INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2021-2022 – 1st Period

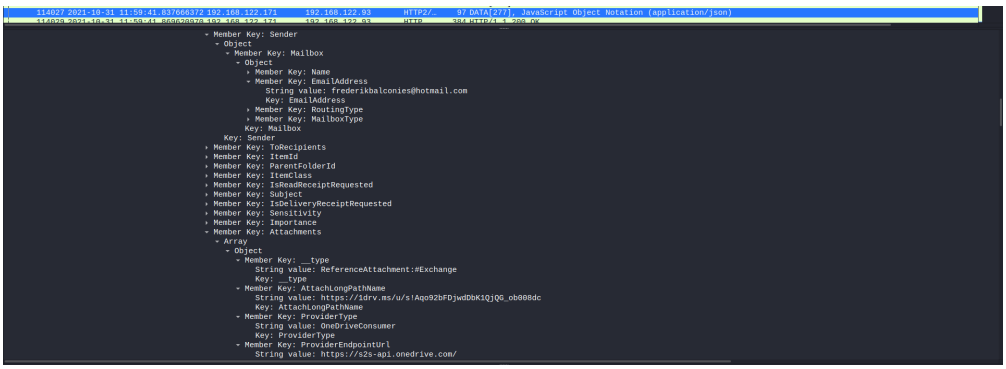
Digital Forensics Report

Fátima Napoleão - 91605
Miguel Henriques - 102148
Ielga Oliveira - 92479

1 Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the authenticity of these documents?

No trace de rede encontramos uma response http (frame 115526) em que o json continha um email enviado de frederikbalconies@hotmail.com para levyfvelucci@outlook.com com um atachment , após fazermos download do atachment verificámos que continha um malware. Após análise deste malware verificamos que este se conectava ao computador da Abby, enviava pedidos http em que a resposta seria um comando encriptado em que o malware desencripta e executa esse comando, este comando pode ser um comando bash ou para fazer download de um ficheiro, após executar o comando envia um POST request em que o body pode conter duas coisas diferentes, se for um comando bash é cmd=”resultado encriptado” e se for download de um ficheiro envia file=”ficheiro encriptado”. Para desencriptarmos utilizamos o wireshark para ver os pedidos http e extrairmos os conteúdos encriptados para um ficheiro manualmente. Depois de ter-mos os dados todos no ficheiro desenvolvemos um script,encontra-se na pasta arquivos->scripts, que utiliza a função decrypt do malware e percorre todos os dados encriptados e desencripta, como resultado tivemos alguns comandos bash(arquivos->logs) e os cinco pdfs que estavam na pen de Charles Daniels(arquivos->pdf).

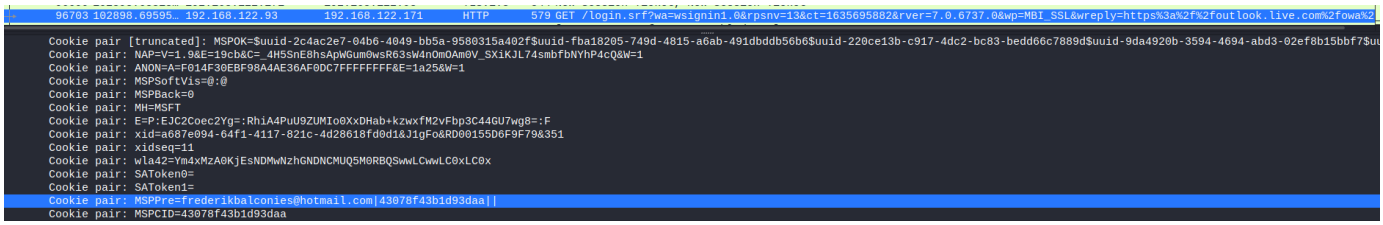
Link: atachment (https://1drv.ms/u/s!Aqo92bFDjwdDbK1QjQG_ob008dc)



***From** Frederick Balconies **to** President*

"Mr. President, The marketing team would like to publish a panoramic video of our stadium on social media. Please provide some feedback, so I can tell them if they can do it or not. For safety reasons, please download and unzip the attachment file into"

Analizamos os packets do computador da Abby e existem requests http para o proxy com o email do Frederik Balconies nas cookies (como se pode ver na frame 96703 que parece ser um request ao login do email, arquivos -> Frame_Abby) e uma resposta em que vem como conteúdo o email do Frederik Balconies que contem o attachment (frame 114027), ou seja, acreditamos que tenha entrado no email do Frederik Balconies e mandou o malware para o email do presidente para ter acesso aos pdfs.



Após termos feito download dos ficheiros verificamos o md5sum de todos e são iguais aos dos laboratórios anteriores, o que nos leva a concluir que são os mesmos pdfs que Abby enviou para Daniels.

Ficheiro	**MD5 Valor**	**Descrição**
a.pdf	f0882eedb95122f39e692a9397c1f5c5	Red Hawks FC internal
b.pdf	2be65457105ca324381952538fc94de7	The Hawks supporter
c.pdf	e02839232a2283ac0843de8ecfc980a0	Red Hawks FC statement
d.pdf	33bd1f8ed5f5692c5bf1e5a87d6110b2	Bank statement
e.pdf	44d015d11ecd0ec4ecaa6cb350032d17	James Santo Profile

Na Trace dos registos de email de ryancoast10@outlook.com e levyfvelucci@outlook.com encontramos trocas de emails sobre uma quantia exagerada de frangos que na verdade trata-se de uma quantia avultante(3.000.000.00) que Velucci recebeu na sua conta. Ryan serve como intermediário de Velucci e George. Neste email George pede a sua parte e comprova que Velucci recebeu esta quantia. Visto que o único elo que ambos tinham era a transferência de James então nos leva a concluir que esta quantia presente no extrato (d.pdf) é relativa a venda do jogador.

