

# Manual do Operador: Insider Threat

Gabriel I. Q. Costa<sup>1</sup>, Victor H. F. Ramalho<sup>1</sup>

<sup>1</sup>Instituto Metr pole Digital – Universidade Federal do Rio Grande do Norte (UFRN)  
Natal – RN – Brasil

`gabriel.igorq@gmail.com, valelc@ufrn.edu.br`

Este manual tem o objetivo de gui -lo de forma a executar da maneira correta o sistema de an lise de amea as internas desenvolvido. A aplica  o foi inteiramente desenvolvida utilizando-se o Eclipse, logo, recomenda-se que a sua execu  o seja realizada por esta plataforma ou outro tipo de IDE.

## 1. Crie um novo projeto

Ao abrir a IDE crie um novo *Java Project* e dentro dele insira a pasta “src” contendo os arquivos do sistema. Em seguida, atualize o projeto clicando com o bot o direito nele e selecionando a op  o “Refresh”.

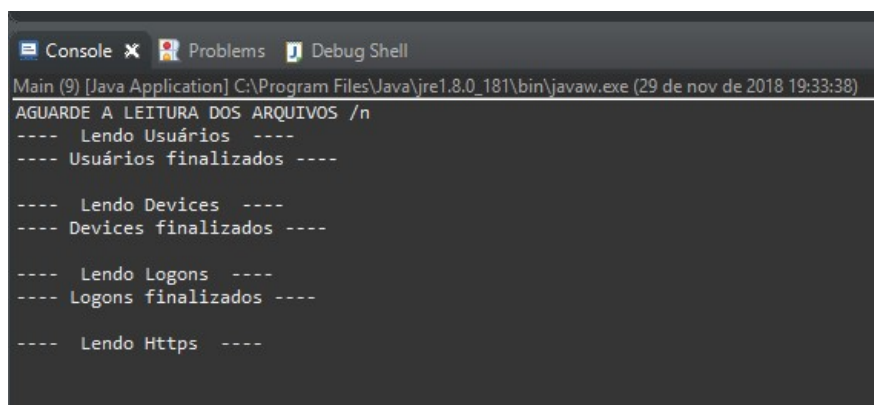
## 2. Adicione os arquivos csv faltantes

Por limita  es do Sigaa, plataforma por onde o projeto foi enviado, existem dois arquivos faltantes para a execu  o do sistema, por possuir um tamanho muito grande. S o os arquivos `logon.csv` e `http.csv`. Esses arquivos s o obtidos a partir da pasta R1 encaminhada para o desenvolvimento do projeto. Insira esses arquivos dentro do pacote `br.ufrn.imd.lp2.files`.

Aten  o: Os arquivos precisam estar necessariamente nesse pacote e os seus nomes devem ser exatamente como citados. Mudan as no nome dos arquivos, ou no pacote em que eles est o, resultar  em falhas na execu  o.

## 3. Execu  o da aplica  o

Completada a etapa anterior, basta que voc  execute o projeto na IDE. A execu  o inicia-se lendo cada um dos arquivos `.csv` do pacote `br.ufrn.imd.lp2.files`. Enquanto os arquivos estiverem sendo lidos, mensagens ser o apresentadas no console.



```
Console Problems Debug Shell
Main (9) [Java Application] C:\Program Files\Java\jre1.8.0_181\bin\javaw.exe (29 de nov de 2018 19:33:38)
AGUARDE A LEITURA DOS ARQUIVOS /n
---- Lendo Usu rios ----
---- Usu rios finalizados ----

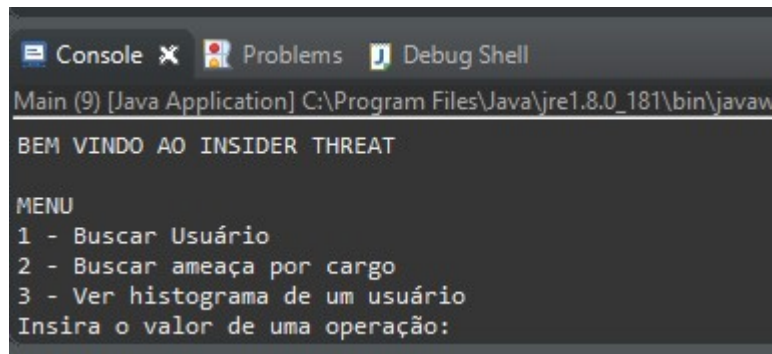
---- Lendo Devices ----
---- Devices finalizados ----

---- Lendo Logons ----
---- Logons finalizados ----

---- Lendo Https ----
```

Figura 1: Leitura de arquivos csv no console

Ao se encerrar a leitura de todos os arquivos csv será apresentado um menu textual, informando 3 tipos de ações possíveis para se executar.



