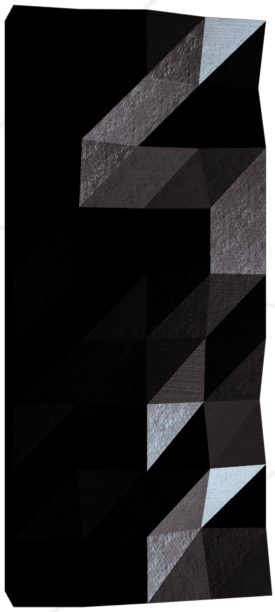

# Project UNIX

## War

42 Staff pedago@staff.42.fr

*Summary: In this project, you will code a "polymorphic" virus.*

*Version: 3*

# Contents

# Chapter I

# Preamble

Here is Wikipedia's drill about `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, Famine, 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 An-

thology. 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.

# Chapter II

# Introduction

A polymorphic virus is a computer virus that modifies its representation when replicating. This prevents antivirus software from identifying its signature. Though it apparently changes (from the point of view of an antivirus program reading the infected one), the way the virus works (its infection method and payload) remains unchanged: algorithms are not modified. Their translation in machine-code is.

# Chapter III

# Objectives

Thanks to the Pestilence subject, you have a clear view of self-replicating programming under condition with a minor obfuscation. You will quickly realize, though, that despite your many efforts, you still have a long way to go for your program to be perfectly quiet.

For, the real problems in the world of virology are the antivirus of course. And because the world grows hard and fast, you have to adapt hard and fast! Of course, though, we're going to simplify the concept in this subject.

Together, we will upgrade our knowledge of polymorphic programming. Once again, the concept will be simplified. This method can be useful in a broad array of fields to find a solution to very specific problematics.

We're gonna create a better program using the base or the Pestilence project. But you will quickly understand the radical changes we will have to operate to validate this program once again :)

# Chapter IV

# Mandatory part

`War` is a binary of your own design that will have to:

- like `Famine`, infect the binaries present in 2 specific folders and apply a signature in them without altering the binary's working.
- like `Pestilence`, not trigger the infection routine if a targeted process is running, if the program is launched with any kind of debugger and present a part of the infection routine in an obfuscated way.

This time, we will learn to to modify a binary to the runtime to modify its signature and make our virus even quieter. This is why the implemented modified signature will have - and is going - to carry an additional FINGERPRINT to look remotely like this:

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

This FINGERPRINT is important because this is the part that will be modified when your infected binaries start running. This FINGERPRINT will NEVER be the same, whichever the infection source (virus itself or infected binary). Of course, the infection doesn't modify the way the infected binary(ies) in the folder in question work(s).

For this project, you will have the following constraints:

- The executable will be named `War`.
- This executable is coded in assembler, C or C++. Nothing else. Java will be tolerated for this project.
- Your program will not display anything on the standard output. No error either.
- You will **HAVE TO** work in a VM.
- You're free to chose the targeted OS. You will have to set up an accurate VM during the evaluation.

- Your program will have to act on the /tmp/test and /tmp/test2 folders or the equivalent depending on your targeted OS type. And on these folders ONLY. You're responsible for your program's spreading.
- **WARNING!** There will only be one infection on the chosen binary.
- Infections will start on 64 bits binaries of your OS.

# Chapter V

# Use example

Here is a potential use example:

Let's lay the foundation:

```
# 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
```

We create a sample.c for our 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
#
```

We copy our binaries ( tests + ls ) for our 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
#
```

We run `War` without the "test" process and observe the result:

```
# 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
#
```

We clearly see the evolution of the "signature". Of course, you will have to make the modification as visible as possible. The part of the signature that has to evaluate has to be controlled. If it's random, you will be graded accordingly. Let me remind you a double infection is prohibited.

For this part, I highly advise you develop your own logic in assembler. Some methods will help you achieve this result in C/C++, but frankly, this will really impair your work on this project.

We run `War` with the "test" process, as well as the initial environment and observe the result:

```
# 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"
#
```

Let's try to run `War` with gdb, with a little message to make it clear:

```
# 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"
#
```

# Chapter VI

# Bonus part

Bonus will be taken into account only if the mandatory part is PERFECT. PERFECT meaning it is completed, that its behavior cannot be faulted, even because of the slightest mistake, improper use, etc... Practically, it means that if the mandatory part is not validated, none of the bonus will be taken in consideration.

Bonus ideas:

- Being able to infect 32 bits binaries.
- Being able to infect every file starting from your OS root in a recursive way.

You will optimize this part executing infected binaries...

- Allowing infection on non-binary files.
- Using packing-like methods directly on the virus to make the binary as light as possible.
- You can have fun using your virus to add a backdoor but make sure that no error is visible... Especially if your backdoor allows to open a port on your machine.

# Chapter VII

# Turn-in and peer-evaluation

- This project will only be reviewed by humans. You're free to organize and name your files as you will as long as you respect the following instructions.
- The routine making your program "polymorphic" will be controlled. This is very important.
- You must reasonably manage the errors. Your program will not quit unexpectedly (Segmentation fault, etc...).
- As usual, turn in your work on your repo `GiT`. Only the work included on your repo will be reviewed during the evaluation.
- During evaluation, you must be in a VM. For your information, the grading scale was built with a stable 64 bits Debian 7.0.
- You can use anything you will need except libraries that will do the dirty work for you. This would be considered cheating.
- You can post your questions on the forum, Jabber, IRC, Slack...