INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Ciber Segurança Forense

MEIC / METI 2018-2019 - 1º Semestre

Relatório Forense Digital

Autores: (Grupo 6) Ruben Condesso, nº81969; Miguel Carreiro, nº82012; Telma Andrade, nº93982

Introdução

O objetivo deste trabalho é analisar os artefactos digitais extraídos pelo analista forense, e responder às 4 perguntas que se seguem, onde cada uma será justificada, tendo como base, todas as pistas encontradas relevantes para este caso. As ferramentas usadas neste trabalho, encontram-se dentro da pasta *Ferrametas_Usadas*. Dentro da pasta *Screenshots*, estão imagens relevantes na nossa investigação, e que dizem respeito a vários passos que fomos dando ao longo do tempo, inclusive aquando o uso das ferramentas utilizadas. Dentro da pasta *Resultados_Obtidos/Sally_Original_Files*, estão os ficheiros recuperados do PC da *Sally*, a chave (recuperada) usada na encriptação dos ficheiros, alguns ficheiros relevantes que estavam no PC aquando o ataque informático (pasta *Downloads*, *Documents*, *./Thunerbird*), e finalmente, os resultados obtidos do ficheiro de memória, provenientes do *Volatility*. No fim do relatório, segue uma tabela com o valor dos *md5*'s relativos aos ficheiros obtidos.

Perguntas

1 Can you determine how the malware has taken over Sally's computer?

O enunciado dava-nos informações relativas a algumas ações que a *Sally* tinha feito, antes de descobrir que o seu PC tinha sido alvo de um ataque informático. O facto de ser referido que a *Sally* tinha instalado um programa de edição de imagem, o *ImageJ*, e que inclusive tinha o usado nesse dia, levou-nos a suspeitar que esse programa poderia estar na origem do ataque.

Usando o programa *Volatility*, começamos por listar os processos (comando *linux_pslist*) existentes na memória. À primeira vista, olhando para o nome de cada processo, não havia nenhum que parecesse suspeito (*screenshot image06_listProcesses*). Decidimos, então, averiguar as pastas e diretorias onde cada processo tinha sido executado (comando *linux_aux*), e reparámos em dois processos, com o nome *main* (-p 14911 e -o 14920), sendo que tinham sido executados na diretoria */home/sally/Downloads*, onde se encontravam os ficheiros da *Sally*. Optámos por analisar o mapa de memória de ambos os processos (comando *linux_proc_maps -p <ID> do processo*), e foi no segundo processo *main* que descobrimos mais indícios relevantes, sendo que havia muitos ficheiros relacionados com encriptação, dado a diretoria onde foram executados (*/Crypto/Cipher*). Gerámos o *dump* de memória deste processo (-p 14921), e usando a ferramenta *strings*, fomos investigar o *output* dos ficheiros gerados, onde descobrimos várias referências à encriptação dos ficheiros da *Sally*, como a mensagem do *pop-up*, várias referências à encriptação, e o endereço email do suposto atacante. Desta forma, tínhamos descoberto o processo que desencadeou a encriptação dos ficheiros. Usando a ferramenta *testdisk*, encontrámos dentro do PC da *Sally*, na diretoria */home/sally/Downloads*, um ficheiro com o nome *main*, que representava o programa que desencadeou o processo referido. Dentro desse ficheiro, havia apenas um *id*, o que nos levou a pensar, que depois de atuar, o código do ficheiro tinha sido apagado.

No entanto, não conseguimos estabelecer uma relação entre este processo e o possível programa que podia ter sido responsável pelo ataque (*ImageJ*), como era a nossa primeira suspeita. O enunciado dá-nos a informação que a *Sally*, além de ter instalado esse programa, verificou o seu *mail* e navegou na *web*. Podia, então, ter sido esta a porta para a entrada do *malware* para o PC da *Sally*.