Analisando o documento interno dos Red Hawks, Velucci enviou este email com o conhecimento de Ryan Coast, ou seja, ambos estão envolvidos na transferência do jogador. Também a partir da troca de emails chegamos a conclusão de que Velucci também iria dar uma parte do que recebeu para Ryan.

***From** Ryan **to** Velucci*

"Just following on that email that George just sent: I'm still waiting for my share... We have discussed this far too many times already You got 3 million chickens out of that deal and you promised me 500 thousand to go along with it... You've had almost 2 months to send me cut and I'm still waiting. If you want this dinner celebration to go through, you need to send me the chickens. Otherwise, you may need to face some unexpected problems Please send the chickens to my Bitcoin address, as it is."

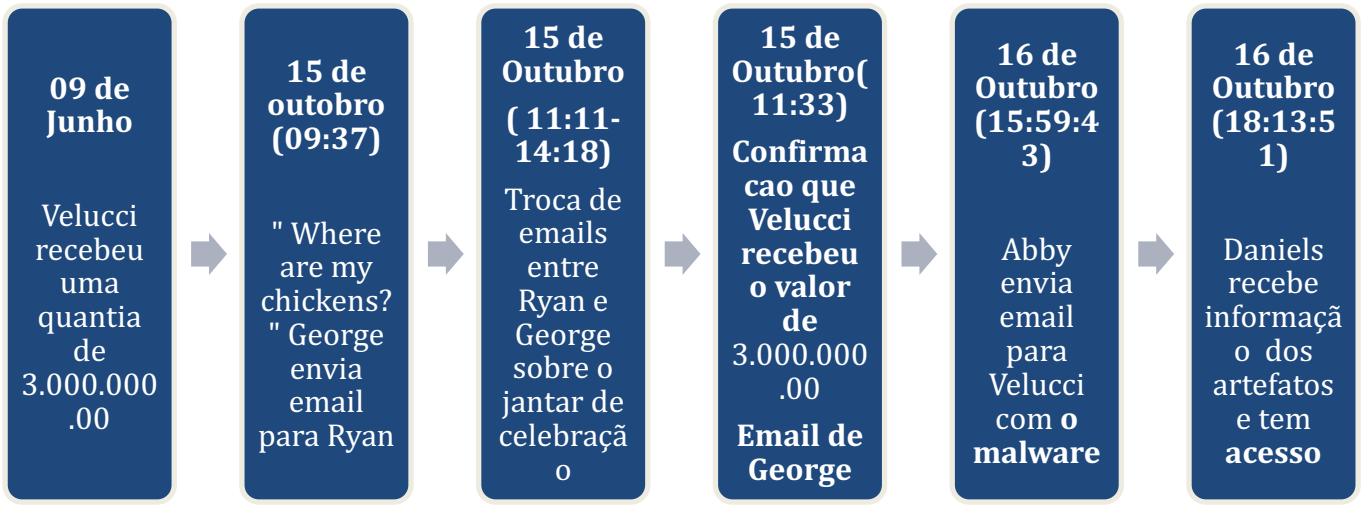
***From** Velucci **to** Ryan*

"Easy Ryan don't worry! Now that things have become calmer, I will send you your share of the deal today. I have already told you that I don't know how to use this bitcoin thing, so I'll just transfer it by the traditional way during my lunch break. I've heard these things are only used by criminals and we surely aren't criminals, just simple businessmen trying to make a living It is not like we are going to get caught anyway."

2 What can you tell about the identity of the person(s) responsible for leaking the secrets?

O verdadeiro responsável pela fuga da informação foi a interna, Abby Chapman, que se fez passar pelo administrador de redes, Frederick Balconies, e assim por intermédio de um email(contido nos artefactos), enganou o presidente Velucci, fazendo com que baixasse e fizesse unzip de um ficheiro que na verdade se tratava de um malware que Abby usou para extrair as informações do computador de Velucci, ou seja todos os documentos que passou para Charles Daniels (Os cinco pdfs).

3 Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the secrets ended up in Charles Daniels' computers?



Toda esta informação esta presente nos emails que encontramos. (Arquivos->emails)

4 What can you deduce from all the evidence collected in the context of the investigation? If the investigation was to continue, what should be the next steps to verify your hypotheses?

Após análise e confirmação da veracidade de todas as evidências por nós coletadas, podemos deduzir que o presidente da Red Hawks, Levy Fran Velucci, está de facto envolvido na transação fraudulenta de James Santos e, pelas mesmas evidências foi-nos possível identificar mais uma pessoa envolvida nesta transação, o vice presidente da Red Hawks, Ryan Coast, que esteve em contacto por email com o agente de James Santos, que pelo mesmo email nos foi possível deduzir que, este e outras pessoas que não pudemos identificar as suas identidades estão também envolvidos nesta fraudulenta transação.

O próximo passo para verificar a nossa hipótese, analisar todas as evidências coletadas, testar a nossa hipótese mediante a todos os factos e evidências conhecidas, para podermos verificar e validar a nossa hipótese e, caso não possa ser apoiada pelas evidências e factos, seja descartada e se desenvolvam outras hipóteses, ou caso seja validada possa então ser apresentada ao ministério público.