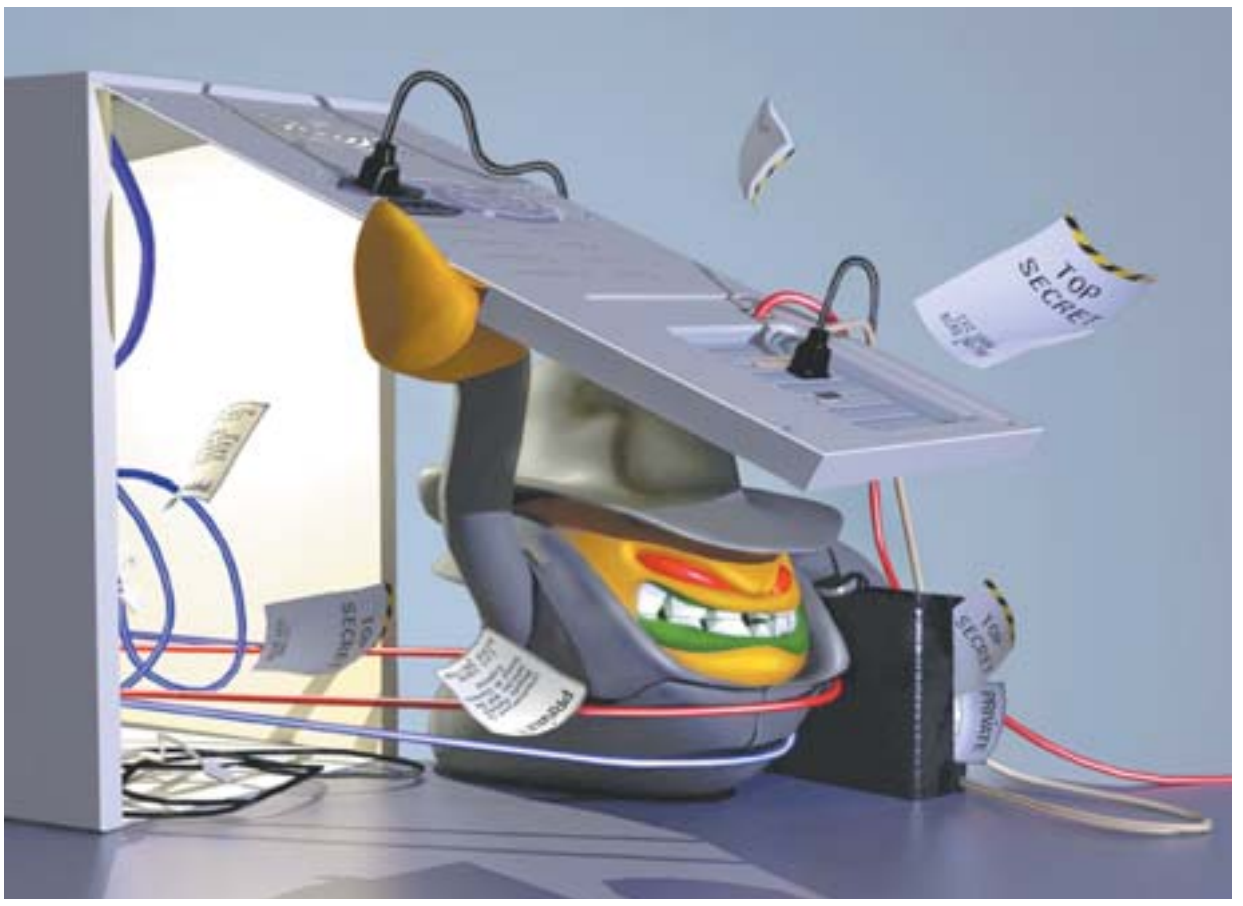

GOLPISTAS estão utilizando como porta de entrada dois programas presentes na maioria dos computadores

PRAGAS

Ataque virtual utiliza arquivos PDF e SWF

Malware utiliza os dois programas para assustar as vítimas, oferecendo um arquivo executável para remover as infecções

Um grupo de detecção de ameaças web da empresa de segurança AVG Technologies descobriu que um falso verificador de sistema está realizando ataques múltiplos usando arquivos PDF e SWF, além de pelo menos dois Java exploits.

