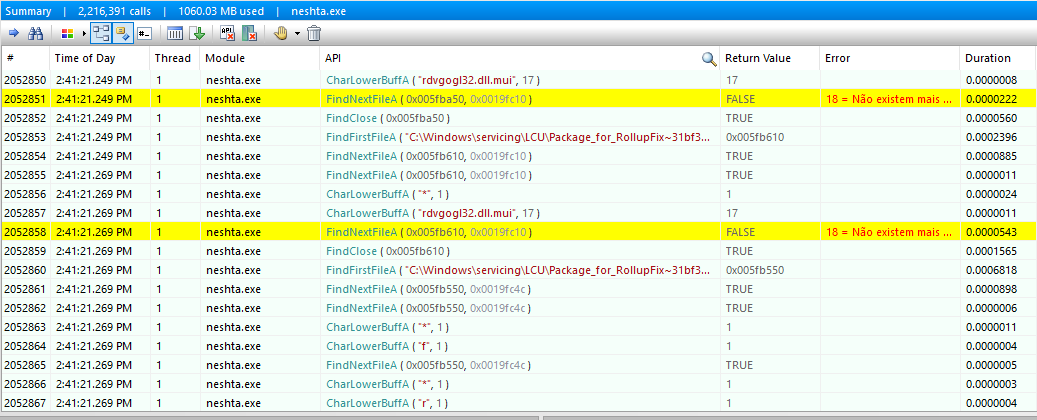
**Análise dinâmica do malware Win32.Neshta.a**

Para iniciar, desligamos todas as conexões externas da VM, como a rede de internet e as pastas compartilhadas, isolando e criando um ambiente seguro, apesar de já conhecermos o malware e inferindo que ele pode, apenas, fazer contato externo através de discos plugados através da função GetLogicalDrives.

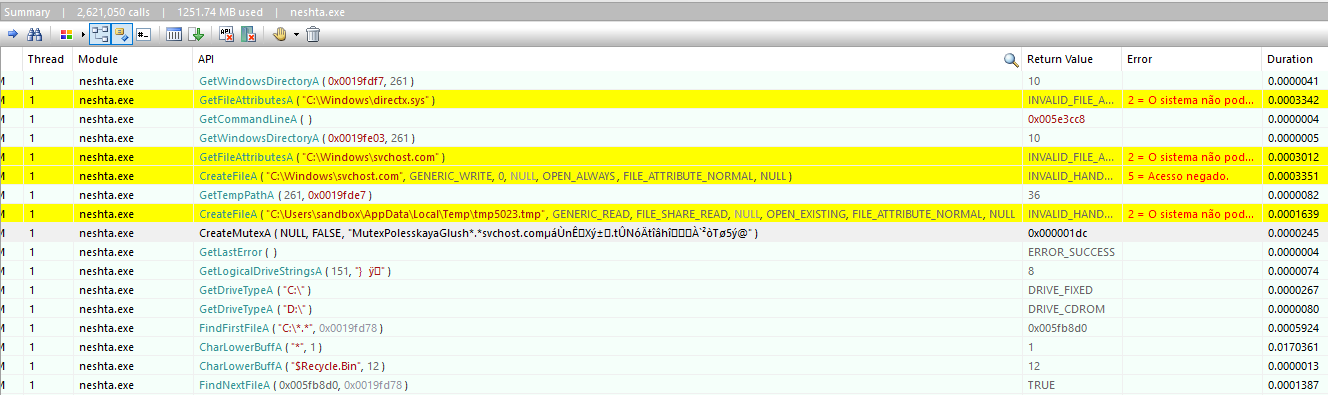
As ferramentas utilizadas serão: O API Monitor, para monitorar qualquer processo criado pelo arquivo do malware, assim como chamadas de função ou qualquer outra interação com o resto do sistema, o Process Monitor, para termos um escopo reduzido, visando apenas as operações CreateFile e WriteFile.

