Sandboxes Uncovered: Desmistificando sistemas de análise de malware

Dario S. F. Filho
André R. Abed Grégio

Agenda

- Motivação
- Objetivos
- Sistemas Observados
- Abordagem Utilizada
- Informações Obtidas dos Sistemas
- Análise das Informações Obtidas
- Conclusão

Motivação

- Algumas análise retornadas apresentavam informações “estranhas”.
- Descobrir mais sobre informações “estranhas ” que aparecem nos relatórios.
- Aprender detalhes não revelados sobre como é feita a análise.

Objetivos

- Obter, se possível, mais detalhes sobre como ocorre a análise.
- Que ferramentas são utilizadas na análise.
- Verificar se há algum “descuido” no sistema de análise.

Sistemas Observados

Sistemas Observados

- Escolhidos baseados em:
  - Disponibilidade
  - Popularidade
  - Relevância

Abordagem Utilizada

Abordagem Utilizada - Nota

Não foram efetuados ataques, uso de técnicas subversivas, exploits, forjas, etc.

Somente foram submetidos binários, conforme esperado pelos sistemas de análise.

Abordagem Utilizada

- Descobrir maiores detalhes sobre alguns processos/ arquivos que apareciam nas análises.
  - Inicialmente com o uso de programas que tentavam imprimir no “stdout” as informações que se procurava.
  - Funcionou para o sistema A porém o sistema C não mostra a saída do programa.

Abordagem Utilizada

- Para contornar o problema de um dos sistemas, foi utilizado um modelo cliente/servidor onde o binário submetido ao sistema era o cliente e se conectava em uma máquina servidor.
- Caso a saida do stdout do outro sistema estivesse parseada, utilizou-se também o cliente/servidor para obter as informações.

Abordagem Utilizada

- Foi possível utilizar essas informações para obter arquivos que eram utilizados no processo de análise.
  - Arquivos executáveis.
  - Arquivos texto.

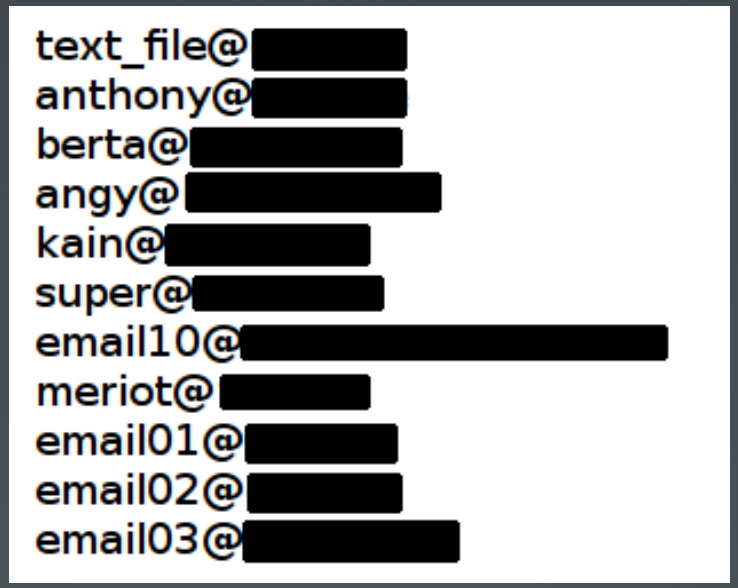
Informações Obtidas no Sistema 1

Análise Inicial

- Verificaram-se alguns arquivos no diretório raiz do sistema
- 3 executáveis com nomes aleatórios.
- 3 arquivos texto com nomes aleatórios.
  - Os arquivos tinham terminações htm, html e txt
- 1 arquivo texto com nome start.txt

Sobre os arquivos textos

- 3 dos arquivos texto continham a mesma informação.
  - Alguns endereços de e-mail.



- O arquivo start.txt continha um linha apenas.
  - Composta por um caractere e o path do arquivo submetido para análise.

E C:\nada.exe

Sobre os executáveis

- Já os executáveis eram diferentes:
  - 1 - Captura imagens da tela e simulação de pressionamento de tecla
  - 2 – Execução de ações repetidas no sistema.
  - 3 – Operações de preparação do ambiente e execução do binário em análise.

Executável 1

- Inicialmente ele cria um arquivo de log, C:\autoit.txt
- Depois cria uma pasta, C:\images
- Após isso ele entra em um loop.
  - Coloca o ponteiro do mouse em alguma posição aleatória.
  - Manda um pressionamento da tecla UP.
  - Pega uma lista de todas as janelas.

Executável 1

- Continuando no loop....
  - Para cada uma das janelas da lista ele verifica se:

  1)Ela está ativa.

  2)Se ela está visível.

  - Após essas verificações, ele tira um “snapshot” da janela e o armazena na pasta images.
  - São armazenadas informações no arquivo de log também...

