|  |  |  |
| --- | --- | --- |
| **EXAME PERICIAL** | **NUIPC**  **M57.biz**   |  | | --- | |  |   **PERÍCIA**  05/2023 |
|  | *Remessa de Expediente Parcial*  *[volume 1 de 1]* |
| **Perito(s): João Rodrigo Mota da Costa** | |

ENQUADRAMENTO

------Em cumprimento da indicação de perito para o processo pena M57.biz foi dado início ao processo com vista a apurar a existência de provas referentes aos atos apresentados na queixa referente ao processo de investigação de exfiltração de dados da start-up M57.biz. A M57.biz é uma corporação virtual, em que a maioria dos documentos são enviados e recebidos via e-mail. Neste contexto, uma folha de cálculo do Excel (m57biz.xls) contendo informações confidenciais foi divulgada como anexo num fórum de “suporte técnico” pertencente a um website de um concorrente. A queixa realizada tem como fundamento o facto de o ficheiro em questão ter sido criado e enviado (origem) da conta da Jean (CFO), visto ter sido solicitado anteriormente via e-mail a pedido da sua supervisora, Alison (Presidente). Contudo, ambas negam qualquer envolvimento na exfiltração dos dados para o exterior da organização. Nesta sequência, a arguida Jean é acusada de facultarilegalmente informações confidenciais, espionagem, sabotagem e violação da segurança e integridade da organização. Assim sendo, pretende-se averiguar quem, quando e como os dados em questão foram acedidos e consequentemente, exfiltrados. ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------- -------------------------------------------------------------------------------------------------------------------------------------

ÍNDICE

|  |
| --- |
| CAPA DE VOLUME 1 DE 1 1  [ENQUADRAMENTO 2](#_Toc135059661)  [ÍNDICE 3](#_Toc135059662)  [FOLHA DE OBRA 4](#_Toc135059663)  [MATERIAL EXAMINADO 5](#_Toc135059664)  [CÓPIA FORENSE 6](#_Toc135059665)  [EXTRAÇÃO DE DADOS 6](#_Toc135059666)  [LINHA TEMPORAL 6](#_Toc135059667)  [RELATÓRIO FORENSE 7](#_Toc135059668)  [**INTRODUÇÃO E PROCEDIMENTOS** 7](#_Toc135059669)  [**DESENVOLVIMENTO/RESULTADOS** 8](#_Toc135059670)  [OLHA DE OBRA 9](#_Toc135059671)  [MATERIAL EXAMINADO 10](#_Toc135059672)  [CÓPIA FORENSE 11](#_Toc135059673)  [EXTRAÇÃO DE DADOS 12](#_Toc135059674)  [LINHA TEMPORAL 12](#_Toc135059675)  [RELATÓRIO FORENSE 13](#_Toc135059676)  [GLOSSÁRIO TÉCNICO 13](#_Toc135059677)  [FOLHA DE SUPORTE 18](#_Toc135059678)  [AUTO DE ENTREGA 19](#_Toc135059679) |

FOLHA DE OBRA

|  |
| --- |
| **EXECUÇÃO** |

|  |  |
| --- | --- |
| **DATA** | 28 de maio de 2023 |
| **LOCAL** | Lisboa |
| **IDENTIDADE DO(S) EXECUTANTE(S)** | João Rodrigo Mota da Costa |

|  |
| --- |
| **EQUIPAMENTO #01** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TIPO** | Cópia de uma imagem de um disco interno | |  |  |
| **MARCA** | - | | **MODELO** | - |
| **Nº SÉRIE** | - | | **Nº DISCOS** | 1 (um) |
| **ESTADO** | - | | **FOTOGRAFADO** | Sim |
| **IDENTIFICAÇÃO ATRIBUIDA** | | C004 | | |
| **OBSERVAÇÕES** | | Cópia da imagem do disco principal do computador com o sistema operativo - Microsoft Windows XP Service Pack 3, Device ID c9954b38-9b17-43fd-a1f3-11a884607c26 | | |

|  |
| --- |
| **SUPORTE #01** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TIPO** | Disco Rígido | |  |  | |
| **MARCA** | - | | **MODELO** | - | |
| **Nº SÉRIE** | - | | **INTERFACE** | - | |
| **CAPACIDADE DO SUPORTE** | | 10GB | | | |
| **TIPO DE INTERVENÇÃO** | | Cópia Forense | | | |
| **VERIFICAÇÃO DE SEGURANÇA** | | Sim / Positivo | | | |
| **ESTADO** | | - | **FOTOGRAFADO** | | Sim |
| **IDENTIFICAÇÃO ATRIBUIDA** | | PRT01 | | | |
| **OBSERVAÇÕES** | |  | | | |

