

Relatório de Análise de Logs do Servidor de E-mail

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

Autor/Requerente: Ministério Público

Réu/Requerido: João da Silva, residente em Lisboa

Mandatários: Dr. Ana Pereira (OA 12345) – Advogada de defesa; Dr. Luís Carvalho (OA 67890) – Advogado de defesa; Dr. Marta Santos (OA 54321) – Procuradora do Ministério Público

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

Data: 12 de fevereiro de 2026

1. Objetivo do Relatório

O presente relatório tem por finalidade demonstrar, mediante a análise dos registos (logs) do servidor de e-mail da entidade **Banco XYZ – S.A.**, a origem dos e-mails de phishing que deram origem às transferências bancárias fraudulentas no montante total de **€32 000**, realizadas entre os dias **10 e 25 de março de 2023**. O documento visa subsidiar a instrução criminal, permitindo a identificação dos remetentes, a rota de transmissão e os pontos de vulnerabilidade explorados.

2. Metodologia

Etapa	Descrição	Ferramentas Utilizadas
2.1.	Aquisição dos logs – Exportação integral dos registos do servidor de e-mail (SMTP, IMAP e POP3) entre 01/03/2023 e 31/03/2023.	rsync, scp com encriptação SSH
2.2.	Preservação da cadeia de custódia – Criação de hash SHA-256 para cada ficheiro de log antes da análise.	sha256sum
2.3.	Normalização – Conversão dos registos para o formato RFC 5424 e indexação em base de dados Elasticsearch.	Logstash, Kibana
2.4.	Filtragem – Aplicação de query para identificar mensagens com assunto “Urgente – Verificação de Conta” ou remetente “no-reply@bankxyz.com” .	Elasticsearch DSL
2.5.	Correlacionamento – Cruzamento dos registos de e-mail com os registos de firewall (IP de origem/destino) e com os registos de transação bancária.	Splunk, Python (pandas)

Etapa	Descrição	Ferramentas Utilizadas
2.6.	Geolocalização – Resolução dos endereços IP para localização geográfica.	geoiplookup, MaxMind DB
2.7.	Elaboração do relatório – Consolidação dos achados e preparação de evidência pericial.	Microsoft Word, LaTeX (para anexos)

3. Análise dos Registos

3.1. Identificação dos e-mails suspeitos Foram detectadas **27** mensagens eletrônicas com o padrão de assunto “Urgente – Verificação de Conta”, enviadas a diferentes clientes do Banco XYZ. As mensagens continham um link encurtado que redirecionava para um domínio fraudulento (**secure-bank-login.xyz**).

A tabela abaixo resume as características das mensagens mais relevantes:

Nº	Data/Hora (GMT)	Remetente (SMTP)	Destinatário	IP de Origem	País de Origem	Link Contido
1	12 de março de 2023, 09:14:27	phish-alert@secure-bank-login.xyz	jeandasilva@email.com	185.62.45.112	Ucrânia	https://bit.ly/3fX9KzA
2	14 de março de 2023, 14:03:58	no-reply@bankxyz.com (spoofed)	jeandasilva@email.com	203.0.113.45	Brasil	https://bit.ly/3fX9KzA
3	19 de março de 2023, 08:47:12	support@secure-bank-login.xyz	jeandasilva@email.com	45.77.232.19	Rússia	https://bit.ly/3fX9KzA
4	22 de março de 2023, 12:22:05	alerta@bankxyz.com (spoofed)	jeandasilva@email.com	190.210.12.78	México	https://bit.ly/3fX9KzA

Observação: Os endereços de e-mail remetentes foram falsificados (spoofing) mediante manipulação do cabeçalho **From**; o **Received-From** indica claramente o IP real de origem.

3.2. Rastreamento da rota de transmissão A sequência de hops (saltos) revelada pelos registos **Received** demonstra que os e-mails foram encaminhados pelos seguintes servidores:

1. **mx1.spamhaus.org** (IP 185.62.45.112) – Entrada na rede de filtragem de spam.
2. **mailrelay1.isp-uk.net** (IP 203.0.113.45) – Relay de saída da ISP do remetente.
3. **gateway.mailsecurity.pt** (IP 45.77.232.19) – Servidor de segurança da empresa de hospedagem.
4. **smtp.bankxyz.com** (IP 190.210.12.78) – Servidor de receção do Banco XYZ (destinatário final).

A análise de **TLS handshake** indica que a comunicação entre os passos 2 e 3 foi cifrada com **TLS 1.2**, porém o primeiro salto (mx1.spamhaus.org) ocorreu em texto-plano, permitindo a interceptação de metadados.

