumidas sendo verificado se o esse resumo já se encontra na base de dados de spam. Se se encontrar, a mensagem é dada como spam, ou pelo menos é-lhe acrescido a probabilidade de ser spam.

Filtragem heurística

A filtragem heurística basea-se no principio de que as mensagens de spam terem características tipificadas, como por exemplo a ampla utilização de HTML com muitas imagens ou títulos muito chamativos. Estes testes são pesados através de um processo de aprendizagem onde são disponibilizados emails legitimos e de spam.

Estes sistemas tipicamente consomem recursos computacionais importantes, como CPU e memória.

Bayesianos

Um motor de filtragem Bayesiano aprende progressivamente o vocabulário utilizado nos emails, distinguindo o spam dos emails legítimos. A alimentação do motor é conduzida pelos utilizadores ou administradores de sistemas. Este tipo de filtros é mais adequado ao nível de um grupo em que existe um vocabulário comum.

Estes filtros são altamente eficazes quando utilizados individualmente, e são uma das poucas soluções que, quando usada isoladamente, consegue filtrar quase todo o spam após a fase de treino do motor de filtragem.

6.4 Outras medidas

Desafio/resposta

Com este método desafia-se o remetente do email a resolver um problema, e, só depois dessa barreira ultrapassada com sucesso, o email é entregue ao utilizador.

O desafio pode ser simplesmente responder a um email, copiando uma password que lá conste.

Exemplo do fluxo de emails com um sistema de desafio resposta:

1. Aparece um email novo;
2. Caso o remetente não esteja numa whitelist, o destinatáro gera automaticamente uma password e desafia o remetente do email a devolvê-la;
    - O remetente recebe a password, e devolve-a (resposta);
    - A password é validada e o email do ponto "1" é finalmente entregue, sendo o remetente colocado numa whitelist.

Para o sistema ser mais prático, deve ser combinado com whitelists para endereços pré-configurados ou que já tenham passado o teste no passado.

Este sistema elimina todo o spam mas é algo radical e tem pelo menos os seguintes inconvenientes:

- Alguns utilizadores não conseguirão ou não estarão dispostos a responder ao desafio;
- O remetente é normalmente forjado no spam pelo que o desafio seria entregue, em muitos casos, a utilizadores inocentes;
- Este sistema tem potencial para entrar em "dead-lock" se um desafio tiver como resposta outro desafio.

7 Software, Produtos e serviços

Como seria de esperar a oferta do mercado reagiu ao problema do spam, disponibilizando um vasto leque de soluções, passando por:

- Appliances - Equipamentos pré-carregados com software de filtragem de email, prontos a funcionar com um mínimo de configurações do administrador de rede;
    - Ex: Ironport; Barracuda Spam Firewall; Panda GateDefender Performa;
- Software especifico de filtragem para instalação em computadores dos utilizadores;
    - Ex: SpamAssassin - http://wiki.apache.org/spamassassin/; Kaspersky Anti-Spam;
- Serviços geridos (managed services) – nesta modalidade faz-se passar todo o email da organização por uma entidade terceira que retira o spam do fluxo de emails;
    - Ex: Accessio Hosted Service / Company: MiaVia, Inc; AnubisNetworks / http://www.anubisnetworks.com/pt/; CleanMessage / Company: CleanMessage; ClearMX / Company: ClearMX; easy@ antispam / Company: Interjuncture Corp; Email Protection Agency / Company: Email Protection Agency Ltd; Mailprotector / Company: VirtualConnect Technologies, Inc; MailWise Filter / Company: MailWise, LLC; MessageLabs; MX Logic / Company: MX Logic, Inc; MXSweep Email Security / Company: MXSweep Ltd; Postini Perimeter Manager / Company: Postini, Inc; SecurenceMail / Company: US Internet Corp; SpamMX / Company:

Interkey, Inc; Symantec Hosted Mail Security / Company: Symantec Corporation; White Mail / Company: Hivercon Ltd.

