

VIDA

EXPERIÊNCIAS DIGITAIS

! ILUMINAÇÃO

A automação das casas cria brechas. Um sequestrador digital pode controlar luzes e eletrodomésticos conectados

! COMPUTADOR

O computador é a principal porta de acesso do sequestrador digital. Ele pode bloquear uma máquina ou uma rede inteira

O CRIME QUA

O sequestro de dados de pessoas e empresas é a próxima grande ameaça di



No Japão, em janeiro, hackers bloquearam o acesso de centenas de famílias a suas TVs digitais



No início deste ano, na Áustria, um ataque digital impediu um hotel de emitir novos cartões para abrir as portas dos quartos



Links maliciosos chegam também por mensagens. Fotos íntimas são um alvo frequente dos sequestradores digitais

SE PERFEITO

gital por uma razão assustadora: é quase impossível rastrear os criminosos

Bruno Ferrari

Na manhã de 23 de fevereiro, uma quinta-feira antes do Carnaval, a empresária Maria Nogueira* foi chamada por um funcionário da área de tecnologia de sua fábrica de autopeças, em Santana do Parnaíba, São Paulo. Ele havia recebido um e-mail de um remetente identificado como “MK Scorpion”. Num inglês macarrônico, misturado a palavras em russo, Scorpion apresentava-se como hacker, informava que havia invadido o sistema da fábrica e bloqueado informações cruciais para produzir as peças. Para desbloquear essas informações, Maria teria de transferir, em 24 horas, três unidades da moeda virtual bitcoin (em torno de R\$ 12 mil). Após o prazo, o valor subiria. Sem muito conhecimento de tecnologia da informação, a empresária nem sequer compreendeu a exigência de resgate. Ao pedir mais detalhes para Scorpion, recebeu como resposta um tutorial detalhado sobre como comprar um bitcoin e transferir para a conta do hacker. “Percebi que se tratava de um sequestro da minha empresa”, diz.

Maria nem teve tempo de relaxar. Dois dias depois, em pleno sábado de Carnaval, sofreu outro ataque. Dessa vez, era um e-mail em inglês bem escrito, em tom amistoso, com alguns caracteres em chinês na assinatura. A empresária já sabia do que se tratava. “Fiquei com receio do prejuízo que teria com a interrupção da produção. Sem encontrar uma solução imediata, acabei pagando de novo”, conta. A empresária recebeu dos hackers então os links por e-mail para baixar um programa, junto a um código para reaver os dados sequestrados. O prejuízo? R\$ 25 mil dos dois resgates mais R\$ 300 mil dos dias em que os sistemas da fábrica foram afetados.

A empresária foi vítima de um golpe conhecido como ransomware. Ele ocorre quando um hacker invade o computador, o smartphone ou algum dispositivo conectado à internet, bloqueia informações por meio de criptografia. Se o dono das informações quiser vê-las novamente, precisa pagar um resgate, ransom, em inglês (*saiba mais no quadro ao lado*). Esse tipo de crime tem atraído cada vez mais adeptos, que se aproveitam da falta de conhecimento das vítimas em relação à segurança digital e da facilidade para obter as ferramentas para criptografar os dados. Outro aspecto convidativo é a impunidade:

as polícias têm dificuldade em investigar ataques, já que os criminosos costumam agir a partir de outro país.

Por enquanto, os hackers têm como alvo principal donos de empresas pequenas e médias. Essas vítimas costumam ter proteção digital falha se comparada à usada por grandes empresários. Mas já se vê uma tendência mais assustadora: esses ataques devem migrar para dentro de nossas casas.

A primeira porta de entrada é o smartphone. Crescem no mundo casos de ataques enviados por mensagens instantâneas e e-mails. Hackers bloqueiam o álbum de fotos e pedem resgates de valores pequenos para que a vítima pague com mais facilidade. Os criminosos ganham em escala. Autoridades de diferentes países também preveem que, com o aumento de dispositivos conectados, teremos ataques a fechaduras digitais, geladeiras e sistemas de luz residenciais. No Reino Unido, o Centro Nacional de Segurança Cibernética alertou os cidadãos para os perigos envolvendo ataques de ransomware e a popularização de dispositivos ligados à internet, como relógios, TVs e outros eletrodomésticos. Autoridades do Japão já sofrem com esse fato: em janeiro, a polícia do país registrou mais de 300 ataques a TVs conectadas.