3.3. Correlação com as transferências fraudulentas Os registos de transação bancária mostram que as transferências de €32 000 foram efetuadas nas seguintes datas e horas:

Transferência	Valor	Data/Hora (GMT)	Conta Origem	Conta Destino	IP de Origem da sessão
T1	€10 000	13 de março de 2023, 10:05:12	PT50 1234 5678 9012 3456 7890 1	PT50 9876 5432 1098 7654 3210 9	185.62.45.112
T2	€12 000	18 de março de 2023, 09:47:33	PT50 1234 5678 9012 3456 7890 1	PT50 1122 3344 5566 7788 9900 2	45.77.232.19
T3	€10 000	24 de março de 2023, 13:21:55	PT50 1234 5678 9012 3456 7890 1	PT50 2233 4455 6677 8899 0011 3	190.210.12.78

A correspondência entre os IPs de origem dos e-mails de phishing e os IPs das sessões de banca eletrónica evidencia que o atacante utilizou a mesma infraestrutura de rede para **obter as credenciais** (via página de login falsa) e, em seguida, **executar as transferências**.

3.4. Evidência de comprometimento da conta de e-mail A análise do registo **IMAP** da conta **joaodasilva@email.com** revela a criação de uma regra automática (filter) em **15 de março de 2023**, com a seguinte configuração:

```
if subject contains "Verificação de Conta"
  then forward to attacker@darkmail.net
```

Este filtro foi introduzido a partir do IP **185.62.45.112**, corroborando a hipótese de que o atacante, após obter as credenciais, configurou a conta para redirecionar automaticamente futuros e-mails de phishing, facilitando a recolha de novas vítimas.

4. Conclusões

- Origem dos e-mails de phishing** – Os e-mails foram enviados a partir de servidores localizados em **Ucrânia, Brasil, Rússia e México**, todos associados a endereços IP que constam em bases de dados de actividades maliciosas (Spamhaus, AbuseIPDB).
- Rota de transmissão** – A cadeia de hops demonstra a utilização de serviços de **relay** e de **encurtadores de URL** (bit.ly) para mascarar o destino final, dificultando a deteção precoce.
- Ligação direta às transferências fraudulentas** – O mesmo conjunto de IPs (185.62.45.112, 45.77.232.19 e 190.210.12.78) aparece tanto nos registos de e-mail como nas sessões de banca eletrónica, configurando uma **correlação inequívoca** entre a fase de captura de credenciais e a fase de execução da burla.
- Comprometimento da conta de e-mail da vítima** – A criação da regra de encaminhamento automática evidencia a **tomada de controlo da caixa de correio** pelo autor da fraude, reforçando o argumento de que o réu (João da Silva) **não foi o autor direto** das mensagens, mas sim a vítima de um ataque de phishing.
- Responsabilidade do autor** – Apesar da ausência de prova direta de autoria por parte de João da Silva, os factos demonstram que o **cibercriminal** utilizou a identidade da vítima para efetuar as transferências. As provas apresentadas são suficientemente robustas para sustentar a acusação de burla informática contra o réu, caso se demonstre que o mesmo agiu com conhecimento e intenção de fraudar, ou, alternativamente, para justificar a **exoneração** do réu se for provado que agiu de boa-fé e foi enganado.

5. Recomendações Técnicas

Nº	Medida	Justificação
5.1	Bloqueio imediato dos IPs 185.62.45.112 , 45.77.232.19 e 190.210.12.78 nas firewalls do Banco XYZ e nas listas de bloqueio de spam.	Elimina a possibilidade de novas sessões fraudulentas.
5.2	Revogação e re-emissão de credenciais de acesso à banca eletrónica para todas as contas afetadas.	Previne reutilização das credenciais comprometidas.
5.3	Implementação de DMARC, SPF e DKIM rigorosos nos domínios do Banco XYZ.	Reduz a eficácia de spoofing de e-mail.
5.4	Formação de sensibilização para clientes sobre phishing, incluindo a verificação de URLs e a desconfiança de e-mails não solicitados.	Diminui a taxa de sucesso de ataques futuros.
5.5	Monitorização contínua dos registos de login com análise de comportamento (UEBA) para detetar anomalias de IP e horário.	Permite a deteção precoce de acessos suspeitos.

6. Anexos

1. **Anexo A – Extracto dos registos SMTP (formato RFC 5424)** – 15 linhas representativas.
2. **Anexo B – Hash SHA-256 dos ficheiros de log** (para comprovar integridade).
3. **Anexo C – Captura de ecrã da regra de encaminhamento automática na conta de e-mail da vítima.**
4. **Anexo D – Relatório de geolocalização dos IPs suspeitos (MaxMind).**

Prepared by:

Dr. Marta Santos – Procuradora do Ministério Público (OA 54321)

Reviewed by:

Dr. Ana Pereira – Advogada de defesa (OA 12345) – *consultora pericial*

Documento elaborado em conformidade com o Código de Processo Penal e o Código de Processo Civil, Artigos 389.º a 393.º, para efeitos de instrução criminal.