MATERIAL EXAMINADO

|  |  |
| --- | --- |
| **FOTOGRAFIA Nº** | 01 |
| **IDENTIFICAÇÃO** | C004 |
| **TIPO** | Disco Rígido |
| **VISTA** | Superior |

|  |
| --- |
|  |

CÓPIA FORENSE

|  |  |
| --- | --- |
| **IDENTIFICAÇÃO** | PRT01 |
| **TIPO** | Disco Rígido interno |

|  |
| --- |
| Created By AccessData® FTK® Imager 4.5.0.3 |

EXTRAÇÃO DE DADOS

|  |  |  |
| --- | --- | --- |
| **IDENTIFICAÇÃO** | PRT01 |  |
| **TIPO** | Imagem de um disco interno |  |
| **ANEXOS** | HTML file |  |

|  |
| --- |
| Lista em anexo em suporte digital  Caso-27712.9JASTB/04-Investigacao/01-Ficheiros/PRT\_01/HTML%20Report/index.html |

LINHA TEMPORAL

|  |  |
| --- | --- |
| **IDENTIFICAÇÃO** | PRT01 |
| **TIPO** | Pen Drive USB |
| **ANEXOS** | DVD |

|  |
| --- |
| Os acontecimentos ocorrem entre… |

|  |
| --- |
|  |

RELATÓRIO FORENSE

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **DATA** | 28 de maio de 2023 |
| **LOCAL** | Lisboa |
| **IDENTIDADE DO(S) EXAMINADOR(ES)** | João Rodrigo Mota da Costa |

|  |  |
| --- | --- |
|  | |
| **OBJETOS DE EXAME**  **CAPACIDADE DO SUPORTE** | 1 (uma) cópia de uma imagem de um disco interno  10GB |
| **IDENTIFICAÇÃO** | PRT01 |
| **RESUMO DIGITAL (*HASH VALUE*)** | MD5: 595e6d3bc26603d645637070ff610c0b |
| **SISTEMA OPERATIVO INSTALADO** | Sim; SO: Microsoft Windows XP Service Pack 3;  Device ID c9954b38-9b17-43fd-a1f3-11a884607c26 |
|  |  |

|  |  |
| --- | --- |
| **ANEXOS RESULTANTES DE EXAME FORENSE JUNTOS** | 1 (um) Relatório em formato electrónico (DVD 01), FLS. 1 a 38  1 (um) Glossário Técnico, FLS. 39 a 42 |

|  |  |
| --- | --- |
|  |  |

**INTRODUÇÃO E PROCEDIMENTOS**

------Recebeu-se uma cópia forense do conteúdo do respetivo equipamento pertencente a arguida, identificado como “PRT01”, tendo-se elaborado o respetivo relatório de cópia. Procedeu-se à extração do seu conteúdo, dos quais foram extraídos fotogramas e dados técnicos. Tal como consta na folha de obra, todo o exame e consequente análise, foram produzidos sobre a cópia forense após validação desta, mantendo assim a integridade do dispositivo original. ------------------------------------------------------------------------------------------

**DESENVOLVIMENTO/RESULTADOS**

------ Analisada a cópia forense, com recurso a aplicações forenses em uso neste laboratório, em conformidade com os quesitos indicados e face à limitação temporal para a realização da perícia, foi possível constatar o seguinte: -------------------------------------------------------------------------------------------------------------------------- -------O dispositivo identificado como “PRT01” com capacidade, aproximada, de 10 GB, encontra-se configurado com três volumes lógicos, sendo que o primeiro, com a capacidade de 63 sectores, encontra-se não alocado e sem qualquer tipo de informação. O Segundo volume tem 20948697 sectores, e encontra-se com o sistema de ficheiros NTFS / exFAT. Por fim, o terceiro volume tem 22760 sectores, e encontra-se não alocado e sem qualquer tipo de informação. ------------------------------------------------------------------------------------------