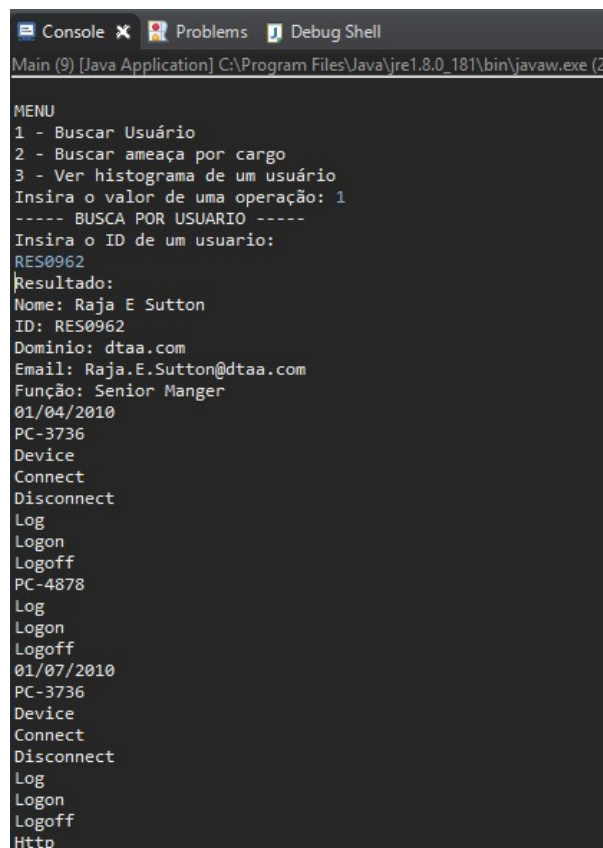
```
Console Problems Debug Shell
Main (9) [Java Application] C:\Program Files\Java\jre1.8.0_181\bin\javaw
BEM VINDO AO INSIDER THREAT

MENU
1 - Buscar Usuário
2 - Buscar ameaça por cargo
3 - Ver histograma de um usuário
Insira o valor de uma operação:
```

Figura 2: Menu da aplicação

O menu apresentado te dá três opções de ações a serem executadas:

1. Buscar Usuário: Para realizar esta ação digite 1 no console. Em seguida, será pedido que o ID de um usuário seja inserido. Caso o ID de fato exista, será apresentada em texto a árvore do usuário, contendo no topo os seus dados, em seguida uma data, o dispositivo, o tipo de ação realizada e as ações executadas de fato por aquele usuário naquele dia. Para cada data, são apresentados esse conjunto de informações. Caso o ID não exista, será retornada uma mensagem informando que o ID foi inválido.

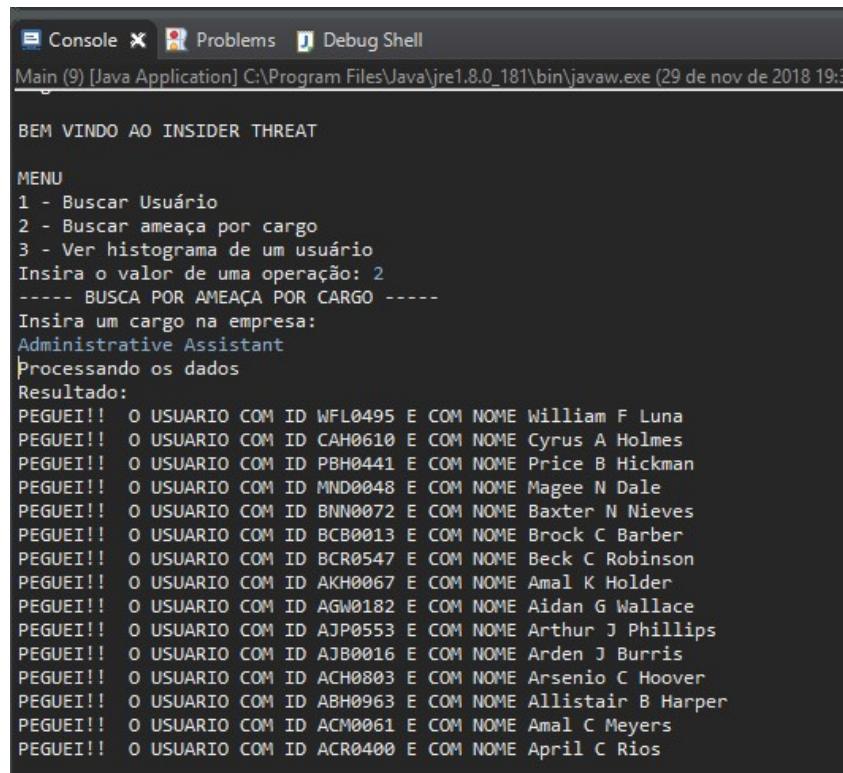


```
Console Problems Debug Shell
Main (9) [Java Application] C:\Program Files\Java\jre1.8.0_181\bin\javaw.exe (2)

MENU
1 - Buscar Usuário
2 - Buscar ameaça por cargo
3 - Ver histograma de um usuário
Insira o valor de uma operação: 1
----- BUSCA POR USUARIO -----
Insira o ID de um usuario:
RES0962
Resultado:
Nome: Raja E Sutton
ID: RES0962
Dominio: dtaa.com
Email: Raja.E.Sutton@dtaa.com
Função: Senior Manger
01/04/2010
PC-3736
Device
Connect
Disconnect
Log
Logon
Logoff
PC-4878
Log
Logon
Logoff
01/07/2010
PC-3736
Device
Connect
Disconnect
Log
Logon
Logoff
Http
```

