FCCN UNIDADE DA FCT
Tecnologia para o Conhecimento

CSIRT IN A BOX 2022

ANÁLISE FORENSE

Pedro Silva

RCTS CERT

CERT RCTS

AGENDA

- Introdução
- Caso Prático
- Resultados

INTRODUÇÃO

- Obter uma imagem do disco
- Integridade dos dados
- Processar imagem
- Malware Sandbox

ANÁLISE FORENSE

1. Qual o comando/processo que está a consumir o CPU? (de notar que a máquina foi pausada quando foi descoberto que estava a consumir desmesuradamente CPU!)

2. Por favor, verifique quando é que existiram acessos indevidos, qual o IP de origem e qual o protocolo usado?

3. Quantas vezes foi efetuado login com sucesso por parte deste IP/Utilizador?

4. Foi instalada uma nova fonte de pacotes, qual? E por que utilizador?

5. Foi descarregado software ilícito (pergunta 1), qual o nome do software e qual a diretória para onde foi descarregado? Qual a sua versão?

6. Qual a password do utilizador ncadmin para aceder ao postgresql?

Caso Prático
(50 minutos)

RESULTADOS (1/3)

1. Se fizermos um "ps aux" conseguimos perceber que existe um processo que não é suposto estar a correr:

./xmrig -o rx.unmineable.com:3333 -a rx -k -u DOGE:{DRqzogerxW9UhYsheJsNEExEfY8zx9jCk2}

2. Se visitarmos a directoria onde existem os logs do sistema "/var/log", e face ao OS instalado "cat /etc/issue", conseguiremos perceber que estamos a trabalhar num OS ubuntu.

No OS ubuntu os logs de acesso são armazenados no ficheiro auth.log.

Assim sendo podemos determinar quem conseguiu aceder ao sistema com o uso do seguinte comando:

zgrep /var/log/auth.log*

Apesar de alguns acessos ao sistema a partir de redes locais, existem também acessos a partir do IP 81.246.165.252 que não é susposto existirem.

Accepted password for ncadmin from 81.246.165.252 port 14417 ssh2

RESULTADOS (2/3)

3. Agora que sabemos o IP de origem e o protocolo, conseguiremos contar quantas vezes o utilizador ncadmin conseguiu acesso a partir do IP 81.246.165.252 com o seguinte comando:

zgrep /var/log/auth.log* | grep 81.246.165.252 | wc –l

Quatro

May 20 17:42:21 nextcloud sshd[62673]: Accepted password for ncadmin from 81.246.165.252 port 57277 ssh2

May 20 17:43:03 nextcloud sshd[62842]: Accepted password for ncadmin from 81.246.165.252 port 26807 ssh2

May 23 11:12:52 nextcloud sshd[3858]: Accepted password for ncadmin from 81.246.165.252 port 13418 ssh2

May 23 11:22:05 nextcloud sshd[4701]: Accepted password for ncadmin from 81.246.165.252 port 14417 ssh2

4. Mais uma vez na directoria onde os logs são guardados "/var/log" conseguimos ter acesso ao registo de comandos efectuados anteriormente.

Aqui conseguiremos pesquisar de modo a perceber quando é que foi instalado o ppa. Sabendo a sintaxe usada para instalar um ppa:

"add-apt-repository ppa:[REPO]/[TBA] "

Bastava para tal, uma vez na directoria "/var/log" executar o seguinte comando: sudo zgrep "ppa:" *

A linha com o ppa do bfgminer resulta do comando:

ppa:luke-jr/bfgminer root

RESULTADOS (3/3)

5. Seria mais fácil responder a esta pergunta, depois de termos conseguido responder à pergunta número 1, pois sabíamos o nome do software instalado. Uma vez munidos com o nome do software conseguimos fazer uma simples procura no sistema:

find / -iname "xmrig"

/root/.xmrig/xmrig-6.17.0/xmrig

6. Por fim a resposta à pergunta 6 também estava no ficheiro /var/log/auth.log.

Seria mais fácil se soubessemos que o binário que existe no processo de instalação do postgresql é o psql. Podemos assim fazer uma pesquisa pelo uso deste executável, mas também era mencionado o utilizador em questão, ncadmin. Ou filtrando por psql ou pelo utilizador podíamos fazer:

1. zgrep psql auth.log*
2. zgrep ncadmin auth.log* | grep -i password

Qualquer um dos 2 comandos nos mostram a password a usar para aceder ao psql com o user ncadmin:

/usr/bin/psql -c ALTER USER ncadmin WITH PASSWORD '9ZhwvLNzTYwxOS0TZQr85DPR7eyX'

Obrigado!