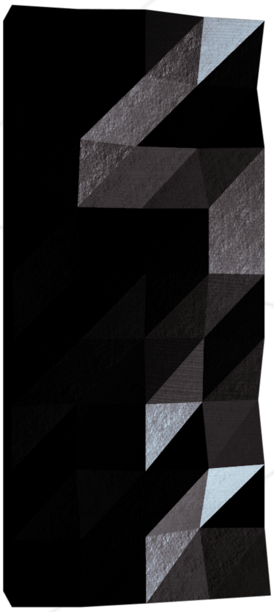

Project UNIX

War

42 Staff pedago@staff.42.fr

Résumé: Ce projet consiste à coder votre troisieme virus dit "polymorphe".

Table des matières

Chapitre I

Préambule

Voila ce que dit Wikipedia sur `War` :

`War` (originally called Eric Burdon and War) is an American funk band from Long Beach, California, known for the hit songs "Spill the Wine", "The World Is a Ghetto", "The Cisco Kid", "Why Can't We Be Friends ?", "Low Rider", and "Summer". Formed in 1969, War was a musical crossover band which fused elements of rock, funk, jazz, Latin, rhythm and blues, and reggae. Their album The World Is a Ghetto was the best-selling album of 1973. The band also transcended racial and cultural barriers with a multi-ethnic line-up. War was also subject to many line-up changes over the course of its formation, leaving member Leroy "Lonnie" Jordan as the only original member in the current line-up ; four other members created a new group called the Lowrider Band.

1960s : Beginnings
In 1962, Howard E. Scott and Harold Brown formed a group called The Creators in Long Beach, California. Within a few years, they had added Charles Miller, Morris "B. B." Dickerson and Lonnie Jordan to the lineup. Lee Oskar and Papa Dee Allen later joined as well. They all shared a love of diverse styles of music, which they had absorbed living in the racially mixed Los Angeles ghettos. The Creators recorded several singles on Dore Records while working with Tjay Contrelli, a saxophonist from the band Love. In 1968, the Creators became Nightshift (named because Brown worked nights at a steel yard) and started performing with Deacon Jones, a football player and singer.

The original War was conceived by record producer Jerry Goldstein ("My Boyfriend's Back", "Hang on Sloopy", "I Want Candy") and singer Eric Burdon (ex-lead singer of the British band the Animals). In 1969, Goldstein saw musicians who would eventually become War playing at the Rag Doll in North Hollywood, backing Deacon Jones, and he was attracted to the band's sound. Jordan claimed that the band's goal was to spread a message of brotherhood and harmony, using instruments and voices to speak out against racism, hunger, gangs, crimes, and turf Lowriders, and promote hope and the spirit of brotherhood. Eric Burdon and War began playing live shows to audiences throughout Southern California before entering into the studio to record their debut album Eric Burdon Declares "War". The album's best known track, "Spill the Wine", was a hit and launched the band's career.

1970s : Height of popularity

Eric Burdon and War toured extensively across Europe and the United States. A reviewer from New Musical Express called War "the best live band I ever saw" after their first UK gig in London's Hyde Park. Their show at Ronnie Scott's Club in London on September 18, 1970 is historically notable for being the very last public performance for Jimi Hendrix, who joined them onstage for the last 35 minutes of Burdon's and War's 2nd set ; a day later he was dead. A second Eric Burdon and War album, a two-disc set titled The Black-Man's Burdon was released in 1970, before Burdon left the band in the middle of its European tour. They finished the tour without him and returned to record their first album as War.

War (1971) met with only modest success, but later that year, the band released All Day Music which included the singles "All Day Music" and "Slippin' into Darkness". The latter single sold over one million copies, and was awarded a gold disc by the R.I.A.A. in June 1972. In 1972 they released The World Is a Ghetto which was even more successful. Its second single, "The Cisco Kid" shipped gold, and the album attained the number two spot on Billboard Hot 100 chart, and was Billboard magazine's Album of the Year as the best-selling album of 1973.

