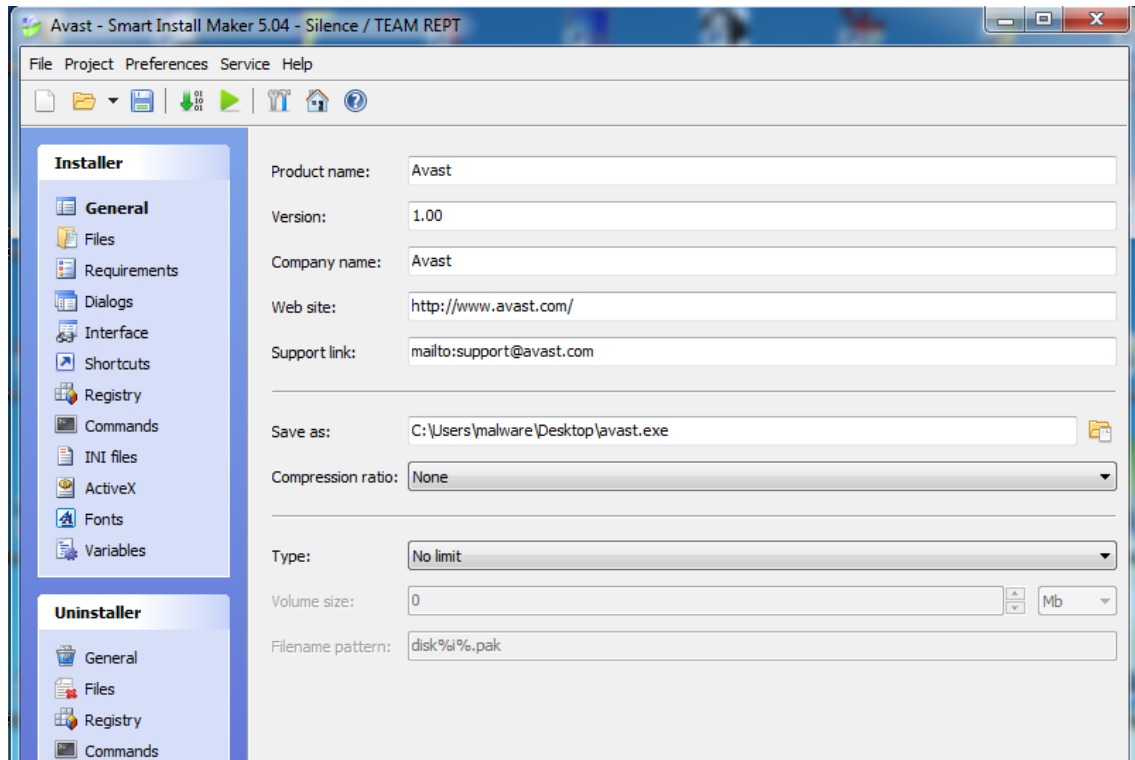
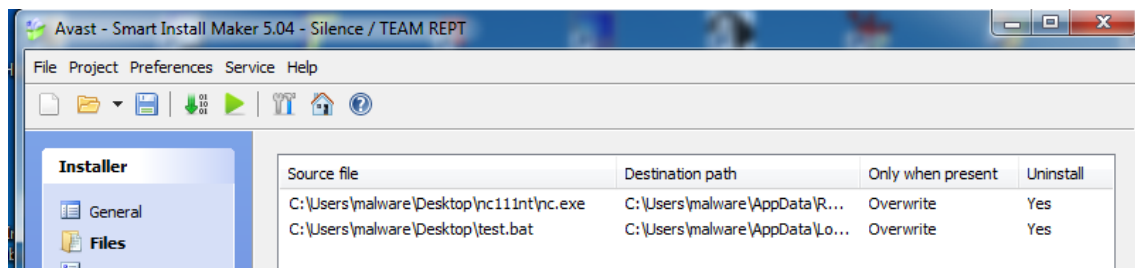


Para realizar el dropper realizamos los siguientes pasos:

