# Mainframe Surrogat Chains

By Jake Labelle
<jake.labelle@hotmail.co.uk>
08/08/2020

# Who Am I

- Jake Labelle
- ~~Associate~~ Security Consultant at F-Secure
- Been on a couple Mainframe Jobs (not a expert)
- Streaming from Basingstoke, UK
- Was going to put a picture but just look to the right

# z/OS High Level

- Mainframe operating System
- Datasets
- REXX
- JCL
- RACF
- OMVS

# DATASETS

- 'USER01.REXXLIB(HELLO)'
- FLAT FILESYSTEM
- APOSTROPHES
- PDS (MEMBERS)

# REXX

- SCRIPTING LANGUAGE
- ADDRESS
- OUTTRAP

```
/*rexx*/

DATASET_TEST = “'USER2.TEST'”

address TSO “LISTDSD “DATASET_TEST
```

# JCL

- JOB CONTROL LANGUAGE
- BATCH JOB
- JOB CARD - USER=X

```
//USER1K JOB 'EXAMPLE',NOTIFY=&SYSUID,USER="id",MSGCLASS=H

//TSOCMD   EXEC PGM=IKJEFT01"
//SYSTSPRT DD SYSOUT=*"
//SYSTSIN  DD *"
EXEC 'GATOR.GATOR' '"oldid"'"
//*
```

# JCL IN A REXX

```
/*REXX*/
PARSE ARG id ',' oldid
QUEUE "//"id"K JOB 'RECURSE',NOTIFY=&SYSUID,USER="id",MSGCLASS=H,"
QUEUE "// MSGLEVEL=(1,1)"
QUEUE "//TSOCMD   EXEC PGM=IKJEFT01"
QUEUE "//SYSTSPRT DD SYSOUT=*"
QUEUE "//SYSTSIN  DD *"
QUEUE "EXEC 'GATOR.GATOR' '"oldid"'"
QUEUE "//*"
QUEUE "$$"
o = OUTTRAP("output.",,"CONCAT")
"SUBMIT * END($$)"
o = OUTTRAP(OFF)
```

# OMVS

- UNIX SUBSYSTEM
- LIKE WSL
- RACF MANAGES SECURITY

# RACF

- Resource Access Control Facility
- DIFFERENT TYPES OF RESOURCES E.G DATASETS, SURROGATS
- RESOURCE OWNERS
- UACC
- PERMIT
- SPECIAL = ROOT

# SURROGAT

- RACF RESOURCE
- *.SUBMIT
- BPX.SRV.*
- DFHSTART.*
- READ ACCESS

# SURROGAT CHAINS

- LOTS OF USERS – WHO KNOWS WHAT THEY WERE FOR
- RUNNING FOR DECADES
- USER1 → USER2 → USER3
- RLIST SURROGAT *
- USER1 CANT SEE USER2 → USER3
- *.SUBMIT IS A BATCH JOB
- COULD MANUALLY SUBMIT REVERSE SHELLS BUT SEE POINT 1
- COULD USE A USER WITH READ ACCESS TO ALL RESOURCES (SPECIAL)

# GATOR

- BEGIN.REXX
- GATOR.REXX
- SUBM.REXX
- UNIXM.REXX
- PLUGINS.REXX

# BEGIN.REXX

- GETS OUTPUT DATASETS READY
- GETS UNIX FILES READY
- ADDS CURRENT USER TO PATH
- STARTS GATOR.REXX

# GATOR.REXX

- GETS PATH
- IF SPECIAL STOP
- RUNS PLUGINS.REXX
- LISTS SURROGATS
- CHECKS THAT SURROGATS HAVENT BEEN VISITED YET
- IF *.SUBMIT -> SUBM.REXX
- IF BPX.SRV.* -> UNIXM.REXX

# SUBM.REXX

- SUBMITS A JCL AS THE SURROGAT USER WHICH RUNS GATOR.REXX

# UNIXM.REXX

- JCL WHICH RUNS GATOR
- FILE IN OMVS
- GATOR CALL IT WITH
- bpxbatch sh su -s " [TARGET_USER] " -c '/tmp/unixm

