Windows Security

IT SECURITY ACADEMY

www.SecAcademy.com

User Account control

Two account types: standard users and administrators

When a user launches an application, the user's access token is added to it:

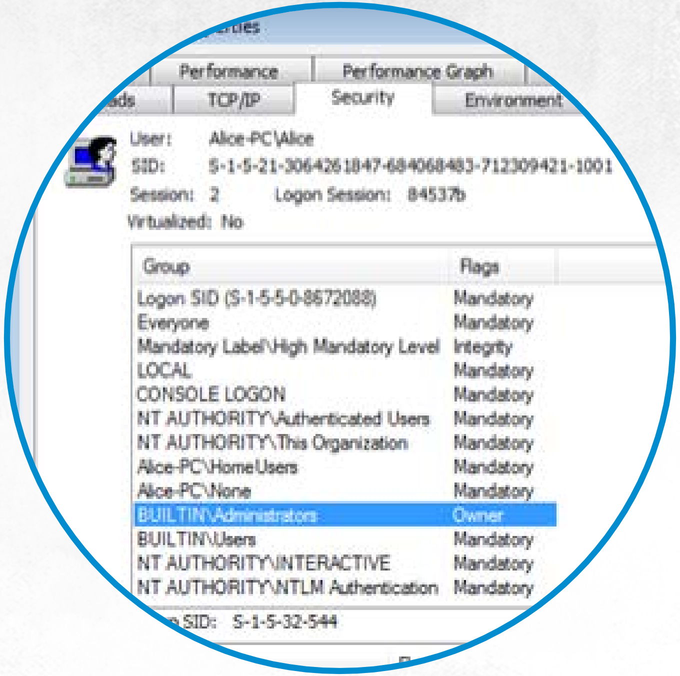
- At system logon, users receive an access token. The token contains a user SID and a list of rights and privileges the user has as well as information on the user's membership in security groups
- The access token is added to each process the user launches
- Windows Vista and newer systems check privileges and memberships of all users who log on. If the user has administrative rights, another access token is created, this time for a standard user. This means an administrator has two access tokens: a full administrator access token (AT) and a standard user access token (SAT)
- When a user launches a process, it only gets one of these tokens. The default option is to use the SAT token
- Once a token is applied to a process, it cannot be changed
- If UAC detects that a process requires elevated privileges to run, it will prompt a request for the application to run as elevated
- Processes launched by a program that has the AT token automatically inherit the token

User Account control

The SAT token is granted to a privileged user if

The user belongs to one of the four local security groups with elevated privileges:

- Administrators
- Backup operators
- Network configuration operators
- Power users



User: Alice-PC\Alice
SID: S-1-5-21-3064261847-684068483-712309421-1001
Session: 2 Logon Session: 84537b
Virtualized: No

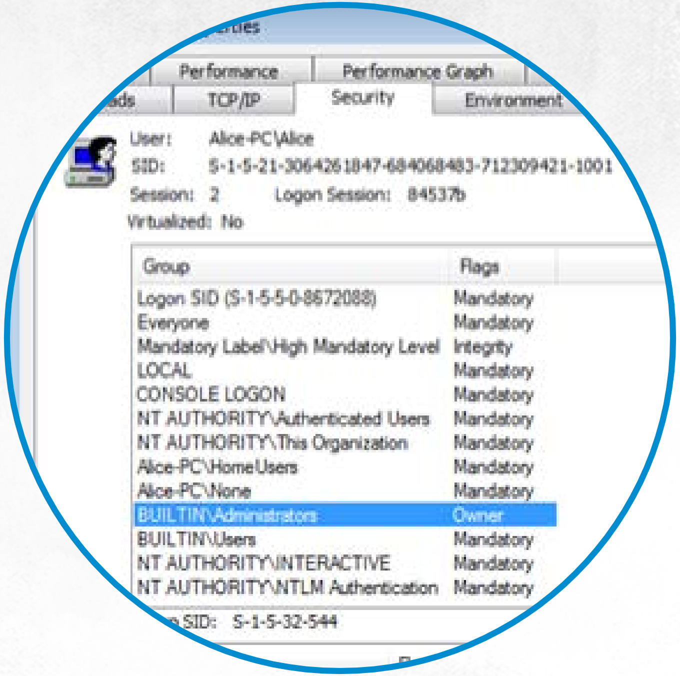
Group	Flags
Logon SID (S-1-5-5-0-8672088)	Mandatory
Everyone	Mandatory
Mandatory Label\High Mandatory Level	Integrity
LOCAL	Mandatory
CONSOLE LOGON	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\This Organization	Mandatory
Alice-PC\HomeUsers	Mandatory
Alice-PC\None	Mandatory
BUILTIN\Administrators	Owner
BUILTIN\Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory
NT AUTHORITY\NTLM Authentication	Mandatory