The next album, Deliver the Word (1973) contained the hits "Gypsy Man" and a studio version of "Me and Baby Brother" (previously issued as a live recording), which peaked at #8 and #15 on the Billboard chart. The album went on to sell nearly two million copies. The next album, Why Can't We Be Friends ? was released in 1975. It included "Low Rider" and the title track, which were among the band's biggest hits.

In 1976, War released a greatest hits record which contained one new song "Summer", which, as a single, went gold and peaked at number 7 on the Billboard chart. Also released that year were Love is All Around by Eric Burdon and War, containing mostly unreleased recordings from 1969 and 1970, and Platinum Jazz, a one-off album for jazz label Blue Note. The latter double album had cover art to match the greatest hits album, and was half new material and half compilation, focusing on (but not restricted to) instrumental music. The group continued to attain success with their next album, Galaxy (1977) whose title single was inspired by Star Wars. War's next project was a soundtrack album for the movie Youngblood in 1978.

1980s : The Music Band

In 1979, following the departure of B.B. Dickerson during recording sessions for their next album (replaced by Luther Rabb on bass who completed the album), the band considered changing their name to The Music Band, but decided at the last minute to continue as War, and use The Music Band as the title of a series of albums. The series originally consisted of two studio albums (The Music Band, The Music Band 2, both in 1979) and a live album (The Music Band Live, 1980), but after the band left MCA in 1981 and had already made records for other labels, MCA expanded the series with a compilation (The Best of the Music Band, 1982) and a third original album of left-over material (The Music Band – Jazz, 1983).

The group lost another member when Charles Miller (saxophone) was murdered in 1980. He had already been replaced by Pat Rizzo (ex Sly and the Family Stone) in 1979. Other new members joining at this time were Alice Tweed Smith (credited as "Tweed Smith" and "Alice Tweed Smyth" on various albums) on percussion and vocals (giving the band its first female vocalist), and Ronnie Hammon as a third drummer.

After making the one-off single "Cinco de Mayo" for LA Records in 1981 (Jerry Goldstein's own label, which also reissued Eric Burdon Declares "War" under the title Spill the Wine the same year), War signed with RCA Victor Records and recorded Outlaw (1982) which included the single plus additional singles "You Got the Power", "Outlaw", and "Just Because". It was followed by Life (is So Strange) (1983) from which the title track was also a single. War's records from 1979 to 1983 were not as successful as those from the preceding decade, and after the two RCA albums, the band's activities became sporadic. They did not record another full album until a decade later. The 1987 compilation album The Best of War ...and More included two new tracks, "Livin' in the Red" and "Whose Cadillac Is That ?", and a remixed version of "Low Rider" (in addition to the original version). Papa Dee Allen died of a heart attack (myocardial infarction) which struck him onstage in 1988.

1990s : Reformations

Sampling of War by hip hop artists was prevalent enough to merit the compilation album Rap Declares War in 1992, which was sanctioned by the band.

In 1993, War reformed with most surviving previous members (including original members Brown, Jordan, Oskar, and Scott, and later members Hammon and Rizzo), augmented by a large line-up of supporting musicians and still under the management and production of Jerry Goldstein, and released a new album, Peace (1994).

In 1996, the group attempted to gain independence from Goldstein, but were unable to do so under the name "War" which remains a trademark owned by Goldstein and Far Out Productions. In response, Brown, Oskar, Scott, and a returning B.B. Dickerson (who had not worked with War since 1979) adopted a name which referenced one of War's biggest hits : Lowrider Band. They are yet to record a studio album.

Lonnie Jordan opted to remain with Goldstein and create a new version of War with himself as the only original member. Some other musicians who had joined between 1983 and 1993 were also part of the new line-up. Both the "new" War and the Lowrider Band are currently active as live performance acts.

1996 also saw the release of a double CD compilation, Anthology (1970–1994), later updated in 2003 with a few track substitutions, as The Very Best of War. Another CD compilation from 1999, Grooves and Messages, included a second disc of remixes done by various producers.

