

## Parecer Pericial – Análise de Phishing e Traços Digitais

**Processo:** 2023/0456 – Burla Informática por Phishing – Transferências Fraudulentas de €32 000

**Autor:** Ministério Público

**Réu:** João da Silva, residente em Lisboa, Rua das Flores, 12-B, 1150-200 Lisboa, NIF 234 567 890

**Juiz de Instrução Criminal n.º 4:** Juiz Carlos Alberto Ferreira – Tribunal Judicial de Lisboa

**Data:** 20 de junho de 2024

### 1. Identificação do Perito

Nome	Eng. Carlos Mendes
Qualificação	Licenciado em Engenharia Informática, Especialista em Segurança da Informação (CISSP) – Perito Oficial nomeado pelo Tribunal Judicial de Lisboa (N.º OA 98765).
NIF	123 456 789
Endereço Profissional	Rua da Boavista, 45, 3.º Esq., 1200-066 Lisboa
Contacto	tel. +351 213 555 123 – c.mendes@peritos.pt

### 2. Objeto do Parecer

O presente parecer tem por finalidade analisar, sob o ponto de vista técnico-forense, os **e-mails de phishing** que deram origem às transferências bancárias fraudulentas no montante total de **€32 000**, ocorridas entre **10 e 25 de março de 2023**, bem como identificar a origem dos endereços IP associados e avaliar a possível ligação dos mesmos ao réu João da Silva.

### 3. Metodologia Aplicada

1. **Aquisição e preservação das evidências** – Cópias forenses bit-a-bit dos servidores de correio eletrónico da empresa “BancoSecure S.A.” (log-files, cabeçalhos completos dos e-mails, ficheiros .eml) foram realizadas em conformidade com a cadeia de custódia (N.º CC 2023/0456-01).
2. **Análise de cabeçalhos de e-mail** – Utilização da ferramenta **MailHeader Analyzer v3.2** para extrair os campos *Received*, *X-Originating-IP*, *Message-ID* e *DKIM-Signature*.
3. **Correlações de IP** – Consulta a bases de dados de geolocalização (IP2Location, MaxMind) e a registos de atribuição de blocos IP junto da ANACOM.
4. **Exame de artefactos de malware** – Extração de anexos suspeitos e análise em sandbox (Cuckoo Sandbox v2.0) para identificar payloads e técnicas de “credential harvesting”.
5. **Comparação de fingerprints de dispositivos** – Verificação de hashes MD5/SHA-256 dos ficheiros de configuração do cliente de correio (Outlook) e de scripts de automação (PowerShell) encontrados nos dispositivos do réu (PC-Portátil nº 001/2022, smartphone Android nº 987654321).
6. **Entrevista técnica** – Interrogatório ao administrador de sistemas da “BancoSecure S.A.” para validar a configuração dos servidores de correio e os registos de acesso.

### 4. Análise dos Factos

**4.1. E-mails de Phishing Recebidos** Foram identificados **sete (7) e-mails** que contêm o link malicioso utilizado para induzir o titular da conta a inserir credenciais bancárias. A tabela abaixo resume os principais elementos de cada mensagem:

N.º	Data/Hora (UTC)	Endereço de origem (IP)	Domínio “From”	Assunto	Anexo
1	12/03/2023 08:34:21	185.62.45.112	support@banksecure-secure.com	“Atualização de Segurança – Ação Necessária”	invoice.pdf (malware)
2	13/03/2023 09:12:07	185.62.45.112	security@banksecure-secure.com	“Confirmação de Transação”	none
3	15/03/2023 14:05:43	212.34.78.90	alert@banksecure-secure.com	“Alerta de Atividade Suspeita”	login.docx (macro)
4	17/03/2023 10:22:18	212.34.78.90	noreply@banksecure-secure.com	“Rever Credenciais”	none
5	19/03/2023 11:45:55	185.62.45.112	support@banksecure-secure.com	“Procedimento de Verificação”	none
6	22/03/2023 13:30:02	212.34.78.90	security@banksecure-secure.com	“Bloqueio Temporário de Conta”	none
7	24/03/2023 09:58:39	185.62.45.112	alert@banksecure-secure.com	“Reativação de Conta”	none

#### 4.2. Traços de IP

- **IP 185.62.45.112** – Bloco atribuído à empresa “TechSolutions Lda.”, sede em **Porto**, NIF 112 334 556. Registo de uso **entre 08:00 e 20:00** (horário local).
- **IP 212.34.78.90** – Bloco atribuído ao provedor “FiberNet – Serviços de Internet, S.A.”, sede em **Lisboa**, NIF 223 445 667. Utilizado **entre 09:00 e 22:00** (horário local).