Decidimos investigar as ligações feitas pelo PC (comando *linux_netscan*), guardadas no ficheiro de memória. Reparámos que muitas das ligações tinham sido estabelecidas usando o porto 993, que por sua vez é o porto atribuído ao IMAP, protocolo referente ao correio eletrónico. Assim, concluímos que a *Sally*, efetivamente acedeu ao *mail*, mas não pelo *browser* mas sim por uma ferramenta de *mail*. O *Thunderbird* era uma possibilidade, pois era compatível com o *Linux*, ao contrário do *Outlook* por exemplo. Fomos ver se, no disco da *Sally*, havia algum ficheiro referente a este programa. Usando a ferramenta *testdisk*, encontrámos a diretoria */home/sally/.ThunderBird*, dentro do disco do PC, o que confirmou o uso deste programa para aceder ao *mail* (*screenshot image01_Testdisk*). De seguida, instalámos o *Thunderbird* na nossa máquina e abrimos os ficheiros que estavam dentro da pasta *.ThunderBird*, com o objetivo de ter acesso aos *e-mails* recebidos e enviados pela *Sally* antes do ataque. E assim, descobrimos como é que o *malware* entrou no PC da *Sally*: através de um *e-mail* recebido do endereço *jason_halloween@protonmail.com*, contendo o ficheiro *main* como *attachment* (*screenshot image05_badEmail*). Verificámos que a *Sally*, efetivamente, abriu o *mail* e descarregou esse ficheiro para o seu PC (como tínhamos referido no parágrafo anterior). No ponto 4, está ilustrado as várias ações tomadas pela *Sally*, desde que ligou o PC até que o *malware* atuou. De notar que, tivemos em conta as horas destas várias ações (receber o *mail*, abrir o *mail*, execução do programa, etc..), e que estas "batiam" certo com as nossas conclusões (*screenshot image07_badEmail_time*).

Estas conclusões, indicam como é que o *malware* entrou no PC mas não explicam como é que o atacante teve acesso à chave usada na encriptação dos ficheiros, sendo que esta foi gerada localmente no PC. Voltando a examinar o *output* das ligações feitas pelo PC da *Sally*, vemos que uma das ligações feitas usou o porto 22 (ficheiro */Resultados_Obtidos/With_Volatility/Netscan*). Este porto diz respeito ao SSH, que por sua vez permite fazer um *login* remoto a vários sistemas de computadores e consequente, o envio de ficheiros, logo poderá ter sido esta a forma como a chave foi transferida do PC para o atacante. Há que ter em conta, o IP de destino desta ligação: 146.193.41.57, que corresponde ao INESC 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*.

2 Can you recover Sally's original files? If you do not succeed at retrieving the original files, can you at least extract some of its fragments?

Voltámos a usar a ferramenta *testdisk*, para termos acesso os ficheiros que se encontravam no PC da *Sally*, quando ocorreu o ataque. Sabíamos, pelo enunciado, que os ficheiros a serem recuperados encontravam-se dentro do diretoria */home/sally/Documents*.

Sabíamos à *priori* que o algoritmo de criptografia usado pelo *malware*, foi AES usando o *counter mode* com uma chave de 128 *bits*, e com a análise feita no ponto anterior, sabíamos também que a chave tinha sido gerada no PC da *Sally*. 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. Tínhamos, também à priori, o conhecimento 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*.

3 What can you tell about the identity of the attacker?

Dado o teor do conteúdo dado nas aulas teóricas desta disciplina, sabíamos que era praticamente impossível descobrir a verdadeira identidade do atacante. No entanto, conseguimos descobrir algumas pistas relativas ao paradeiro do mesmo.