Figura 3: Exemplo de busca por usuário

2. Buscar ameaça por cargo: Para realizar esta ação digite 2 no console. Em seguida será pedido que um exemplo de cargo seja inserido. Assim como no método anterior, caso o cargo não exista será retornada uma mensagem informando que o argumento foi inválido. Se o cargo existir, ele irá retornar uma lista de possíveis funcionários suspeitos, cujas distâncias euclidianas são outliers em relação aos demais funcionários que exercem aquele cargo.

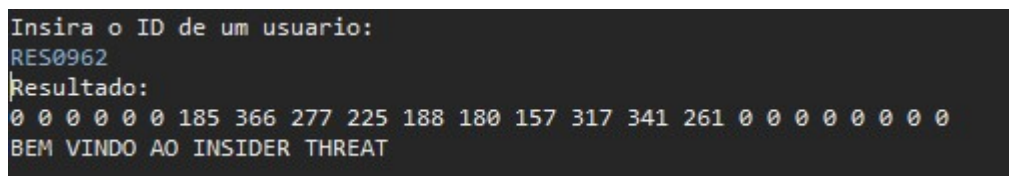


```
Console Problems Debug Shell
Main (9) [Java Application] C:\Program Files\Java\jre1.8.0_181\bin\javaw.exe (29 de nov de 2018 19:3
BEM VINDO AO INSIDER THREAT

MENU
1 - Buscar Usuário
2 - Buscar ameaça por cargo
3 - Ver histograma de um usuário
Insira o valor de uma operação: 2
----- BUSCA POR AMEAÇA POR CARGO -----
Insira um cargo na empresa:
Administrative Assistant
Processando os dados
Resultado:
PEGUEI!! O USUARIO COM ID WFL0495 E COM NOME William F Luna
PEGUEI!! O USUARIO COM ID CAH0610 E COM NOME Cyrus A Holmes
PEGUEI!! O USUARIO COM ID PBH0441 E COM NOME Price B Hickman
PEGUEI!! O USUARIO COM ID MND0048 E COM NOME Magee N Dale
PEGUEI!! O USUARIO COM ID BNN0072 E COM NOME Baxter N Nieves
PEGUEI!! O USUARIO COM ID BCB0013 E COM NOME Brock C Barber
PEGUEI!! O USUARIO COM ID BCR0547 E COM NOME Beck C Robinson
PEGUEI!! O USUARIO COM ID AKH0067 E COM NOME Amal K Holder
PEGUEI!! O USUARIO COM ID AGW0182 E COM NOME Aidan G Wallace
PEGUEI!! O USUARIO COM ID AJP0553 E COM NOME Arthur J Phillips
PEGUEI!! O USUARIO COM ID AJB0016 E COM NOME Arden J Burris
PEGUEI!! O USUARIO COM ID ACH0803 E COM NOME Arsenio C Hoover
PEGUEI!! O USUARIO COM ID ABH0963 E COM NOME Allistair B Harper
PEGUEI!! O USUARIO COM ID ACM0061 E COM NOME Amal C Meyers
PEGUEI!! O USUARIO COM ID ACR0400 E COM NOME April C Rios
```

Figura 4: Exemplo de busca por suspeitos

3. Ver histograma de um usuário: Para executar esta ação basta inserir 3 no console. Em seguida será pedido para informar um ID de usuário, que caso seja inválido, irá retornar uma mensagem e caso seja válido, retornará uma lista de valores inteiros correspondentes ao histograma daquele usuário.



```
Insira o ID de um usuario:
RES0962
Resultado:
0 0 0 0 0 0 185 366 277 225 188 180 157 317 341 261 0 0 0 0 0 0 0
BEM VINDO AO INSIDER THREAT
```

Figura 5: Exemplo de visualização de histograma

Para encerrar a aplicação, digite o valor 0 no console, onde aparecerá a mensagem: “Até Mais!!”