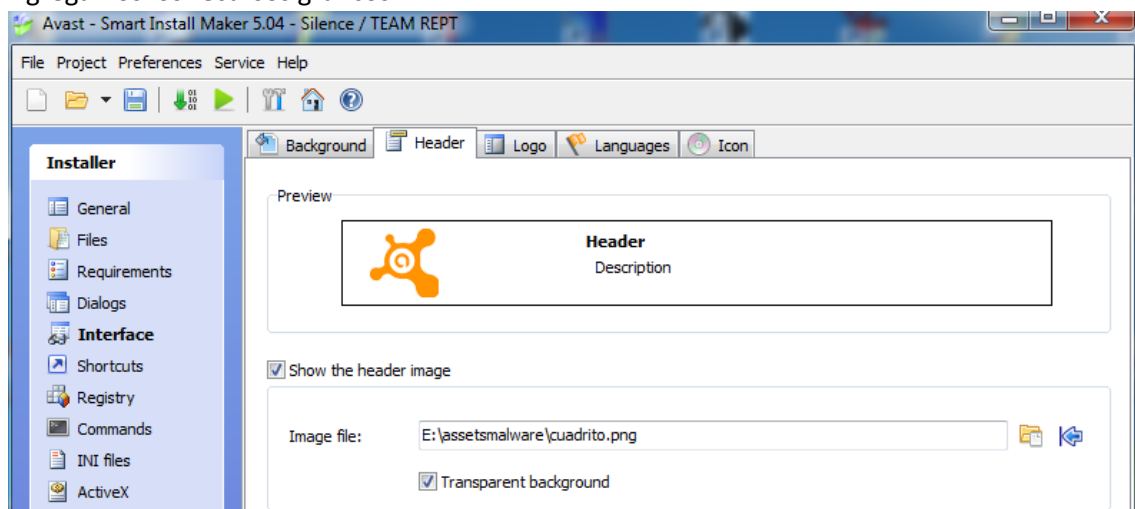
Iniciamos Smart Install Maker:

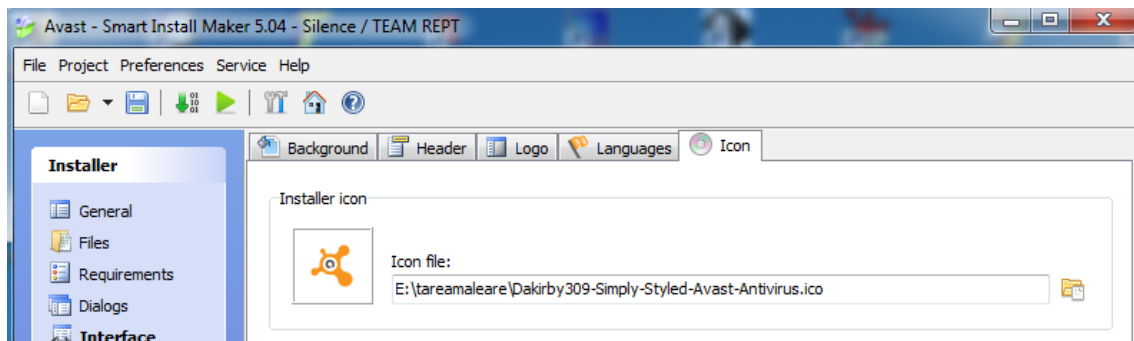
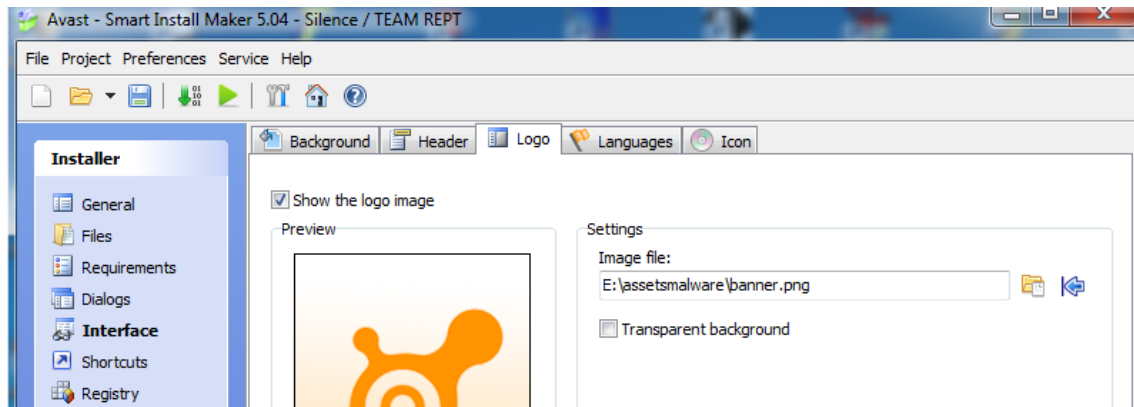