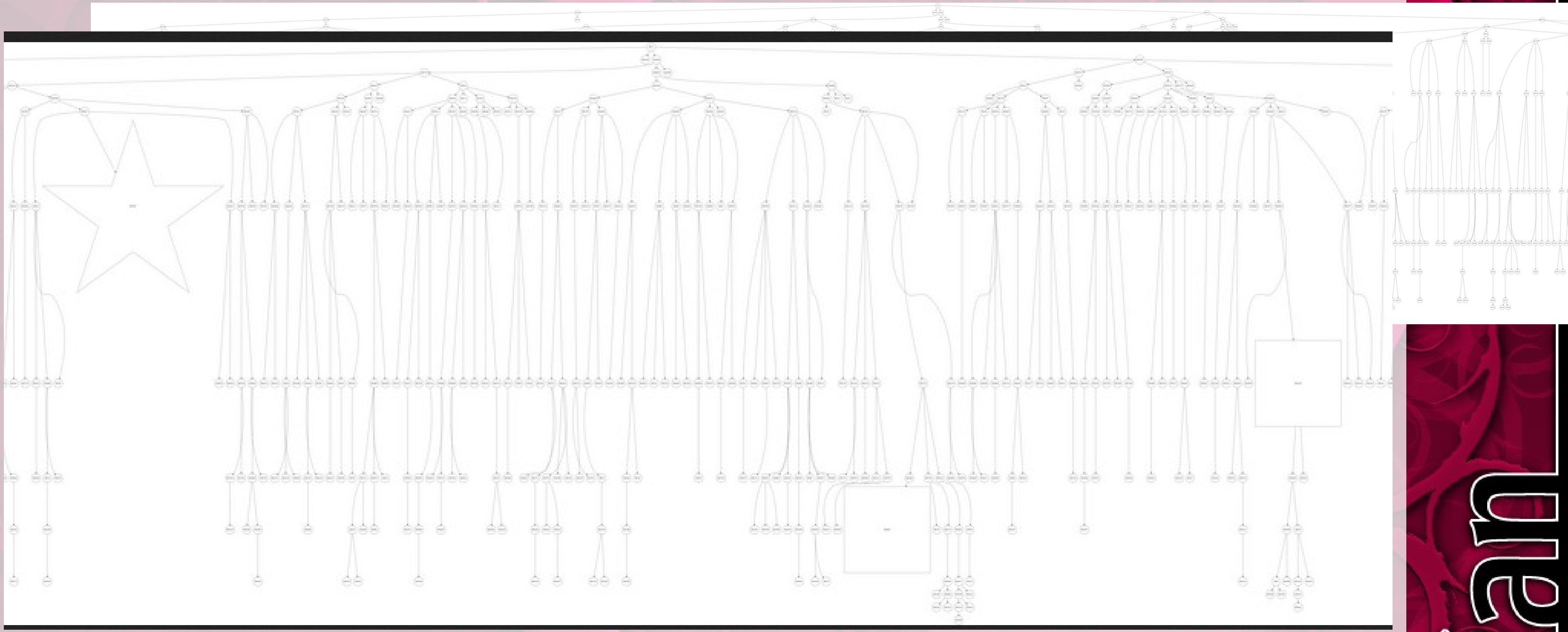
# PLUGINS.REXX

- LIST OF REXX SCRIPTS TO RUN ON EACH USER
- RUN ENUMERATION SCRIPTS
- EASY TO ADD MORE

# TESTING

- WITH ZPDT(EMUALTED ZOS) CREATED 1000 USERS
- RANDOMLY ASSIGNED A COUPLE OPERATORS AND SPECIAL
- ADD A COUPLE OF SURROGATS OF EACH TYPE TO EACH USER
- RAN GATOR

# GRAPHVIS



# SHELL MACRO

- FROM THE USER THAT RAN GATOR
- RECURSIVELY SUBMIT JCL PASSING THE TARGET AND HOW FAR IT IS IN THE PATH TO THE TARGET
- AT THE END SUBMIT A CATSO SHELL (LIKE A METERPRETER)

# SETUP.SH

- S3270 SCRIPT
- UPLOADS ALL THE REXX SCRIPTS

# TK4-

- BASED ON 1980'S MAINFRAME OS (MVS 3.8J)
- RUNS ON A RASPBERRY PI
- ALL OPENSOURCE/PUBLIC DOMAIN
- http://wotho.ethz.ch/tk4-/
- Run mvs to start it
- X3270 [MVS IP] 3270 - (ONCE ITS READY)
- TOP RIGHT KEYBOARD - CLEAR
- USERNAME HERC01 PASSWORD CUL8TR

# KICKS AND BREXX

- KICKS A CICS CLONE CAN BE INSTALLED
- https://www.youtube.com/watch?v=u_ZSH9OagTM
- BREXX CAN BE INSTALLED ALLOWING YOU TO RUN REXX SCRIPTS

# HERCULES

- Q Public Licence
- MAINFRAME EMULATOR
- TK4- RUNS ON THIS
- THERE IS A OLD ZOS VERSION ONLINE
- BUT PIRACY IS BAD MKAY