Realização de uma análise dinâmica avançada em malware

Giovanni Fuentes Giannetti: Lucas de Araújo Oliveira. IFSP. giovanni.fg2002@gmail.com
Palavras-chave: *Malware, Análise dinâmica, ransomware*

Introdução

Vivenciamos a cada dia no mundo digital diferentes formas de ataques virtuais que objetivam principalmente a coleta ilícita de dados pessoais, sendo os dados financeiros os principais objetivos de coleta por parte dos cyber criminosos. Eilam (2005:180) cita outros motivos, como por exemplo apenas uma curiosidade para estudo ou o simples desejo de invadir algum sistema.

Uma forma de obter tais informações e em um curto espaço de tempo é por meio de criação de softwares que coletarão de uma forma automática estes dados. Estes softwares são conhecidos como Malwares. Depois de infiltrado no sistema operacional, podem dentre outras atividades, acessarem determinados arquivos, capturar tráfego de rede e teclas pressionadas do teclado e dependendo da complexidade do malware, escutar o ambiente ou obter imagens através da webcam (VELHO, 2016:410)

Segundo Velho (2016:411), estes malwares podem se infectar nos dispositivos das vítimas por meio destes canais de entrada:

- Explorar alguma vulnerabilidade: Execução de um exploit específico para uma determinada vulnerabilidade em algum programa instalado no dispositivo;
- Execução de mídias externas: Dispositivos removíveis como pen-drivers são uma grande porta de entrada destes malwares emcomputadores;
- Engenharia social: Técnica bastante utilizada na tentativa de enganar a vítima fazendo com que a pessoa acesse ou clique em algum site que fará a instalação do malware;
- Execução consciente do malware: O usuário instala o malware, normalmente em ambiente controlado, para fazer uma análise do comportamento deste programa.

Diversas são as classificações destes malwares de acordo com seu objetivo e complexidade. Devido ao grande número de classes, uma malware pode pertencer a mais de uma categoria. Alguns exemplos de classes: spyware, backdoor, worm, bot, cavalo de tróia, rootkit e vírus.

Assim como em qualquer área onde ocorra algum crime que deva ser investigado, o mundo virtual não é diferente. Várias são as situações onde um exame pericial se faz necessário. Estas análises objetivam principalmente tentar identificar a autoria e descrever a dinâmica e funcionamento do malware, como por exemplo portas abertas, conexões reversas e etc.

A análise de malware pode ser classificada em 2 grandes grupos (que geram algumas subdivisões): análise estática e análise dinâmica. A análise estática envolve a obtenção de informações sobre o malware semexecutá-lo. Para tanto, algumas técnicas são utilizadas, como por exemplo: análise de strings, identificação de APIs e disassembling. Dentro ainda desta categoria, existe 2subdivisões que são: análise estática básica e análise estática avançada (VELHO, 2016:415)

A análise dinâmica, diferente da análise estática, realiza o estudo do funcionamento do malware com o programa em execução. Neste cenário busca-se analisar as alterações realizadas no sistema operacional, arquivos e rede. Para evitar grandes efeitos colaterais, esta análise sempre é feita em ambiente controlado. De forma semelhante à análise estática, esta classe também possui 2 subdivisões: análise dinâmica básica e análise dinâmica avançada.

Tanto a análise estática avançada e a análise dinâmica avançada, fazem uso de uma técnica chamada engenharia reversa. Segundo Hoglund e Mcgraw (2006:64), a engenharia reversa é um processo onde busca-se entender todas as funções de um software, desde os

aspectos internos e de sua construção. É possível ainda aprender sobre toda sua estrutura e lógica, podendo reconstruir o código fonte e salvá-lo. Diante disto, algumas empresas colocam fortes restrições em seus softwares para evitar a utilização da engenhariareversa.

Uma das ferramentas utilizadas na engenharia reversa é o disassembler. Também conhecido como desmontador, esta ferramenta converte código legível de máquina em linguagem assembly. Já um depurador permite a análise de um programa quando está em execução. Um exemplo desta ferramenta é o OllyDbg. Outras ferramentas que serão exploradas na análise dinâmica são: proccess explorer, process monitor, network monitor e tcpview.

Objetivos

O objetivo geral deste projeto é realizar a análise de um determinado malware aplicando as técnicas e ferramentas de uma análise dinâmica avançada. Como objetivo específico, busca-se entender as técnicas e ferramentas utilizadas na identificação de malwares e apresentar resultados de comportamento de um determinado malware (portas, conexões e alterações).

Material e Métodos

Após estudos do referencial bibliográfico, deu-se início à preparação do ambiente para realização dos testes. Para simular uma situação real, foi feito o download de um vírus real através do site https://bazar.abuse.ch. O arquivo escolhido para download foi o "netfilim_32_2.exe".

Uma máquina virtual foi instalada e configurada com as ferramentas facilitando a execução do malware sem prejuízo aos dados da máquina física. Uma das vantagens de se utilizar máquinas virtuais é a possibilidade de criação de snapshots, ou seja, pontos de restauração.

