ALERTA CIBERCRIME

13 de julho de 2017

'*Phishing*' dirigido a clientes do Montepio Geral

1. Está em curso mais uma campanha de "*phishing*" dirigido a clientes do Montepio Geral, que repete os procedimentos de várias campanhas anteriores.

2. Como habitual nestes casos, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. As mensagens desta nova campanha sinalizadas pelo Gabinete Cibercrime foram recebidas entre 9 e 12 de julho de 2017.
Nestas mensagens anuncia-se, como habitual, ser necessário proceder a *confirmação do acesso* no *site web* do Montepio Geral, para *manter a segurança da conta*. Anuncia-se que, caso tal confirmação não seja efetuada até 15 de julho, haverá lugar à cobrança de uma *coima de 27,99 euros*.
Trata-se, evidentemente, de mensagens fraudulentas, não provenientes do Montepio Geral.

3. Nalguns destes casos, as mensagens sinalizadas eram particularmente insidiosas, uma vez que indicavam serem provenientes do endereço de email "Montepio" (correspondendo a montepioppp@montepio.pt, montepio@aerolink.es e montepio@montepio.missoescuiaba.com.br, o que parecia indiciar serem endereços legítimos do Montepio Geral. Porém, assim não acontecia.
Tais mensagens provieram de servidores que usaram os endereços de IP 185.146.3.107 (pertencente ao fornecedor de serviços *PS Internet Company LLC*, baseado no Cazaquistão), 95.173.179.82 (pertencente ao fornecedor de serviços *Netinternet Bilisim Teknolojileri AS*, baseao na Turquia) e 188.165.130.96 (pertencente ao fornecedor de serviços *Proxy Protection LLC*, baseado na Califórnia, EUA, especializado no fornecimento de serviços de computação em nuvem, com anonimato).

4. As mensagens fraudulentas continham *links*, que referiam serem de acesso à página *web* do Montepio Geral. Esses *links* conduziam a *sites* Internet onde se reproduziam, de forma muitíssimo fiel, todos os conteúdos disponibilizados no *site* autêntico do Montepio. Porém, tais *sites* não são geridos por aquele banco nem por ele autorizados. A estas páginas falsas, clonadas da página do Montepio Geral, correspondiam os URL http://https.montepio.suporte-gerencia.com/, registado num *registrar*[1] brasileiro (*UOL Host* - http://www.uolhost.com.br) e http://www.jlink.de/media/system/js/aa.php, registado num *registrar* alemão (*Mittwald CM Service GmbH und Co.KG* - https://www.mittwald.de) tendo este último sido, entretanto, removido.

[1] Um *registrar* é uma organização credenciada para vender, ao público, nomes de domínio.

5. Recorda-se que a autêntica página do Montepio Geral está alojada em https://www.montepio.pt. Porém, a página fraudulenta é muitíssimo parecida, praticamente igual em aparência, aos olhos do utilizador comum, com a autêntica página do Montepio Geral. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados necessários ao acesso, no legítimo *site* do Montepio Geral, à sua conta bancária. E assim, permitirá que terceiros procedam a todos os movimentos bancários possíveis por esta via.