Agregamos los archivos:

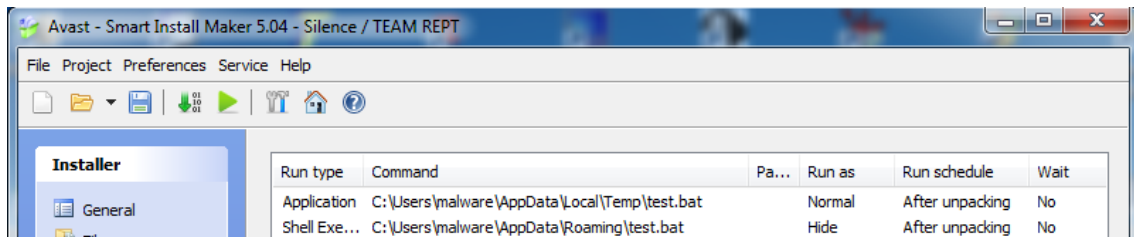


Agregamos los recursos graficos:

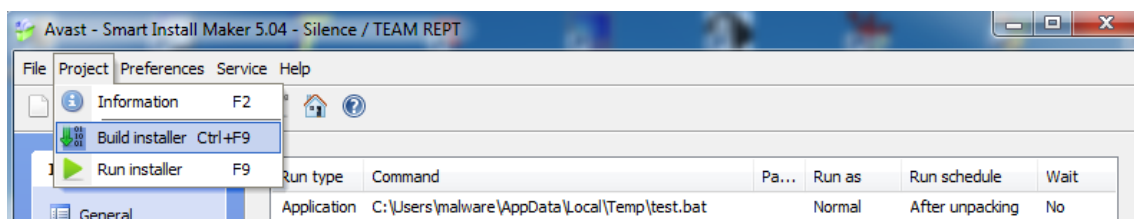




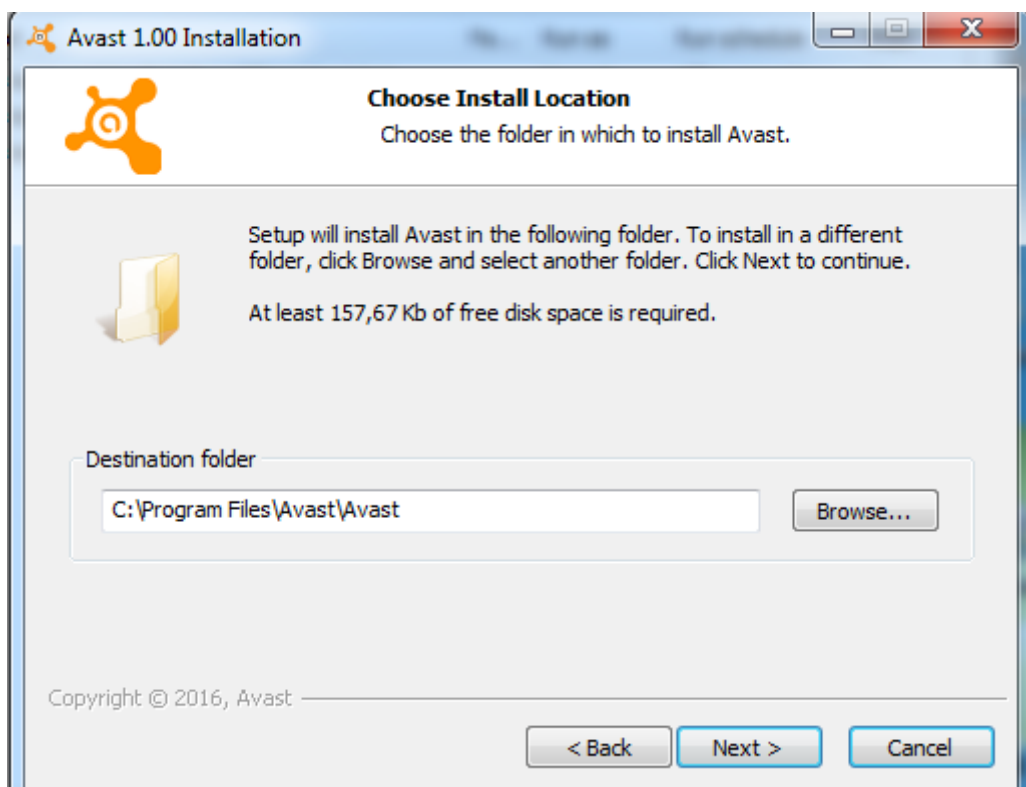