Resultados e Discussão

Em um primeiro momento, foram utilizadas as ferramentas PeStudio, DIE e IDA (MENTE BINÁRIA, 2022). A execução do malware na ferramenta PeStudio mostrou, por meio de uma análise estática, informações como: data de compilação, entropia, linguagem de programação utilizada, dentre outras. Um detalhe interessante nesta ferramenta é que algumas rotinas do malware estavam na lista negra do programa, também confirmado através do site www.virustotal.com

O Detect It Easy (DIE), cujo foco não é apenas para análise de malware e sim para qualquer tipo de software, possui um grande diferencial que é a pesquisa por strings. O IDA, também apresenta uma forma interessante de pesquisas em Strings. Ambas as ferramentas mostraram os *imports* que o malware utiliza em sua execução.

Em um segundo momento, foi utilizado a ferramenta Api Monitor. Foi possível constatar algumas chamadas para DLLs importantes do sistema operacional, como por exemplo: kernel32.dll, shell32.dll, dentre outras. Foi possível observar também informações de contato do possível desenvolvedor do malware.

O malware trabalha com 9 threads e após execução do malware, em ambiente controlado, foi possível constatar que o mesmo cifra arquivos do disco rígido com a extensão .netfilim. Este processo de cifragem em arquivos do disco é caracterizado com um ransomware.

A figura abaixo apresenta a exata rotina que faz a cifragem dos arquivos no disco.

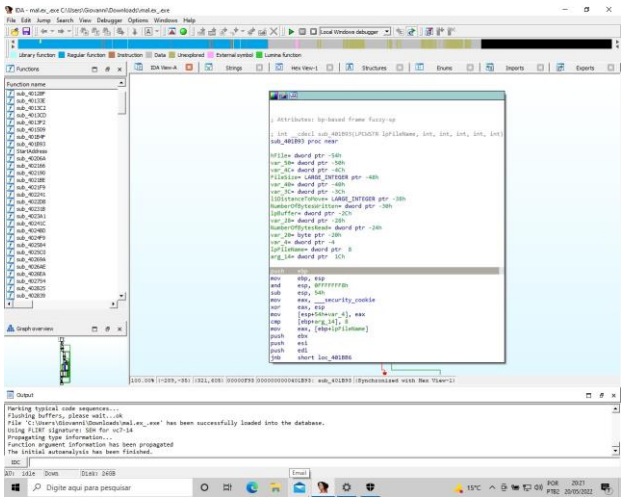

Figura 1 - função que cifra os arquivos
Fonte: Print tirado pelo autor (2022)

A figura 2 apresenta o malware em execução. É possível observar que existe o processo de cifragem dos arquivos com a extensão .netfilim.

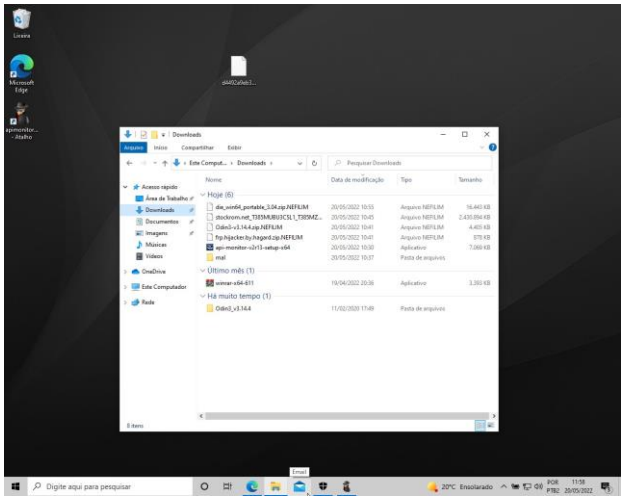

Figura 2 - Arquivos cifrados pelo ransomware
Fonte: Print tirado pelo autor (2022)

Conclusões

Com a execução de um malware aleatório e auxílio das ferramentas citadas, foi possível concluir que o mesmo trata-se de um ransomware, cuja natureza é cifrar os arquivos do disco e solicitar resgate para envio da senha para decifrar.

Não foram encontrados na análise do malware tentativas de conexões de rede.

Por fim, as ferramentas e técnicas utilizadas deram suporte necessário para uma análise dinâmica e o fato do malware não estar com código ofuscado facilitou a análise do mesmo.

Referências Bibliográficas

EILAM, Eldad. Reversing: Secrets of Reverse engineering. Indianapolis, IN. John Wiley & Sons Inc, 2005.

HOGLUND, Greg; MCGRAW, Gary. Como Quebrar códigos – A Arte de explorar (e proteger) software. São Paulo, SP. Pearson Makron Books, 2006.

Mente Binária. Disponível em <https://www.mentebinaria.com.br/> Acesso em 10/05/2022.

VELHO, Jesus Antonio. et al. Tratado da Computação Forense. Campinas, SP: Millennium Editora, 2016.