Golpe usa Chrome para alterar boletos online no Brasil

Se você é usuário do Google Chrome, fique atento: cibercriminosos brasileiros têm espalhado extensões maliciosas com o objetivo de alterar boletos gerados online, direcionando o pagamento para outra conta bancária.

O golpe foi descoberto pela empresa de segurança Kaspersky.

Segundo comunicado, as extensões estavam hospedadas na loja oficial, a Chrome Web Store, disfarçadas como bônus de 100 minutos para usuários do serviço Skype to Go, conforme mostra a imagem abaixo.

Ao ser instalada, a funcionalidade solicita permissão para acessar todo o conteúdo exibido em todas as abas abertas no navegador e usará o nome “Skype To Go”:

Sem especificar números, a Kaspersky informa que "diversos usuários" instalaram a extensão maliciosa e postaram seus comentários na página:

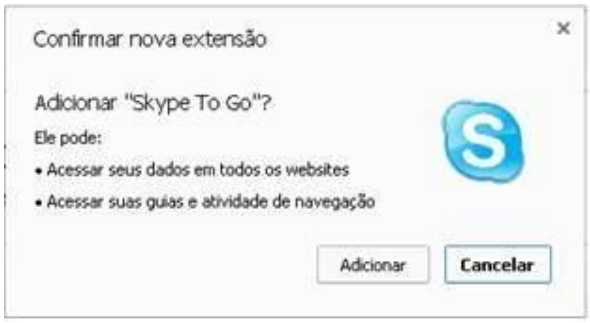
Três versões diferentes foram encontradas. De acordo com as informações, o plugin monitora todo o conteúdo exibido nas abas, buscando por termos como "boleto" e alterando os números da linha digitável.

A extensão está programada para se comunicar com um servidor de Controle e Comando (C&C) de onde o cibercriminoso envia a nova linha digitável a ser inserida no boleto, no ato em que o documento é gerado no navegador. O recurso invalida o código de barras do boleto, porém não altera o valor.

Segundo a Kaspersky, o esquema ataca boletos de qualquer banco, como se nota abaixo:

boleto_amigos.php	12-Nov-2013 18:57 5.3K
boleto_bancoob.php	11-Nov-2013 22:25 5.3K
boleto_banespa.php	11-Nov-2013 22:25 5.0K
boleto_banestes.php	11-Nov-2013 22:25 5.1K
boleto_bb.php	13-Nov-2013 20:14 6.1K
boleto_besc.php	11-Nov-2013 22:25 4.9K
boleto_bradesco.php	13-Nov-2013 00:09 5.1K
boleto_cef.php	14-Nov-2013 00:07 5.5K
boleto_cef_sigcb.php	11-Nov-2013 22:25 5.5K
boleto_cef_sinco.php	11-Nov-2013 22:25 5.6K
boleto_hsbc.php	13-Nov-2013 20:27 5.5K
boleto_hsbc1.php	11-Nov-2013 23:49 4.8K
boleto_itau.php	11-Nov-2013 22:25 5.0K
boleto_nossacaixa.php	11-Nov-2013 22:26 5.5K
boleto_real.php	11-Nov-2013 22:26 4.9K
boleto_santander_banespa.php	11-Nov-2013 22:26 5.1K
boleto_sicredi.php	11-Nov-2013 22:26 6.0K
boleto_sofisa.php	11-Nov-2013 22:26 5.2K
boleto_sudameris.php	11-Nov-2013 22:26 5.7K
boleto_unibanco.php	11-Nov-2013 22:26 5.1K

A empresa diz que o Google foi alertado e removeu as extensões depois de 24 horas, porém ressalta que novas versões podem aparecer por lá. A recomendação é que o usuário evite a instalação, mesmo que ela esteja na Chrome Web Store. Caso deseje ir em frente, é aconselhável verificar as permissões solicitadas e negar acesso aos dados em todos os sites visitados.



Ficou interessado neste assunto? Leia mais em (http://200.19.105.194/ceavi/arquivos/id_submenu/508/5_dicas_para_navegar_com_mais_seguranca_usando_o_google_chrome.pdf).

Fonte: http://olhardigital.uol.com.br/noticia/38894/38894