Existe o indício do IP de destino, da ligação feita por SSH, pertencer ao INESC Lisboa, como foi referido no ponto anterior. Houve mais umas ligações suspeitas encontradas, pois nos endereços de origem (que deviam ser todos privados), aparece, em duas alturas diferentes, um IP público (42.120.28.149). Verificamos, posteriormente que esse IP era referente a uma localidade na China ((ficheiro */Resultados_Obtidos/With_Volatility/Netscan*). Tal, pode indiciar, por exemplo, o uso de *IP Spoofing*, por parte do atacante para ocultar o seu paradeiro. Há que ter em conta, que estes indícios são facilmente adulterados, e não podemos ter certeza da confirmação dos mesmos, e desta forma, não passam de indícios. Relativamente ao *e-mail* recebido, podemos averiguar qual o endereço de *mail* e o domínio a que pertence, *protonmail.com*. Consultado o *site* deste domínio, podemos ver que se trata de um serviço que permite criar uma conta de *mail* anónima, onde não são guardados endereços IP usados nas trocas de *mail*. Desta forma, não podemos retirar informações relativas ao IP usado no *mail* recebido.

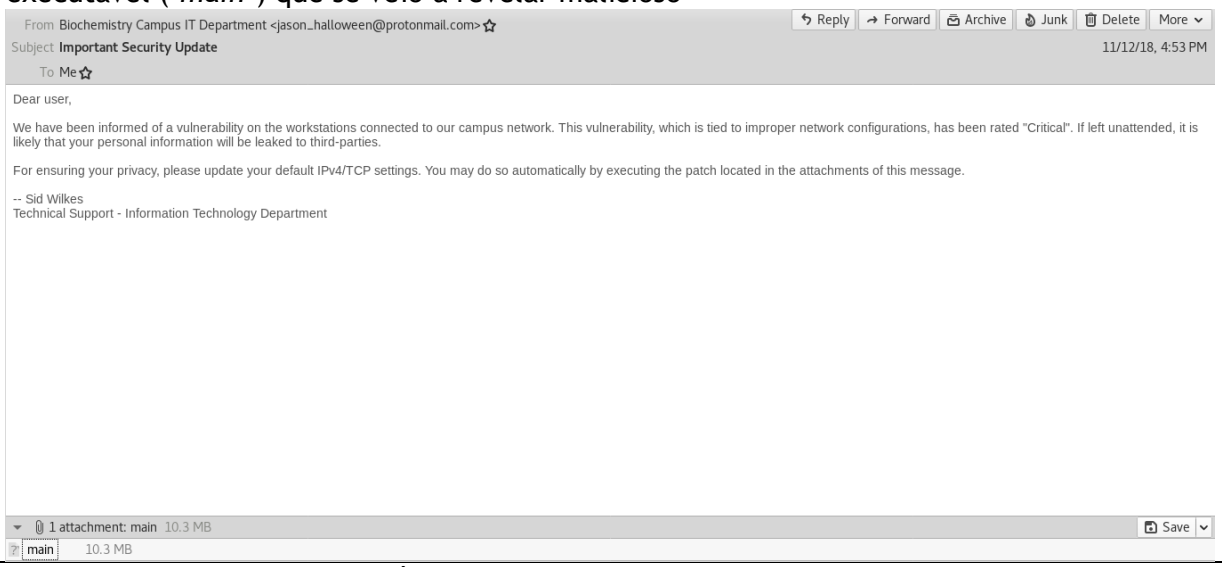
Não conseguimos retirar mais nenhuma informação válida referente ao atacante, além dos indícios referidos anteriormente. Podíamos tentar fazer uma ponte entre todos os indícios encontrados, mais não chegaríamos mais longe do que uma série de especulações.

