***Indícios/Suspeitas encontradas***

Começámos por fazer o comando *md5sum* para todos os ficheiros, para verificar que o resultado desse comando correspondia com o *value* dado para cada ficheiro, no enunciado, e assim confirmar que nenhum ficheiro foi corrompido ao descarregar para a nossa máquina.

***Ficheiro: Cathedral.png***

* Fizemos *head* do ficheiro e verificamos que os primeiros dígitos do ficheiro dizem PNG, que faz, à partida, sentido sendo que a extensão do ficheiro é PNG;
* Ao fazermos o *hexdump* do ficheiro verificamos que os primeiros dígitos em hexadecimal são 5089 474e 0a0d 0a1a, que remete ao tipo de ficheiro PNG;
* ;

***Ficheiro: snow.bmp***

* Fizemos o *hexdump* do ficheiro e verificámos que os primeiros dígitos correspondem a 4d42 que remete ao ficheiros dessa extensão;
* Fizemos de seguida o *tail* do ficheiro e no fim conseguimos encontrar as últimas palavras que estavam no ficheiro, numa língua que especulámos ser em Alemão dada a natureza do problema. Usando o *translate* do *google* verificámos que significava o seguinte: "Vou enviar-lhe cinco arquivos: (1) planos de *drone* A, (2) planos de *drone* B, (3) especificações técnicas, (4) senhas de servidores de arquivos***.*** DroneX", o que nos leva a suspeitar num roubo de alguns ficheiros;
* Ao ler 5 arquivos remete-nos a pensar que poderá ser referente a cada ficheiro de imagem (PNG) e ao ficheiro ZIP, ou seja, que cada ficheiro tenha alguma informação escondida, nomeadamente os planos de cada *drone*, as especificações técnicas e as senhas de servidores de arquivos;

***Ficheiro: compress.py***

* Ao investigar o código fonte do ficheiro, verificámos que no ficheiro se encontra uma frase que diz: "*LSB steganography tool: hide files within least significant bits of images*" e " *the password is optional and must be a number*", o que pode ser pistas para os nossos passos seguintes;
* Para tentar investigar o código deste programa, o que fizemos foi descompilar o código fazendo *uncompyle2 compress.py*, ou seja, recorremos ao programa *uncompyle2*, e dessa forma conseguimos abrir o código e tentar percebê-lo e porventura descobrir alguma pista;
* Sabendo que este ficheiro o que faz é esconder alguma informação nos bits menos significativos, e usando comandos como *head*, *hexdump*, etc.. não irão conseguir apanhar essa informação. Iremos então tentar reverter o código para tentarmos encontrar alguma informação que esteja escondida nos ficheiros dados usado este programa revertido;

***Ficheiro: munich.txt***

* Executámos vários comandos, como o *tail*, o *head* e o *hexdump* para tentar encontrar alguma anormalidade, no entanto, até agora parece ser um ficheiro de texto normal, o que pode ser razão para suspeitar;
* A única coisa relevante que descobrimos é que é um ficheiro de texto do *Wikipedia*;
* Ao tentarmos resolver a questão da password do online\_banking.zip, descobrimos que este ficheiro pode conter a password que permite desbloquear o ficheiro zip. Assim, colocámos todas as palavras deste ficheiro num dicionário e tentámos usar o programa *fcrackzip* para tentar descobrir se alguma das palavras do dicionário correspondia à password correta. E o programa obteve a password: **Stadelheim**, e, ao verificar essa password no ficheiro conseguimos desencriptar o zip online\_banking, permitindo avançar um pouco mais na nossa investigação;
* Dentro do ZIP encontramos dois ficheiros: *online\_banking.docx* e *drone-A.bmp*, onde ao abrir o primeiro ficheiro usando *libreoffice*, por exemplo, se encontra uma password: 51782;

***Ficheiro: drone-A.bmp***

* Começámos por investigar o código hexadecimal deste ficheiro. No final do mesmo encontrámos um provável timestamp da fotografia: “tEXtdate:create.2014-12-09T14:18:22+01:00”. Uma pesquisa no google do excerto “tEXtdate:create” levou a uma suspeita de que o formato original da imagem fosse png. Assim, fomos verificar qual a assinatura válida do ficheiro png, e comparámos a assinatura do ficheiro com a assinatura normal de png:

Assinatura PNG:89 50 4E 47 0D 0A 1A 0A

Assinatura ficheiro: 5C 78 30 47 0D 0A 1A 0A

Foi possível constatar que os primeiros 6 dígitos hexadecimais da assinatura são diferentes da assinatura normal de um ficheiro PNG. Assim, procedemos à alteração do ficheiro para que inclua a assinatura correta, bem como à mudança da extensão de bmp para png. Ao abrir o ficheiro, já foi possível visualizar a foto que mostra o esquema de um drone;