nic.br
Núcleo de Informação
e Coordenação

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Reunião da Comissão de Trabalho Anti-Spam

Data : 13/03/2008
Local: NIC.br

Participantes:

Henrique Faulhaber – Conselheiro e Coordenador da CT-Spam
Cristine Hoepers – Analista de Segurança do CERT.br
Klaus Steding-Jessen - Analista de Segurança do CERT.br
Hartmut Glaser - Diretor Administrativo e Financeiro do NIC.br
Carlos Alberto Afonso - Representante do Terceiro Setor do CGI.br
Marcelo Fernandes Costa – Representante do Terceiro Setor do CGI.br
Jaime Wagner – Representante dos Provedores de acesso e conteúdo da Internet do CGI.br
Nivaldo Cleto – Representante do Setor Empresarial Usuário do CGI.br
Vera Braz – Secretária Executiva do NIC.br

Abertura:

A pauta da reunião foi sugerida pelo Sr. Henrique Faulhaber – coordenador da CT-Spam

Gerência de porta 25 em redes de banda larga de perfil residencial
(apresentada durante a 13ª Reunião Ordinária da CBC-1 da Anatel, CPqD, Campinas, SP)
http://www.cert.br/docs/palestras/certbr-cbc1-13-anatel2008.pdf

Foram discutidos tópicos sobre a apresentação feita por Cristine e Klaus do CERT.br a respeito de gerência de porta 25, porta usada para a transferência de mail entre servidores de email, utilizando o protocolo SMTP (*Simple Mail Transfer Protocol*). A apresentação trata da proposta de diferenciação entre o tráfego de submissão de mensagens (do cliente para o agente de submissão) do tráfego de transferência de mensagens (entre servidores de email). Klaus comentou que o Brasil esteve em primeiro lugar na CBL (*composite blocking list*, que é uma lista de bloqueio de IPs envolvidos em entrega direta de mensagens, tipicamente *proxies* abertos sendo abusados) sendo ultrapassado pela China. Foram discutidos dados sobre o Projeto Spampots o qual mensura o abuso de máquinas de usuários finais para o envio de spam sendo feitas pesquisas com 10 máquinas honeypots*, onde concluiu-se que o volume de spam sendo originado de máquinas brasileiras abusadas por terceiros é extremamente significativo. Soube-se também que Taiwan quer utilizar os dados coletados para futura investigação. Sobre abuso de *relays* abertos, Cristine citou que não existem reclamações desta categoria ao CERT.br há mais de um ano.

