APT Simulator

Information Security Inc.

iSEC
information security inc.

Contents

- About APT Simulator
- Testing Environment
- Use Cases
- Focus
- Integrated Projects / Software
- Installing APT Simulator
- Running APT Simulator
- References

About APT Simulator

- APT Simulator is a Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised
- Blueteam => what can you detect and how fast can you handle it

Testing Environment

- Windows 10 x64

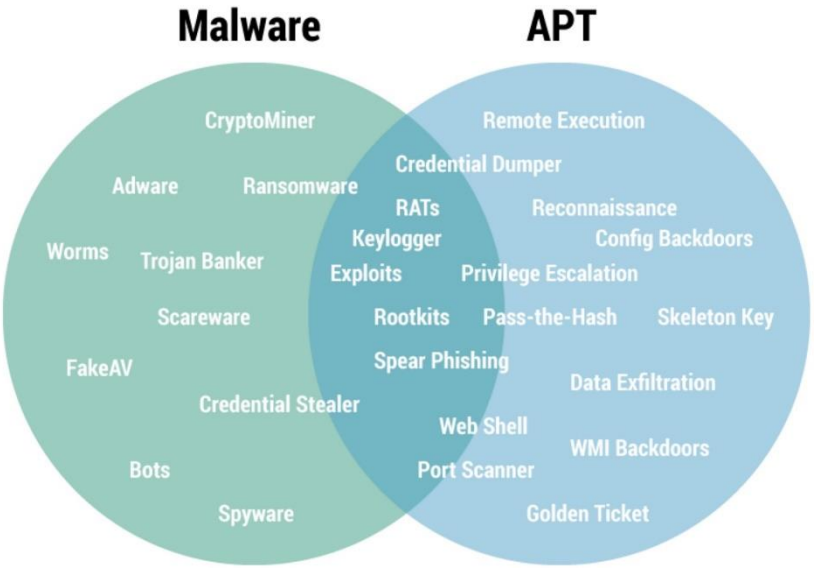
Edition	Windows 10 Pro
Version	1703
OS Build	15063.786
Processor	Intel(R) Core(TM) i7-4910MQ CPU @ 2.90GHz 2.90 GHz
Installed RAM	3.04 GB
System type	64-bit operating system, x64-based processor

Use Cases

- POCs: Endpoint detection agents / compromise assessment tools
- Test your security monitoring's detection capabilities
- Test your SOCs response on a threat that isn't EICAR or a port scan
- Prepare an environment for digital forensics classes

