Segurança contra spams precisa ser reforçada em 2009

As tendências sobre *spam* e *malware* hoje em dia, podem ser caracterizadas por um número maior de ataques mais direcionados, sofisticados e disfarçados. O número de *spam*, por exemplo, vem aumentando significativamente. Seu volume cresceu 100%, subindo para quase 200 bilhões de mensagens diariamente em todo o mundo, ou seja, bem mais que 20 mensagens por dia, para cada homem, mulher e criança existente no planeta.

O número de ataques aumenta, coincidindo com acontecimentos populares ou grandes manchetes para dar à mensagem um caráter idôneo. Esses ataques têm como objetivo disseminar conteúdo malicioso, usando como "mulas" assuntos de grande interesse do público, como notícias sobre esportes, política e desastres naturais.

Além disso, o *spam* também está se tornando mais perigoso. As primeiras versões basicamente continham um texto com objetivo de vender algum tipo de produto. Desde então os *spammers* têm se sofisticado muito. Em 2007, tivemos uma grande variedade de *spams* com anexos. Os criadores de testaram mais de 20 tipos de arquivos diferentes para determinar o melhor. Os ataques rápidos de *spam* se tornaram lugar comum, com o incrível aumento dos surtos. As empresas de anti-spam lutaram muito para combatê-los o mais rápido possível. Isso deixou muito pouco tempo para reação, e muitos usuários de *anti-spam* acabaram duvidando da qualidade dos produtos que utilizavam.

Porém, com o aumento da eficácia dos filtros de *anti-spam* para barrar este tipo de anexo, já no final de 2007 e começo de 2008, os *spammers* estavam usando uma nova tática para driblar as defesas. Mais de 83% dos *spams* continham uma *URL* para um servidor *web* falso que freqüentemente abrigava *malwares* . De acordo com as tendências de combinação de diferentes técnicas de *malware*, o número de vírus baseado em *URL* cresceu 256%.

Essas mensagens normalmente driblam mecanismos tradicionais de *spam* que procuram palavras-chave ou elementos gráficos com cotações. Quando eles aterrissam na caixa de entrada do destinatário, já conseguiram atravessar uma das partes mais confidenciais da rede corporativa. Tudo o que ele espera agora é um clique errado para se ativar e liberar o acesso à rede interna ou levar o internauta a uma página onde oferecem seus produtos / serviços. Como as *URLs* utilizadas neste tipo de ataque são muito dinâmicas, alterando seu endereço de 4 ou 6 horas, além de driblar as ferramentas de *anti-spam*, passam despercebidos pelas soluções tradicionais de filtros *URL*, que cada vez mais vêm se fixando como uma solução de controle de produtividade e não uma solução real de segurança *web*.

Outro fator que marcou o mercado de segurança foi o aparecimento da *Self Defending Bot Network*. Os criadores de vírus evoluíram dos antigos ataques em massa como o do Netsky e do Bagel. Em 2007, os vírus já eram polimórficos e estavam normalmente associados à proliferação de sofisticados *botnets*, como o *Feebs* e o *Storm*.

O *Storm* e o *MPack* dominaram as manchetes sobre segurança na Internet, não apenas por causa da extensão e do escopo, mas porque trouxeram novas técnicas mais sofisticadas, que demonstram o refinamento dos *softwares* maliciosos. Os criadores de *malware* estão gastando cada vez mais recursos

para desenvolver uma plataforma durável e reutilizável. Os métodos de entrega também estão mudando para ataques combinados que reúnem *e-mail* e *web services*.

Os ataques de 2008 partem diretamente de dentro da rede corporativa “protegida”. Muitos administradores acreditam que protegeram suas infra-estruturas para as quais os *spams* são apenas coisinhas irritantes. Mas a verdade é que o *spam* está sendo usado como um *gateway* para conduzir os usuários para sites perigosos. Para responder a isso, as empresas precisam implementar os sistemas mais avançados de segurança de *e-mail* e *web* que sejam capazes de bloquear as ameaças recebidas, reforçar a classificação, varrer todo o tráfego *web* iniciado pelo usuário e fazer monitorações o mais detalhadas possível em busca de prováveis infecções internas por *malware*.

Date Created
08/01/2009