

Tribunal Judicial de Lisboa

Secção de Instrução Criminal

Processo Penal n.º 2023/0456 – Burla Informática por Phishing

Data: 15 de março de 2024

RELATÓRIO DE PERÍCIA ADICIONAL

Verificação de Dispositivo Móvel – Smartphone do Réu João da Silva Perito: Eng. Carlos M. Ribeiro, NIF 219 876 543, residente em Rua da Boavista, 45, 3.º Esq.º, 1200-115 Lisboa.

Qualificação: Licenciado em Engenharia Informática (Universidade de Lisboa), Pós-graduação em Segurança da Informação (Instituto Superior Técnico) e perito judicial credenciado pelo Conselho Superior da Magistratura (n.º 2021/07).

Mandatário: Dr. Marta Santos, Procuradora do Ministério Público, OA 54321.

Objeto da Perícia: Analisar o smartphone (marca Apple, modelo iPhone 12, número de série **DX3J5K7L8M9N**, IMEI **353456789012345**) apresentado como prova material no processo acima referenciado, com a finalidade de identificar vestígios digitais relativos à campanha de phishing que culminou nas transferências bancárias fraudulentas no montante de **€ 32 000,00** ocorridas entre 10 e 25 de março de 2023.

1. Fundamentação Legal

A presente perícia foi determinada nos termos do artigo 378.º do Código de Processo Civil, combinado com o artigo 217.º do Código Penal, e foi solicitada pelo Juiz de Instrução Criminal n.º 4 do Tribunal Judicial de Lisboa, mediante despacho de 02 de março de 2024 (processo n.º 2023/0456).

2. Metodologia Adoptada

Etapa	Descrição	Ferramentas Utilizadas
2.1	Preservação da Cadeia de Custódia – Embalagem anti-estática, registo fotográfico e assinatura de termo de entrega.	Formulário de Cadeia de Custódia (modelo TJ-LIS), câmara digital.
2.2	Imaginação Forense – Criação de imagem bit-a-bit (hash SHA-256) do armazenamento interno e da eSIM.	Cellebrite UFED 7.0, FTK Imager 4.5.
2.3	Extração de Dados – Análise de aplicativos instalados (Mail, Mensagens, WhatsApp, Instagram, Gmail, Banking Apps).	Oxygen Forensic Detective 12, Magnet AXIOM.

Etapa	Descrição	Ferramentas Utilizadas
2.4	Análise de Registos de Rede – Recuperação de logs Wi-Fi, DHCP, e conexões VPN.	Wireshark 4.0, NetworkMiner.
2.5	Correlação Temporal – Mapeamento de eventos entre 01 e 31 de março de 2023.	Timeline Explorer.
2.6	Verificação de Artefactos de Phishing – Busca de URLs maliciosas, anexos suspeitos, e mensagens de engenharia social.	PhishTool, VirusTotal API.

Todos os procedimentos foram realizados em ambiente controlado, sem conexão à internet, e com preservação da integridade dos dados (hashes verificados antes e depois de cada etapa).

3. Resultados Obtidos

3.1. Dados de Identificação do Dispositivo

Campo	Valor
Marca / Modelo	Apple iPhone 12
Número de Série	DX3J5K7L8M9N
IMEI	353456789012345
Versão do iOS	16.3.1
Data de Aquisição	12 de janeiro de 2022
Última Atualização	07 de março de 2024

3.2. Aplicações Relevantes Encontradas

Aplicação	Versão	Data de Instalação	Última Utilização
Gmail	2024.02.15	15/02/2022	24/03/2023
Outlook	4.2309.1	20/03/2022	23/03/2023
WhatsApp	2.23.15	10/02/2022	25/03/2023
Instagram	260.0.0	05/01/2022	20/03/2023
BancoDigital (app bancária)	6.5.2	01/02/2022	25/03/2023

3.3. Registos de Comunicação Suspeita

1. **E-mail** – 12 mensagens recebidas entre 09 e 24 de março de 2023 com o assunto “*Urgente – Atualização de Dados de Conta*”. Todas continham um link encurtado (bit.ly/xyz123) que redirecionava para o domínio **secure-bank-login.com**, identificado como site de phishing (classificado como “malicioso” pelo VirusTotal com 97 % de deteção).
2. **SMS** – 5 mensagens de texto, enviadas pelo número **+351 910 123 456**, contendo a frase “*A sua conta foi comprometida, clique aqui: <https://bank-alert.pt/verify>*”. O número foi associado a um serviço de “SMS spoofing” identificado em investigação policial.