Numa de fase de projecto para instalação de uma solução anti-spam será de analisar e especificar pelo menos os seguintes aspectos:

- Capacidade de fazer verificações simples e filtragem mais complexa, incluindo: verificações SPF e Sender-ID; Verificações variadas nos cabeçalhos – existência do domínio do remetente e outras; White/Grey/black-listing; Filtragem heurística e Bayesiana.
- Modelo de actualização das heurísticas e outras fontes de parametrização do motor de classificação;
    - Como se fará a aprendizagem do motor de classificação?
        - Será o fornecedor a fazer essa alimentação?
        - Pretende-se contribuir internamente? Como?
- Disponibilidade adequada – actualmente o email é na maioria dos casos um serviço crítico cuja disponibilidade importa não comprometer por introdução de novos elementos na arquitectura;
- Capacidade de tratar emails filtrados / tratamento dos falsos positivos – Como aceder aos emails filtrados? O envio automático pelo sistema de um email resumo diário ou semanal (digest) é confortável para o utilizador;
- Anti-vírus – normalmente pretende-se que o sistema também faça filtragem de vírus, e, se possível, phishing e outros males do email;
- Questões de privacidade – podem colocar-se questões de privacidade no tratamento do email caso os endereços sejam pessoais. Estas questões podem ainda ser agudizadas caso se opte por um "managed service" em que o email passe por uma instituição terceira.
- Custos de exploração – os custos de exploração pode ser consideráveis face ao custo de aquisição, e por vezes podem ser menosprezados ou mistificados na fase de pré-

venda – licenças; actualização automática das heurísticas e outras fontes para classificação; actualização de software; custo de escalabilidade;

8 Conclusões

O problema do spam não tem solução à vista, sendo necessário geri-lo para mitigar o seu efeito mais negativo, que é o gasto de tempo e outros recursos para tratar o fluxo de mensagens ilegítimas.

As possíveis medidas mitigadoras são sobretudo a nível técnico e de regulamentação. Através de medidas técnicas automáticas é possível reduzir substancialmente o nível de spam que chega às caixas de correio dos utilizadores. As medidas técnicas, quanto mais agressivas forem na classificação de spam, maior probabilidade tem de classificar erradamente, e, consequentemente, de bloquear mensagens legítimas. A regulamentação, sendo do tipo "opt-in", exige que o envio de correio comercial seja feito apenas quando há consentimento prévio para esse envio. Porém observa-se na prática que os spammers aderem pouco à regulamentação, caso contrário não existiria um problema de spam.

A FCCN como entidade gestora da Rede Ciência Tecnologia e Sociedade, desde há vários anos tem vindo a tomar e promover medidas de controlo do fenómeno, como por exemplo o isolamento na rede de relays SMTP abertos, promoção da adopção do SPF, disponibilização de um serviço de resposta a incidentes de segurança informáticos, entre outras medidas.

Este documento, nessa mesma linha de actuação, tem por objectivo deu a conhecer a envolvente do problema do spam em vários planos, sugerindo medidas para adopção nas instituições da RCTS.

De levantamento de situação feito às NRENs congéneres da FCCN na Europa, assistiu-se principalmente a ausência de serviços centrais de filtragem de spam. As que tem tais serviços, disponibilizam sistemas de filtragem básicos, presumivelmente de baixa

interactividade e integração com os utilizadores finais e seus sistemas envolventes, e com baixa probabilidade de falsos positivos.

Foram apresentadas mais de uma dúzia de medidas técnicas anti-spam que são passíveis de serem implementadas recorrendo a software freeware, investindo porém tempo nas respectivas instalações, configurações e manutenção. Foram também apresentados os tipos mais comuns de oferta comercial para controlo do spam, e os pontos mais críticos a acautelar na fase de análise de tais sistemas.

Uma das medidas mitigadoras consideradas mais prometedoras é a adopção do SPF, quer na vertente de publicação do registo no DNS, quer na verificação SPF antes da aceitação do email. A descrição técnica do SPF, vertida em RFC, encontra-se em fase experimental durante pelo menos por dois anos, havendo uma solução técnica concorrente. Há ainda desafios técnicos a resolver sobretudo com o reecaminhamento de emails. Nos domínios Portugueses, debaixo do TLD .PT, cerca de 4,3% domínios tem publicados registos SPF, maioritariamente na modalidade "soft-fail". No sistema "Megamail.pt" fazem-se cerca de 23.000 rejeições de email por dia devido a reprovações SPF, o que constitui mais de 10% dos emails entrados no sistema. A FCCN disponibiliza apoio técnico gratuito de configuração SPF às instituições ligadas à RCTS através do serviço CERT.PT.

