manchete

Público

23-03-2020

Periodicidade: Diário
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 31885

Temática: Justica
Dimensão: 1199 cm²
Imagem: S/Cor
Página (s): 1/22


Empresas aceleram resposta a explosão do comércio online

Cibercrime
Piratas informáticos atacam clientes da EDP, BCP e Crédito Agrícola

Sociedade, 22

manchete

Público

23-03-2020

Periodicidade: Diário
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 31885

Temática: Justica
Dimensão: 1199 cm²
Imagem: S/Cor
Página (s): 1/22

Piratas informáticos atacam clientes de dois bancos e da EDP

O Gabinete Cibercrime da Procuradoria-Geral da República deu o alerta de mensagens de *phishing* a 13, 16 e 17 de Março. O facto de estar muita gente em teletrabalho pode potenciar ataques, avisam as autoridades

Cibercrime
Sónia Trigueirão

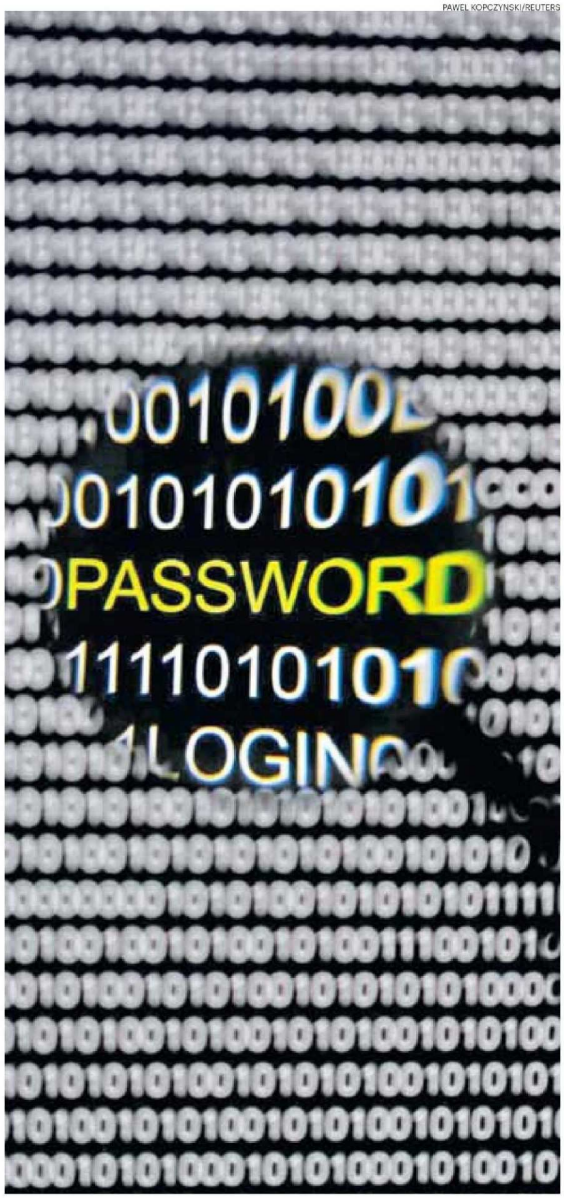
Piratas informáticos lançaram várias campanhas de *phishing* com o objectivo de conseguir os dados de acesso das contas dos clientes dos bancos Millennium BPC e Crédito Agrícola e até os dados dos cartões de crédito dos clientes da EDP. O alerta foi dado pelo Gabinete Cibercrime (GC) da Procuradoria-Geral da República, que publicou a informação na sua página da Internet depois de ter detectado os ataques nos dias 13, 16 e 17 de Março.

O *phishing* é um golpe que consiste em criar *sites* falsos com o endereço, nome e a imagem semelhantes a páginas de bancos para enganar as vítimas, enviando depois informações às pessoas via *email*. A partir desse esquema, o criminoso consegue roubar informações pessoais, como senhas de acesso, dados bancários e números de cartões de crédito.

No caso da EDP, a campanha de *phishing* foi dirigida a pessoas que eram simultaneamente clientes e titulares de cartões de crédito Visa e Mastercard. Os autores pretendiam convencer as vítimas a facultar-lhes dados dos seus cartões de crédito, com o argumento de que pretendiam reembolsar-lhes quantias.