n SID: S-1-5-32-544

User Account control

The user has one of the nine additional privileges:

- SeCreateTokenPrivilege (allows users to create new token objects)
- SeTcbPrivilege (allows users to act as part of the operating system)
- SeTakeOwnershipPrivilege (allows uses to take ownerships of objects owned by all users)
- SeLoadDriverPrivilege (allows users to load and run drivers)
- SeRestorePrivilege (allows users to restore backups, including system files, which can make changes to system settings)
- SeImpersonatePrivilege (allows users to run processes with other privileges)
- SeRelabelPrivilege (allows users to modify the labels of processes and objects)
- SeDebugPrivilege



User: Alice-PC\Alice
SID: S-1-5-21-3064261847-684068483-712309421-1001
Session: 2 Logon Session: 84537b
Virtualized: No

Group	Flags
Logon SID (S-1-5-5-0-8672088)	Mandatory
Everyone	Mandatory
Mandatory Label\High Mandatory Level	Integrity
LOCAL	Mandatory
CONSOLE LOGON	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\This Organization	Mandatory
Alice-PC\HomeUsers	Mandatory
Alice-PC\None	Mandatory
BUILTIN\Administrators	Owner
BUILTIN\Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory
NT AUTHORITY\NTLM Authentication	Mandatory

n SID: S-1-5-32-544

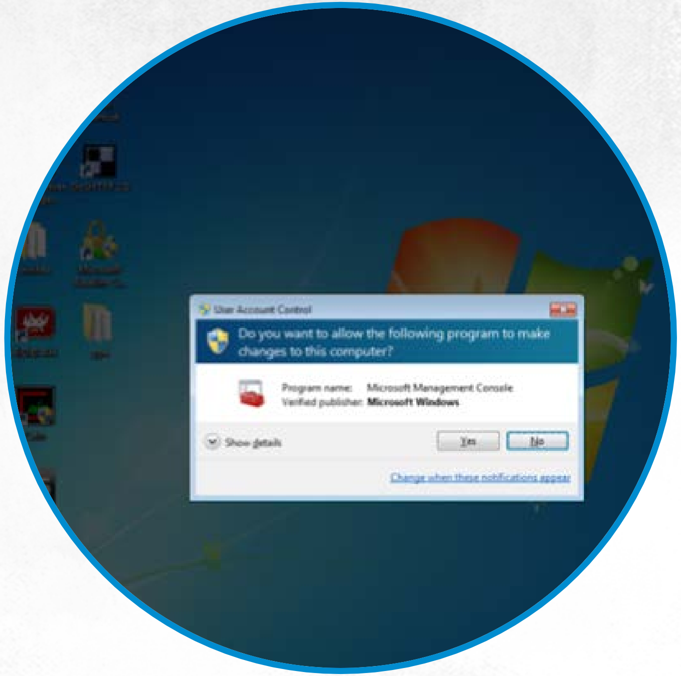
User Account control

Pressing Ctrl+Alt+Del is not required for security in elevation prompts

When a program that requires administrator-level of privileges to run is launched, the user is switched to the secure desktop mode

How the secure desktop works:

- It aims to reduce the risk connected to attackers and malware spoofing the UAC dialogue boxes
- Preventing overlooking elevation requests when desktop is crammed with many windows

