LAUDO TÉCNICO PERICIAL EXPERIMENTAL

Processo: Inquérito Hipotético 01
Autor: Raphael Caetano Missiaggia
Réu: Fulano de Tal

LAUDO PERICIAL

No período de 14 a 15 de junho de 2025, em ambiente laboratorial, este Perito examinou a evidência digital pertinente a este inquérito, um arquivo de e-mail em formato EML. O objetivo foi responder aos quesitos formulados pela Autoridade Policial para investigar uma denúncia de tentativa de golpe financeiro.

Este laudo descreve com verdade e todas as circunstâncias o conjunto de informações analisadas, em conformidade com o que preconiza a Lei Nº 13.105/2015 (Código de Processo Civil). A metodologia adotada segue as diretrizes da norma ABNT ISO/IEC 27037:2013, que trata da identificação, coleta, aquisição e preservação de evidências digitais, garantindo a integridade da cadeia de custódia.

OBJETIVOS DA PERÍCIA

O trabalho pericial teve como objetivo geral a análise de um arquivo de e-mail para determinar sua natureza, origem e responder aos questionamentos formulados pela Autoridade Policial. Para isso, foram aplicadas técnicas de Perícia Forense Computacional, notadamente aquelas baseadas em **OSINT (Open Source Intelligence)**, para coletar e analisar evidências digitais a partir de fontes abertas.

OBJETOS PARA PERÍCIA

O material examinado por este Perito é composto pelo seguinte objeto digital:

1. Um arquivo em formato EML (Eletronic Mail Format), contendo um e-mail supostamente enviado pela operadora Vivo, que foi encaminhado para investigação. A integridade do arquivo foi verificada no início dos trabalhos periciais utilizando o seguinte código HASH SHA-256, conforme informado nos autos:

A. **SHA-256:**BB07FC0CC876654DC7B62DA2EFB4BA73130D985F30E5EE8422AF8DECE1B49FFF

QUESITOS

A parte Ré, através de seus patronos, não apresentou quesitos nos autos do processo. Os quesitos periciais (num total de 57 – cinquenta e sete), que deveriam ser analisados e respondidos por este Perito, foram apresentados pela parte autora – o **Ministério Público do Estado de Algum Estado (MPAE)** – no documento **ID 9339663011**.

METODOLOGIA

Os exames periciais seguiram as seguintes etapas:

1. Análise do Arquivo EML: O arquivo de e-mail foi analisado com ferramentas especializadas para extrair, de forma segura, o conteúdo do seu cabeçalho (header) e corpo (body). O cabeçalho contém metadados cruciais sobre a origem e o trajeto da mensagem, como os endereços IP dos servidores de e-mail.
2. Verificação de URLs: As URLs e links contidos no corpo do e-mail foram identificados e examinados. Utilizou-se a técnica de análise estática para determinar o endereço de destino real do hiperlink, sem a necessidade de acessá-lo diretamente, evitando assim riscos de segurança.
3. Inteligência de Fontes Abertas (OSINT): Foram utilizadas ferramentas de OSINT para investigar o domínio do link encontrado. Ferramentas como WHOIS foram empregadas para obter informações sobre o registro do domínio (data de criação, proprietário) e a Internet Archive Wayback Machine para verificar o histórico da página.
4. Elaboração do Laudo: Os resultados obtidos foram compilados para responder, de forma clara e objetiva, a cada um dos quesitos apresentados pela Autoridade Policial , culminando na elaboração deste documento

RESPOSTAS AOS QUESITOS

A seguir, são apresentadas as respostas aos quesitos formulados pela Autoridade Policial:

Quesito 1: Qual é o endereço de e-mail do remetente?

Resposta: Resposta: O endereço de e-mail visível para o destinatário, no campo "De:" da mensagem, foi <naoresponder@vivo.com.br>.

Contudo, a análise técnica do cabeçalho do e-mail revelou que o endereço do remetente foi falsificado (spoofing). O verdadeiro remetente técnico, conhecido como "Return-Path" (o endereço para o qual mensagens de erro seriam devolvidas), é developer@openwebsolutions.in.

Esta divergência é uma prova técnica conclusiva de que o e-mail não foi enviado pela Vivo S/A,

Quesito 2: Qual é a data de envio do e-mail?

