ALERTA CIBERCRIME

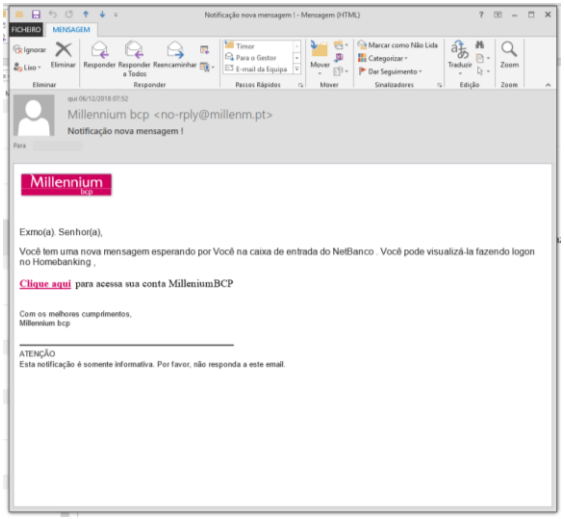
6 de dezembro de 2018

'*Phishing*' dirigido a clientes do Millenium BCP

1. Está em curso, pelo menos desde a manhã de 6 de dezembro de 2018, uma campanha de "*phishing*", dirigida a clientes do banco Millenium BCP.

2. Como habitual nestes casos, o processo começou com a expedição, para inúmeros destinatários, de mensagens fraudulentas de correio eletrónico. A primeira mensagem desta campanha sinalizada pelo Gabinete Cibercrime (*Imagem 1*) foi recebidas às 7 horas e 57 minutos de 6 de dezembro de 2018. Nestas mensagens anuncia-se estar pendente de abertura uma mensagem do banco, a qual é possível aceder por via de um *link* incluído no texto.
Trata-se, evidentemente, de mensagens fraudulentas, não provenientes do banco Millenium BCP.

Imagem 1

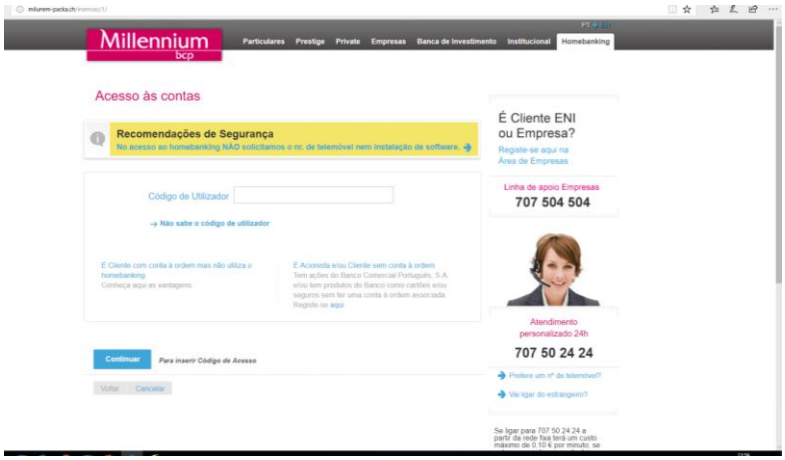


3. As mensagens indicavam como *Assunto*, "Notificação nova mensagem" e indicavam provir de um endereço de correio eletrónico "Millennium bcp", a que correspondia no-rply@millenm.pt. Além disso, incorporavam um logotipo igual ao efetivamente utilizado por aquele banco. Porém, este endereço não pertence ao banco em causa.
Na verdade, no caso sinalizado, a mensagem teve origem no domínio @discoveryvip.com, tendo sido usado para a sua remessa o endereço de IP 89.38.145.233, pertencente a um fornecedor de serviço Internet (*Aruba S.p.A. - CLoud Services UK*), com sede em Itália, mas cujos servidores informáticos estão localizados em várias jurisdições (designadamente no Reino Unido). Este fornecedor de serviço é

especializado em serviços na *cloud* (https://www.arubacloud.com) e, sobretudo, alojamento de conteúdos na internet em VPS - *Virtual Private Servers* (https://www.arubacloud.com/vps/virtual-private-server-range.aspx).

4. Por outro lado, o *link* que se referiu, contido nas mensagens fraudulentas, conduz a um s*ite* Internet onde se reproduzem, de forma muitíssimo fiel, todos os conteúdos disponibilizados no *site* autêntico do banco Millenium BCP. Porém, tal *site* não é gerido por aquele banco nem por ele autorizado. A esta página falsa (*Imagem 2*), clonada da página do banco Millenium BCP, corresponde o URL http://milunem-packa.ch/inamoac/1/, registado num *registrar* alemão (*CPS-Datensysteme GmbH* – https://www.cps-datensysteme.de), que igualmente vende de serviços de computação em nuvem (*cloud*), com anonimato.

Imagem 2



5. Recorda-se que a autêntica página do Millenium BCP, está alojada em https://ind.millenniumbcp.pt (*Imagem 3*). Porém, a página fraudulenta é muitíssimo parecida, praticamente igual em aparência, aos olhos do utilizador comum, com a autêntica página do Millenium BCP. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos dados de acesso, no legítimo *site* do Millenium BCP, à sua conta bancária. E assim, permitirá que terceiros procedam a movimentos bancários por esta via.

Imagem 3