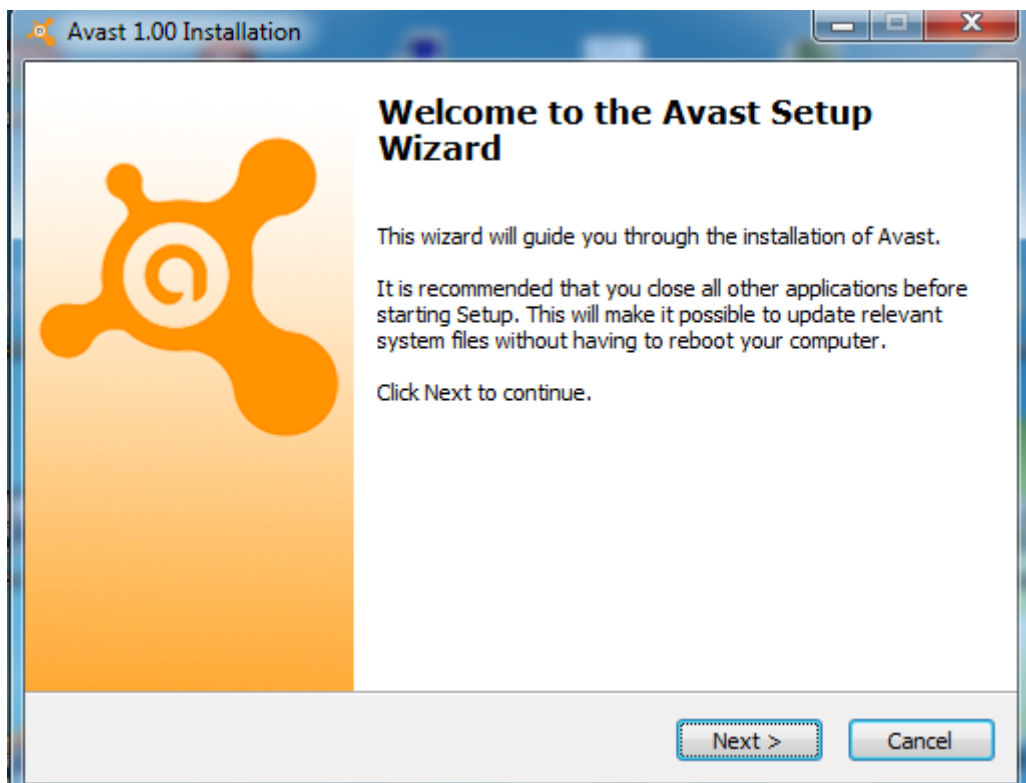
En la opcion de comandos seleccionamos el script (tuve que ponerlo de las 2 formas: como aplicaci3n y shell ya que de otra forma no se ejecutaba).

