ALERTA CIBERCRIME

29 de junho 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. A primeira mensagem desta nova campanha sinalizada pelo Gabinete Cibercrime data de hoje, 29 de junho de 2017, pelas 11 horas e 15 minutos. Espera-se que venham a identificar-se outras.
Nesta mensagem anuncia-se 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 29 de junho, haverá lugar à cobrança de uma "coima de 85,99 euros".
Trata-se, evidentemente, de mensagem fraudulenta, não proveniente do Montepio Geral.

3. Neste caso específico, a mensagem sinalizada era particularmente insidiosa, uma vez que era proveniente do endereço de email "Montepio Geral [montepio5808831@montepio.com]", o que parecia indiciar ser um endereço legítimo do Montepio Geral. Porém, assim não acontecia.
Tal mensagem proveio de um servidor que usou o endereço de IP 212.237.59.19, pertencente ao fornecedor de serviços "*Aruba S.p.A. - Cloud Services*" (https://www.arubacloud.com/), baseado em Itália e especializado no fornecimento de serviços de computação em nuvem, com segurança (anonimato, antes de mais).

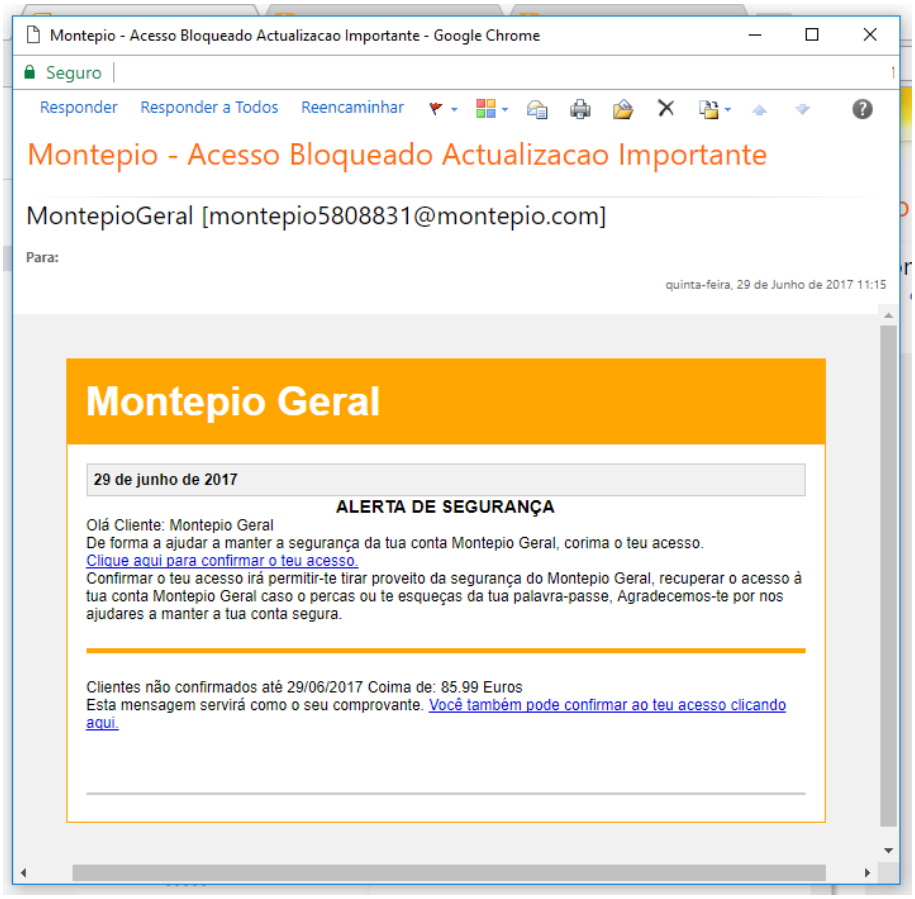
4. A mensagem fraudulenta contém um *link*, que refere ser de acesso à página *web* do Montepio Geral. Esse *link* conduz a um *site* Internet onde se reproduzem, de forma muitíssimo fiel, todos os conteúdos disponibilizados no *site* autêntico do Montepio. Porém, tal *site* não é gerido por aquele banco nem por ele autorizado. A esta página falsa, clonada da página do Montepio Geral, corresponde o URL http://super.hgfsoftwareschk.com.br (correspondendo-lhe o endereço de IP 217.61.20.118). O registo deste domínio foi efetuado num *registrar*[1] brasileiro (*UOL Host* - http://www.uolhost.uol.com.br/registro-de-dominio.html), mas os conteúdos do *site* parecem estar fisicamente alojados nos servidores da "*Aruba S.p.A. - Cloud Services*".

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

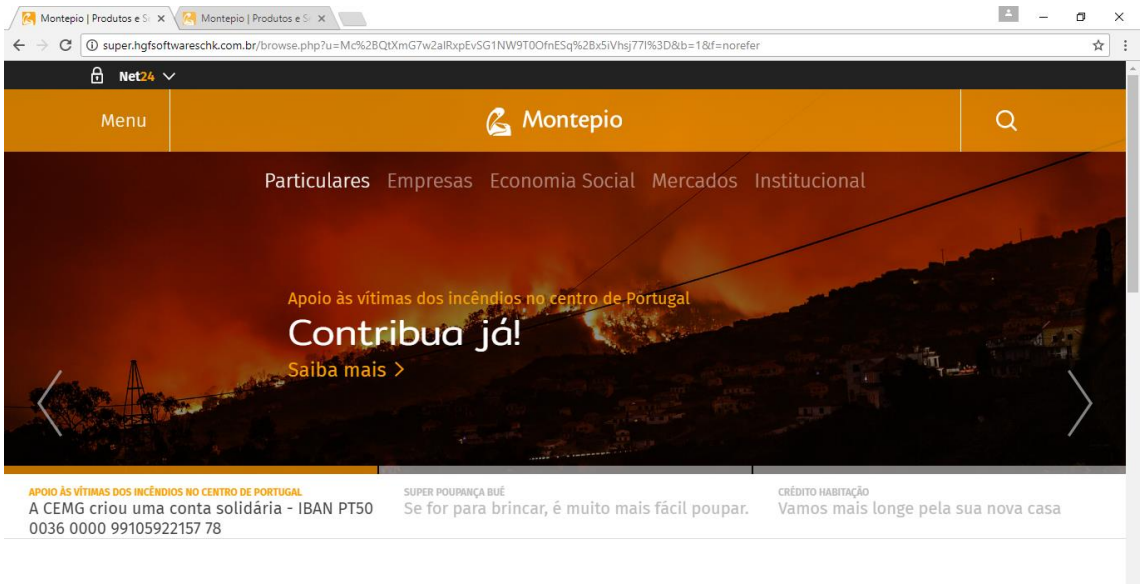
5. Recorda-se que a autêntica página do Montepio Geral está alojada em https://www.montepio.pt. Porém, a página fraudulenta é muitíssimo parecida, praticamente igual em aparência, aos olhos do utilizador comum, com a autêntica página do Montepio Geral. Se a vítima aceder a ela e nela introduzir a informação 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.

6. Juntam-se, em anexo, imagens recolhidas *online*, da mensagem fraudulenta e da página *web* falsa - como Anexo 1 e Anexo 2, respetivamente.

ANEXO 1



ANEXO 2



(http://super.hgfsoftwareschk.com.br/browse.php?u=Mc%2BQtXmG7w2alRxpEvSG1NW9T0OfnESq%2Bx5iVhsj77I%3D&b=1&f=norefer)