CERIAS

The Center for Education and Research in Information Assurance and Security

Malware Privilege Level vs. Infection Strength on Windows 7 (Work in Progress)

Eric Buedel

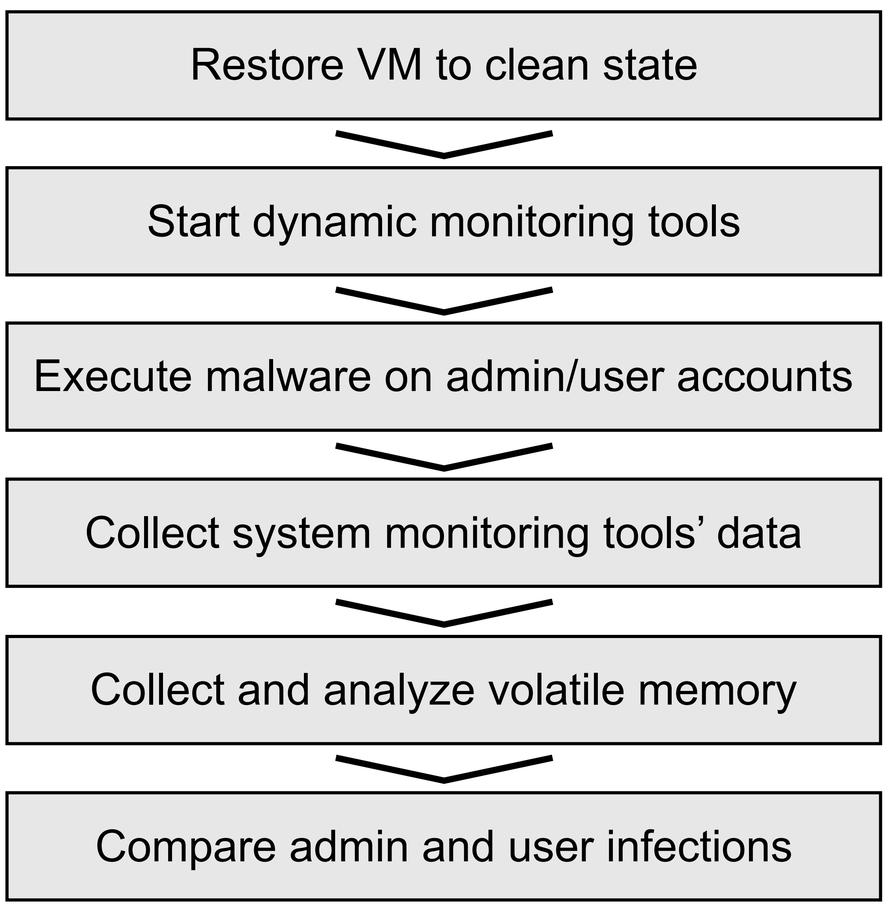
Department of Computer and Information Technology

Problem

Many Windows users use an administrator account for all computing tasks, violating the Principle of Least Privilege. In the event of a malware infection, the malware could take advantage of the administrator privileges if other features, such as User Account Control (UAC), are used incorrectly, making the infection more deadly [1].

A 2010 study showed that most users do not use UAC correctly, so the users who use an administrator account as their sole account on Windows may be especially vulnerable to malware infections [2]. The goal of this research is to determine if such users are indeed more vulnerable to malware infections.

Methodology



Process Monitor, Process Explorer, and RegShot were used to dynamically monitor the virtual machine while the malware executed. DumpIt was used to capture the VM's volatile memory.

Volatility and DAMM (Differential Analysis of Malware in Memory) were used to analyze the memory snapshots and find any data that suggested a successful infection.

The following is an example of finding hints of a successful malware infection using the methods of this research.

During the dynamic monitoring of the system, Process Monitor logs suspicious behavior of "iexplore.exe", the process name of Internet Explorer:

Process	PID	Operation	Path
iexplore.exe	3280	CreateFile	C:\Windows\InstallDir\Server.exe

Process Monitor shows malicious file creation by hijacked iexplore.exe

Once the volatile memory is collected, Volatility's psscan plugin shows there is one "svchost.exe" process with a different parent process ID (PPID) and it has injected code:

Process	PID	PPID
svchost.exe	308	400
svchost.exe	252	400
svchost.exe	1940	2524

Volatility's psscan plugin reveals fake svchost.exe process

```
Process: svchost.exe Pid: 1940 Address: 0x10000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 75, MemCommit: 1, PrivateMemory: 1,
Protection: 6
```

Volatility's malfind plugin locates injected code

VirusTotal, a service that analyzes files, identifies the injected code as a packed executable, and half of the antivirus scanners supported by VirusTotal flag it as malicious:

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	1992-06-19 22:22:17
Entry Point	0x000492D0
Number of sections	3

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy
UPX0	4096	266240	0	0.00
UPX1	270336	32768	30208	6.70
.rsrc	303104	4096	1024	4.04

VirusTotal shows the injected code is a packed i386 executable

For a given sample, the user account was said to be less vulnerable to infection if there was at least one action the malware performed on the admin but not the user account.

[1] Russinovich, M. (2007, June). Inside Windows Vista UAC. *TechNet*, 32-36.
[2] Motiee, S., Hawkey, K., & Beznosov, K. (2010, July). Do Windows users follow the principle of least privilege?. *Symposium on Usable Privacy and Security (SOUPS)*.

PURDUE UNIVERSITY