ALERTA CIBERCRIME

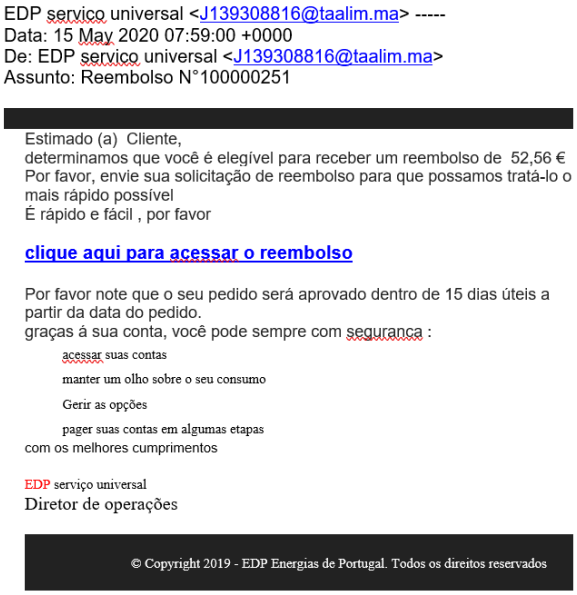
15 de maio de 2020

'*Phishing*' dirigido a clientes da EDP e a titulares de cartões de crédito

1. Está em curso uma nova campanha de *phishing*, dirigida a vítimas que sejam simultaneamente clientes da *EDP* e titulares de cartões de crédito *Visa*, *Mastercard* ou *JCB*. Nesta campanha, os seus autores pretendem convencer as vítimas a facultar-lhes dados dos seus cartões de crédito, com o argumento de que pretendem reembolsar-lhes quantias.

2. Como habitual em casos de *phishing*, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. Registou-se uma campanha anterior exatamente do mesmo teor[1] durante o passado mês de março. Agora, foi sinalizada pelo Gabinete Cibercrime uma concreta mensagem desta campanha a 15 de maio de 2020, às 7 horas e 59 minutos.

3. Nestas mensagens, com o título no assunto, "*Reembolso N°100000251*", anuncia-se que o destinatário, cliente da *EDP*, irá "*receber um reembolso de 52,56 €*". Para o efeito, indica-se de seguida um *link*, assinalado com a expressão "*clique aqui para acessar o reembolso*". As mensagens vêm assinadas com a expressão "*EDP serviço universal, Diretor de operações*".



EDP servico universal <J139308816@taalim.ma> -----
Data: 15 May 2020 07:59:00 +0000
De: EDP servico universal <J139308816@taalim.ma>
Assunto: Reembolso N°100000251

Estimado (a) Cliente,
determinamos que você é elegível para receber um reembolso de 52,56 €
Por favor, envie sua solicitação de reembolso para que possamos tratá-lo o mais rápido possível
É rápido e fácil , por favor

clique aqui para acessar o reembolso

Por favor note que o seu pedido será aprovado dentro de 15 dias úteis a partir da data do pedido.
graças á sua conta, você pode sempre com segurança :

acessar suas contas
manter um olho sobre o seu consumo
Gerir as opções
pager suas contas em algumas etapas

com os melhores cumprimentos

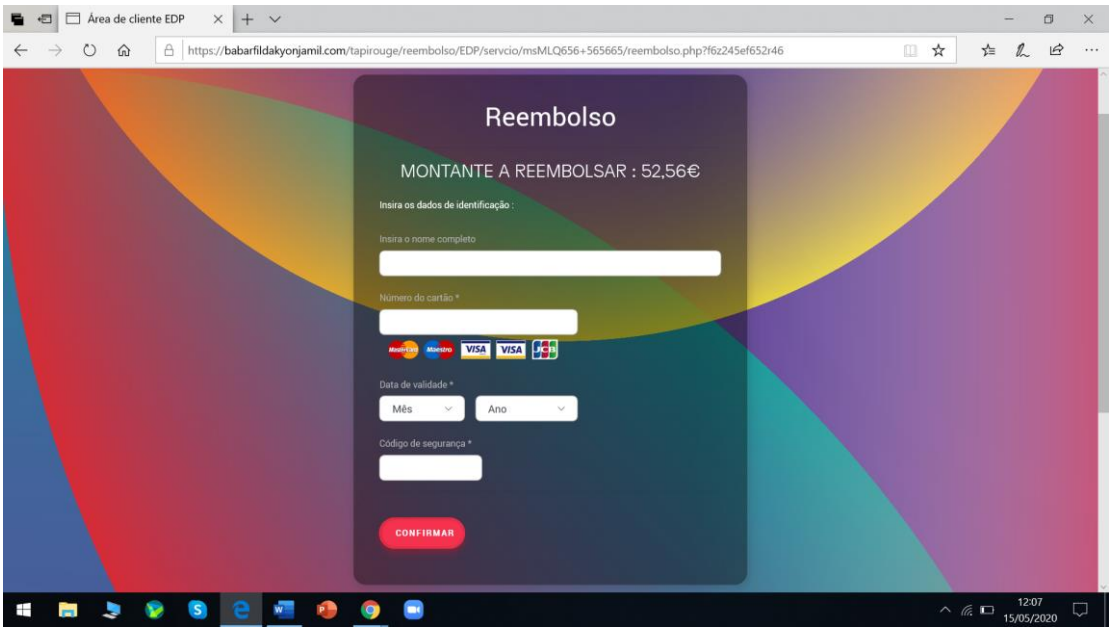
EDP serviço universal
Diretor de operações