3. **WhatsApp** – 3 conversas (IDs 20230312-001, 20230317-004, 20230322-009) nas quais o réu recebeu ficheiros PDF intitulados “*Extrato Bancário.pdf*”. Os PDFs continham macro-scripts que, ao serem abertos, redirecionavam para o mesmo domínio de phishing mencionado no ponto 1.

3.4. Registos de Transferências Bancárias

Do aplicativo **BancoDigital** foram extraídos os registos de transações. Destacam-se três transferências realizadas a partir da conta **IBAN PT50 1234 5678 9012 3456 7890** para a conta **IBAN PT50 9876 5432 1098 7654 3210** (titular desconhecido), nos dias **12, 18 e 24 de março de 2023**, totalizando **€ 32 000,00**. Cada operação foi autorizada mediante a introdução do PIN de 6 dígitos (**842915**) e a validação por Touch ID, ambos registados nos logs do dispositivo.

3.5. Artefactos de Persistência

- **Perfil de Configuração MDM** (Mobile Device Management) criado em 08 de março de 2023, permitindo a instalação de perfis de VPN que redirecionavam o tráfego para servidores controlados pelos autores da campanha.
 - **Cache de Navegador Safari** contendo cookies de sessão do domínio fraudulento, com timestamps coincidentes com as datas das transferências.
-

4. Análise e Interpretação

1. **Presença de Material Phishing** – A existência de múltiplas mensagens eletrónicas (e-mail, SMS, WhatsApp) contendo links e anexos maliciosos demonstra que o smartphone de João da Silva foi utilizado como vetor de receção e, possivelmente, de disseminação da campanha de phishing.
 2. **Ligação Temporal** – Os registos de acesso ao site fraudulento (bit.ly/xyz123) coincidem, com precisão de minutos, com os momentos de introdução do PIN e da validação Touch ID nas três transferências bancárias, sugerindo que o réu interagiu conscientemente com o conteúdo malicioso.
 3. **Autoridade do Dispositivo** – O facto de o PIN de 6 dígitos estar armazenado em texto-plano no **Keychain** do iOS (acessível apenas mediante jailbreak, que foi realizado em 01 de março de 2023) indica que o réu ou terceiros com acesso ao dispositivo removeram as restrições de segurança, facilitando a captura das credenciais.
 4. **Cadeia de Custódia** – Todas as imagens forenses apresentaram hashes idênticos antes e depois da análise (SHA-256: **9F2A8C3B7E1D4F5A6B7C8D9E0F1A2B3C4D5E6F7A8B9C0D1E2F3A4B5C6D7E8F9**), garantindo a integridade dos dados.
 5. **Conclusão Técnica** – Os dados recolhidos permitem inferir, com alto grau de certeza (95 %), que o smartphone em questão foi o meio instrumental utilizado pelo réu para receber e acionar os links de phishing que resultaram nas transferências fraudulentas de € 32 000,00.
-

5. Conclusão do Perito

À luz dos factos acima descritos, **concluo** que:

- a análise forense do smartphone de João da Silva revelou a presença inequívoca de material de phishing, bem como a execução de ações que culminaram nas transferências bancárias ilícitas;
- a cadeia de custódia foi mantida de forma rigorosa, assegurando a admissibilidade dos elementos probatórios em tribunal;

- recomenda-se, como medida complementar, a realização de perícia ao computador pessoal do réu e à conta de e-mail institucional, a fim de confirmar a extensão da campanha e identificar eventuais co-autores.

Este parecer pericial é emitido para fins de instrução criminal, nos termos do disposto no Código de Processo Penal, e deverá ser juntado aos autos do processo penal n.º 2023/0456.

Lisboa, 15 de março de 2024

Anexos

Anexo	Descrição
A	Imagem forense completa do dispositivo (arquivo .E01) – hash SHA-256: 9F2A8C3B7E1D4F5A6B7C8D9E0F1A2B3C4D5E6F7A8B9C0D1E2F3A4B5C6D
B	Lista de URLs suspeitas (bit.ly/xyz123, https://bank-alert.pt/verify) com relatórios de VirusTotal.
C	Capturas de ecrã das mensagens de e-mail e SMS (formato .png).
D	Registo de transações bancárias extraído da aplicação BancoDigital (PDF).
E	Relatório de logs de rede (Wi-Fi, VPN) – formato .csv.

Eng. Carlos M. Ribeiro

Perito Judicial Credenciado – OA 112233