Ambos os IPs apresentam **registos de VPN** (OpenVPN, porta 1194) nas mesmas janelas temporais em que foram enviados os e-mails de phishing, indicando a possibilidade de mascaramento da origem real.

#### 4.3. Evidências de Associação ao Réu

1. **Log de acesso ao Wi-Fi doméstico** – O router da residência de João da Silva (SSID “Silva-Home”) registou, nos dias 12, 15, 19 e 22 de março de 2023, **conexões simultâneas** com o endereço MAC **00-1A-2B-3C-4D-5E**, o mesmo encontrado no dispositivo portátil **PC-Portátil nº 001/2022** (marca Dell, modelo XPS 13).
2. **Hash de ficheiro malicioso** – O anexo *invoice.pdf* analisado revelou o hash **SHA-256: 3F9A7C2E5B1D4A6C8E9F0B2D7A1C3E5F6B8D9A0C**. O mesmo hash foi identificado num ficheiro guardado na pasta “Downloads” do PC-Portátil nº 001/2022, com data de criação **12/03/2023 08:35**.
3. **Credenciais de e-mail** – O utilizador “jsilva2023” (identificador interno do servidor de correio da “BancoSecure S.A.”) foi utilizado para enviar os e-mails de phishing. As credenciais (username e password) foram encontradas num ficheiro “config.json” no PC-Portátil nº 001/2022, com data de modificação **10/03/2023 07:58**.
4. **Registo de chamadas ao suporte da VPN** – O provedor “FiberNet” fornece logs de suporte técnico; o cliente “jsilva2023” solicitou a ativação de um túnel VPN (ID 5789) em **10 de março de 2023**, às

**07:45**, com IP de origem **212.34.78.90**.

#### 4.4. Conclusões Técnicas

- Os e-mails de phishing foram enviados a partir dos endereços IP **185.62.45.112** e **212.34.78.90**, ambos associados a serviços de VPN que permitem ocultar a localização real do remetente.
- A análise dos registos de rede da residência do réu demonstra que o **PC-Portátil nº 001/2022**, pertencente a João da Silva, esteve ligado ao mesmo ponto de acesso Wi-Fi nas mesmas datas e horas em que os e-mails foram enviados.
- O ficheiro malicioso utilizado (hash SHA-256 acima mencionado) foi encontrado no disco do referido portátil, corroborando a hipótese de que o dispositivo foi a fonte da campanha de phishing.
- As credenciais de e-mail utilizadas para a falsificação dos remetentes correspondem a um utilizador interno da “BancoSecure S.A.”, as quais foram armazenadas em texto-plano no dispositivo do réu, violando as políticas de segurança da empresa.

#### 5. Fundamentação Jurídica

1. **Artigo 217.º do Código Penal** – “A burla informática consiste na obtenção, por meios de fraude informática, de vantagem patrimonial ilícita”.
2. **Artigo 8.º do Código de Processo Penal** – A prova pericial, quando requerida, tem por objetivo esclarecer factos técnicos que escapam ao conhecimento do juiz.
3. **Artigo 71.º do Código de Processo Civil (aplicável subsidiariamente)** – A prova pericial deve ser realizada por perito nomeado ou aceito pelas partes, devendo o laudo conter a identificação completa do perito, a metodologia empregada e a conclusão fundamentada.

Conforme a jurisprudência consolidada (STJ, Acórdão 1234/21, de 15 de janeiro de 2022), a existência de **traces digitais** que ligam o dispositivo do suspeito à prática delitiva constitui prova suficiente para a demonstração de autoria, desde que preservada a cadeia de custódia e comprovada a integridade dos dados.

#### 6. Conclusão do Perito

À luz dos factos analisados e da metodologia aplicada, concluo que:

- **Existe forte probabilidade de autoria** do réu **João da Silva** nas transferências fraudulentas de €32 000, mediante a prática de phishing descrita.
- Os **endereços IP** utilizados foram mascarados por VPN, mas a **correlação temporal e técnica** entre os registos de rede doméstica, os ficheiros presentes no portátil do réu e as credenciais de e-mail demonstra que o réu foi, ao menos, o **operador** da campanha.
- Recomenda-se que o Ministério Público inclua, nos autos, **cópias forenses** dos dispositivos do réu, bem como os **logs de VPN** e os **registos de Wi-Fi**, como prova material adicional.

Este parecer foi elaborado em conformidade com as normas técnicas de informática forense e está submetido à apreciação do Juízo competente.

Assinatura

Eng. Carlos Mendes  
Perito Oficial – N.º OA 98765

Lisboa, 20 de junho de 2024