# Notícias Gerais

Para notícias sempre atualizadas e com a opinião de quem vive o mercado do Linux e do Software Livre, acesse nosso site: **www.linuxmagazine.com.br**

## Crackers brasileiros e gangue europeia criam nova técnica para alterar boletos

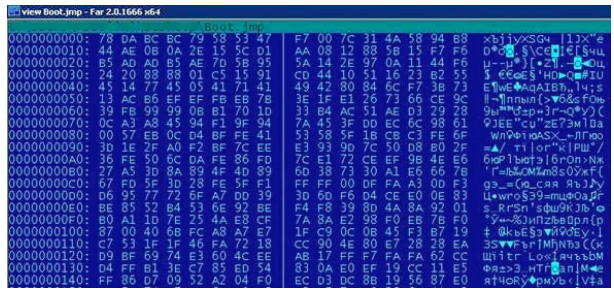
Você certamente já deve estar cansado de ver notícias na TV e na internet sobre como os golpes online estão ficando cada vez mais sofisticados – e perigosos. Algumas das táticas mais comuns usadas por cibercriminosos é enviar e-mails em nome de instituições oficiais que, no final das contas, são verdadeiras armadilhas para usuários mais desatentos.

Agora, analistas da Kaspersky Lab descobriram que crackers brasileiros desenvolveram uma nova técnica que altera boletos bancários com o objetivo de infectar e roubar mais internautas. O novo procedimento consiste em usar arquivos não-executáveis e criptografados com uma chave de 32 bits, que posteriormente são comprimidos pelo padrão ZLIB. A técnica é muito similar ao do trojan Gameover Zeus, um vírus que desviou US$ 100 millhões no mundo todo e que só foi desativado em junho deste ano.

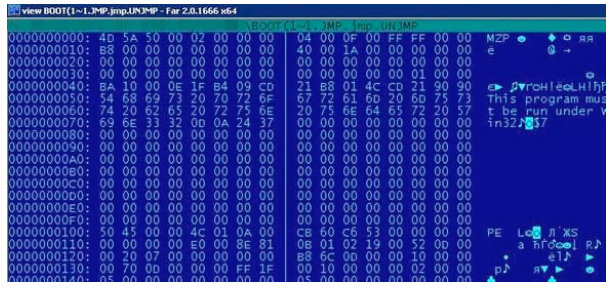
De acordo com a Kaspersky, criminosos brasileiros estão trabalhando e cooperando com algumas gangues do Leste Europeu envolvidas no desenvolvimento e disseminação do Zeus e suas variantes. Essas ameaças são direcionadas principalmente na infecção de caixas eletrônicos e dispositivos de pagamento (PoS). Os analistas afirmam que já surgiram os resultados dessa cooperação entre os cibercrminosos daqui e da Europa, em especial um malware que está afetando pagamentos em boleto realizados no Brasil.

Em feveireiro do ano passado, o especialista em segurança Gary Warner escreveu sobre uma nova versão da campanha Zeus que baixava alguns arquivos estranhos e não-executáveis com a extensão .ENC para a máquina infectada. Segundo o laboratório CrySys, que estudou a extensão, os crackers fazem uso dessa técnica para burlar diversas proteções, como firewall, filtros da web, sistemas de detecção de instrusão na rede e outras defesas usadas em redes corporativas.

Os criminosos brasileiros, por sua vez, decidiram usar a extensão .JMP em arquivos criptografados do mesmo jeito: baixado por esses pequenos Trojans usados em campanhas maliciosas que visam alterar boletos bancários. É assim que um arquivo criptografado se parece no começo:



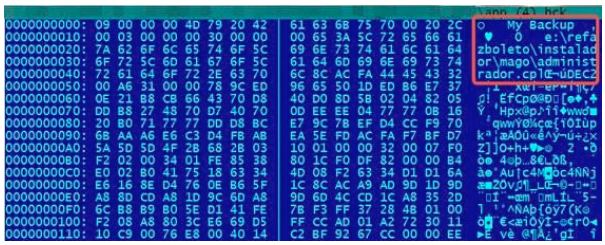
Após remover a criptografia é possível vê-lo como um arquivo .EXE executável normal:



A Kaspersky Lab alega que os crackers brasileiros estão criptografando os grandes arquivos (payloads) usando essa técnica, incluindo algumas ferramentas de remoção de software como o antirootkit Partizan e trojans desenvolvidos em Delphi que incluem imagens de páginas das

instituições bancárias brasileiras. O objetivo é deixar os arquivos que compõem a infecção de maneira criptografada e indetectável, não sendo reconhecido como um executável normal.

