

Processo Penal n.º 2023/0456 – Burla Informática por Phishing – Transferências Fraudulentas de €32 000

Autor/Requerente: Ministério Público

Réu/Requerido: João da Silva, residente em Rua da Palma, 3-B, 1150-269 Lisboa

Juiz: Juiz de Instrução Criminal nº 4 do Tribunal Judicial de Lisboa

Prova Eletrónica – Registo de Endereço IP – 192.0.2.45 – 18 de março de 2023

1. Identificação da prova

Campo	Conteúdo
Tipo de prova	Registo de endereço IP (log) obtido a partir do servidor de correio eletrónico “mail.bankx.pt”
Data da recolha	22 de março de 2023
Data de ocorrência dos factos analisados	18 de março de 2023
Endereço IP objeto da análise	192.0.2.45
N.º de processo	2023/0456
Autor da perícia	Dr. Carlos Mendes – Perito Informático (OA 112233)
Entidade requisitante	Ministério Público – Secção de Instrução Criminal, Tribunal Judicial de Lisboa
Local de armazenamento da prova	Arquivo Digital do Ministério Público – Pasta “Provas Eletrónicas – 2023/0456”

2. Contexto factual Em 10, 15 e 18 de março de 2023, foram enviadas duas mensagens eletrónicas de phishing, supostamente provenientes da entidade bancária “BankX”, com o objetivo de induzir o titular da conta bancária “João da Silva” a efetuar transferências para contas controladas pelo réu. Ambas as mensagens continham um link malicioso que, ao ser acionado, redirecionou o utilizador para um site falsificado onde foram introduzidos os seus credenciais bancárias, culminando nas transferências fraudulentas de €32 000, efetuadas entre 10 e 25 de março de 2023.

A presente prova tem por finalidade demonstrar a **reincidência do mesmo endereço IP (192.0.2.45)** na origem das duas mensagens de phishing, reforçando a tese de autoria única e deliberada por parte do réu.

3. Metodologia de recolha e preservação da prova

- Pedido de cooperação judicial** – Ofício nº 2023/0187/MP, datado de 15 de março de 2023, dirigido ao provedor de serviços de correio eletrónico “MailX Ltda.”, solicitando a entrega dos registos de logs referentes ao período de 10 a 20 de março de 2023.
- Recepção dos logs** – Em 20 de março de 2023, foram recebidos os arquivos “mail_log_20230310_20230320.csv” contendo 1 842 linhas de registo, devidamente assinados digitalmente com certificado qualificado da empresa.
- Preservação** – Os arquivos foram armazenados em formato **PDF/A-3** e **SHA-256** calculado (código: 3fa7b9c1d2e8f5a6b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7c8d9e0f1a2).

4. **Análise forense** – Realizada no laboratório de peritagem informática do Ministério Público, utilizando software especializado (EnCase Forensic 2022, versão 10.4) e seguindo as boas práticas descritas no **Manual de Peritagem Informática** (Direção-Geral da Política de Justiça, 2021).

4. Resultados da análise

Timestamp (UTC)	Endereço IP de origem	Destinatário	Assunto da mensagem	Identificador da mensagem (Message-ID)
2023-03-10 14:27:53	192.0.2.45	cliente@bankx.pt	“Notificação de Segurança – Atualize a sua conta”	<20230310142753.1.192.0.2.45@mail.bankx.pt>
2023-03-15 09:12:07	192.0.2.45	cliente@bankx.pt	“Ação necessária – Verificação de transação suspeita”	<20230315091207.1.192.0.2.45@mail.bankx.pt>
2023-03-18 16:45:22	192.0.2.45	cliente@bankx.pt	“Alerta de fraude – Atualize os seus dados”	<20230318164522.1.192.0.2.45@mail.bankx.pt>

Observação: Os três registos acima correspondem a **mensagens de phishing** enviadas ao mesmo destinatário (conta bancária do réu) e apresentam **identificador de mensagem** distinto, mas **identificado com o mesmo endereço IP de origem** (192.0.2.45). Não foram detectados outros endereços IP que tenham enviado mensagens com conteúdo idêntico no período analisado.

5. Conclusões do perito

1. **A constatação de que o endereço IP 192.0.2.45 foi utilizado em três envios diferentes de mensagens de phishing** demonstra a existência de um padrão de atuação coordenada.
2. **A coincidência temporal** entre o envio das mensagens (10, 15 e 18 de março de 2023) e as datas em que as transferências fraudulentas foram efetuadas (10, 18 e 25 de março de 2023) corrobora a hipótese de que o mesmo agente, operando a partir do referido IP, foi responsável pelos atos ilícitos.
3. **A ausência de outros IPs** com o mesmo padrão de conteúdo e destinatário indica que o endereço 192.0.2.45 é a **fonte única** das mensagens analisadas.
4. **De acordo com o artigo 442.º do Código de Processo Civil**, a prova eletrónica apresentada cumpre os requisitos de autenticidade, integridade e fiabilidade, estando plenamente admissível em tribunal.

Em face do exposto, concluo que **o registo de endereço IP 192.0.2.45 constitui prova robusta da autoria das mensagens de phishing** que deram origem às transferências fraudulentas objeto do presente processo.

6. Certificação da prova Eu, **Dr. Carlos Mendes**, perito informático, titular da cédula profissional n.º OA 112233, declaro, sob compromisso de honra, que:

- Os documentos apresentados são cópias fiéis dos registos originais fornecidos pelo provedor “MailX Ltda.”;
- As cópias foram preservadas mediante hash SHA-256, conforme indicado;
- A análise foi realizada de forma imparcial e em estrita conformidade com as normas técnicas aplicáveis;
- As conclusões aqui expostas refletem, de forma objetiva, os resultados técnicos obtidos.

Lisboa, **22 de março de 2023**

Assinatura Digital:

```
-----BEGIN PGP SIGNATURE-----
iQEzBAEBCAAAFiEE1yZk9ZpKxZ9JY0tU+2xv3t7qSg0FA1+F1eMACgkQ+2xv3t7qSg0F1fAQA1
... (assinatura digital) ...
-----END PGP SIGNATURE-----
```

7. Anexos

1. **Anexo I – Log completo (mail_log_20230310_20230320.csv)** – PDF/A-3, hash SHA-256: 3fa7b9c1d2e8f5a6b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7c8d9e0f1a2.
2. **Anexo II – Captura de e-mail (headers) das três mensagens de phishing** – PDF.
3. **Anexo III – Relatório de Peritagem Informática (versão completa)** – PDF, 27 páginas.

Documento elaborado e subscrito eletronicamente nos termos do Decreto-Lei n.º 68/2008, de 13 de março, e da Portaria n.º 13/2020, de 27 de janeiro, que regulamentam a produção, conservação e apresentação de provas eletrónicas nos processos judiciais.