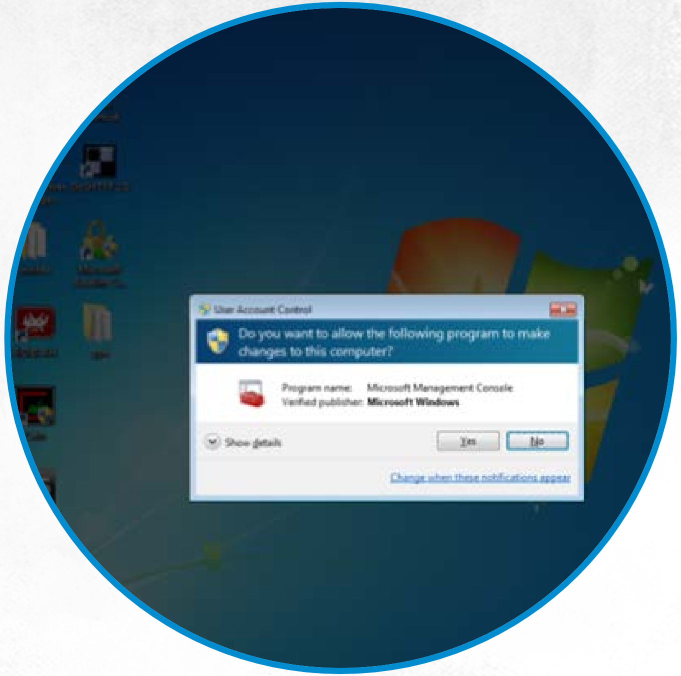


Do you want to allow the following program to make changes to this computer?

Program name: Microsoft Management Console
Verified publisher: Microsoft Windows

User Account control

While this security principle is essential to keep systems safe, it is often ignored due to many applications being written to require administrator privileges to run



User Account Control

Do you want to allow the following program to make changes to this computer?

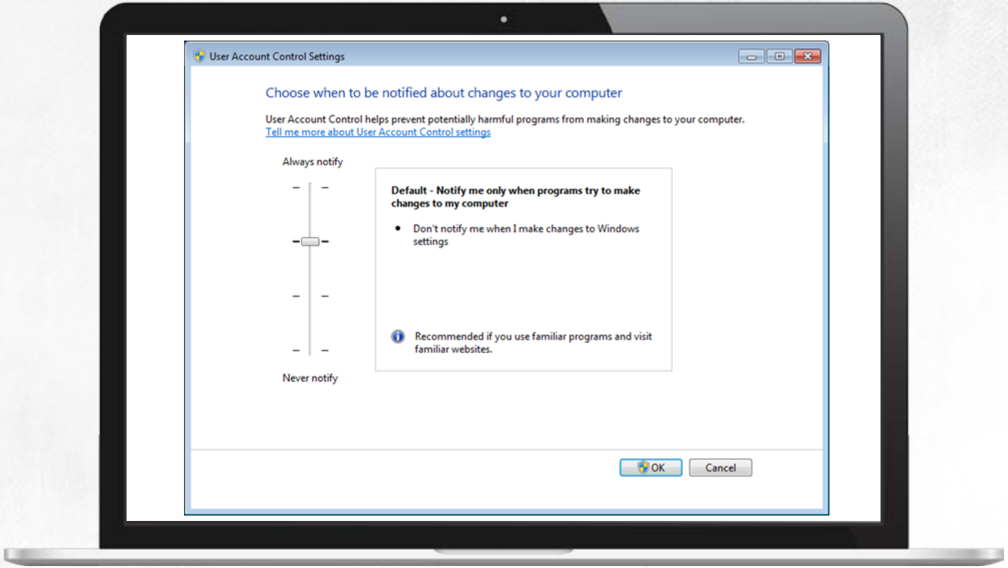
Program name: Microsoft Management Console

Verified publisher: Microsoft Windows

User Account Control

UAC configuration has been considerably streamlined in beginning with Windows 7

In Windows Vista, UAC could only be turned on or off in the Control Panel, while calibrating individual options required users to set appropriate group policies manually



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites.