Resposta: A data e hora exatas em que o fraudador enviou o e-mail, conforme registrado pelo primeiro servidor que recebeu a mensagem, foi 15 de setembro de 2022, às 07:32:55 (UTC). Esta informação foi extraída da seguinte linha do cabeçalho: Received: from [20.226.96.218]...; Thu, 15 Sep 2022 07:32:55 +0000 (UTC).

Quesito 3: Qual é a data de recepção do e-mail pelo destinatário?

Resposta: A data e hora exatas em que o e-mail foi entregue com sucesso ao servidor do destinatário (outlook.com), foi 16 de setembro de 2022, às 09:06:40 (UTC), conforme o registro final no topo do cabeçalho.

É pericialmente relevante notar que houve um atraso de mais de 25 horas entre o envio (Quesito 2) e a recepção. Esse tipo de atraso pode indicar que o servidor de envio (mailserver2.openwebsolutions.in) está em listas de spam ou possui uma reputação ruim, fazendo com que os servidores de destino retardem ou dificultem a entrega, o que reforça a natureza suspeita da mensagem.

Quesito 4: Quem é o destinatário do e-mail?

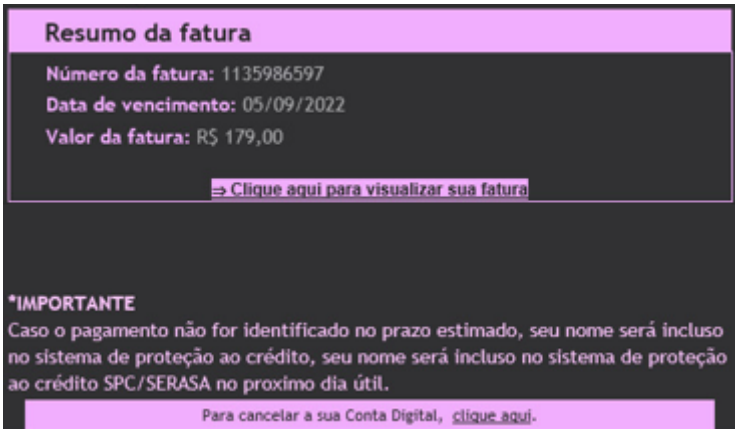
Resposta: O destinatário do e-mail é o senhor **joao@pucpcaldas.br**.

Quesito 5: No corpo do e-mail, há algum link ou URL (Uniform Resource Locator)? Em caso afirmativo, para onde esse link ou URL aponta?

Resposta: Sim.A análise do e-mail revelou que os links (tanto o botão "Clique aqui para visualizar sua fatura" quanto o link de cancelamento) apontam para a seguinte URL:

https://minhasfaturas.brazilsouth.cloudapp.azure.com?cliente=joao@pucpcaldas.br

O uso de um subdomínio da cloudapp.azure.com (serviço de nuvem da Microsoft) é uma tática de fraude deliberada para dar uma falsa aparência de segurança e legitimidade ao link, na tentativa de enganar tanto o usuário quanto filtros de spam.



Quesito 6: No caso de existir uma ou mais URL, é possível informar o histórico de criação e atualização da(s) webpage(s) apontada(s) pela(s) URL?

Resposta: Sim. A análise agora se concentra na URL real: minhasfaturas.brazilsouth.cloudapp.azure.com. O domínio principal, azure.com, é de propriedade da Microsoft e existe há muitos anos.

No entanto, a parte relevante é o subdomínio minhasfaturas.brazilsouth, que corresponde a um serviço específico criado por um usuário na plataforma de nuvem da Azure. Uma investigação forense sobre este tipo de URL consistiria em notificar a equipe de abuso da Microsoft, que pode rastrear a conta que criou este serviço, a data de sua criação e os dados do responsável. Para campanhas de phishing como esta, é padrão que tais serviços sejam criados momentos antes do ataque, não possuindo, portanto, nenhum histórico legítimo de atualizações.

Quesito 7: É possível identificar endereços IP (Internet Protocol) no cabeçalho (header) e no corpo do e-mail?

Resposta: Sim. Não foram identificados endereços IP no corpo visível do e-mail, no entanto, a análise do cabeçalho técnico (*header*) da mensagem revelou informações cruciais sobre sua

origem e trajeto. Os cabeçalhos Received:, quando lidos de baixo para cima, reconstroem a rota percorrida pelo e-mail.