In the 21st century

On 21 April 2008, Eric Burdon and War reunited for the first time in 37 years to perform a one-time-only concert at the London Royal Albert Hall. The reunion was actually only between Eric Burdon and Lonnie Jordan, as the other original surviving members had not been asked to be a part of the reunion. The concert coincided with Avenue / Rhino Records' Eric Burdon and War reissues which included Eric Burdon Declares "War" and The Black-Man's Burdon, plus compilations The Best of Eric Burdon and War and Anthology. In 2008, Lonnie Jordan's edition of War released a live album / DVD of songs originally from 1969 to 1975 : Greatest Hits Live. War were unsuccessfully nominated for 2009 induction into the Rock and Roll Hall of Fame. There were rumours that Burdon would join them again in summer 2009, but it did not happen. In 2011, War played "Low Rider" and many other hits at the Rack n' Roll in Stamford, Connecticut with Remember September and Westchester School of Rock.

In 2014 the "new" War released a new studio album Evolutionary. Also in 2014, War was a nominee for induction into the Rock and Roll Hall of Fame.

Chapitre II

Introduction

Un virus polymorphe est un virus informatique qui, lors de sa réplication, modifie sa représentation, ce qui empêche un logiciel antivirus de l'identifier par sa signature. Bien qu'en apparence le virus change (du point de vue d'un programme antivirus qui lit le programme infecté), le fonctionnement du virus (sa méthode d'infection et sa charge utile) reste le même : les algorithmes ne sont pas modifiés, mais leur traduction en code-machine l'est.

Chapitre III

Objectifs

Avec le sujet Pestilence vous avez maintenant une bonne vision sur la programmation de type auto-répliquante sous condition avec obfuscation mineure. Mais vous allez vite vous rendre compte que malgré tous ces efforts, il reste encore du chemin à parcourir pour rendre votre programme discret.

Car, le vrai problème dans le monde de la virologie est bien entendu les antivirus et par la difficulté ainsi que l'avancée rapide de ce monde, vous devrez pouvoir vous adapter vite ! Bien entendu, dans le cadre d'un sujet, on va simplifier largement le concept.

On va améliorer ensemble nos connaissances sur la programmation polymorphique. Encore une fois, on va largement simplifier le concept. Cette méthode peut être utile dans un tas de domaines en général pour solutioner des problèmatiques très spécifiques.

On va donc créer un meilleur programme en reprenant la base du projet Pestilence. Mais vous allez assez vite comprendre que des changements drastiques vont être obligatoire pour valider ce projet encore une fois :)

Chapitre IV

Partie obligatoire

War est un binaire de votre conception qui devra :

- comme Famine, infecter des binaires présents dans 2 dossiers spécifiques et y appliquer une signature, sans altérer le fonctionnement du-dit binaire.
- comme Pestilence, ne pas déclencher la routine d'infection si un processus ciblé est en cours d'exécution, si le programme est lancé via un debugueur quelconque, et présenter une partie de la routine d'infection de manière obfusquée.

Ce coup-ci, on va rendre encore plus discret notre virus en apprenant à modifier un binaire au runtime pour modifier sa signature. Ici, on va donc modifier la signature à implémenter va et devra embarquer un FINGERPRINT supplémentaire pour avoir a peu près cette forme :

```
War version 1.0 (c)oded by <first-login> - <second-login> - [FINGERPRINT]
```

Ce FINGERPRINT est important ici, car ce sera cette partie qui sera modifié à l'exécution de vos binaires infectés. Ce FINGERPRINT ne sera JAMAIS le même quelque soit la source de l'infection (virus lui meme ou binaire infecté). Bien sur, l'infection ne modifie en rien le fonctionnement du ou des binaire(s) infectés dans les dossiers concernés.

Vos contraintes pour ce projet seront les suivantes :

- L'exécutable devra se nommer War.
- Cet exécutable est codé en assembleur, en C ou en C++ et rien d'autre. On tolère le JAVA pour ce projet, mais c'est tout.
- Votre programme ne va rien afficher sur la sortie standard ni d'erreur.
- Vous devrez **OBLIGATOIREMENT** travailler dans une VM.
- Le système d'exploitation cible est comme toujours libre de choix. Toutefois, vous devrez aménager lors de votre correction une VM appropriée.
- Votre programme va devoir agir sur les dossiers /tmp/test et /tmp/test2 ou équivalent en fonction de votre système d'exploitation cible, et UNIQUEMENT dans

ces dossiers. Le contrôle de la propagation de votre programme est de votre responsabilité.