------ Das imagens analisadas nenhuma delas contém conteúdo relevante para o caso. ------------------------------ ------ O ficheiro em questão, o m57biz.xls, pode ser encontrado na seguinte localização: Documents and Settings/Jean/Desktop/m57biz.xls. Foi criado no dia 12-junho-2008 12:13:51 GMT e a última modificação foi realizada no dia 20-julho-2008 01:28:03 GMT, e apresenta uma hash MD5 com o valor de e23a4eb7f2562f53e88c9dca8b26a153. -------------------------------------------------------------------------------------- -------Durante a análise à conta do computador da Jean foi encontrado um ficheiro suspeito com a extensão html, correspondendo ao histórico de uma conversa de chat do AIM, supostamente, entre a Jean e a Alison. O ficheiro encontra-se na seguinte localização: Documents and Settings/Jean/My Documents/AIMLogger/m57jean/IM Logs/alisonm57.html. A conversa ocorreu no dia 18 de julho de 2008, com início às 6:05:38 AM e fim às 12:55:17 AM e posteriormente, no dia 1 de julho de 2008 com início às 00:50-01:46:45 AM. Após uma análise cuidadosa, é possível considerar a hipótese de que alguém se está a fazer passar pela Jean, uma vez que durante a conversa esta refere-se a um chefe homem, quando na realidade é uma mulher – a Alison. Deste modo, esta evidência sugere que a conta da Jean foi comprometida. ----------------------------------------------------------------- -------As mensagens de e-mail enviadas e recebidas foram analisadas através do Ficheiro de Dados do Outlook, localizado na diretoria: /Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst. ---------------------------------------------------------------------------------------- ------De acordo, com a análise das mensagens de e-mail, foi possível verificar que existe uma troca de e-mails entre a Jean (jean@m57.biz) e a Alison (alison@m57.biz) desde o dia 6 de julho de 2008. Neste contexto, destacam-se algumas mensagens suspeitas nomeadamente, o e-mail vindo da Alison a solicitar a criação e o envio do ficheiro em causa (m57biz.xls). -------É de salientar a mensagem de e-mail enviada pela Alison para a Jean, no dia 6 de julho de 2008, indicando “Please do not send me links like this. I have no way of knowing if they are from you or from some hacker.”---- -------O e-mail enviado a partir da conta de e-mail da Jean, contendo o ficheiro com os dados confidenciais, foi analisado cuidadosamente e verificou-se que realmente foi enviado da conta da Jean no dia 20 de Julho de 2008, às 01:28:47 (GMT). Deste modo, a Jean realmente enviou o ficheiro em causa, uma vez que anteriormente recebeu um email com o remetente alison@m57.biz, que seria, supostamente, sua chefe Alison, a solicitá-lo. Contudo, na realidade a Jean estava a enviar o ficheiro em causa para o e-mail tuckgorge@gmail.com. Esta evidência indica que alguém se está a fazer passar pela Alison e deste modo, pediu o ficheiro em causa à Jean e esta enviou-o, pensando que estava a enviar para a sua chefe Alison. -------------------------------------------------- ------------------------------------------------------------------------------------------------------------------------------------

AUTO DE ENTREGA

|  |
| --- |
|  |

Exmo(a). Sr(a)

No âmbito do inquérito supra, foi efetuado Exame Forense ao equipamento informático, de acordo com o solicitado no início do presente NUIPC e conforme descrição dos autos de exame forense que antecedem. Assim, submeto o presente expediente à consideração de V. Exª, para que se digne determinar o que tiver por conveniente.

Lisboa, 28 de maio de 2023

|  |  |
| --- | --- |
|  | O Perito  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  João Rodrigo Mota da Costa |
|  |  |