



APT Simulator

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

```
=====  
APT simulator  
Florian Roth, v0.4 February 2018  
=====
```

Testing Environment

- Windows 10 x64

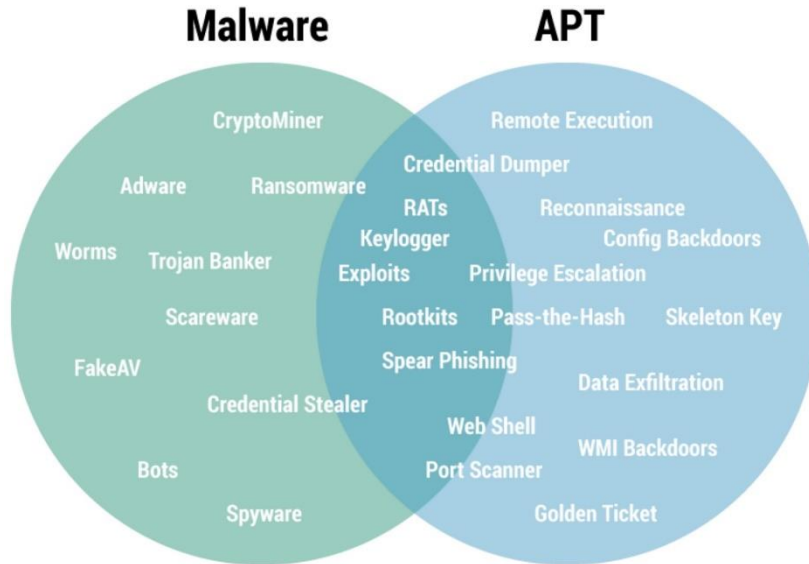
Edition	Windows 10 Pro
Version	1703
OS Build	15063.786
Processor	Intel(R) Core(TM) i7-4910MQ CPU @ 2.90GHz 2.90 GHz
Installed RAM	3.04 GB
System type	64-bit operating system, x64-based processor

Use Cases

- POCs: Endpoint detection agents / compromise assessment tools
- Test your security monitoring's detection capabilities
- Test your SOC's 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

<https://github.com/Neo23x0/APTSimulator/releases>

Tags

Latest release

v0.4
09ef77a

APT Simulator Version 0.4

Neo23x0 released this 10 hours ago · 1 commit to master since this release

Assets

APTSimulator_pw_appt.zip

Source code (zip)

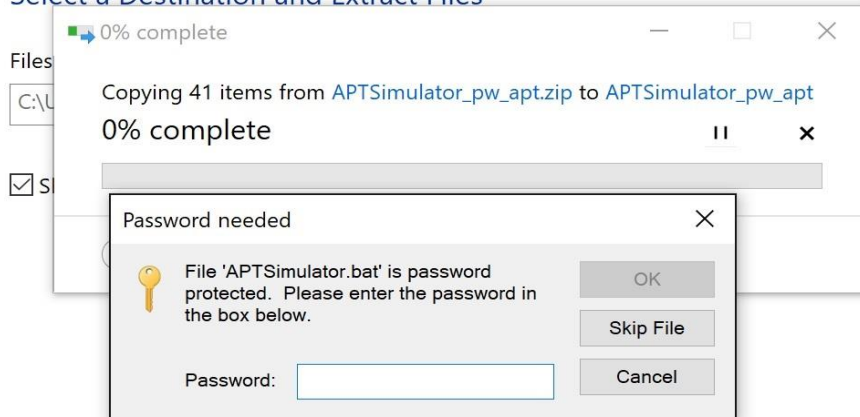
Source code (tar.gz)

Installing APT Simulator

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

←  Extract Compressed (Zipped) Folders

Select a Destination and Extract Files



Running APT Simulator

- Start a cmd.exe as Administrator

```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>
```

Running APT Simulator

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

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\User3\Documents\APTSimulator_pw_apt\APTSimulator
C:\Users\User3\Documents\APTSimulator_pw_apt\APTSimulator>APTSimulator.bat

=====
  APT Simulator
  Florian Roth, v0.4 February 2018
=====

This program is meant to simulate an APT on the local system by
distributing traces of typical APT attacks.