O PLANO DETALHADO DO

Como funcionam os ataques de ransom

1
ATAQUE

Como funciona o ransomware



O hacker invade o computador da vítima, normalmente após ela clicar num link malicioso

2
INFECÇÃO

Como hackers encontram suas vítimas



PHISHING

Os criminosos enviam e-mails ou mensagens com links maliciosos. Ao clicar neles, a máquina é infectada



POR PÁGINAS INFECTADAS

Muitos anúncios espalhados pela internet escondem links maliciosos



DOWNLOAD

DE SOFTWARE Sites para baixar programas, apps e filmes piratas estão repletos de vírus



PEN DRIVE

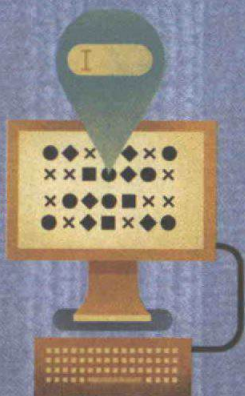
Criminosos deixam pen drives perto de escritórios. Quem acha e usa o dispositivo acaba infectando a rede

SEQUESTRO DIGITAL

ware e por que é tão difícil rastrear os criminosos



O criminoso copia os dados para um servidor externo protegido por um código e toma os arquivos do computador da vítima inacessíveis



A vítima vê os arquivos, mas o computador não reconhece a extensão. Para reaver os dados, é preciso usar um código enviado pelos criminosos



Os criminosos enviam links com tutoriais de como fazer o pagamento usando a moeda virtual bitcoin. Há até SACs dedicados a facilitar o pagamento

3 OPÇÕES DA VÍTIMA

Como proceder depois que o ataque ocorre



IGNORAR O ATAQUE

Quem tem cópias dos dados (ou não precisa deles) pode ignorar o ataque e remover o vírus



ENCONTRAR UMA CHAVE

Há um consórcio de empresas de segurança digital que liberam senhas para recuperar arquivos criptografados por criminosos. É necessário, porém, que o servidor usado pelo hacker já tenha sido alguma vez desovertado e "derrubado" por empresas de segurança ou autoridades



PAGAR

Uma parte das vítimas paga, porque o valor do resgate é baixo ou por temer ameaças, como divulgação de fotos íntimas

4 IMPUNIDADE

Por que os criminosos não são descobertos



IP MASCARADO

Os hackers mudam seu endereço de IP, ou seja, sua localização, a fim de confundir autoridades



PAGAMENTO EM BITCOIN

Os hackers pedem que a vítima pague em moeda virtual, mais difícil de ser rastreada

Hackers bloqueavam o acesso aos aparelhos e os liberavam após o pagamento de US\$ 100 em frações de bitcoin.

O brasileiro tem motivo para se preocupar porque o ritmo de ataque às empresas brasileiras mostra o segundo maior crescimento do mundo, atrás apenas da Índia (*leia mais no quadro na página 66*). Não que esse tipo de crime seja coisa de país subdesenvolvido. Um relatório do FBI, a polícia federal americana, estimou as perdas das vítimas nos Estados Unidos em US\$ 209 milhões só nos três primeiros meses do ano passado, um salto enorme em relação a 2015, quando as perdas somaram US\$ 25 milhões no ano todo. O FBI ressaltou que o volume deve ser bem maior, já que uma minoria das vítimas reporta o ataque. A Europol, polícia internacional europeia, afirmou num relatório que, em 2016, o ransomware se tornou o crime cibernético mais difundido no continente, acima do roubo de dados e da invasão de contas bancárias. A dimensão da ameaça levou o governo americano – num esforço conjunto da Agência Nacional de Segurança (NSA), da Central de Inteligência (CIA) e outras agências – a fazer uma cartilha para orientar profissionais de tecnologia e segurança em organizações de todos os portes. O perigo generalizado também aparece nos relatórios das empresas de segurança da informação. Segundo a russa Kaspersky Lab, entre abril de 2015 e março 2016, houve mais de 2,3 milhões de ataques do tipo no mundo. A Intel Security afirma que globalmente o aumento em 2016 foi na casa dos 80% e que o ápice deverá ocorrer em meados deste ano. A empresa de segurança digital Trend Micro publicou neste mês um estudo que ouviu 300 empresas no Brasil. Segundo o relatório, 51% das companhias sofreram tentativas de ataques de ransomware ao longo de 2016. Por que, pergunta o cidadão conectado, os criminosos não se contentam em atacar empresas e empresários? Resposta: porque, para os bandidos, é fácil ganhar muito aplicando vários pequenos golpes.