Essa ameaça circula há bastante tempo, sendo que em versões anteriores se disfarçava como uma falsa cópia do AVG. Agora, ele está utilizando como porta de entrada dois programas presentes na maioria dos computadores.

Seu modo de atuação apresenta uma página falsa de varredura e diz ao usuário que um malware foi encontrado no seu computador, oferecendo então um arquivo executável para remover as infecções. Esse ataque funciona a partir de uma falha do Shockwave Flash (SWF) e do Java PDF.

No caso do SWF, os criminosos exploram uma vulnerabilidade que ataca as versões desatualizadas do Adobe Flash Player ou Adobe Reader, permitindo a execução desse código arbitrário.

Manter as aplicações Adobe sempre atualizadas é uma boa garantia de impedir a exploração das falhas de segurança das versões anteriores. Já os exploits de PDF são javscripts maliciosos dentro de arquivos PDF.

Quando executado, se aproveitam de falhas de segurança para fazer downloads não desejados que podem instalar outros códigos maliciosos na máquina da vítima. Todo o ataque é feito com a intenção de instalar um cavalo de Troia sem o consentimento da vítima.

Recentemente, o laboratório de detecção de ameaças da AVG registrou uma queda nas infecções por falsos verificadores de sistema. Além do fato da prisão na Rússia do chefe de uma empresa de pagamentos que se especializou em ajudar criminosos, as agências de cartão de crédito têm tornado a vida mais difícil dos scammers que usam falsos softwares para roubar dinheiro das vítimas.

"Esta nova estratégia de infecções pode ser o resultado da procura de uma nova fonte de renda", explica Mariano Sumrell, da AVG Brasil.

Em todos os casos, é possível melhorar substancialmente a segurança ao manter todos os navegadores e plug-ins, além dos softwares Adobe e o Java, sempre atualizados. Outra ação simples e eficiente é sempre manter em dia o antivírus e outros softwares de segurança.

Nova enxurrada de ameaças via e-mails

Um dilúvio de malwares maliciosos transportados por e-mails. Foi essa classificação que a empresa de segurança Symantec atribuiu aos ataques registrados no mês de setembro, documentados no Relatório Symantec Intelligence.

Segundo o estudo, aproximadamente 72% de todo malware carregado por e-mail podem ser caracterizados como tipos agressivos de malware chamados de polimórficos genéricos, identificados pela primeira vez no relatório da empresa.

O relatório mostrou que, no final de julho, a taxa foi 23,7%; em agosto, caiu ligeiramente para 18,5%, antes de atingir 72% no mês passado.

"Esse marco sem precedentes destaca a natureza dos ataques dos cibercriminosos às empresas em 2011, que exploram totalmente os pontos fracos das medidas de segurança dos sistemas mais tradicionais", afirma Paul Wood, analista de inteligência sênior do Symantec.cloud.

Apesar dos níveis de spam terem permanecido relativamente estáveis durante o mês de setembro, o Relatório Symantec Intelligence observou o uso de vulnerabilidades identificadas em determinadas versões mais antigas do popular software para blogs WordPress em um grande número de sites na internet.

E-mails de spam contendo links para esses sites comprometidos também são espalhados.

A exploração dessas vulnerabilidades para servir aos interesses dos spammers é um alerta da importância de atualização do software com as versões e patches mais recentes.

Uma pesquisa adicional também revela que o JavaScript está se tornando cada vez mais popular como linguagem de programação usada por spammers e autores de malware.

O JavaScript é cada vez mais usado para ocultar o local para onde os spammers estão redirecionando as vítimas e, em alguns casos, também para esconder páginas inteiras da web.

MALWARES agressivos invadem os e-mails dos usuários. Todo cuidado é pouco

Morte de Jobs inspira golpe

Criminosos da rede aproveitaram a morte do cofundador da Apple, Steve Jobs, morto na última quarta-feira, para aplicar golpes.

A Sophos identificou uma página no Facebook que traz uma falsa homenagem ao executivo e promete sorteio de iPads. Milhares de pessoas já clicaram.

Quem clica no link é convidado a preencher um formulário on-line e a escolher o modelo de tablet que deseja.

O computador não é infectado por programas nocivos, mas os dados confidenciais são utilizados pelos bandidos virtuais para criar armadilhas.