Never notify

Exercise

User account control

Process virtualisation

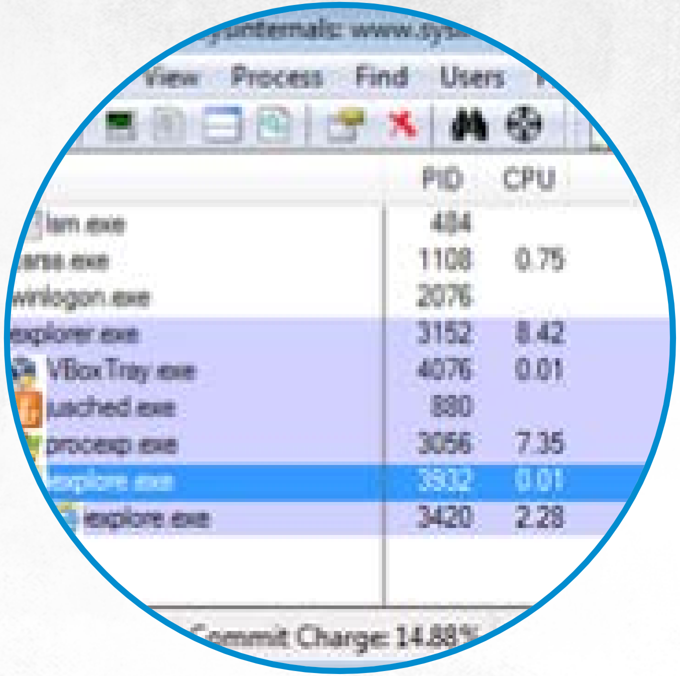
Internet Explorer protected mode

Goal: preventing the automatic launch of programs downloaded from the Internet and preventing these programs from writing to system settings and user files

Realisation: running the browser at low integrity

The ieuser.exe process, acting as a proxy, requires users to confirm if they want to run all programs that come from the Internet

Internet Explorer Protected Mode is the only security mechanism that takes full advantage of mandatory integrity control

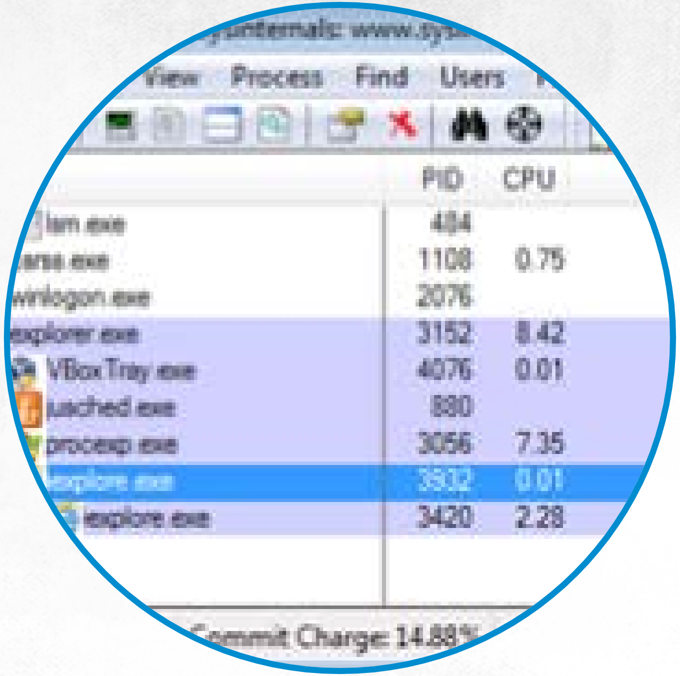


```
                 PID   CPU
lsm.exe          484
sass.exe         1108  0.75
winlogon.exe     2076
explorer.exe     3152  8.42
VBoxTray.exe     4076  0.01
jusched.exe      880
procexp.exe      3056  7.35
iexplore.exe     3932  0.01
iexplore.exe     3420  2.28
Commit Charge: 14.88%
```

Internet Explorer protected mode

That said, it does not ensure the total isolation of programs downloaded from the Internet as it only disables them from writing to user data, whereas reading is allowed

Processes running at low integrity share a user session with other programs launched by the user that have the same integrity level



```
                 PID    CPU
lsm.exe          484
arss.exe         1108   0.75
winlogon.exe     2076
explorer.exe     3152   8.42
  VBoxTray.exe   4076   0.01
  jusched.exe    880
  procexp.exe    3056   7.35
  iexplore.exe   3932   0.01
    iexplore.exe 3420   2.28

Commit Charge: 14.88%
```