Focus

- The focus of this tool is to simulate adversary activity, not malware

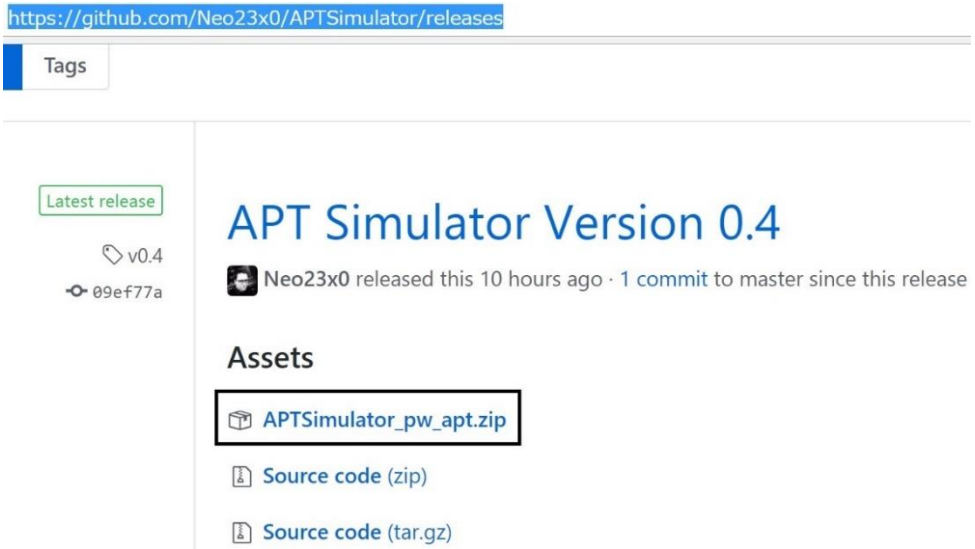


Integrated Projects / Software

- Mimikatz
- PowerSploit
- PowerCat
- PsExec
- ProcDump
- 7Zip
- curl

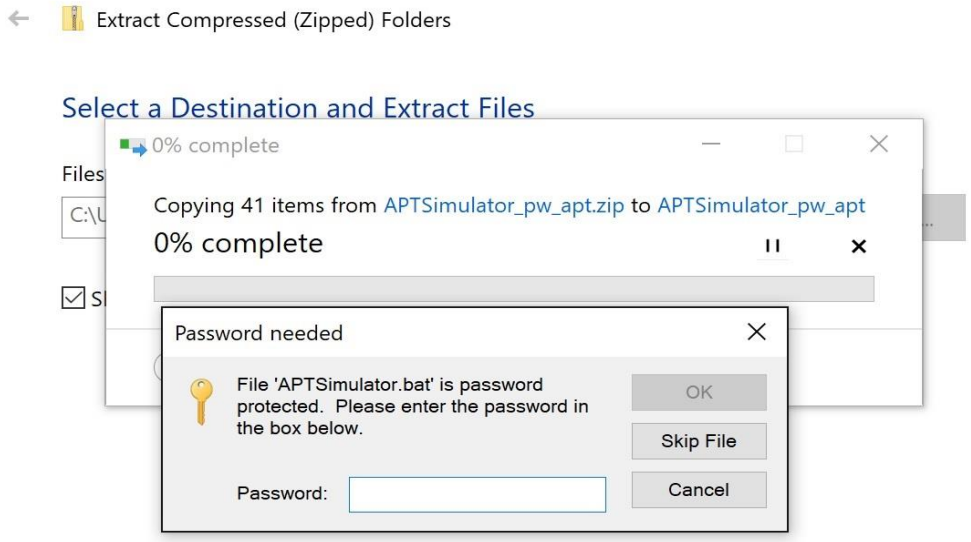
Installing APT Simulator

- Downloading the latest release from the "release" section



Installing APT Simulator

- Extracting the package on a demo system (Password: apt)