*Honeypots** são computadores configurados de modo a apenas emular determinados sistemas operacionais e serviços.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Cristine comentou que diversos provedores, como exemplo UOL/Terra, já disponibilizam o padrão *message submission* e que, em alguns deles, usuários novos já têm seus leitores de email configurados para usar este padrão. Cristine afirmou que, futuramente, todos os usuários deverão reconfigurar suas máquinas para usar "*mail submission*", para que efetivamente seja utilizada a porta 587/TCP para a submissão de email. Cristine salientou a importância da gerência de porta 25 e do aumento da rastreabilidade da submissão de mensagens -- essas medidas permitiriam detectar rapidamente a existência de *trojans*, identificando sua origem e, conseqüentemente, levando à redução do abuso. Klaus disse que planeja-se dar bastante tempo para a migração para esse novo sistema, utilizando *message submission*, que já está em uso por grandes provedores como UOL/Terra. Até que a maioria dos provedores tenha tido tempo de migrar não se alteraria a política atual com relação a tráfego de saída de porta 25/TCP. Somente após a migração por parte dos provedores, as teles começariam a filtrar tráfego originado de conexões de caráter residencial com destino a porta 25/TCP. Carlos Afonso mostrou preocupação com relação a milhares de pequenas empresas que não dispõe de verba para colocar uma linha exclusiva nas suas empresas para gasto com uma conexão empresarial a fim de testar seus softwares. Também demostrou receio de que o bloqueio desta porta possa levar ao bloqueio indiscriminado de outras portas, prejudicando até mesmo as negociações empresariais. Cristine confirmou que a Telefônica ainda não se pronunciou quanto à essa alteração, prejudicando o avanço das discussões deste assunto com outras teles. Informou que a área de planejamento da Telefônica deve ser envolvida nessas negociações, além da área de segurança. Citou, também, que foi realizada a última reunião da CBC-1 (que futuramente irá se juntar à CBC-13, que terá outra denominação) e que é provável que o coordenador da nova CBC seja o Sr. José Bicalho. Hartmut Glaser evidenciou que deverá ser feita uma abordagem junto aos alto executivos das Empresas, os quais certamente são favoráveis a essas mudanças. Glaser sugeriu uma discussão com o Sr. Valente, da Telefônica – (ex Conselheiro da Anatel), ou com Ercio Alberto Zilli, que é membro da CT-Spam. Cristine sugeriu que a CT-Spam deveria fazer um cronograma para o processo de adoção de gerência de porta 25 e, adicionalmente, criar tutoriais *online* explicando o processo de configuração de message submission para os provedores que ainda não o implementam. Glaser recomendou que seja feita reunião com alguns representantes do CGI.br junto aos executivos da ABRAFIX (onde o Sr. Alexandre Annenberg também é representante)e outra reunião durante a Futurecom- http://www.futurecom2008.com.br onde se reúnem altos executivos das operadoras e poderá ser um boa oportunidade para se fazer discutir o assunto. Jaime Wagner propõe que seja feita abordagem com uma operadora de cada vez sendo a Telefônica a primeira a ser contatada. Após discussão foi acordado que inicialmente haverá conversa com o Sr. Plínio para saber de que modo a Anatel poderá auxiliar o CGI.br e já no caso da Telefônica que se discuta diretamente com quem os setores que podem definir a adoção. Cristine irá conversar com a Sra. Alicia (área de Segurança da Telefônica) para que ela indique as áreas. Jaime Wagner entrará em contato com o Sr. Eduardo Parajo da ABRANET.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Encaminhamento do projeto de lei anti-spam para o Congresso

Henrique Faulhaber disse que o Projeto de Lei sobre spam, do Senador Eduardo Azeredo, continua em tramitação pelo Congresso, seguindo para a Comissão de Ciência e Tecnologia. A respeito do e-mail enviado pela lista do CT-spam pelo Assessor Parlamentar contratado pelo CGI.br – Leonardo Bucher, houve manifestações importantes, uma feita pelo Jaime Wagner sobre opt-out* e do Conselheiro Suplente Omar Kaminski a respeito da multa excessiva. Jaime Wagner afirmou que essa legislação não vai afetar o envio de "email criminoso", isto é, mail enviado por *malware* ou pessoas mal intencionadas. Ainda segundo Jaime Wagner uma legislação anti-spam afetaria apenas as empresas de marketing legítimo. Faulhaber disse que alguns empresários de email marketing estão se reunindo na ABRANET discutido e apoiando a adoção de *opt-in*. Seguiu-se discussão sobre a forma de recebimento dos e-mails indesejados, e a comparação entre as opções *soft opt-in** e *opt-out**. Klaus deu como exemplo dos problemas do *opt-out* os e-mails que orientam o usuário com a opção "clique aqui para sair" e os riscos de expor os usuários a problemas com *phishing*, *trojans*, etc que utilizarem este tema para induzir a instalação de um código malicioso. Wagner argumentou que se a empresa possuir endereço físico o usuário poderá enviar uma carta registrada solicitando o não recebimento de mensagens e no caso do envio continuar, seria viável ele recorrer ao Juizado de Pequenas Causas e mover uma ação contra a empresa. Marcelo Fernandes comentou que esse procedimento é possível, mas é necessário uma ata notarial, de custo proibitivo para a maioria dos usuários. Wagner afirmou que é a missão do marketing é criar desejo -- uma mensagem pode não ser solicitada, porém ser desejada. Klaus argumentou que não é justo que o ônus do trabalho adicional -- neste caso de apagar mensagens não solicitadas -- caia nos usuários, que são os afetados por perda de mensagens importantes, tempo gasto apagando mensagens, etc. Glaser sugeriu que seja feita reunião em Porto Alegre inicialmente com representantes de Marketing e na seqüência com os de Internet, não com o objetivo de atacar o e-mail marketing mas sim discutir o tema junto à AGADI e à Internetsul. Faulhaber disse que hoje o pessoal de Marketing, mesmo quem adota opt-in, está precisando ajustar o envio de sua propaganda através da rede junto aos provedores, devido às muitas regras anti-spam existentes. Cristine mostrou preocupação de que futuramente o e-mail marketing deixe de ser uma ferramenta de propaganda pelo número de spams, a tendência é que os usuários desconfiem e automaticamente desconsiderem qualquer mensagem. Jaime Wagner levantou também a possibilidade de regionalização de IPs, para identificação geográfica e possibilidade de envio mais direcionado de emails. Foi levantado na discussão que pode não ser possível fazê-lo. Jaime Wagner deverá discutir todos esses assuntos durante reunião em Porto Alegre e futuramente viabilizar uma reunião entre empresas de e-mail Marketing com o CERT.br e o CGI.br.

