Phishing bancário? Sim é mesmo real, e com ‘callcenter’ renovado.

Phishing bancário é um dos mais proeminentes esquemas disseminados em Portugal e com maior retorno para os cibercriminosos. Algumas das variáveis que contribuem para a disseminação massiva deste tipo de scams é a escassa literacia digital por parte dos utilizadores; que diga-se, tiveram o primeiro contacto com esta veloz transformação digital já numa fase um tudo nada tardia.

Nesta analise são apresentados dois diferentes tipos de phishkit utilizados por cibercriminosos de origem brasileira em Portugal. As landing-pages são similares aos sistemas homebanking da organização alvo, mas os backoffice de controlo são recentes desenvolvimentos.

# #Phishkit_1

A vaga associada ao #Phiskitkit_1 — nomenclatura para categorizar esta campanha durante o artigo — é distribuída massivamente através de SMS maliciosas (smishing). Mais detalhes sobre este tipo de esquema e técnicas associadas podem ser consultadas nas seguintes publicações:

Phishing bancário as a service em Portugal com novo servidor C2

Taking the bait: The modus operandi of massive social engineering waves impacting banks in Portugal

Neste caso em específico, a URL partilhada no corpo da SMS remete a vitima para a landing-page da campanha.

hxxps://nbseguranca.]sbs/ 45.9.190.]98

Para tornar o esquema o mais próximo possível do sistema legítimo, os criminosos utilizam um certificado digital no domínio assinado pela entidade: “Let’s Encrypt“, uma CA que não deve ser confiável quando acedemos sistemas sensíveis e críticos, incluindo portais homebanking.

Figura 1: Certificado SSL obtido via Let’s Encrypt CA.

Após aceder à landing-page inicial, é apresentada uma barra de progresso de validação de forma a motivar a vítima a permanecer na página.

Figura 2: Página inicial da campanha com uma barra de progresso de forma a iludir as vítimas a permanecer na página.

Em detalhe, esta peça de teatro é conseguida através de umas linhas de código em JavaScript, como pode ser observado em seguida.

Figura 3: Código JavaScript responsável por preencher a barra de progresso apresentada na Figura 2 e no final apresentar o primeiro formulário que solicita dados sensiveis.

Após a barra de progresso terminar o processo de loading, é apresentado o primeiro formulário onde são solicitados os primeiros detalhes à vitima, incluindo:

-> Nome -> IBAN -> Montante para Cancelamento

Figura 4: Landing-page onde os primeiros detalhes são solicitados à vitima.

Quando a informação solicitada é corretamente preenchida, o click no botão “Continuar” irá exibir uma página de espera até que alguma interação em backoffice por parte dos operadores seja consumada. Um modus operandi bem conhecido das análise já partilhadas neste blog.

Figura 5: Página de “Verificação de dados” é apresentada enquanto não existir interação em background por parte dos operadores do esquema.

## ‘Callcenter’ renovado — Por trás da cena

Sempre que uma nova vítima tropeça na armadilha, os sinos tocam. Não é de todo uma brincadeira, no backoffice usado pelos criminosos para controlar as operações uma campainha toca sempre que um novo cliente é regsitado na base de dados.

Figura 6: Backoffice utilizado pelos criminosos na campanha denominada por #phishkit_1.

Aqui, é possível controlar que tipo de detalhes são solicitado por etapas, incluindo posições do cartão matriz, códigos de SMS (tokens), upload do cartão matriz, etc. As duas imagens abaixo apresentam parte do processo malicioso.

### Solicitação de posições do cartão matriz

Figura 7: Detalhes do cartão matriz solicitados à vitima via backoffice.

### Solicitação do upload do cartão matriz

Figura 8: Solicitação do carregamento do cartão matriz.

# #Phishkit_2

Um outro phishkit está também a ser distribuído por SMS e email.

https://s.id/NovoB https://adventurerides.travel/ https://curiosityjump.com/ https://drupal.nettrackers.in/

Os domínios partilhados acima também possuem certificado SSL "Let's Encrypt". A landing-page inicial é muito similar ao homebanking oficial.

Figura 9: Landing-page inicial da campanha #phishkit_2.

Sem entrar em detalhes técnicos sobre as páginas seguintes, uma vez que o modus operandi já foi escrutinado em publicações anterior, ao introduzir o número de adesão a vítima é direcionada para uma segunda página onde é solicitado o PIN de acesso, e posteriormente, uma página de "loading" é então apresentada.

Como observado no esquema anteriormente descrito, esta é precisamente a janela de oportunidade dos criminosos. Em backoffice, eles coorderam toda a operação solicitando detalhes adicionais às vítimas por etapas.

Figura 10: Página de solicitação de PIN e "loading" — exato momento em que os criminosos coorderam que tipos de dados serão solicitados em seguida.

## A nova empreitada: 'Callcenter' — A operação em segundo plano

O backoffice identifiifcado durante a análise parece ainda em desenvolvimento, e foram muitos os detalhes que direcionam nesse sentido. Para além de algumas funcionalidades ainda não estarem completamente disponíveis, a propria API utilizada no backoffice para envio dos detalhes para um outro servidor / nó centralizado algures na Internet possuía indicadores e artefactos de teste.

Figura 11: Backoffice referente ao #phishkit_2.

Alguns dos detalhes referentes à API podem ser observados na Figura 12 abaixo, com o parametro "novobancopoc" (prova de conceito) bem identificado.

Figura 12: Detalhes associados à API referente ao #phishkit_2.

# No More Fun o.O'

O código fonte do backoffice é geralmente um sítio interessante para análise. Para além de diversas lacunas de codificação facilmente perceptíveis, é o local perfeito para a abertura à caça do low hanging fruit — experts perceberão no imediato o uso desta tão conhecida expressão.

Figura 13: Endpoint responsável pelo drop da base de dados.

Um endpoint responsável por eliminar a base de dados do sistema foi identificado. Os simpáticos desenvolvedores a facilitarem o trabalho dos experts da área.

## The fun is over, and now the world is safe again!

Aos utilizadores sugere-se uma vez mais, alguma sensibilidade e análise quando confrontados com situações desta natureza. Quanto às organizações alvo neste tipo de investidas, sugere-se também algum controlo no tipo de acessos às contas dos utilizadores, nomeadamente através:

- Controlo de acesso por endereço de IP; temos observado que alguns grupos criminosos realizam os acessos através de endereços de IP geo-localizados no Brasil, e em alguns casos, sem VPN e através dos endereços de IP residenciais de forma a evitar firewalls.
- criação de honey-accounts, de forma a que os criminosos pensem estar a realizar a operação maliciosa numa conta legítima. Ao mesmo tempo este tipo de abordagem permite capturar indicadores do grupo malicioso, incluindo a sua geolocalização, tipo de dispositivo de acesso etc.

Todos os endereços foram adicionados ao 0xSI_f33d para que as organizações possam proceder ao bloqueio dos endereços de IP/domínios de forma eficaz.

Em caso de suspeita de campanhas de phishing ou malware partilhe a situação com as autoridades ou através do formulário disponível aqui, ou submeta a URL maliciosa/suspeita para o 0xSI_f33d.

# Indicadores de Compromisso (IoCs)

https://s.id/NovoB https://adventurerides.travel https://curiosityjump.com https://drupal.nettrackers.in hxxps://nbseguranca.]sbs 45.9.190.]98

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d — a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.