- **ATTENTION !** Une seule infection sur ledit binaire est possible, pas plus.
- Les infections se feront dans un premier temps sur des binaires du type de votre système d'exploitation ayant pour architecture 64 bits.

Chapitre V

Exemple d'utilisation

Voici un exemple d'utilisation possible :

On prepare le terrain :

```
# ls -al ~/War
total 736
drwxr-xr-x 3 root root   4096 May 24 08:03 .
drwxr-xr-x 5 root root   4096 May 24 07:32 ..
-rwxr-xr-x 1 root root 744284 May 24 08:03 War
```

On crée sample.c pour nos tests :

```
# nl sample.c
1 #include <stdio.h>
2 int
3 main(void) {
4      printf("Hello, World!\n");
5      return 0;
6 }
# gcc -m64 ~/Virus/sample/sample.c
#
```

On copie nos binaires (tests + ls) pour nos tests :

```
# cp ~/Virus/sample/sample /tmp/test2/.
# ls -al /tmp/test
total 16
drwxr-xr-x  2 root root 4096 May 24 08:07 .
drwxrwxrwt 13 root root 4096 May 24 08:08 ..
-rwxr-xr-x  1 root root 6712 May 24 08:11 sample
# /tmp/test/sample
Hello, World!
# file /tmp/test/sample
/tmp/test/sample: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /
    lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=938[...]10b, not stripped
# strings /tmp/test/sample | grep "wandre"
# cp /bin/ls /tmp/test2/
# ls -al /tmp/test2
total 132
drwxr-xr-x  2 root root   4096 May 24 08:11 .
drwxrwxrwt 14 root root   4096 May 24 08:11 ..
-rwxr-xr-x  1 root root 126480 May 24 08:12 ls
# file /tmp/test2/ls
/ tmp/test2/ls: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /
    lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=67e[...]281, stripped
#
```

On lance `War` sans le processus "test" et on voit le resultat :

```
# pgrep "test"
# ./War
# strings /tmp/test/sample | grep "wandre"
virus.custom version 1.2 (c)oded may-2017 by wandre - 42424242
# /tmp/test/sample
Welcome!
# strings /tmp/test2/ls | grep "wandre"
virus.custom version 1.2 (c)oded may-2017 by wandre - 43434343
# /tmp/test2/ls -la /tmp/test2/
total 132
drwxr-xr-x  2 root root   4096 May  3 12:03 .
drwxrwxrwt 14 root root   4096 May  3 12:01 ..
-rwxr-xr-x  1 root root xxxxxx May  3 12:19 ls
# gcc -m64 ~/Virus/sample/sample.c -o /tmp/test/sample
# ls -al /tmp/test
total 16
drwxr-xr-x  2 root root 4096 May  3 12:03 .
drwxrwxrwt 13 root root 4096 May  3 12:01 ..
-rwxr-xr-x  1 root root xxxx May  3 12:19 sample
# /tmp/test/sample
Welcome!
# file /tmp/test/sample
/tmp/test/sample: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /
     lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=
     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx, not stripped
# strings /tmp/test/sample | grep "wandre"
# /tmp/test2/ls -la /tmp/test2/
total 132
drwxr-xr-x  2 root root   4096 May  3 12:03 .
drwxrwxrwt 14 root root   4096 May  3 12:01 ..
-rwxr-xr-x  1 root root xxxxxx May  3 12:20 ls
# strings /tmp/test/sample | grep "wandre"
virus.custom version 1.2 (c)oded may-2017 by wandre - 444444
#
```

On voit clairement une évolution de la "signature". Il faut bien entendu faire en sorte que la modification soit visible clairement. La partie de la signature qui doit évoluer doit être controlée. Si celle-ci est aléatoire la note sera en conséquence... Je rappelle qu'une double infection ne doit pas être possible.

Pour cette partie je vous encourage grandement à développer votre logique en assembleur. Il existe des méthodes pour parvenir à ce résultat en C/C++ mais en toute franchise, cela risque de compliquer fortement la réalisation de ce projet.