A tendência de migração dos ataques para pessoas físicas preocupa no Brasil, dada a situação ruim do país em relação a outros crimes digitais. Somos hoje, ►

segundo a Kaspersky, o maior alvo de ataques de phishing (o envio de links maliciosos por e-mail ou mensagem no celular, que induzem ao clique), principal porta de acesso dos sequestradores digitais a nossos dados. O país sofre também com o maior número de ataques de trojans bancários, golpe que rouba dados de correntistas e transfere dinheiro de suas contas. Na semana passada, a Polícia Federal iniciou a segunda fase da Operação Darkode, que prendeu membros de uma quadrilha que fraudava sistemas bancários. Estima-se que o esquema tenha causado prejuízo de mais de R\$ 2,5 milhões.

Num dos maiores ataques cibernéticos registrados no Brasil recentemente, a corretora XP Investimentos viu os dados de 29 mil clientes ir parar na mão de hackers. Os criminosos pediram o equivalente a R\$ 22 milhões em bitcoins para não revelar o roubo ao público. A companhia não cedeu à chantagem e alguns clientes chegaram a ser contactados com pedidos de resgate. Até o momento, os dados não vazaram. Tampouco chegou-se aos criminosos.

Ao longo das últimas semanas, ÉPOCA acompanhou casos de brasileiros donos de empresas de vários portes que sofreram ataques de ransomware. Todas pediram que não fossem identificadas. Por se tratar de exigências de resgate relativamente baixo para o orçamento de empresas – os criminosos pedem em média entre R\$ 5 mil e R\$ 20 mil –, muitas aceitam pagar e não comunicam a polícia. Quando decidem procurar alguma autoridade, as vítimas desses ataques raramente encontram respaldo adequado. “Cheguei a procurar a delegacia especializada em crimes digitais de São Paulo, mas fui orientada a fazer o registro da ocorrência numa delegacia comum”, diz Maria. “Acabei eu mesma contratando um ‘hacker do bem’ para investigar as brechas e blindar nosso sistema contra novos ataques.”

ÉPOCA procurou órgãos públicos que podem vir a enfrentar esse tipo de crime. O grupo de trabalho de crimes cibernéticos do Ministério Público Federal (MPF) afirma estar ciente do crescimento do ransomware global, mas considera o crime, por enquanto, fora de seu escopo. “Se atingir bens da União,



além da PF há também o setor do Gabinete de Segurança Institucional da Presidência da República com pessoal preparado para lidar com ataques cibernéticos”, informa o MPF. A PF dispõe de técnicos que estudam o assunto, mas, procurada pela reportagem, preferiu não se manifestar. “Há pelo menos três crimes envolvidos num ataque de ransomware: extorsão, crime de ameaça e, no caso de um indivíduo, o delito de invasão de dispositivo informático”, diz Gisele Truzzi, advogada especialista em Direito Digital do escritório Truzzi Advogados.

Prestadores de serviços em geral são os principais alvos, já que a interrupção de seus negócios causa prejuízo financeiro ou de imagem imediatamente, o que

estimula o pagamento rápido do resgate. No final do ano passado, parte do sistema de transporte público da cidade de San Francisco, na Califórnia, ficou parada após um ataque de ransomware. Os criminosos pediram US\$ 73 mil para liberar o sistema, que controla o acesso aos trens e a parte dos ônibus da cidade. Não houve cobrança de passagem por dois dias. No terceiro, a companhia optou por pagar o resgate para evitar prejuízo maior. Também no ano passado houve ataques a hospitais em Wichita, no Kansas, e em Los Angeles, na Califórnia. Os criminosos bloquearam o acesso a prontuários de pacientes e exigiram pagamentos de resgate. No Brasil, houve ao menos um caso similar, comunicado por uma em-