9 Referências e bibliografia

A secção "Contra medidas técnicas" basea-se fortemente no documento "ANTI-spam TOOLKIT OF RECOMMENDED POLICIES AND MEASURES" da "Task Force on Spam" da Comunidade Europeia.

10 ANEXO I - Política Anti-spam na RCTS

(documento acessível via www.fccn.pt -> rcts -> regras)

Política Anti-spam

1. Definição de spam

A definição de spam significa o envio de comunicações comerciais por via electróncia (para fins de marketing ou publicitários) não solicitadas pelo destinatário. Uma definição mais extensa poderá ser encontrada nas referências abaixo [1,2]. Uma outra designação habitual de spam é Unsolicited Commercial Email (UCE), ou ainda Unsolicited Bulk Email (UBE). Referência legislativas: artigo 22.º e 23.º do Decreto-Lei 7/2004, de 7 de Janeiro - Lei do Comércio Electrónico; Legislação conexa: designadamente, Lei 67/98, Lei 69/98, Lei 6/99, Código da Publicidade, Lei da defesa do consumidor, artigos 37.º e 60.º da CRP, D.L n.º 143/2001, Directivas 95/46/CE e 97/66/CE.

2. spam na RCTS

Verifica-se com frequência crescente na RCTS a configuração deficiente de Mail Transfer Agents (MTAs), que permite a qualquer cliente de Internet enviar para essas máquinas emails com um grande número de destinatários (vítimas de spam). Um MTA mal configurado, tenta propagar todos esses emails, usando para tal recursos partilhados por todos os utilizadores da RCTS, causando um desperdício indesejável desses recursos. Um MTA bem configurado apenas propaga emails vindos de endereços bem conhecidos, normalmente pertencentes às redes locais afectas à entidade que administra o MTA.

As vítimas de spam tendem a queixar-se via email para um vasto conjunto de endereços, relacionados com a administração da máquina e operador internet de suporte, neste caso a FCCN.

A busca de relays SMTP abertos por parte dos Spammers, tem já um grau de sofisticação que inclui procuras exaustivas de espaço de endereçamento. Não parece portanto provável que o problema desapareça sem uma intervenção devidamente estruturada por parte dos ISPs [4]. Recentemente verificou-se que alguns operadores internacionais adoptaram uma política de corte unilateral de tráfego de máquinas usadas para propagar spam.

3. Tratamento de relays abertos na RCTS

Neste contexto, e ao abrigo do ponto 4 das Restrições definidas na Carta do Utilizador da RCTS, que refere: "Não é permitida qualquer utilização da RCTS que interfira de forma lesiva com outros utilizadores, equipamentos ou serviços.", a FCCN considerou adequado passar a ter o procedimento descrito de seguida, a partir do dia 1 de Novembro de 2000.

Procedimento a seguir pela FCCN sempre que forem reportados ou detectados casos de spam.

a) A FCCN testará a existência do(s) referido(s) relay(s) aberto(s) em sistemas ligados à RCTS.

b) Se se confirmar(em) a FCCN notificará por email os Contactos Administrativo e Técnico da entidade em causa, dando um prazo de 7 dias para a resolução do problema. Esta notificação incluirá instruções sobre as formas de resolução dos problemas para os Relays mais populares.

c) Se findo esse prazo o problema se mantiver, a FCCN procederá ao corte da conectividade na RCTS para todos os serviços com origem e destino no(s) endereço(s) em causa. O corte de conectividade será precedido do envio de uma última notificação à entidade.

d) Estes endereços serão colocados numa lista cujo URL será comunicado na notificação do ponto c), de modo a permitir às entidades afectadas confirmar a evolução da mesma. Este URL não será divulgado fora do grupo das entidades bloqueadas e será protegido por password.

e) Sempre que uma entidade considerar que já resolveu o(s) problema(s), deverá notificar o Help Desk da FCCN desse facto indicando o(s) endereço(s) IP que foram corrigidos..

f) A FCCN confirmará tecnicamente essa correcção e caso se confirme, procederá ao restabelecimento da conectividade total e retirará da

"lista negra" os endereços em causa.