Outra variante do ataque são os arquivos .BCK. Eles foram empacotados usando um aplicativo desconhecido – o malware traz em seu cabeçalho a assinatura de algum software comercial de cbackup. Visualizar o inicio do arquivo criptografado é suficiente para descobrir o que há dentro dele: um outro arquivo malicioso, que na maioria dos casos trata-se de arquivos CPL usados nas campanhas dos boletos. Na imagem ao lado, dentro da área demarcada em vermelho, é possível notar o comando "refazboleto", apontando para um arquivo CPL:



Para não se tornar mais uma vítima, as dicas são aquelas que você já deve conhecer: instalar um bom antivírus no seu computador e atualizá-lo constantemente. Sempre desconte de e-mails enviados por desconhecidos e nunca clique em links ou baixe arquivos em anexo dentro dessas mensagens. Além disso, se desconfiar que sua máquina foi infectada, evite usar os serviços financeiros online do seu banco e procure um especialista. ■

# Em nome da segurança, 'NSA alemã' pretende voltar a usar máquinas de escrever

A piada parece estar prestes a se tornar literal também na Alemanha. Patrick Sensburg, diretor de um grupo do parlamento alemão responsável por investigar o escândalo de espionagem da NSA, afirmou que a equipe pode voltar a usar máquinas de escrever como forma de evitar o vazamento de informação, seja por meio de vigilância digital de governos ou ataques hackers.

Como publicou o Ars Technica, o grupo já possui uma máquina de escrever em operação, e pode comprar mais delas, do tipo não eletrônico, caso veja necessidade. É uma atitude que já foi tomada também pelo governo russo, que voltou ao mundo analógico em uma série de comunicados confidenciais do Kremlin e já gastou quase US$ 15 mil na compra de equipamentos do tipo.

A afirmação de Sensburg, nesta terça (15), vem em resposta à prisão de um indivíduo chamado pela imprensa apenas de Markus R., um espião alemão acusado de compartilhar segredos do governo germânico com a CIA. Cerca de 218 documentos confidenciais teriam sido vazados desde 2012, em troca do pagamento de US$ 34 mil.

A descoberta foi feita após um descuido do espião, que enviou um email sem criptografia para seu contato na áustria. A primeira decorrência do fato, antes mesmo de sua divulgação pública, teria sido a expulsão do diretor dos escritórios da CIA na Alemanha, que apenas dificultou ainda mais as relações entre os países, já abalada desde a revelação de que a NSA espionou diversos governantes alemães, incluindo a primeira ministra Angela Merkel.

Para o ex-embaixador da Alemanha nos Estados Unidos, Klaus Scharioth, essa pode ser considerada a maior crise entre os dois países desde a Segunda Guerra Mundial. Agora, o governo germânico quer garantir que mais vazamentos não ocorram e que a NSA, além de outros órgãos de segurança americanos, interrompam a vigilância ostensiva sobre seu território. Justamente para evitar esse tipo de coisa, Sensburg afirmou que seu próprio smartphone, bem como o de todos os outros membros do grupo de investigação, serão submetidos a uma auditoria para garantir a integridade dos dados armazenados ali. A ideia é que toda comunicação interna aconteça apenas sob forte criptografia.

Além disso, o diretor do grupo de investigações disse que continua firme em sua intenção de interrogar e coletar depoimentos de Edward Snowden, o ex-analista da NSA que divulgou as primeiras informações sobre o escândalo. Para ele, o ideal é que o especialista comparecesse a uma audiência na Alemanha, mas como isso não tem se provado possível, ele ficaria satisfeito também com uma videoconferência. Atualmente, ele se encontra em asilo na Rússia. ■