Ao executar o malware no API Monitor com o Process Monitor em suporte, podemos observar que uma das primeiras funções a serem chamadas é a GetKeyboardType, isso pode ser mais uma pista de que o programa pode possui exceções em certos tipos de teclado, numa tentativa de evitar a propagação em certas regiões do mundo.

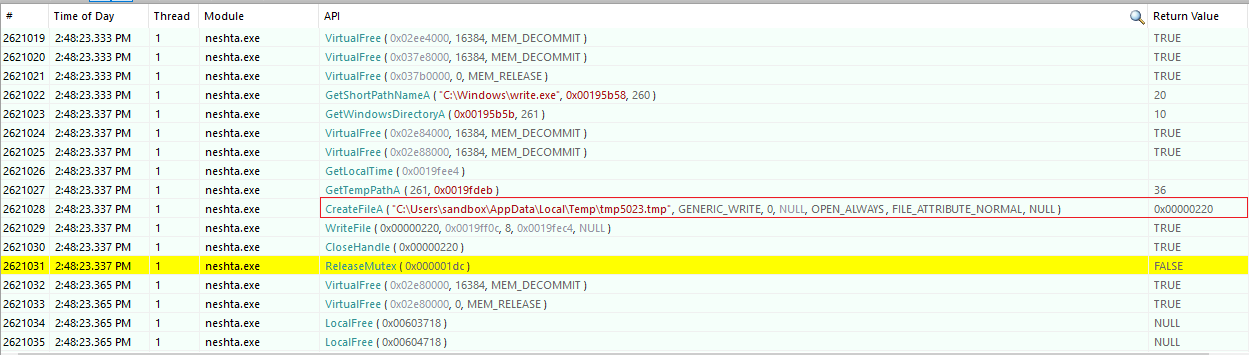
Após 10 minutos da execução, o programa já tinha feito mais de duas milhões de chamadas de função, as quais eram claramente recursivas, rodando pelos diretórios da máquina virtual com o FindNextFileA e o FindFirstFileA. O programa demora ao todo, em torno de 19 minutos para terminar todas as chamadas de função recursivas, sendo ao todo 2.621.050 chamadas de função.