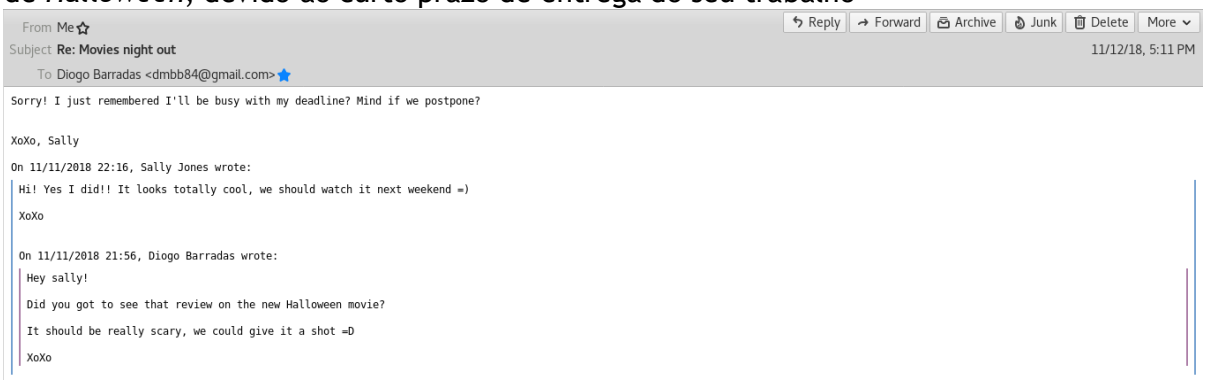
4 Elaborate a timeline of the most significant events of the case

Na elaboração da *timeline* foram tidas em conta não só as evidências apresentadas nos pontos anteriores, mas também outros elementos que nos apresentaram informações que, embora não sejam fundamentais para a elaboração de provas, ajudam a definir com maior exatidão a ordem cronológica dos eventos, podendo ser úteis, caso surjam novas evidências que se relacionem com estas. Na pasta */home/sally*, correspondente à conta de utilizador da *Sally*, encontram-se vários ficheiros que registaram a atividade da mesma, no seu PC. Foi possível obter o histórico de navegação do *browser Mozilla Firefox*, que se encontra numa base de dados (*places.sqlite*) localizada na pasta */home/sally/Documents/cancer_cells/cancer_images/sya22z5v.default*, incluindo o *link*, título da página e um *timestamp* da última visita (no formato *Unix*).

Observando a pasta */home/sally/.local/share*, reparámos na existência do ficheiro *recently-used.xbel*. Abrindo esse ficheiro, constatámos que se encontrava no formato XML, e que tinha referências à data de adição, modificação e visita de ficheiros e pastas, bem como dois *links* para páginas específicas do *website* *www.freedesktop.org*. Analisando o mesmo, foi possível descobrir uma explicação acerca dos parâmetros exibidos (*https://www.freedesktop.org/wiki/Specifications/desktop-bookmark-spec/*), o que ajudou a completar a *timeline* de eventos. A *timeline* está organizada por acontecimento, e *timestamp* em que esse acontecimento ocorreu (data e hora, com segundos caso exista essa informação). Os acontecimentos relevantes possuem o respetivo *timestamp* a negrito.

Data/hora dd-mm-aaaa hh:mm:ss	**Acontecimento**
11-11-2018 21:56:13	*Sally* recebe um e-mail de Diogo Barradas (dmbb84@gmail.com) a convidá-la para ver um filme de *Halloween* 
11-11-2018 22:16	*Sally* responde ao e-mail aceitando o convite para o próximo fim-de-semana (17/18 de novembro de 2018)

	
12-11-2018 16:53:20	*Sally* recebe o e-mail de um suposto departamento IT do campus de bioquímica, com um aviso sobre uma vulnerabilidade presente na rede do campus de investigação e um executável (‘*main*’) que se veio a revelar malicioso 
12-11-2018 17:05:43	*Sally* liga o computador, vários processos associados ao sistema operativo *Linux* são iniciados 
12-11-2018 17:05:55	*Sally* visita alguns websites usando o *browser Mozilla Firefox*. Começa por pesquisar no *Google* “*cancer research*”, vendo alguns *websites* relacionados com o tema (*Cancer Research UK*, *Elsevier*)
12-11-2018 17:08:00	*Sally* muda de assunto e pesquisa sobre alguns filmes de Halloween, bem como filmes de terror