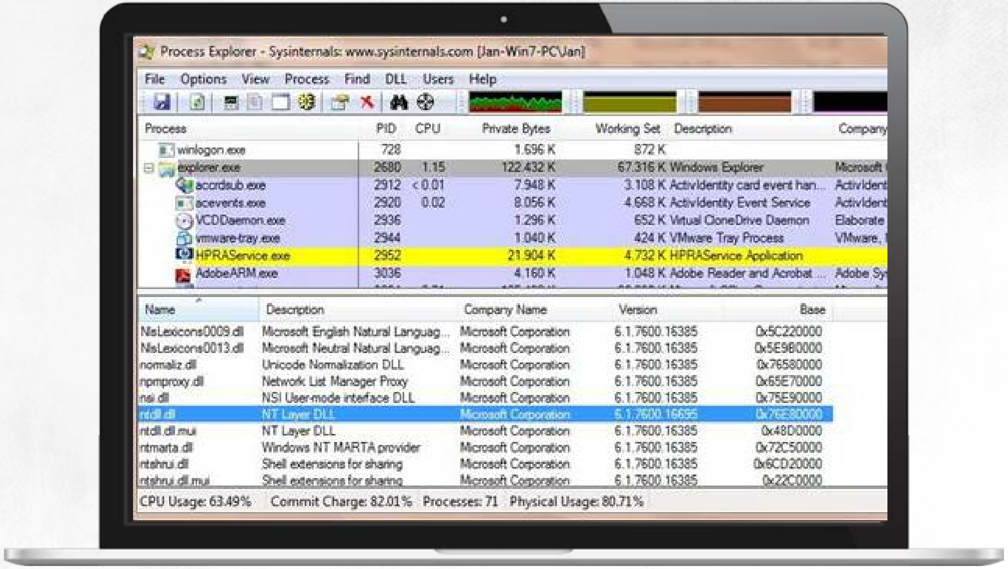
Additional secuirty features

ASLR and DEP

How it works: an operating system can be loaded from one of 256 locations. ASLR is a security technique that involves using a randomised memory address for this procedure

At every restart Windows libraries will be located in a different RAM part

Also programs launched by users may be ASLR-protected You can use EMET to turn on ASLR


Process Explorer - Sysinternals: www.sysinternals.com [Jan-Win7-PC\Jan]
File
Options
View
Process
Find
DLL
Users
Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company
winlogon.exe	728		1.696 K	872 K		
explorer.exe	2680	1.15	122.432 K	67.316 K	Windows Explorer	Microsoft
acordsub.exe	2912	< 0.01	7.948 K	3.108 K	ActivIdentity card event han...	ActivIdent
acevents.exe	2920	0.02	8.056 K	4.668 K	ActivIdentity Event Service	ActivIdent
VCDDaemon.exe	2936		1.296 K	652 K	Virtual CloneDrive Daemon	Elaborate
vmware-tray.exe	2944		1.040 K	424 K	VMware Tray Process	VMware,
HPRAService.exe	2952		21.904 K	4.732 K	HPRAService Application	
AdobeARM.exe	3036		4.160 K	1.048 K	Adobe Reader and Acrobat ...	Adobe Sy

Name	Description	Company Name	Version	Base
NlsLexicons0009.dll	Microsoft English Natural Languag...	Microsoft Corporation	6.1.7600.16385	0x5C220000
NlsLexicons0013.dll	Microsoft Neutral Natural Languag...	Microsoft Corporation	6.1.7600.16385	0x5E9B0000
normaliz.dll	Unicode Normalization DLL	Microsoft Corporation	6.1.7600.16385	0x76580000
npmproxy.dll	Network List Manager Proxy	Microsoft Corporation	6.1.7600.16385	0x65E70000
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation	6.1.7600.16385	0x75E90000
ntdll.dll	NT Layer DLL	Microsoft Corporation	6.1.7600.16695	0x76E80000
ntdll.dll.mui	NT Layer DLL	Microsoft Corporation	6.1.7600.16385	0x48D0000
ntmarta.dll	Windows NT MARTA provider	Microsoft Corporation	6.1.7600.16385	0x72C50000
ntshrui.dll	Shell extensions for sharing	Microsoft Corporation	6.1.7600.16385	0x6CD20000
ntshrui.dll.mui	Shell extensions for sharing	Microsoft Corporation	6.1.7600.16385	0x22C0000