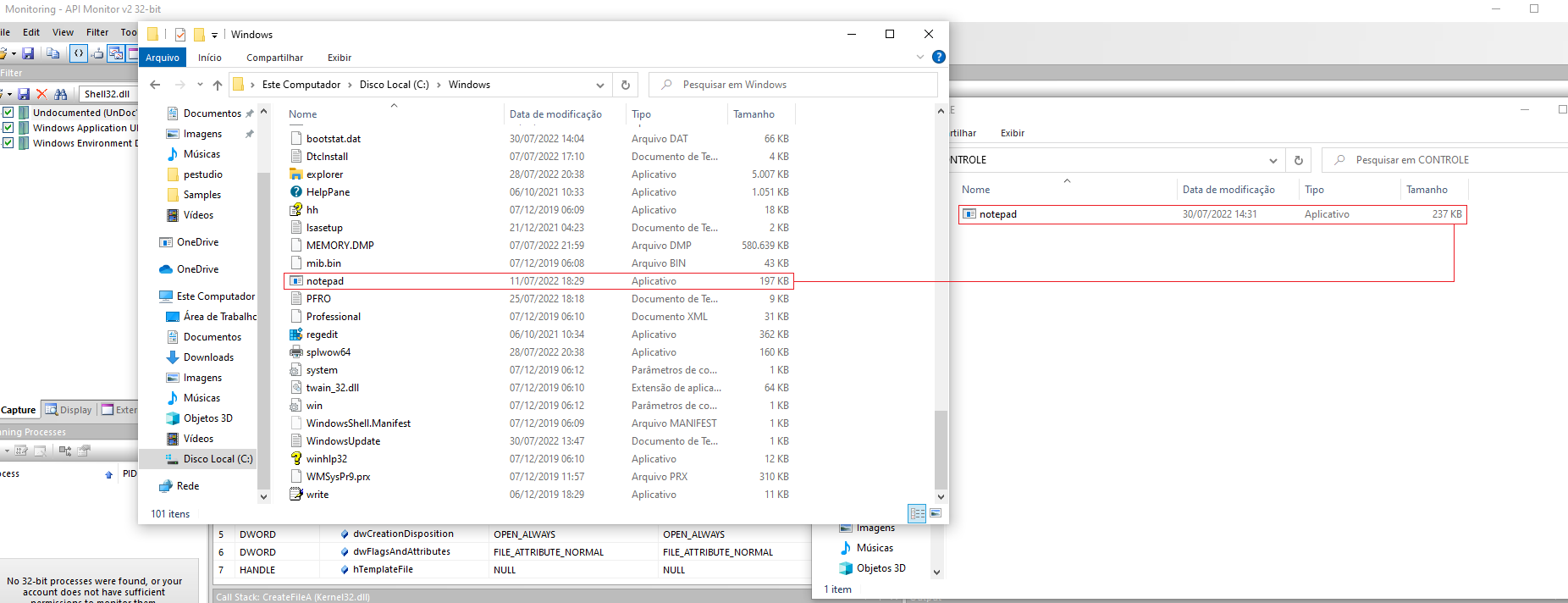
Voltando no início da execução, o malware tenta acessar o arquivo directx.sys e svchost.com, mas eles não existem. Em seguida, o malware tenta criar o arquivo svchost.com no C:\ \Windows com os seguintes parâmetros passados na função CreateFile: GENERIC\_WRITE, 0, NULL, OPEN\_ALWAYS, FILE\_ATTRIBUTE\_NORMAL, NULL. Entretanto, tem o acesso à pasta negado com o retorno INVALID\_HANDLE\_VALUE. Ele também tenta criar o arquivo tmp5023.tmp na pasta de arquivos temporários do Windows, mas falha, pois o sistema não encontra o arquivo especificado, com retorno INVALID\_HANDLE\_VALUE. Além disso, um mutex é criado, a fim de reportar alguma instância do Neshta já em execução e o GetLogicalDrives é chamado para passar os discos existentes no sistema.



Ao final da execução, o malware tenta criar o arquivo tmp5023.tmp novamente com os mesmos parâmetros e dessa vez a função é executada com sucesso. Indo até o diretório, o arquivo pode ser encontrado, ele tem o tamanho de 1kb.