preocupa

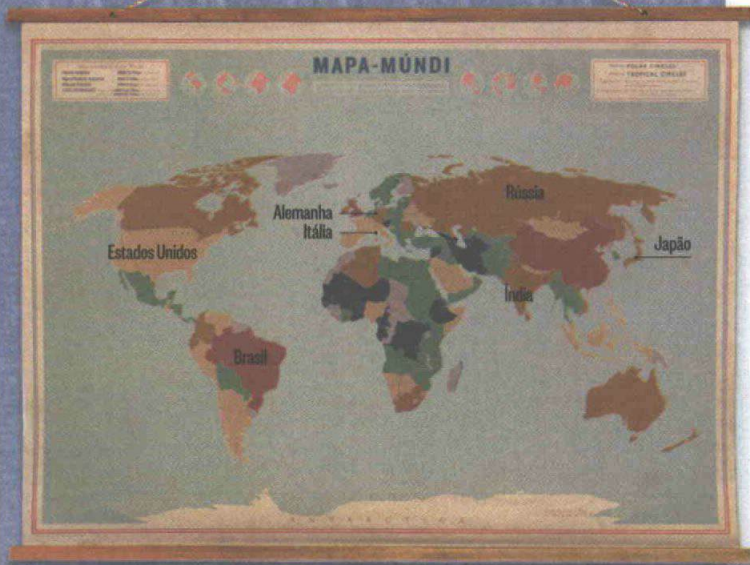
US\$ 209
milhões



em 3 meses
DE 2016

2017

Pelo menos 300 TVs conectadas são bloqueadas por um ataque de ransomware no Japão. É uma nova fase do crime digital



O PARAÍSO DA PESCARIA

O phishing é a principal porta de acesso de sequestradores digitais, e o Brasil aparece no topo do ranking desse tipo de ataque

Fontes: Kaspersky e FBI

Em % do total global de ataques



presa de segurança digital. Foi um dos primeiros ataques de uma família brasileira de ransomware: a TeamXRat (uma “família” é a comunidade de criminosos que usa um mesmo trecho de software original, a partir do qual elabora variações). No início de 2017, houve talvez o caso mais curioso de sequestro de dados até agora. Hóspedes que chegavam ao hotel Romantik Seehotel Jägerwirt, na Áustria, descobriram que não conseguiam entrar no quarto. O sistema não emitia novos cartões de acesso. A administração do hotel recebeu então um e-mail exigindo o pagamento de US\$ 1.800. O hotel cedeu à chantagem.

Sem uma estrutura adequada por parte das polícias para combater esse

tipo de crime, cabe às próprias vítimas criar uma estratégia para se precaver. A boa notícia é que a tarefa é relativamente simples do ponto de vista tecnológico. No caso de Maria, relatado no início deste texto, o problema estava numa versão de antivírus desatualizada e na falta de um sistema adequado para armazenar cópias dos dados, a usar em casos de emergência – um backup. Empresários precisam criar políticas rígidas de manutenção dessas cópias. Assim, o sistema pode até ser atacado e os dados criptografados, mas em pouco tempo é possível restaurá-los. Famílias também têm de fazer cópias de seus dados e recordações digitais. Outro ponto-chave é educar os usuários de

computadores ou outros dispositivos conectados a uma rede – sejam os integrantes de uma família, sejam os funcionários de uma empresa. Os ataques de phishing costumam usar engenharia social: a partir da observação de certos comportamentos, enviam links que convidam ao clique – podem ser notícias sensacionalistas falsas, imagens pornográficas, promoções imperdíveis ou alertas falsos de problemas bancários ou tecnológicos. Criminosos também abordam os assuntos do momento. Recentemente, houve um aumento de ataques que se aproveitaram da curiosidade do cidadão em relação ao FGTS. Manter um antivírus atualizado não resolve, mas ajuda. E, quanto mais conhecimento técnico em segurança, melhor. Isso ajudou Tadeu Gonçalves*, dono de uma empresa de contabilidade em Petrópolis, no Rio de Janeiro.

Ele diz não se arrepender de ter pago caro num sistema de backup para sua empresa. No final de 2015, um de seus 30 funcionários clicou num link malicioso e infectou os servidores do escritório. Em pouco tempo, as informações de quase 250 clientes estavam nas mãos de sequestradores. Gonçalves conseguiu isolar a máquina infectada da rede e restaurar os dados do sistema. Em menos de 24 horas, recuperou o controle da empresa. “Se tivesse perdido aquelas informações, meu negócio teria falido”, diz. “Certamente acabaria pagando o resgate.”

