***Indícios/Suspeitas encontradas***

Começámos por fazer o comando *md5sum* para os ficheiros de memória e do disco da *Sally*, 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: sally\_disk***

* ***Recuperar os ficheiros da Sally:***
* Para termos acesso os ficheiros que se encontravam no PC da *Sally*, quando ocorreu o ataque, usamos a aplicação *testdisk*;
* Sabíamos, pelo enunciado, que os ficheiros a serem recuperados encontravam-se dentro do diretoria */home/sally/Documents*;
* Executámos o comando: *testdisk sally\_disk*, o que abriu a janela da aplicação em causa;
* Clicámos em *proceed*, de seguida escolhemos a opção *Intel* para o tipo de tabela de partição. Depois escolhemos a opção *Advanced*, e na opção *Linux* ( partição a analisar), escolhemos a opção *List* para listar os tipos de ações feitas nessa partição e em que ficheiros foram feitas; (Ver screenshots)
* Podemos ver que uma das ações feitas foi na para *home*, que era do nosso interesse; (Ver screenshots)
* Escolhendo essa opção, clicámos em copiar essa pasta para a nossa máquina, para uma posterior análise;

***Ficheiro sally\_mem:***

* ***Como é que o PC da Sally foi atacado:***
* Começamos por listar os comandos disponíveis no *Volatility* (que seria o *software* a utilizar para analisar a memória), fazendo o comando: *python vol.py --profile=LinuxUbuntu160405x64 -f ../sally\_mem -h* ;
* Começamos por fazer o comando: *python vol.py --profile=LinuxUbuntu160405x64 -f ../sally\_mem linux\_netscan*, para verificar as conexões feitas guardadas na memória;
* Houve umas ligações que nos pareceram suspeitas, pois no endereço de origem ( que deviam ser todos privados, pois seriam referentes ao PC da Sally), apareceu em duas alturas diferentes um IP, na origem, mas que não era privado mas sim público;
* Verificamos de onde era esse IP, fazendo o comando *whois*, e verificámos que tinha como *address*, uma localidade da China. Isto veio indiciar que seria obra do atacante, talvez tenha usado um ataque de *IP Spoofing* (IP pode ter sido adulterado);
* De seguida, decidimos listar todos os processos existentes no ficheiro de memória, fazendo o comando: *python vol.py --profile=LinuxUbuntu160405x64 -f ../sally\_mem linux\_pslist* ;
* Não conseguimos, de imediato, retirar alguma conclusão ou suspeita olhando simplesmente para o nome dos processos. Olhámos com mais atenção para as horas de cada processo para nos ajudar: a esmagadora maioria dos processos foi executada quase de imediato (às 17h 05), o que nos leva a crer que foi tudo processos referentes ao arranque da máquina ou processos do sistema; Existem, depois alguns processos, entre as 17h 06 e as 17h 10, mas parece ser processos do sistema Linux ou processos referentes à rede; Os últimos 3 processos (às 17h 20) são referentes ao *LiME* que foi o programa usado para gerar o ficheiro de memória, logo estes estão excluídos de suspeita; Sobram os processos entre as 17h 13 e as 17h 19, onde estão incluídos dois processos algo suspeitos, com o nome de *main* (-p 14919 e -p 14921);
* Decidimos fazer o comando: : *python vol.py --profile=LinuxUbuntu160405x64 -f ../sally\_mem linux\_psaux*, para nos auxiliar mais nesta procura. E descobrimos que esses dois processos *main*, ocorrem na diretoria */home/sally/Downloads*, o que reforça a nossa suspeita: estes dois processos poderão estar envolvidos na encriptação dos ficheiros da *Sally*, dado a localização onde atuam ambos os processos;
* Decidimos analisar o mapa de memória de ambos os processos, fazendo o comando: : *python vol.py --profile=LinuxUbuntu160405x64 -f ../sally\_mem linux\_proc\_maps -p <ID do processo>*;
* Foi no segundo processo *main* que descobrimos maiores indícios, pois havia muitos ficheiros a ocorrer neste processo relacionados com encriptação, pois verificamos a seguinte diretoria, */Crypto/Cipher*, a ocrrer em muitos deles;
* Decidimos então gerar o *dump* de memória desse processo, fazendo o comando: : *python vol.py --profile=LinuxUbuntu160405x64 -f ../sally\_mem linux\_dump\_map -p 14921 -D < diretório output para o dump>* ;
* Ao analisar alguns dos ficheiros gerados, nomeadamente os ficheiros relacionados com a diretoria referida acima, e usando a ferramenta *strings*, descobrimos várias referências à encriptação dos ficheiros da *Sally*, como a mensagem do *pop-up*, várias referências à encriptação o que veio confirmar as nossas suspeitas, e um endereço *email* do suposto atacante ;
* ***Recuperar os ficheiros da Sally:***
* Com estas análises à memória, podemos concluir que a chave usada para encriptar os ficheiros, se encontra lá escondida;
* Sabíamos à *priori* que o algoritmo de criptografia usado pelo *malware*, foi AES usando o *counter mode* com uma chave de 128 bits;
* Posto isto, usando o programa *aeskeyfind*, que tem como objetivo recuperar chave AES de ficheiros de memória *dump*, e encontrámos a chave usada na encriptação: 47683b9a9663c065353437b35c5d8519;
* Sabíamos, também à *priori*, que o *initial value* (IV) do AES *counter* correspondia aos primeiros 128 bits de cada ficheiro encriptado;
* Tendo estas informações reunidas, adaptámos um código proveniente do *github*, para desencriptar os ficheiros em causa, tendo em conta a forma como estes foram encriptados;
* Desta forma, criámos o código *decrypt\_files.py* que nos permitiu desencriptar todos os ficheiros encriptados pelo atacante, e assim, ter acesso os ficheiros originais da *Sally*;
* ***Identidade do Atacante:***
* Ao verificar que a *password* estava no ficheiro de memória, podemos concluir que essa chave foi gerada no PC da *Sally*, o que implica que essa chave foi enviada depois ao atacante usando algum protocolo (FTP, SSH, etc..);
* Analisando, mais uma vez, o *output* do comando *python vol.py --profile=LinuxUbuntu160405x64 -f ../sally\_mem linux\_netscan*, e já sabendo que existe aquela ligação suspeita, iremos ver que portos foram usados nas várias ligações, para concluirmos que protocolo foi usado na transferência da chave, do PC da *Sally* para o atacante;
* Podemos verificar que existe uma ligação, usando o porto 22 que corresponde ao protocolo SSH (*Secure Shell*), que permite fazer um *login* remoto a vários sistemas de computadores e consequente, envio de ficheiros;
* Logo, podemos suspeitar que foi assim que o atacante conseguiu ter acesso à chave criptográfica;
* Esta ligação foi feita para o IP de destino 146.193.41.57, que corresponde ao INESC, em Lisboa, que poderá indiciar que o atacante se encontrava ligado à rede do INESC (presencialmente ou usando uma VPN), aquando o ataque ao PC da *Sally*;