4. Medidas de configuração Anti-Spam nos MTAs mais comuns

Sendmail:

http://www.sendmail.org/tips/relaying.html

Microsoft Exchange Server:

http://www.microsoft.com/exchange/

http://www.nvt.net/antispam.html

Qmail:

http://www.qmail.org/

NOTA: O qmail não faz, por omissão, relay SMTP. Desta forma o problema nem sequer existe. Se a configuração de relay estiver demasiado aberta, então é necessário proceder a uma restrição na variável de ambiente RELAYCLIENT lançada para o qmail normalmente através do tcp-env, cuja configuração é extraída do ficheiro /etc/hosts.allow.

5. Algumas listas negras públicas

Mail Abuse Prevention System LLC (MAPS)

http://www.mail-abuse.org/

Network Abuse Clearinghouse

http://www.abuse.net/

6. Referências:

[1] RFC2505 Anti-Spam Recommendations for SMTP MTAs. G. Lindberg. February 1999. (Format: TXT=53597 bytes) (Also BCP0030) (Status: BEST CURRENT PRACTICE)

[2] RFC2635 DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*). S. Hambridge, A. Lunde. June 1999. (Format: TXT=44669 bytes) (Also FYI0035) (Status: INFORMATIONAL)

[3] Serviço comercial de queixa de spam http://spamcop.net

[4] Good Practice for combating Unsolicited Bulk Email http://www.ripe.net/ripe/docs/ripe-206.html

11 ANEXO II - Plataforma Nacional anti-spam

11.1 Notícia em www.mctes.pt

(excerto)

2006-05-16

Dia Mundial da Sociedade da Informação: promover a cibersegurança

Lisboa, 16 Maio (MCTES) - A Agência para a Sociedade do Conhecimento (UMIC) e a Fundação para a Computação Científica Nacional (FCCN) assinalam quarta-feira (17 de Maio) o Dia Mundial da Sociedade da Informação com uma sessão subordinada ao tema "Promover a Cibersegurança".

[...]

Está a ser desenvolvido trabalho com fornecedores ISP com vista a preparar a criação na FCCN de uma plataforma anti-spam que possa ser usada de forma colaborativa para combater o spam.

11.2 Notícia no "sapo.pt"

Plataforma Nacional anti-spam a funcionar até final do ano

(Actualizada)

Procurando melhorar a capacidade de resposta dos ISPs portugueses ao spam, o ISP Fórum, uma entidade criada no âmbito do CERT.pt, quer criar uma plataforma nacional anti-spam que junta todos os ISPs na partilha de informação. A proposta foi apresentada hoje por Celso Martinho, director de tecnologia de produto do SAPO, na conferência "Promover a Cibersegurança", que decorreu em Lisboa, mas já estava a ser trabalhada há alguns meses.

Celso Martinho lembrou que o spam é a praga da Internet, representando mais de 60 por cento dos emails enviados, sendo que os vírus existem em apenas 2 por cento. "Os números em Portugal estão alinhados com os internacionais", explicou Celso Martinho com base na experiência de filtragem das mensagens do SAPO e Telepac, mas existe a consciência de que podem ainda melhorar.

A proposta do ISP Fórum aponta para a criação da plataforma nacional até final do ano, com a criação de uma base de conhecimento de spam nacional, desenvolvida e operada pela FCCN com o apoio e empenho de todos os ISPs. A maioria dos ISPs portugueses participa já neste fórum e têm vido a desenvolver a iniciativa que já tem uma especificação definida.

O responsável técnico do SAPO defende que esta plataforma tem o potencial de criar um conhecimento dos padrões de spam em Portugal, que permitirá aos ISPs implementar sistemas de bloqueio mais eficazes garantindo prevenção, flexibilidade e troca de

conhecimento local com vantagens para todo o ecossistema. Após a conferência Celso Martinho explicou ainda ao TeK que a plataforma tem um mdelo de negócio interessante para os ISPs já que não exstem custos. O ISP fornece o tráfego e usufrui do resultado da análise e centralização da inforação produzida.

"Os objectivos são ambiciosos mas não complexos", justifica Celso Martinho. Para já existem alguns ISPs que mostraram abertura para aderir à plataforma, nomeadamente a PT.Com.