12-11-2018 17:11	*Sally* envia um novo e-mail a Diogo Barradas a solicitar o adiamento da visualização do filme de *Halloween*, devido ao curto prazo de entrega do seu trabalho  Reply Forward Archive Junk Delete More From Me Subject **Re: Movies night out** 11/12/18, 5:11 PM To Diogo Barradas <dmbb84@gmail.com> Sorry! I just remembered I'll be busy with my deadline? Mind if we postpone? XoXo, Sally On 11/11/2018 22:16, Sally Jones wrote: Hi! Yes I did!! It looks totally cool, we should watch it next weekend =) XoXo On 11/11/2018 21:56, Diogo Barradas wrote: Hey sally! Did you got to see that review on the new Halloween movie? It should be really scary, we could give it a shot =D XoXo
12-11-2018 17:12:14	*Sally* visita o site do programa *ImageJ* (https://imagej.net)
12-11-2018 17:12:29	*Sally* inicia a descarga do ficheiro *fiji-linux64.zip* (instalador da distribuição *Fiji* do *ImageJ* para *Linux 64-bit*) através dos seguintes *links*: • Página visitada para descarregar: https://imagej.net/Fiji/Downloads • Executável para instalação (comprimido): https://downloads.imagej.net/fiji/latest/fiji-linux64.zip
12-11-2018 17:13:00	*Sally* abre uma imagem contida na pasta *cancer_cells* (*AS_09125_050118150001_A03f05d0.png*)
12-11-2018 17:14:01	*Sally* guarda o executável que recebeu por e-mail na pasta */home/sally/Downloads*, usando para tal o programa *Thunderbird* (cliente de e-mail)
12-11-2018 17:14:18	A transferência do ficheiro *fiji-linux64.zip* termina, e o mesmo é transferido para a pasta */home/sally/Downloads*, uma vez que foi a pasta configurada por *Sally* para receber esta (e eventualmente outras) descarga(s)
12-11-2018 17:14:29	*Sally* abre a pasta */home/sally/Downloads*
12-11-2018 17:15:45	*Sally* executa o ficheiro '*main*', que corresponde ao *malware* que recebeu por e-mail no mesmo dia às 16:53:20
12-11-2018 17:18:17	*Sally* abre o ficheiro TODO.txt
12-11-2018 17:20:15	Os ficheiros contidos na pasta */home/sally/Documents* são encriptados pelo executável '*main*', e passam a ter a extensão '*.encrypted*'. Também são criados novos ficheiros, com o mesmo nome dos anteriores, mas que o seu único conteúdo é uma mensagem a dizer "*Jason's back*!"

Anexo

Pasta	*md5sum*	Nome do ficheiro
	382c7ae1e99380601ec3bffbe762f60d	*sally_disk*
	8864691bed9d3712894ea0eff8f21f2e	*sally_mem*
/home/sally/Documents	23f432689a13006cfe0e982f8ae71459	*Image_Processing_with_ImageJ_decrypted.pdf*
	aa4d4b8006c1941ffa3684f26747b696	*paper_draft.txt.decrypted.txt*
/home/sally/Documents/cancer_cells	b58303dd6f4026663fb1aacaccf5bf94	*AS_09125_050118150001_A03f00d0.decrypted.png*
	1e33b87269c463474f68df10d95eb67b	*AS_09125_050118150001_A03f01d0_decrypted.png*
	defa8c84d13338cf83668cf44ccbe016	*AS_09125_050118150001_A03f02d0_decrypted.png*
	32de7caaac1e191febe5c7e4d48c839a	*AS_09125_050118150001_A03f03d0_decrypted.png*
	1a6093f96040770a97dd257a3d487231	*AS_09125_050118150001_A03f04d0_decrypt.png*
	f75baf3c3f4e06d14355133a6edae13b	*AS_09125_050118150001_A03f05d0_decrypt.png*
(executável enviado no *mail vigarista)*	324ddc336159dd62e182e3abf12c9b0a	*main*
/home/sally/.local/share	93b8a23ac26b8e18aaa4e4b215359f10	*recently-used.xbel*
/home/sally/Documents/cancer_cells/cancer_images/sya22z5v.default	43705223d779720796696614dc8442d8	*places.sqlite*