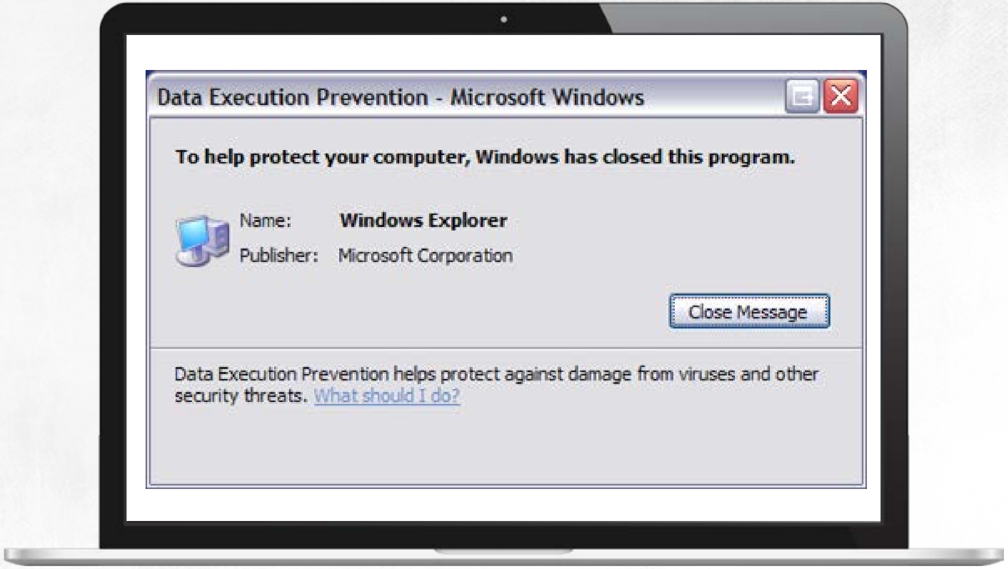
CPU Usage: 63.49%   Commit Charge: 82.01%   Processes: 71   Physical Usage: 80.71%

Additional secuirty features

ASLR and DEP

The function of DEP is to prevent applications from executing code from data. AMD processors use the no-execute page-protection (NX) feature

Intel processors use the Execute Disable Bit (XD) feature



Data Execution Prevention - Microsoft Windows

To help protect your computer, Windows has closed this program.

Name: **Windows Explorer**

Publisher: Microsoft Corporation

Data Execution Prevention helps protect against damage from viruses and other security threats. What should I do?

Exercise

ASLR and DEP

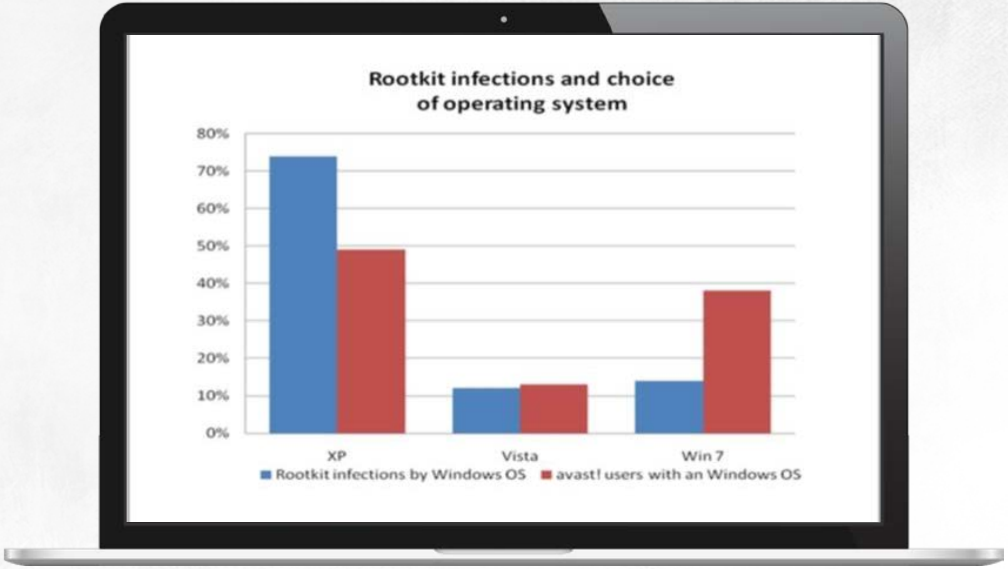
- How ASLR works
- Configuring DEP options
- Protecting applications using EMET