Executável 1 – Arquivo de log

```
********************************************************************************
Timestamp: 1709237050155
window name: Untitled - Notepad
window handle: 0x004300D8
Process: notepad.exe
Image file: C:\images\1.bmp
Text:
********************************************************************************
********************************************************************************
Timestamp: 1709306454495
window name: C:\WINDOWS\system32\cmd.exe
window handle: 0x002300D2
Process: cmd.exe
Image file: C:\images\5.bmp
Text:
********************************************************************************
********************************************************************************
Timestamp: 1709314836343
window name: Calculator
window handle: 0x004700D8
Process: calc.exe
Text: 0. MC MR MS M+ 7 4 1 0 8 5 2 +/- 9 6 3 . / * - + = Backspace CE C 1/x sqt %
Image file: C:\images\6.bmp
********************************************************************************
```

Executável 2

- Quando executado ele imprime a mensagem “Querying system information” e fica nisso.
- Analisando ele melhor descobriu-se que ele fica em um loop infinito realizando as seguintes ações:
  - Procura pelos arquivos do C:\
  - Verifica os processos do sistema
  - Faz uma consulta às subchaves de registro da chave HKEY_LOCAL_MACHINE

Executável 3

- Responsável por ações de controle do ambiente de análise.
- Precisa do arquivo texto start.txt para funcionar.
- É necessário informar 2 parâmetros para o programa executar.
  - Um arquivo texto com nomes de processos.
  - Um arquivo texto com nomes de serviços.

Executável 3

- Inicialmente, o binário vai tratar os arquivos textos passados como parâmetros.
- Após esta etapa, o binário vai modificar o nome de alguns arquivos da pasta do sistema.
- Terminado isto, o programa vai ler o arquivo start.txt e verificar se o arquivo que será analisado é um executável ou um driver.
- Feitos todos os passos anteriores, o executável irá executar o binário ou carregar o driver.

Binário 3 – Saida de uma Execução

```
Runnnig all fake processes...
Number of fake processes: 0
Done.
Running all fake services...
Number of fake services: 0
Done.
Watching directory C:\ for modifications.
Changed C:\file3.exe to .\nmhpi.exe
Changed C:\popupKiller.exe to .\cntehhqhc.exe
Changed C:\stimulator.exe to .\cmlzwmgr.exe
Changed C:\aemail.htm to .\efjg.htm
Changed C:\aemail.html to .\xukfn.html
Changed C:\aemail.txt to .\fkgo.txt
Going to read start.txt
Executable: C:\nada.exe
Executing C:\nada.exe
```

Resumo das Informações Obtidas do Sistema A

- Algumas ferramentas utilizadas na análise.
- Informações possivelmente utilizadas pelo sistema durante a análise
- Binário responsável por realizar configurações do ambiente análise.

Informações Obtidas no Sistema 2

Análise Inicial

- Novamente, encontrado alguns arquivo no diretório raiz do sistema =)
- 1 arquivo start.bat.
- 1 arquivos executável com nome wget.

Sobre os Arquivos

- O arquivo bat continha os procedimentos executados antes da realização de uma análise.
- O arquivos executável era o wget.exe

Arquivo Start.bat

- Mostra os “xunxos” do sistema...
- Utiliza o wget para baixar arquivos de uma máquina da LAN.
  - Um arquivo de registro e um arquivo de inicialização.
- Aparece um mapeamento de rede.

Arquivo reg.reg e <Nome do Sistema>.ini

- O arquivo reg.reg modifica dois registros:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AeDebug
- Quando tentamos obter o arquivo ini nós recebemos um html. As informações deste arquivo apresentam informações sobre os binários que estão sendo analisados pelo sistema....

Arquivo Html

Total:	35689
Waiting:	0
Processed Successfully	16663668
Processing Now (Or Stuck)	3
Not Valid EXEs	1950765

Arquivo capturado há 1 mês atrás.

Total:	37856
Waiting:	0
Processed Successfully	17052890
Processing Now (Or Stuck)	25
Not Valid EXEs	2046934

Arquivo capturado esta semana.

Mapeamento de Rede

- Tentamos descobrir o mapeamento de rede utilizado pelo start.bat porém, não encontramos detalhes nos registros da máquina.
- Então, tentamos encontrar todos os mapeamentos disponíveis na rede.

Mapeamento de Rede

- Com isso, fomos tentar um por um para ver qual continha o SandboxStarter.exe
- Mapeamos o \public e verificamos o que tinha nele.
  - Muita coisa....
  - Aparentemente são arquivos submetidos para análise

Mapeamento de Rede – Arquivos Encontrados

- Paris Hilton XXX Archive.lnk
- -= The Porn Collection =-.exe
- style.asp.rar
- ca(a) .rtf.rar
- Tcait.exe
- Ads by.htm.lnk
- (ei .exe
- Cool_GameSetup.exe
- -= The Porn Collection =-.scr
- Ads by.c.exe

Mapeamento de Rede

- Não foi possível mapear as outras unidades.
- Fomos checar qual era o problema e verificamos que os mapeamentos de rede tinham sido desabilitados.
  - Isso aconteceu alguns minutos após mapear o \public

Resumo das Informações Obtidas do Sistema 2

- Script utilizado antes da análise, responsável por realizar algumas configurações.
- Informações sobre máquina(s) da mesma rede do ambiente de análise.
- Alguns dados sobre os binários recebidos pelo sistema para análise.

Conclusão

Conclusão

- Muita informação pode ser obtida de forma simples sobre o processo de análise.
- Conseguimos analisar alguns binários utilizados.
- Parece que não são tomadas medidas que visem proteger o sistema de análise.

Obrigado!

Perguntas?