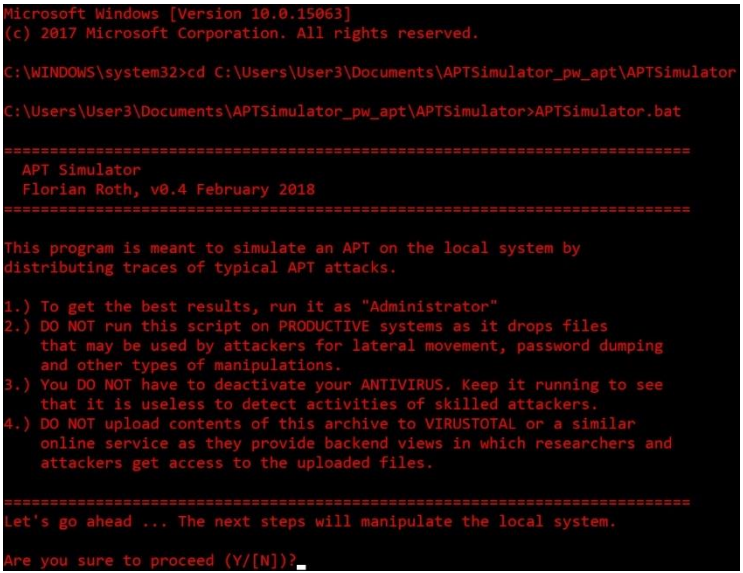


Running APT Simulator

- Start a cmd.exe as Administrator

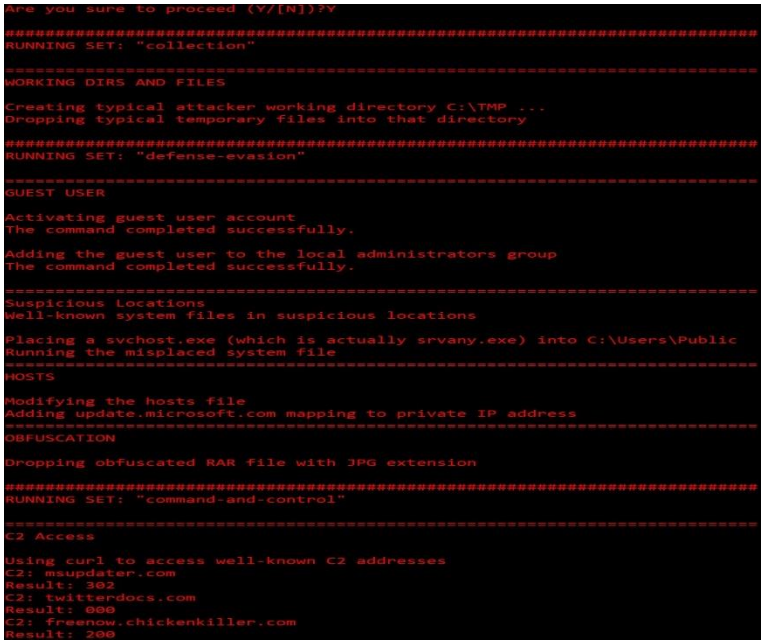
Running APT Simulator

- Navigating to the extracted program folder and run APTSimulator.bat

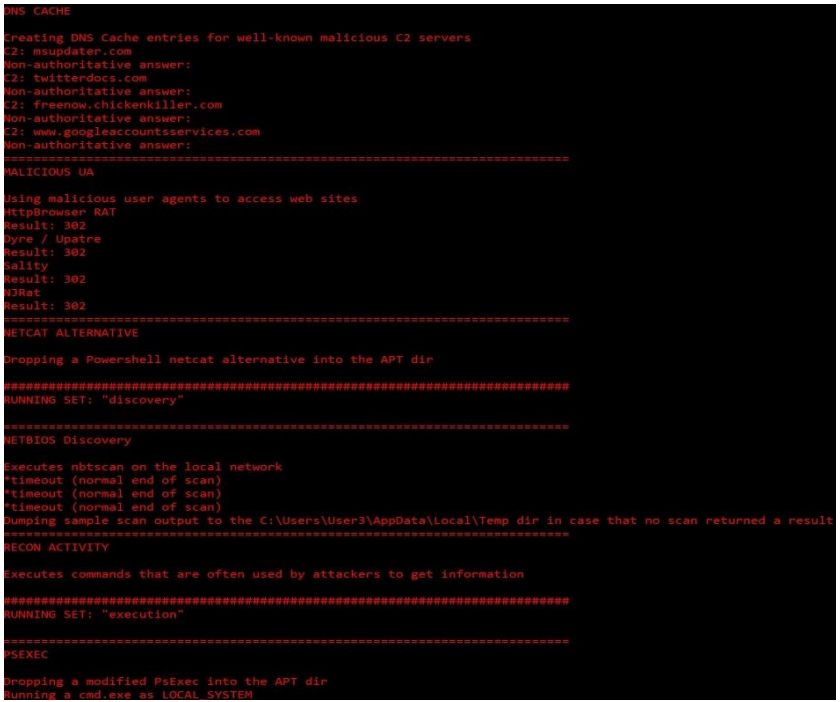


Running APT Simulator

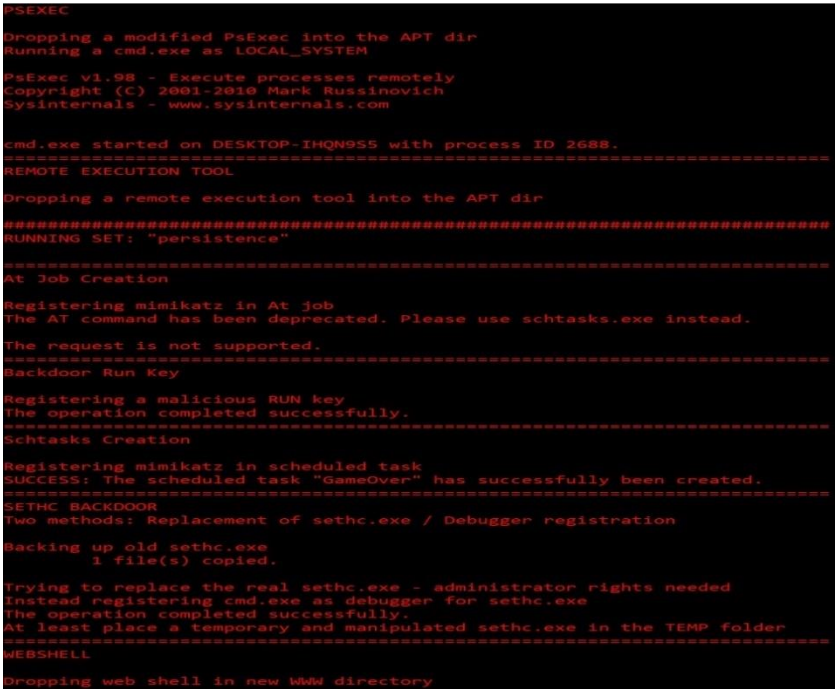
- Typing “Y” and proceed



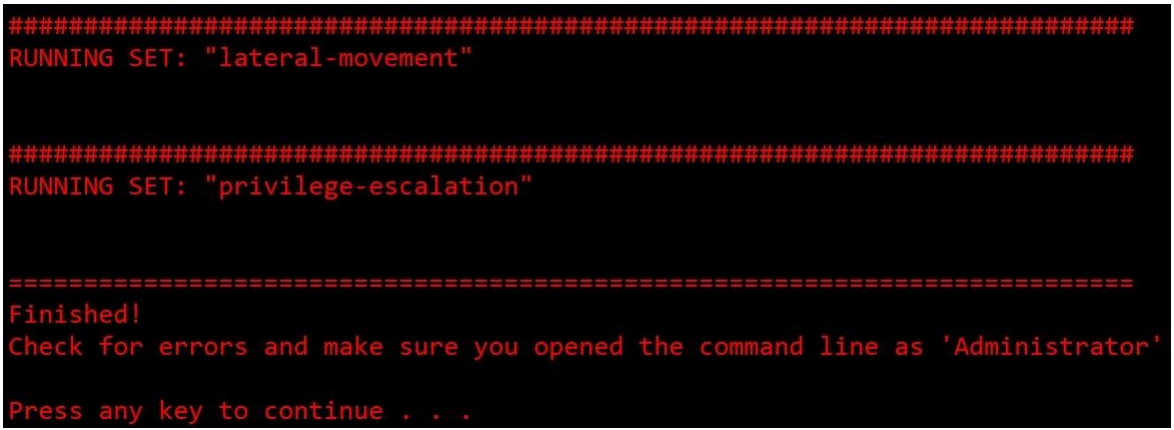
Running APT Simulator



Running APT Simulator



Running APT Simulator



Running APT Simulator

```
Finished!
Check for errors and make sure you opened the command line as 'Administrator'

Press any key to continue . . .

C:\Users\User3\Documents\APTSimulator_pw_apt\APTSimulator>
```

References

- APT Simulator
https://github.com/Neo23x0/APTSimulator
https://github.com/Neo23x0/APTSimulator/releases

- Mimikatz
https://github.com/gentilkiwi/mimikatz