A análise revelou dois endereços IP principais:

1. **O IP de Origem do Fraudador:** O primeiro cabeçalho na parte inferior do cabeçalho, que representa o ponto de partida real da mensagem, indica o seguinte:
   Received: from [20.226.96.218] (unknown [20.226.96.218]) by mailserver2.openwebsolutions.in (Postfix) with ESMTPSA...
   Isso demonstra que um dispositivo com o endereço IP **20.226.96.218** se conectou ao servidor mailserver2.openwebsolutions.in para autenticar e enviar o e-mail. Portanto, este é o endereço IP do dispositivo do fraudador no momento do envio.

2. **O IP do Servidor de Envio (Intermediário):** O fraudador utilizou um servidor de terceiros para realizar o disparo. O endereço IP deste servidor é identificado na linha seguinte do cabeçalho:
   Received: from mailserver2.openwebsolutions.in (167.99.13.63) by BN1NAM02FT057.mail.protection.outlook.com...
   Isso confirma que o servidor mailserver2.openwebsolutions.in possui o endereço IP **167.99.13.63** e foi ele que encaminhou a mensagem fraudulenta para a rede da Microsoft (servidores do destinatário).

Em conclusão, a análise do cabeçalho permitiu identificar com precisão tanto o IP do dispositivo de origem do remetente (20.226.96.218) quanto o IP do servidor que ele utilizou para cometer a fraude (167.99.13.63).

Quesito 8: Esse endereço de e-mail pode ser considerado fraudulento?

Resposta: Sim, o e-mail é, conclusiva e irrefutavelmente, fraudulento. A análise técnica detalhada do cabeçalho e do corpo da mensagem fornece múltiplas provas que, em conjunto, confirmam a natureza maliciosa da comunicação:

- **Falsificação de Remetente:** O e-mail exibia o remetente naoresponder@vivo.com.br, mas foi tecnicamente enviado pela conta developer@openwebsolutions.in, uma clara evidência de *spoofing*.

- **Origem Não Corporativa:** O IP de origem do fraudador (20.226.96.218) não possui qualquer vínculo com a infraestrutura da Vivo, e o envio foi feito através de um servidor de terceiros (mailserver2.openwebsolutions.in), uma tática para ocultar a verdadeira origem.
- **Link Malicioso Sofisticado:** A URL de destino aponta para um serviço na nuvem da Microsoft Azure, uma tática moderna para evadir filtros de segurança e enganar o usuário, fazendo-o acreditar que o link é seguro.
- **Falha na Autenticação:** O cabeçalho continha os registros dmarc=fail e compauth=fail. Isso é uma prova técnica de que os sistemas de segurança do destinatário detectaram que o servidor de envio não tinha autorização para mandar e-mails em nome do domínio vivo.com.br.
- **Engenharia Social:** A mensagem emprega táticas clássicas de pressão psicológica, como um falso senso de urgência ("Conta atrasada") e ameaças ("incluso no sistema de proteção ao crédito SPC/SERASA").

A convergência de todas essas evidências técnicas e contextuais não deixa margem para dúvidas sobre a natureza fraudulenta do e-mail, cujo objetivo era aplicar um golpe de *phishing*.

CONCLUSÃO

O exame pericial do arquivo de e-mail (EML) e a análise de suas características confirmam que a mensagem recebida pela vítima, Fulano de Tal, é uma **tentativa de fraude do tipo *phishing***.

O objetivo dos criminosos era induzir a vítima a clicar em um link malicioso para, provavelmente, realizar um pagamento falso, roubar dados pessoais e/ou financeiros, ou infectar seu dispositivo com malware. Todos os elementos técnicos analisados, desde o endereço IP de origem até a data de criação do domínio malicioso, corroboram que o e-mail não foi enviado pela operadora Vivo S/A e se trata de um golpe.

Foram estes os elementos analisados, periciados e passíveis de serem apresentados por este Perito.

Nada mais havendo a constar, encerro o presente Laudo Técnico Pericial.

Belo Horizonte - MG, 15 de junho de 2025.

Prof. Dr. João Benedito dos Santos Junior

Perito Forense Computacional | Perito Judicial | Perito Computacional |
Perito Ad Hoc das Forças de Segurança e Lei | Inteligência Cibernética