O processo começou com a expedição, para múltiplos destinatários, de mensagens fraudulentas de correio electrónico. "Foram registadas mensagens desta natureza desde o início do mês de Março e foi sinalizada pelo Gabinete Cibercrime uma concreta mensagem desta campanha expedida a 12 de Março de 2020, pelas 10 horas e 46 minutos", refere o alerta. Nas mensagens com o título "Reembolso N°100000251", anunciava-se que o cliente da EDP iria "receber um reembolso de 52,56 euros" e era indicado um *link*, assinalado com a expressão "clique aqui para acessar ao reembolso [sic]". As mensagens iam assinadas "EDP serviço universal, director de operações". O alerta explica que "este *site* não é gerido pela EDP, nem é por ela autorizado" e que se "trata de uma página falsa, que tem como único propósito capturar os dados de cartão de crédito das vítimas".

PAWEL KOPCZYNSKI/REUTERS



Deve desconfiar-se de emails que impelem a abrir *links*, com urgência

A EDP explicou que tem registado esquemas de *phishing* com o objectivo de extorsão de dinheiro ou credenciais aos seus clientes. De acordo com a EDP, "estes esquemas variam no método e frequência", sendo que as últimas fraudes de que a empresa tem registo se "caracterizam pelo envio de *e-mails* de 'reembolso', que circularam há já algum tempo, primeiro em nome da EDP Comercial e mais recentemente da SU Eletricidade, e uma outra, idêntica, registada há cerca de um ano, com o envio de SMS e *e-mails* que incluíam *links* para descarregar supostas facturas". Em todos estes casos, a EDP refere que agiu de acordo com o procedimento que tem estabelecido: "Bloqueio de *sender/domain* para as nossas redes e notificação à entidade gestora do domínio sobre acto criminoso; comunicação ao CNCS (Centro Nacional de Cibersegurança) e articulação entre a equipa de segurança e as áreas de negócio para divulgação de alerta nos canais de comunicação com o cliente."

Através de um esquema de *phishing*, os piratas informáticos tentavam obter dados pessoais dos clientes

No caso do banco Millennium BCP, o processo começou também com a expedição, para muitos destinatários, de mensagens fraudulentas de correio electrónico. A primeira sinalizada pelo Gabinete Cibercrime foi recebida a 17 de Março às 8 horas e 7 minutos, com o assunto "Notificação nova mensagem". É exibido um logótipo similar ao do banco e anuncia-se o seguinte: "Você tem uma nova mensagem esperando por você na caixa de entrada do NetBanco. Você pode visualizá-la fazendo *logon* no Homebanking [sic]". Aparece depois o apelo: "Clique aqui para acessar sua conta MilleniumBCP [sic]". As mensagens vêm assinadas "Millennium BCP". O banco remeteu explicações para a sua página da Internet, onde há dados sobre este ataque e outros exemplos de páginas fraudulentas.

Já o Banco Crédito Agrícola (CA) diz: "Não tivemos conhecimento do alerta e não identificámos até ao momento qualquer situação que tenha originado fraude. O CA tem realizado várias comunicações sobre segurança com o objectivo de sensibilizar e informar todos os clientes utilizadores de canais e por essa razão estão mais atentos."

Porém, o alerta do GC é muito claro. Refere que está em curso uma campanha de *phishing*, dirigida a clientes da instituição bancária Crédito Agrícola. A primeira mensagem sinalizada foi recebida a 13 de Março de 2020, pelas 10 horas e 37 minutos, com o assunto "Importante – informações da conta #0012807325". Ordena depois que "deve fazer *login* na conta do Crédito Agrícola o mais rápido possível e aceitar as novas condições para confirmar e/ou actualizar seus dados pessoais". Há um *link* assinalado com a expressão "Clique aqui". As mensagens vêm assinadas "Crédito Agrícola".

Pedro Verdelho, responsável pelo GC, confirmou ao Público que "efectivamente foi detectada nos últimos dias uma actividade mais frequente de cibercriminalidade, circunstância que foi já sublinhada pela Polícia Judiciária e pelo Centro Nacional de Cibersegurança". Segundo o responsável, "esta maior intensidade ocorre numa altura em que aumentou exponencialmente o número de pessoas em teletrabalho, ao mesmo tempo que a generalidade das entidades públicas e privadas tem solicitado que os contactos dos seus clientes ou utilizadores sejam feitos à distância, por telefone ou por outras vias digitais".

"Assim ocorreu, designadamente, com os bancos e as entidades prestadoras de serviços públicos", sublinha Pedro Verdelho, que deixa conselhos: "Ser cauteloso na abertura de mensagens de correio electrónico e criterioso na respectiva interpretação; desconfiar de mensagens que, com urgência, impelem a abrir *links* ou a fornecer dados pessoais". Na dúvida, contactar o banco e denunciar a suspeita às autoridades.

sonia.trigueirao@publico.pt