O estado de alerta para não clicar em links estranhos nem abrir mensagens que apelam à curiosidade deve ser contínuo. As técnicas usadas por sequestradores digitais evoluem constantemente. “Eles estão sempre um passo à frente das autoridades e empresas de segurança”, diz Caroline Teófilo, sócia e responsável pela área de Segurança da Informação do escritório **Patricia Peck Pinheiro Advogados**. No fim do ano passado, uma variante de ransomware lembrou as táticas macabras do personagem Jigsaw, no filme *Jogos mortais*: a vítima podia optar por pagar um bitcoin e recuperar os dados ou infectar outros dois usuários. Parte da explicação sobre o avanço recente do ransomware está na evolução da tecnologia usada para os ataques. A primeira ►

variante data de 1989. Um pesquisador de aids foi a um congresso dedicado à doença e distribuiu disquetes infectados com um vírus, afirmando que eles continham informações sobre o trabalho de pesquisa. Quem colocava o disquete no computador o bloqueava. Para receber a senha de desbloqueio, era preciso enviar US\$ 189 a uma caixa postal no Panamá. Mas a atuação de bandidos como o cientista-sequestrador era limitada em um mundo predominantemente off-line. A lógica mudou com o surgimento do bitcoin, uma moeda virtual não vinculada a bancos centrais, que ganhou popularidade nos últimos cinco anos. Para fazer um pagamento, basta o dono de uma moeda transferir seu código virtual para o destinatário. Uma rede de corretoras de bitcoins compra e vende essas moedas, cujo valor flutua de acordo com oferta e demanda. São empresas espalhadas por diferentes países e não necessariamente são registradas em órgãos oficiais. A identificação dos proprietários dessas carteiras é mais complicada.

Apesar de não ser impossível rastrear essas atividades, é muito difícil autoridades de um país identificarem os criminosos fora de sua jurisdição. “Em muitos casos, esses criminosos até estão nos países de origem das vítimas”, afirma Caroline Teófilo. “Mas eles adotam técnicas para mascarar o IP (*endereço de origem*), como o uso de redes privadas virtuais (VPNs) e redes tor (*software que cria uma área de atuação anônima na internet*)”, diz. Em outras palavras, é fácil para um criminoso brasileiro se passar por um russo e vice-versa, a fim de despistar investigações.

Os hackers que fazem ataques de ransomware encontram facilmente as armas de que precisam para agir. Em sites de comércio eletrônico populares, é possível encontrar kits com programas e instruções para infecção de computadores por valores que variam de US\$ 300 a US\$ 5 mil, dependendo da complexidade da ferramenta e da criptografia usada. Normalmente, os kits têm nomes que soam inofensivos para despistar, com expressões como “para fins educacionais”. As vendas também ocorrem em fóruns que reúnem crimi-

PRINCIPAIS ATAQUES DE RANSOMWARE

Os casos de sequestro de dados que ganharam mais repercussão



TRANSPORTE EM SAN FRANCISCO Estados Unidos 2016

Um atacante paralisou o sistema de transporte de San Francisco por dois dias e pediu o pagamento de US\$ 73 mil. No terceiro dia, a companhia optou por pagar e retomar o sistema.



HOSPITAL DO CORAÇÃO DO KANSAS Estados Unidos 2016

Hackers invadiram o sistema do hospital e bloquearam prontuários de pacientes. O hospital não revelou o valor, mas admitiu ter pago o resgate exigido.



HOTEL ROMANTIK Áustria 2017

O hotel de luxo recebeu um ataque que bloqueou o sistema responsável por emitir cartões de acesso aos quartos. Os hackers pediram US\$ 1.800. A gerência do hotel decidiu pagar.

nosos virtuais, como no IRC (Internet Relay Chat), uma das mais antigas ferramentas de bate-papo da internet.

As promessas de quem vende o kit são de uma renda mensal que pode chegar a US\$ 25 mil, dependendo da disposição e astúcia do criminoso. Em 2016, uma única campanha de ataques afetou 150 mil vítimas e extorquiu delas US\$ 2,5 milhões. Segundo um estudo da Intel Security, estima-se que a maior das famílias de ransomware, a Crypto-Wall, já tenha arrecadado, ao longo de anos, mais de US\$ 300 milhões. Grandes quadrilhas globais montaram até estruturas complexas de venda e atendimento, uma espécie de SAC do crime digital. Por eles, hackers iniciantes tiram suas dúvidas por e-mail e vítimas recebem a orientação, passo a passo, de como fazer o pagamento dos resgates. As empresas de segurança identificaram também um sistema de pirâmide. Hackers mais experientes oferecem uma infraestrutura de ataque em troca de uma fatia do dinheiro obtido com resgates pelos criminosos que estão começando no golpe.