Opt-out *
Regra de envio de mensagens que define que é **permitido** mandar *e-mails* comerciais/*spam*, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

Opt-in*
Regra de envio de mensagens que define que é **proibido** mandar *e-mails* comerciais/*spam*, a menos que exista uma concordância prévia por parte do destinatário.

Soft opt-in*
Regra semelhante ao *opt-in*, mas neste caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Desta forma, não é necessária a permissão explícita por parte do destinatário para receber *e-mails* deste remetente.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Projeto SpamPots - Próximos passos
http://www.cert.br/docs/whitepapers/spampots/

Cristine comentou que tem sido acompanhado o trabalho da equipe da UFMG sobre a mineração dos dados coletados, porém as pesquisas ainda prosseguem por dependerem de um conjunto de algoritmos que caracterizem os spams e campanhas, temrinados na primeira fase, e citou que os próximos passos seriam a respeito da evolução do spam e do comportamento dos spammers. Marcelo Fernandes salientou que foi contratada uma grande equipe para este trabalho por ser extremamente complexo, tratando inúmeras perguntas e utilizando um *software* desenvolvido a partir do zero. Fernandes disse que a grande vantagem é a de que esse projeto deverá se tornar internacional e, conseqüentemente, o software será utilizado por todos. Henrique Faulhaber disse que deveriam ser respondidas duas questões fundamentais, ainda na primeira fase, que seriam: a relação entre o idioma do conteúdo e a origem do spam; e as características dos spams vindos do Brasil e com conteúdo em português (mesmo o Brasil representando menos de 1% dessa categoria). Klaus comentou o status atual citando que a coleta foi interrompida em setembro/2007 e que permaneceram três sensores ativos porém não participando da coleta oficial. O prazo para término do contato com a equipe da UFMG é Maio de 2008, quando a CT-Spam deverá iniciar a segunda etapa do projeto. Glaser acredita que nessa etapa o número de máquinas deverá ser reduzido e ser feito acompanhamento pontual para melhor avaliação. Glaser mencionou que a OEA possui uma comissão de segurança sobre crimes cibernéticos e que o pessoal do CERT.br tem participado desses encontros. Adicionou que a ITU também estuda esses crimes e que a Cristine irá participar da próxima reunião, em Genebra, no mês de Maio. Acrescentou que o pessoal da ITU (International Telecommunication Union), via Itamaraty, concedeu 03 (três) vagas para representações brasileiras: 01 do CERT.br, 01 do Governo e outra do segmento empresarial, sendo indicado o Henrique Faulhaber (indicação a ser discutida na reunião do CGI.br no dia 14/03). Glaser informou que o representante do MRE na comissão permanente do CGI.br em Genebra é o Sr. Cristiano Berbert , assessorando as áreas intelectual e telecomunicações nas reuniões da ITU e da ICANN. Encerrou-se a reunião ficando pendentes os assuntos MOU China & Taiwan e Site Antispam.