Additional secuirty features

PatchGuard

PatchGuard prevents patching the kernel (changing processes and structures of the kernel in a way not supported by Microsoft) by checking the signature of the most critical system processes like Ntoskrnl.exe, Hal.dll, IDT, SSDT and MSR

If PatchGuard detects they have been modified, it will stop the system

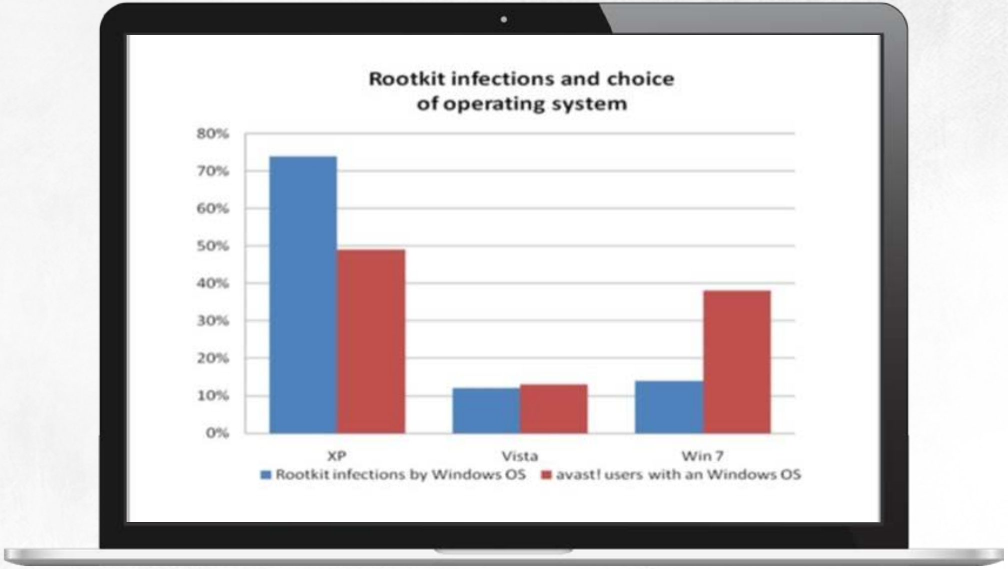


Additional secuirty features

PatchGuard

PatchGuard doesn’t ensure effective security against rootkits and worms

Likewise, it doesn’t offer protection against modifying files on-disk files



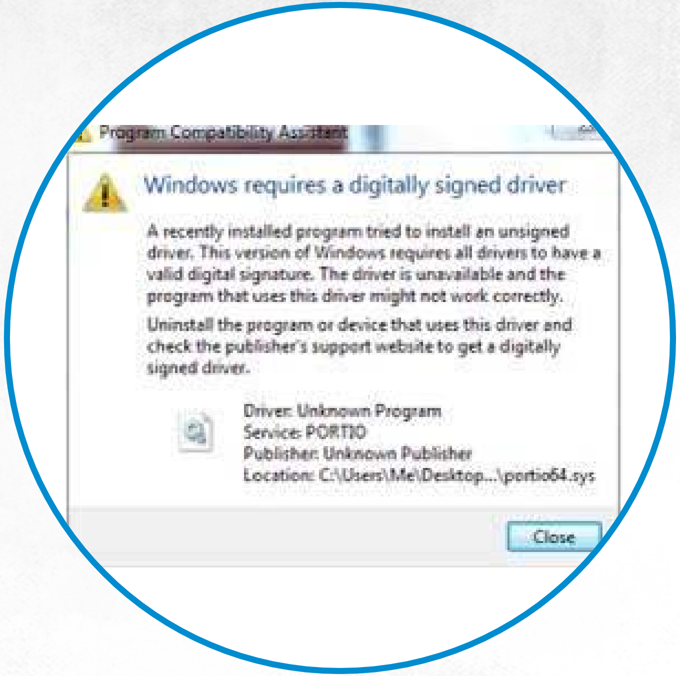
Additional secuirty features

Kernel Mode Code Signing

Kernel Mode Code Signing is a security feature thwarting the installation of faulty or malicious device drivers and facilitating the identification of their manufacturers

To be loaded and started, all drivers have to be digitally signed:

- At system start, a list of revoked and blocked drivers is loaded
- Before a driver is launched, its signature is verified. Additionally, the operating system checks if the certificate used for signing it was issued by a trusted authority and checks if it has been revoked



Program Compatibility Assistant

Windows requires a digitally signed driver

A recently installed program tried to install an unsigned driver. This version of Windows requires all drivers to have a valid digital signature. The driver is unavailable and the program that uses this driver might not work correctly.