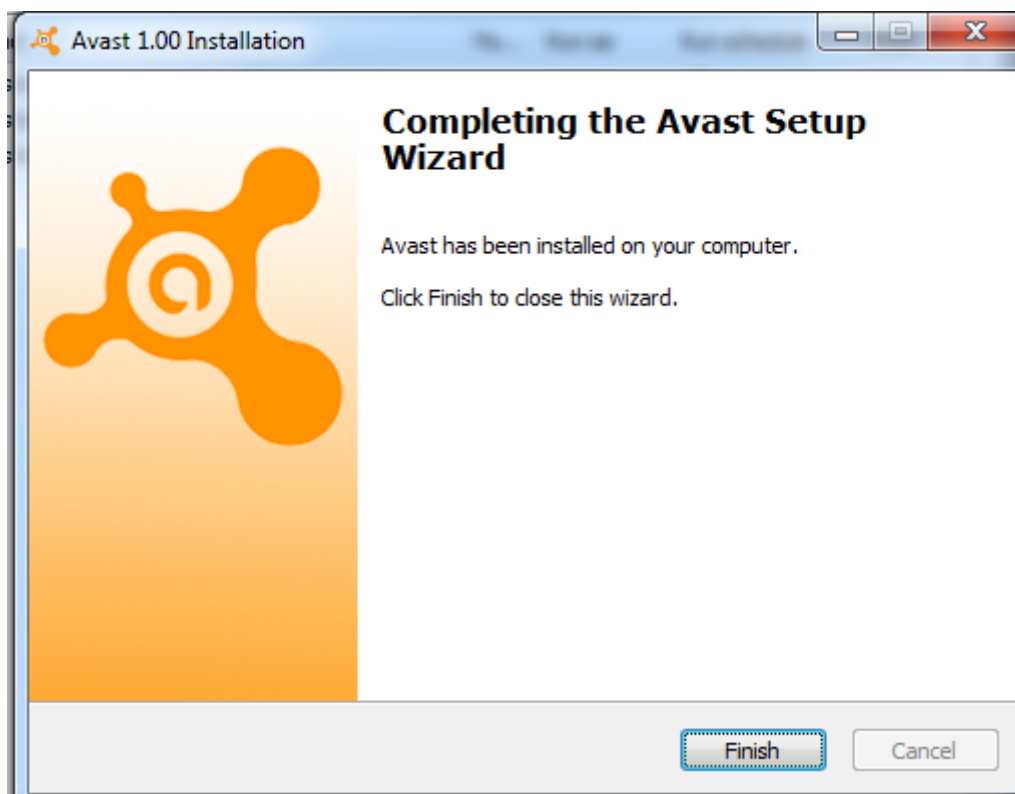
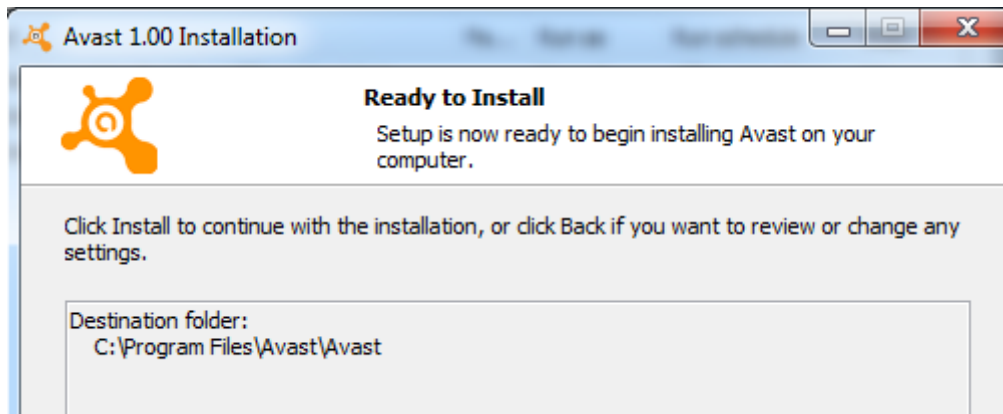


Despues generamos el instalador:

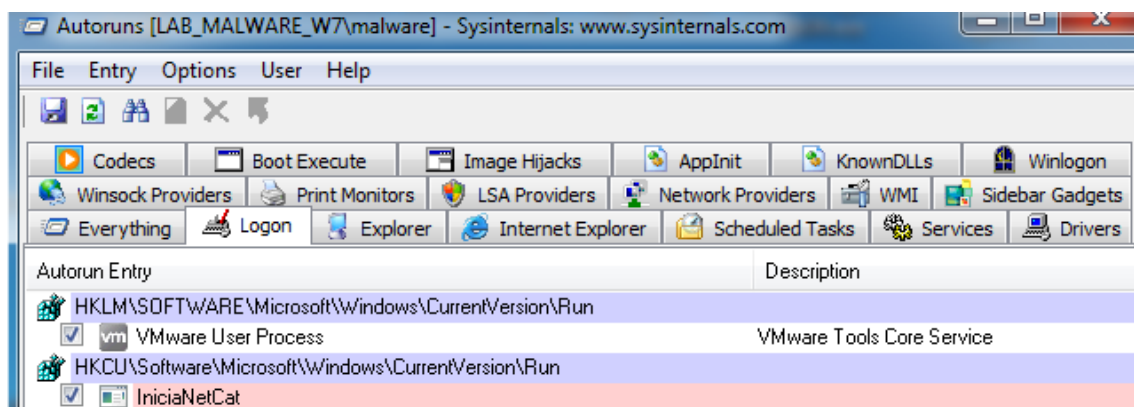


Probamos el ejecutable:

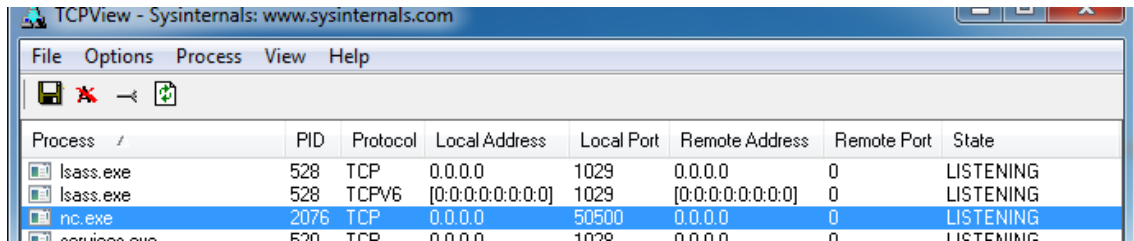




La instalacion termina y la llave en el registro es agregada; para verificar esto utilizamos la herramienta Autoruns:



Reiniciamos la maquina y abrimos TCPView: podemos ver que nc.exe se ejecuta en el arranque:



The screenshot shows the TCPView application window from Sysinternals. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu is a toolbar with icons for file operations. The main area is a table with the following columns: Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State. The table contains three entries, all with 'LISTENING' state:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	528	TCP	0.0.0.0	1029	0.0.0.0	0	LISTENING
lsass.exe	528	TCPV6	[0:0:0:0:0:0:0:0]	1029	[0:0:0:0:0:0:0:0]	0	LISTENING
nc.exe	2076	TCP	0.0.0.0	50500	0.0.0.0	0	LISTENING

Para probar el backdoor intentamos hacer telnet con otra maquina en el mismo segmento:



```
root@kali:~# telnet 192.168.1.10 50500
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Windows\system32>
```

Comprobamos que la conexión se realiza de manera exitosa.

Conclusiones

Podemos ver que realizar un backdoor es muy sencillo (aunque nc.exe no es una herramienta maliciosa) y que el fallo es la confianza del usuario.

Como solución a esto existen algunos métodos:

- Firmar ejecutables

- Hacer hashing de los ejecutables.

De esta manera podemos agregar cierto nivel de confianza al manejar aplicaciones.

Bibliografía

<http://stackoverflow.com/questions/1424248/hash-of-an-exe-file>

<http://www.excelsiorjet.com/kb/34/howto-digitally-sign-executables-and-installers-produced-by-excelsior-jet>