Em declarações à margem da conferência, Mariano Gago, ministro da Ciência, Tecnologia e Ensino Superior, defendeu que a situação de Portugal em termos de cibersegurança é boa, embora haja ainda muito a fazer na consciencialização das entidades, dos cidadãos e das PMEs para os problemas de segurança informática. "É preciso que os cidadãos e as empresas se consciencializem de que a segurança informática é tão importante como as outras questões de segurança física".

A conferência "Promover a Cibersegurança" foi organizada pela UMIC - Agência para a Sociedade da Informação e pela FCCN - Fundação Nacional para a Computação Cientifica e assinala o tema "A Importância da Cibersegurança" que marca as comemorações hoje em curso a propósito do Dia Mundial das Telecomunicações e da Sociedade da Informação.

Nota de Redacção: [2006-0517 20:59] A notícia foi actualizada com mais informação recolhida após a conferência.

Notícias Relacionadas:

2006-05-16 - Cibersegurança no centro do Dia Mundial da Sociedade da Informação

2006-05-17 17:59:00

Casa dos Bits

12 ANEXO III - Unsolicited communications - Fighting Spam

(em "http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm")

Unsolicited communications - Fighting Spam

Article 13(1) of the Privacy and Electronic Communications Directive requires Member States to prohibit the sending of unsolicited commercial communications by fax or e-mail or other electronic messaging systems such as SMS and MMS unless the prior consent of the addressee has been obtained (opt-in system).

The only exception to this rule is in cases where contact details for sending e-mail or SMS messages (but not faxes) have been obtained in the context of a sale. Within such an existing customer relationship the company who obtained the data may use them for the marketing of similar products or services as those it has already sold to the customer. Nevertheless, even then the company has to make clear from the first time of collecting the data, that they may be used for direct marketing and should offer the right to object. Moreover, each subsequent marketing message should include an easy way for the customer to stop further messages (opt-out).

The opt-in system is mandatory for any e-mail, SMS or fax addressed to natural persons for direct marketing. It is optional with regard to legal persons. For the latter category Member States may choose between an opt-in or an opt-out system.

For all categories of addressees, legal and natural persons, Article 13(4) of the Directive prohibits direct marketing messages by e-mail or SMS which conceal or disguise the identity of the sender and which do not include a valid address to which recipients can send a request to cease such messages.

For voice telephony marketing calls, other than by automated machines, Member States may also choose between an opt-in or an opt-out approach.

Useful information on national anti-spam legislation can often be accessed via the national webpages listed here.

13 ANEXO IV – Mensagem IETF sobre SPF

IESG Note

The following documents (RFC 4405, RFC 4406, RFC 4407, and RFC 4408) are published simultaneously as Experimental RFCs, although there is no general technical consensus and efforts to reconcile the two approaches have failed. As such, these documents have not received full IETF review and are published "AS-IS" to document the different approaches as they were considered in the MARID working group.

The IESG takes no position about which approach is to be preferred and cautions the reader that there are serious open issues for each approach and concerns about using them in tandem. The IESG believes that documenting the different approaches does less harm than not documenting them.

Note that the Sender ID experiment may use DNS records that may have been created for the current SPF experiment or earlier versions in this set of experiments. Depending on the content of the record, this may mean that Sender-ID heuristics would be applied incorrectly to a message. Depending on the actions associated by the recipient

with those heuristics, the message may not be delivered or may be discarded on receipt.

Participants relying on Sender ID experiment DNS records are warned that they may lose valid messages in this set of circumstances. aParticipants publishing SPF experiment DNS records should consider the advice given in section 3.4 of RFC 4406 and may wish to publish both v=spf1 and spf2.0 records to avoid the conflict.

Participants in the Sender-ID experiment need to be aware that the way Resent-* header fields are used will result in failure to receive legitimate email when interacting with standards-compliant systems (specifically automatic forwarders which comply with the standards by not adding Resent-* headers, and systems which comply with RFC 822 but have not yet implemented RFC 2822 Resent-* semantics). It would be inappropriate to advance Sender-ID on the standards track without resolving this interoperability problem.

The community is invited to observe the success or failure of the two approaches during the two years following publication, in order that a community consensus can be reached in the future.