ALERTA CIBERCRIME

26 de outubro de 2018

Phishing – Passwords de Correio Eletrónico *(SapoTransfer)*

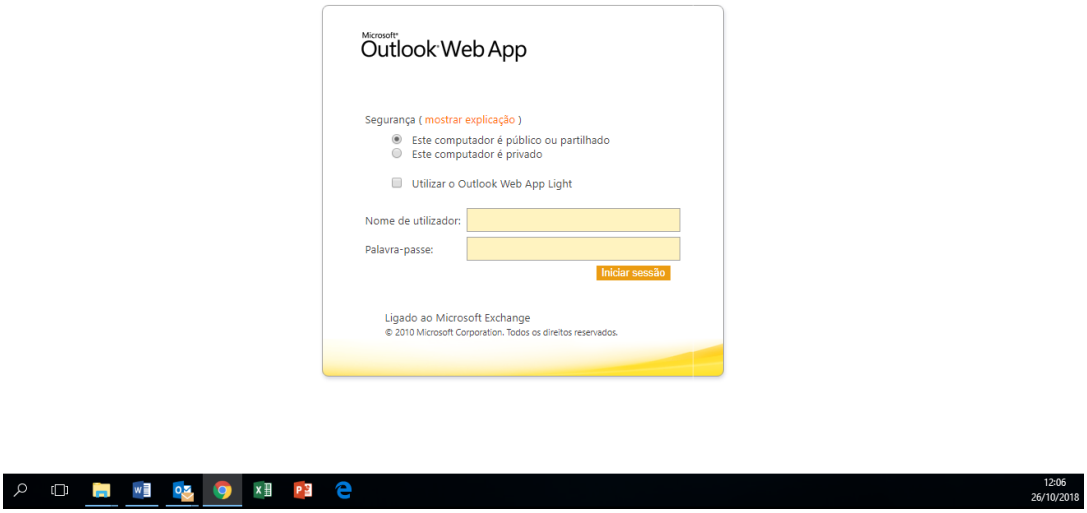
1. Chegou ao Gabinete Cibercrime nota de que está em curso uma campanha de *phishing* pela qual os seus agentes pretendem obter ilegitimamente credenciais de acesso a contas de correio eletrónico. Como é habitual em campanhas de *phishing*, o processo tem início com a remessa, para as vítimas, de mensagens de correio eletrónico com conteúdo enganador.

2. Em concreto caso comunicado ao Gabinete Cibercrime, a mensagem foi expedida a 26 de outubro de 2018, às 2 horas e 22 minutos, pela conta de *email* sapo.transfer@sapo.pt. O texto da mensagem referia que, a partir do endereço dflisboa-dlird@at.gov.pt, tinha sido enviado ao destinatário um ficheiro, por via do serviço de transferência de ficheiros *online* https://transfer.sapo.pt/. O aspeto gráfico da mensagem é igual ao habitualmente utilizado por aquele serviço *online*. A mensagem apelava ao *download* do ficheiro, contendo um botão para o efeito, com pode ver-se na imagem que segue.

3. Porém, esta mensagem não foi remetida por qualquer endereço do domínio @at.gov.pt, nem por via do serviço https://transfer.sapo.pt/: este expede as mensagens a partir do endereço noreply@transfer.sapo.pt e a mensagem criminosa provinha de uma vulgar conta

de *email* no domínio @sapo.pt. O verdadeiro remetente da mensagem usou o serviço de *email* @sapo.pt, acedendo ao mesmo a partir de local desconhecido, utilizando o endereço de IP 198.96.155.3, pertencente à Universidade de Waterloo, na província de Ontário, Canadá, cujo servidor *proxy* funciona como nó de saída TOR. Isto é, o remetente da mensagem pode ter acedido ao serviço @sapo.pt e expedido a mesma utilizando *software* de anonimização, que se destina a impedir a sua localização.

4. Por outro lado, na mensagem, quando o utilizador carregasse no botão "*Download*", o seu *browser* abria uma página na Internet, no endereço https://sapotransfer.netlify.com/oauth/redirect/dst7foawcabbos_jycbeimfbt1plry_fblcfana0peizmbu1jrpwrkpiwfaw3q5ncabrxo5x49mcuy8pb_ewnl7y3er7rf0b/protectedtoken/eta1nzjlnzetzdi0my0mdm1lthkygztytjlmde5/a1/logon. Esta página tem o aspeto gráfico do serviço de acesso a correio eletrónico por via do programa *Outlook Web*, sendo solicitado ao utilizador que introduza as suas credencias de acesso.



5. Porém, esta página na Internet não corresponde a qualquer legítimo serviço de correio eletrónico. Trata-se de um página instalada em servidores do prestador de serviço *Netlify* https://www.netlify.com/, fornecedor de serviços na *cloud* (sobretudo o alojamento remoto de *sites*), com sede em San Francisco, na Califórnia. O seu conteúdo é enganador. Não permite o acesso a qualquer conta de correio eletrónico e pretende apenas convencer o utilizador a facultar as credenciais de acesso à sua legítima conta de correio eletrónico.

6. Para dissimular esta obtenção ilegítima de credenciais, quando o utilizador as introduz, é de imediato redirecionado para a legítima página do serviço https://transfer.sapo.pt/, (para o *link* https://transfer.sapo.pt/downloads/cc3da520-175c-437b-b862-b898b7cea66f/sapotransfer-777f393bc0242X9/), no qual surge a informação de que o *download* em causa expirou.