1.) To get the best results, run it as "Administrator"
2.) DO NOT run this script on PRODUCTIVE systems as it drops files
   that may be used by attackers for lateral movement, password dumping
   and other types of manipulations.
3.) You DO NOT have to deactivate your ANTIVIRUS. Keep it running to see
   that it is useless to detect activities of skilled attackers.
4.) DO NOT upload contents of this archive to VIRUSTOTAL or a similar
   online service as they provide backend views in which researchers and
   attackers get access to the uploaded files.

=====
let's go ahead ... The next steps will manipulate the local system.

Are you sure to proceed (Y/[N])?_
```

Running APT Simulator

- Typing “Y” and proceed

```
Are you sure to proceed (Y/N)?Y
=====
RUNNING SET: "collection"
=====
WORKING DIRS AND FILES
Creating typical attacker working directory C:\TMP ...
Dropping typical temporary files into that directory
=====
RUNNING SET: "defense-evasion"
=====
GUEST USER
Activating guest user account
The command completed successfully.
Adding the guest user to the local administrators group
The command completed successfully.
=====
Suspicious Locations
Well-known system files in suspicious locations
Placing a svchost.exe (which is actually srvany.exe) into C:\Users\Public
Running the misplaced system file
=====
HOSTS
Modifying the hosts file
Adding update.microsoft.com mapping to private IP address
=====
OBFUSCATION
Dropping obfuscated RAR file with JPG extension
=====
RUNNING SET: "command-and-control"
=====
C2 Access
Using curl to access well-known C2 addresses
C2: msupdater.com
Result: 202
C2: twitterdocs.com
Result: 000
C2: freenow.chickenkiller.com
Result: 200
```

Running APT Simulator

```
DNS CACHE
Creating DNS Cache entries for well-known malicious C2 servers
C2: msupdater.com
Non-authoritative answer:
C2: twitterdocs.com
Non-authoritative answer:
C2: freenow.chickenkiller.com
Non-authoritative answer:
C2: www.googleaccountservices.com
Non-authoritative answer:
=====
MALICIOUS UA
Using malicious user agents to access web sites
HttpBrowser RAT
Result: 302
Byrs / Upatre
Result: 302
bality
Result: 302
IJRat
Result: 302
=====
NETCAT ALTERNATIVE
Dropping a Powershell netcat alternative into the APT dir
=====
RUNNING SET: "discovery"
=====
NETBIOS Discovery
Executes nbtscan on the local network
*timeout (normal end of scan)
*timeout (normal end of scan)
*timeout (normal end of scan)
Dumping sample scan output to the C:\Users\User3\AppData\Local\Temp dir in case that no scan returned a result
=====
RECON ACTIVITY
Executes commands that are often used by attackers to get information
=====
RUNNING SET: "execution"
=====
PSEXEC
Dropping a modified PsExec into the APT dir
Running a cmd.exe as LOCAL SYSTEM
```

Running APT Simulator

```
PSEXEC
Dropping a modified PsExec into the APT dir
Running a cmd.exe as LOCAL_SYSTEM

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

cmd.exe started on DESKTOP-IHQ9SS with process ID 2688.
=====
REMOTE EXECUTION TOOL
Dropping a remote execution tool into the APT dir
=====
RUNNING SET: "persistence"
=====
At Job Creation
Registering mimikatz in At Job
The AT command has been deprecated. Please use schtasks.exe instead.

The request is not supported.
=====
Backdoor Run Key
Registering a malicious RUN key
The operation completed successfully.
=====
Schtasks Creation
Registering mimikatz in scheduled task
SUCCESS: The scheduled task "GameOver" has successfully been created.
=====
SETHC BACKDOOR
Two methods: Replacement of sethc.exe / Debugger registration
Backing up old sethc.exe
1 file(s) copied.

Trying to replace the real sethc.exe - administrator rights needed
Instead registering cmd.exe as debugger for sethc.exe
The operation completed successfully.
At least place a temporary and manipulated sethc.exe in the TEMP folder
=====
WEBSHELL
Dropping web shell in new WWW directory
```

Running APT Simulator

```
#####  
RUNNING SET: "lateral-movement"  
  
#####  
RUNNING SET: "privilege-escalation"  
  
=====  
Finished!  
Check for errors and make sure you opened the command line as 'Administrator'  
  
Press any key to continue . . .
```

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_apr\APTSimulator>
```


References

- APT Simulator

<https://github.com/Neo23x0/APTSimulator>

<https://github.com/Neo23x0/APTSimulator/releases>

- Mimikatz

<https://github.com/gentilkiwi/mimikatz>