On lance War avec le processus "test" ainsi que l'environement initial et on voit le resultat :

```
# pgrep "test"
41785
# ./War
# strings /tmp/test/sample | grep "wandre"
# /tmp/test/sample
Welcome!
# strings /tmp/test2/ls | grep "wandre"
# /tmp/test2/ls -la /tmp/test2/
total 132
drwxr-xr-x  2 root root   4096 May  3 12:03 .
drwxrwxrwt 14 root root   4096 May  3 12:01 ..
-rwxr-xr-x  1 root root xxxxxx May  3 12:20 ls
# gcc -m64 ~/Virus/sample/sample.c -o /tmp/test/sample
# ls -al /tmp/test
total 16
drwxr-xr-x  2 root root 4096 May  3 12:03 .
drwxrwxrwt 13 root root 4096 May  3 12:01 ..
-rwxr-xr-x  1 root root xxxx May  3 12:21 sample
# /tmp/test/sample
Welcome!
# file /tmp/test/sample
/tmp/test/sample: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /
     lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=
     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx, not stripped
# strings /tmp/test/sample | grep "wandre"
# /tmp/test2/ls -la /tmp/test2/
total 132
drwxr-xr-x  2 root root   4096 May  3 12:03 .
drwxrwxrwt 14 root root   4096 May  3 12:01 ..
-rwxr-xr-x  1 root root xxxxxx May  3 12:23 ls
# strings /tmp/test/sample | grep "wandre"
#
```

On va tenter de lancer War via gdb, avec un petit message pour que ce soit plus clair :

```
# gdb -q ./War
(gdb) run
Starting program: /root/War
DEBUGGING..
[Inferior 1 (process 2683) exited with code 01]
# strings /tmp/test/sample | grep "wandre"
# /tmp/test/sample
Welcome!
# strings /tmp/test2/ls | grep "wandre"
#
```

Chapitre VI

Partie bonus

Les bonus ne seront comptabilisés que si votre partie obligatoire est PARFAITE. Par PARFAITE, on entend bien évidemment qu'elle est entièrement réalisée, et qu'il n'est pas possible de mettre son comportement en défaut, même en cas d'erreur aussi vicieuse soit-elle, de mauvaise utilisation, etc ... Concrètement, cela signifie que si votre partie obligatoire n'est pas validée, vos bonus seront intégralement IGNORÉS.

Des idées de bonus :

- Pouvoir infecter les binaires d'architecture 32 bits.
- Pouvoir infecter tous les fichiers en partant de la racine de votre système d'exploitation de manière récursive.

Vous devez optimiser cette partie en executant les binaires inféctés..

- Permettre une infection sur des fichiers non binaires.
- Utilisation de méthodes de type packing sur le virus directement dont le but sera de rendre le binaire le plus léger possible.
- Vous pouvez vous amusez à rajouter une backdoor par votre virus mais attention à faire en sorte qu'aucun erreur ne soit visible... Surtout si votre backdoor permet d'ouvrir un port sur votre machine.

Chapitre VII

Rendu et peer-évaluation

- Ce projet ne sera corrigé que par des humains. Vous êtes donc libres d'organiser et nommer vos fichiers comme vous le désirez, en respectant néanmoins les contraintes listées ici.

- Votre routine rendant votre programme "polymorphe" doit être **IMPÉRATIVEMENT** controlée. C'est vraiment important.

- Vous devez gérer les erreurs de façon raisonnée. En aucun cas votre programme ne doit quitter de façon inattendue (Segmentation fault, etc).

- Rendez-votre travail sur votre dépot `GiT` comme d'habitude. Seul le travail présent sur votre dépot sera évalué en soutenance.

- Vous devez être sous une VM durant votre correction. Pour info, le barême a été fait avec une Debian 7.0 stable 64 bits.

- Vous être libre d'utiliser ce dont vous avez besoin, dans la limite des bibliothèques faisant le travail pour vous, ce qui correspondrait à un cas de triche.

- Vous pouvez poser vos questions sur le forum, sur jabber, IRC, slack...