© Copyright 2019 - EDP Energias de Portugal. Todos os direitos reservados

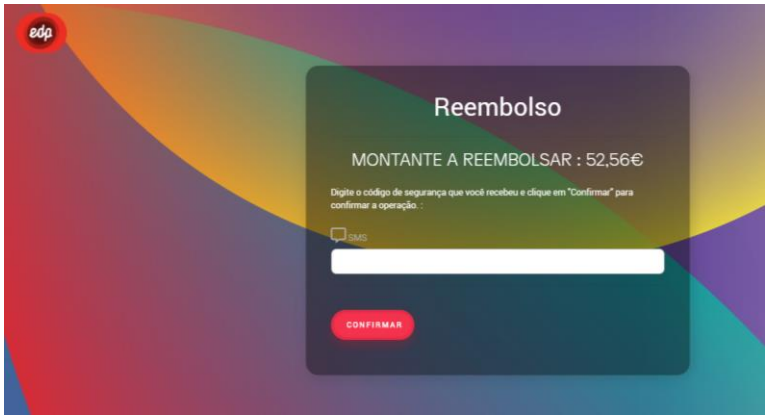
[1] A presente campanha dá sequência à outra, relatada no alerta cibercrime de 16 de março de 2020, disponível aqui: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/alerta_edp_visa_2020_03_14.pdf.

4. Trata-se de mensagens fraudulentas, não provenientes da *EDP*. Não foram remetidas pela *EDP* nem a partir de sistemas informáticos pertencentes a esta companhia.
Aparentemente, tais mensagens foram remetidas da caixa de correio "*EDP servico universal*", mas na verdade provieram do endereço J139308816@taalim.ma. É um endereço de correio eletrónico de uma plataforma pertencente ao Ministério da Educação Nacional de Marrocos.

5. Por sua vez, o *link* que se referiu, contido nas mensagens fraudulentas, conduz a um s*ite* Internet que aparenta ser o da *EDP*, exibindo aparência gráfica e um logotipo normalmente utilizados por aquela companhia.
Esta página *web* inclui espaços em que se solicita a introdução de dados da vítima: o seu nome completo, o número do seu cartão de crédito, a respetiva data de validade e ainda o seu código de segurança.



Caso o utilizador introduza todos estes dados, abre-se uma nova página em que é solicitada a introdução do "*código de segurança que você recebeu*". Porém, a vítima não recebe qualquer código – nem o mesmo é enviado. Aliás, de seguida surge uma nova página com a mensagem "*o código digitado está incorreto ou expirou, um novo código foi enviado a você*."



6. Este *site* não é gerido pela *EDP* nem é por ela autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página da *EDP*. Tem como único propósito capturar os dados de cartão de crédito das vítimas – os quais serão depois livremente utilizados pelo agente do crime.
Esta página fraudulenta utiliza o serviço *Contact Privacy* (https://contactprivacy.com), fornecido pela companhia "*Contact Privacy, Inc*", com sede em Toronto, no Canadá – trata-se de um serviço Internet destinado a esconder a identidade (incluído os dados do endereço, número de telefone ou endereço de email) do dono de uma página *web*, quando uma pesquisa WHOIS é realizada a este propósito. Esta página está, em todo o caso, alojada no fornecedor de serviços "*Tucows Domains Inc*." (http://tucowsdomains.com), igualmente com sede em Toronto, no Canadá, especializado no fornecimento de nomes de domínio e outros serviços de Internet.

7. Como se disse, esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página da *EDP*. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados do seu cartão de crédito, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.

8. Apurou-se que esta página fraudulenta está disponível, a partir do *link* fornecido com a mensagem remetida pelos agentes do crime, desde 11 de maio de 2020, às 9 horas e 22 minutos UTC. Ignora-se, neste momento, o número de vítimas que este procedimento criminal possa ter causado. Todavia, registos consultados revelaram que, entre aquela data e as 13 horas e 32 minutos UTC, aquela página teve 5536 visitas.