

1. My malware lab is in my office, running on Ubuntu
2. If I'm using hexedit/string, I can see several statements such as :

KERNEL32.DLL.WS2\_32.dll...LoadLibraryA..GetProcAddress..VirtualProtect..VirtualAlloc..VirtualFree...Exit  
Process.

3. Registry involve:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "" =  
Winsec32.exe  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices "" =  
Winsec32.exe  
HKEY_CURRENT_USER\Software\Microsoft\OLE "" = Winsec32.exe
```

It installs itself in the registry.

4. Network connection

```
testirc1.sh1xy2bg.NET
```

```
Outgoing connection to remote server: 255.255.255.255 TCP port 6667
```

This is a botnet, to take over host from remote.

5. This is Trojan

Name: Muhammad Najmi Ahmad Zabidi  
Malaysia