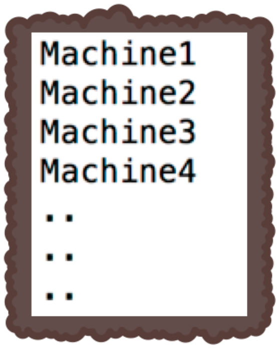
- Shamoon attack requires admin credentials.
- It does not have any code path to a zero day vulnerability. Where it can exploit an OS vulnerability and do privilege escalation.
- Its malware only, so it means it needs all the info like credentials to begin with
- One can’t just click on the dropper and execute it.
- Shamoon does need to be directed somehow.

So what is the entry point?

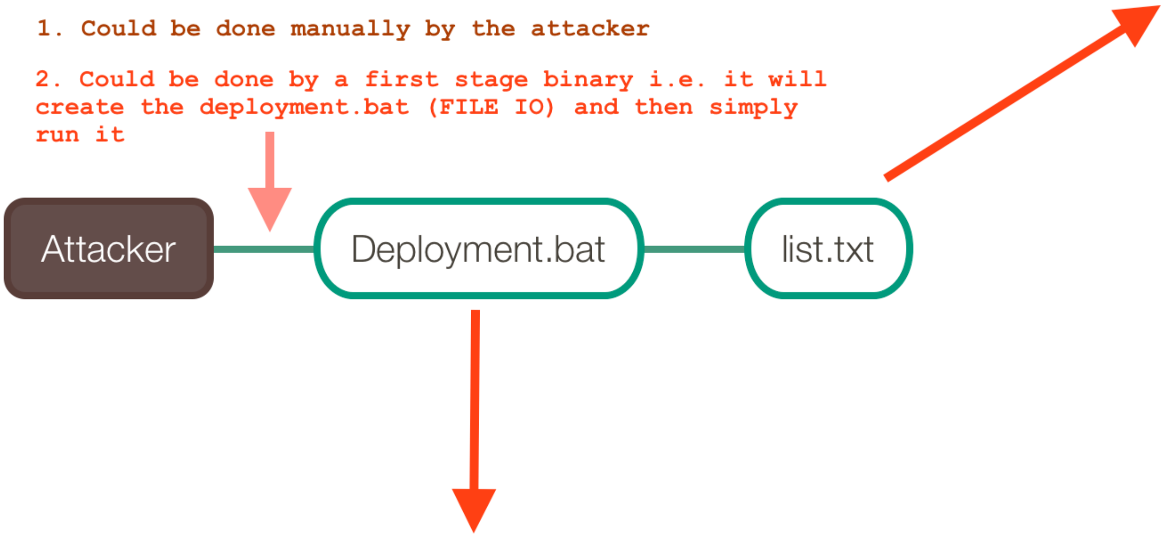
Maybe the attacker logged in to the network and launch the attack. Thats what most of the victims think! Since machines were completely destroyed it wasn’t easy to gather all the files. Over the past few weeks I have noticed a trend where lateral movement was done via following pattern.

- ***psExec***
- ***paExec***
- ***deployment.bat***
- ***list.txt***

All this could be present in a zip archive.

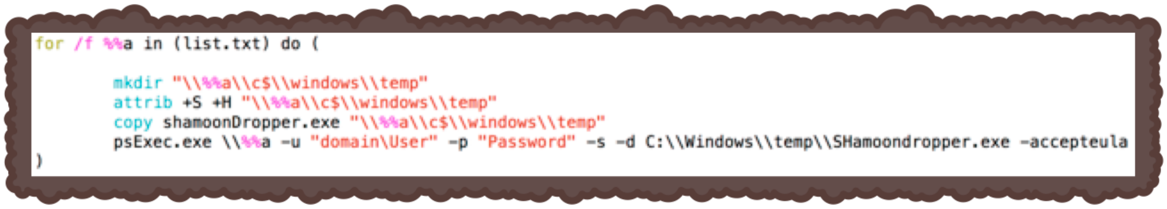


```
Machine1
Machine2
Machine3
Machine4
..
..
..
```



1. Could be done manually by the attacker

2. Could be done by a first stage binary i.e. it will create the deployment.bat (FILE IO) and then simply run it



```
for /f %%a in (list.txt) do (

        mkdir "\\%%a\\c$\\windows\\temp"
        attrib +S +H "\\%%a\\c$\\windows\\temp"
        copy shamoonDropper.exe "\\%%a\\c$\\windows\\temp"
        psExec.exe \\%%a -u "domain\User" -p "Password" -s -d C:\\Windows\\temp\\SHamoondropper.exe -accepteula
)
```

In Shamoon’s case, binaries were copied to system32 folder