Uninstall the program or device that uses this driver and check the publisher's support website to get a digitally signed driver.

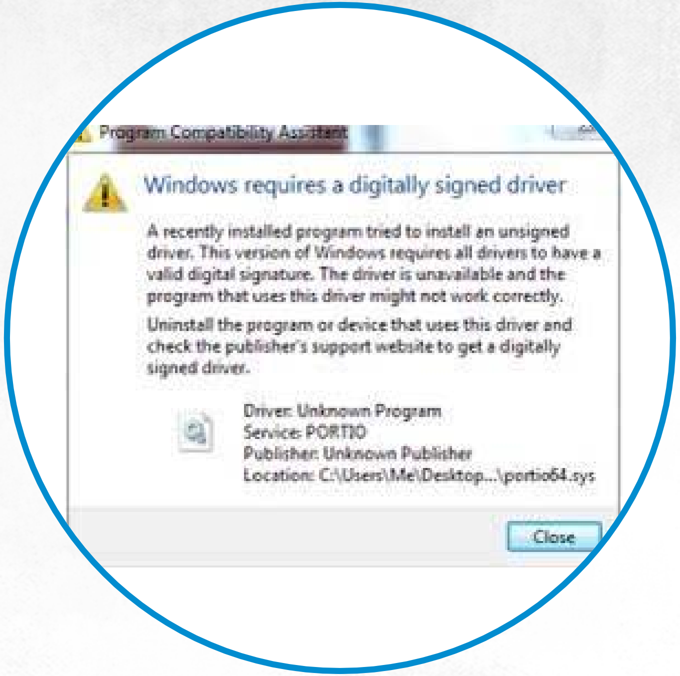
Driver: Unknown Program
Service: PORTIO
Publisher: Unknown Publisher
Location: C:\Users\Me\Desktop...\portio64.sys

Additional secuirty features

Kernel Mode Code Signing

As Kernel Mode Code Signing doesn’t analyse how drivers operate, all it takes for a driver creator to ensure the driver can be loaded is to pay 300$ for a certificate

It has no way of preventing users from modifying on-disk files, which means an attacker may be able to change system files to turn off checking drivers’ digital signatures, or the attacker may delete the list of blocked drivers



Program Compatibility Assistant

Windows requires a digitally signed driver

A recently installed program tried to install an unsigned driver. This version of Windows requires all drivers to have a valid digital signature. The driver is unavailable and the program that uses this driver might not work correctly.

Uninstall the program or device that uses this driver and check the publisher's support website to get a digitally signed driver.

Driver: Unknown Program
Service: PORTIO
Publisher: Unknown Publisher
Location: C:\Users\Me\Desktop...\portio64.sys

THANKS

IT SECURITY ACADEMY

www.SecAcademy.com