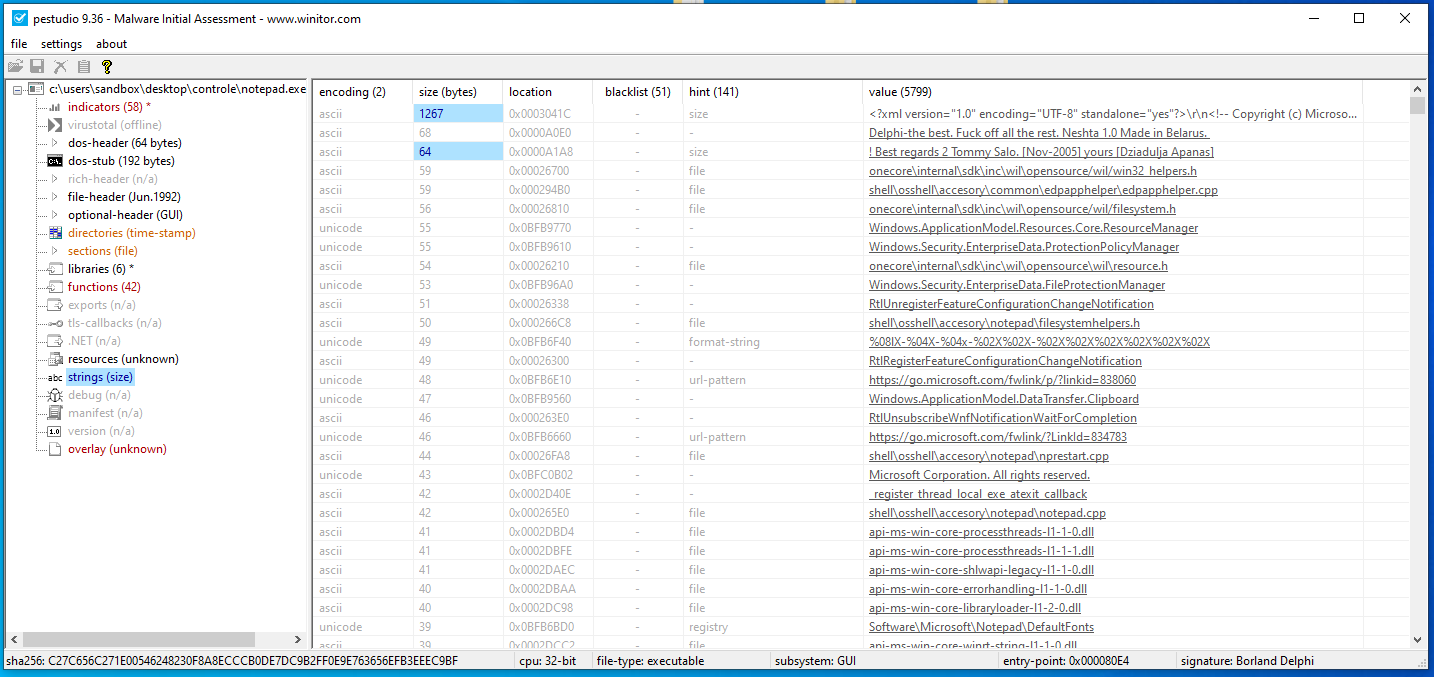


Ao observar os arquivos executáveis do sistema, vemos algo interessante e já esperado, que confirma as ações do malware. Tomaremos o arquivo notepad.exe (o conhecido bloco de notas nativo do Windows) como exemplo, ao analisar o seu valor padrão no Windows 10(197kb) para o valor pós execução do malware(232kb), ao notarmos a diferença de tamanho, veremos que é muito próxima ao valor do executável do malware.



. à esquerda o notepad.exe não infectado, à direita o notepad.exe que estava copiado para a área de trabalho e foi infectado.

A comprovação da escrita foi feita através da ferramenta PEStudio. Pode-se observar a presença de strings e chamadas de funções do malware no executável do notepad.exe



Consequentemente, ao notarmos isso, podemos concluir, com precisão, que o Neshta não infecta os arquivos presentes no diretório C:\ \Windows, na verdade, ele também não infecta os arquivos presentes na pasta Program Files, nem mesmo os arquivos temporários da Appdata(%temp%), todavia, ele ainda infecta os .EXE na Program Files x86, o que indica um anacronismo claro do malware, pois na época em que foi lançado(meados de 2006), computadores com sistemas operacionais 64 bits ainda não eram tão comuns, e a única pasta de armazenamento dos programas era a Program Files, que se referia aos programas de 32 bits, diferente de hoje, nos sistemas de 64 bits, em que se diferencia a pasta de 32 bits com x86 ao fim do nome. Isso revela mais uma característica interessante, programas 64 bits da máquina Windows 10 utilizada nesse sistema podem estar imunes contra o Neshta, pois ele evita esse diretório.

Por fim, observou-se que o Neshta falhou em utilizar a sua persistência no Windows 10, pois ele não conseguiu criar o arquivo svchost[.]com que seria utilizado como um parâmetro no registro para ser executado junto de qualquer outro binário.

O Antivírus Windows Defender, ao fim da análise, foi ativado, para comprovar, de maneira geral, a infecção do sistema pelo Neshta.