Um dos poucos registros de prisões de acusados de sequestro de dados digitais ocorreu na Holanda no final de 2015. Dois hackers da cidade de Amersfoort, de 18 e 22 anos, foram apontados como responsáveis pela família CoinVault. Os ataques resultaram em pagamentos de resgates em 20 países. Mas casos assim são raros. “Os próprios criminosos preferem fazer ataques menos ambiciosos, que gerem um volume menor de denúncias e não chamem a atenção das autoridades”, diz a advogada Caroline. “Eles querem um dinheiro que vem rápido e de diversas fontes”, afirma.

Com o bitcoin e as tecnologias que facilitam o anonimato dos hackers, o ataque de ransomware é praticamente o crime perfeito. O sequestrador não entra em contato com a vítima, quase não deixa vestígios que o incriminem e aplica o mesmo golpe repetidas vezes. A proteção contra esse tipo de ataque, por enquanto, está nas mãos das vítimas em potencial. No caso, você. ♦

**Os nomes foram alterados para garantir a privacidade das vítimas*



GUSTAVO CERBASI

A poupança voltará algum dia à boa forma?

A poupança não é mais a mesma. Já são dois anos de quedas recorde no saldo poupado pelos brasileiros, com saques superando as aplicações em R\$ 53,6 bilhões e R\$ 40,7 bilhões em 2015 e 2016, respectivamente, valores representativos para um saldo total de R\$ 665 bilhões (no final de 2016).

Os motivos são evidentes. Em primeiro lugar, a crise econômica, que obriga as famílias a consumir suas minguadas reservas. O segundo motivo, que considero o mais importante e dificilmente reversível, é o fato de que a poupança deixou de ser a melhor opção – não apenas para os mais endinheirados, mas também para aqueles que poupam pouco e por pouco tempo.

Há até pouco tempo, a poupança era a única opção do trabalhador de baixa renda. Para acessá-la, bastava ter uma conta salário ou abrir uma conta poupança, ambas obrigatoriamente isentas de tarifas, para fazer render o dinheiro não utilizado no consumo. Para acessar investimentos mais complexos e rentáveis, era necessário abrir uma conta-corrente de serviços, com pacotes mensais de tarifas que cobravam do pequeno poupador mais do que a vantagem que ele obtinha nos investimentos.

Por mais vantajosos que fossem os CDBs, títulos públicos, fundos de renda fixa e similares, o custo para acessá-los só se justificava para aplicações mais robustas, o que fortalecia a oportunidade da tradicional poupança. Hoje, com as novas contas eletrônicas isentas de tarifas

(aquelas que você abre e movimenta apenas pela internet), é possível acessar, sem custo, opções de investimento e enviar recursos para corretoras investirem em títulos públicos.

Não há argumento que favoreça a poupança. Dos produtos de renda fixa, seu ganho de 6% ao ano é inferior ao dos títulos públicos e de muitos fundos DI, mesmo após descontar os tributos. A segurança ao investir nela não é maior do que a proteção que o Fundo Garantidor de Crédito dá à maioria dos produtos de renda fixa. Os bons rendimentos dos títulos públicos são acessíveis para quem dispõe de valores reduzidos, a partir de R\$ 30.

Mesmo a complexa e pesada tributação para quem poupa por pouco tempo não favorece a poupança. A liquidez diária dos produtos financeiros de renda fixa é mais vantajosa mesmo com o pagamento de Imposto de Renda e IOF, já que a poupança não rende nada para quem resgata antes de completar 30 dias.

O poupador tem mais opções, com maior rentabilidade, e essa condição continuará ainda por um bom tempo, mesmo com a queda da taxa básica de juros. Bom para o poupador, que ficou mais informado e seletivo, mas um sinal de alerta para o mercado financeiro – afinal, é das aplicações na poupança que vem boa parte dos fundos de baixo custo para financiar a casa própria. ♦

Gustavo Cerbasi (www.gustavocerbasi.com.br)
é especialista em educação financeira.
Facebook: **Gustavo Cerbasi**