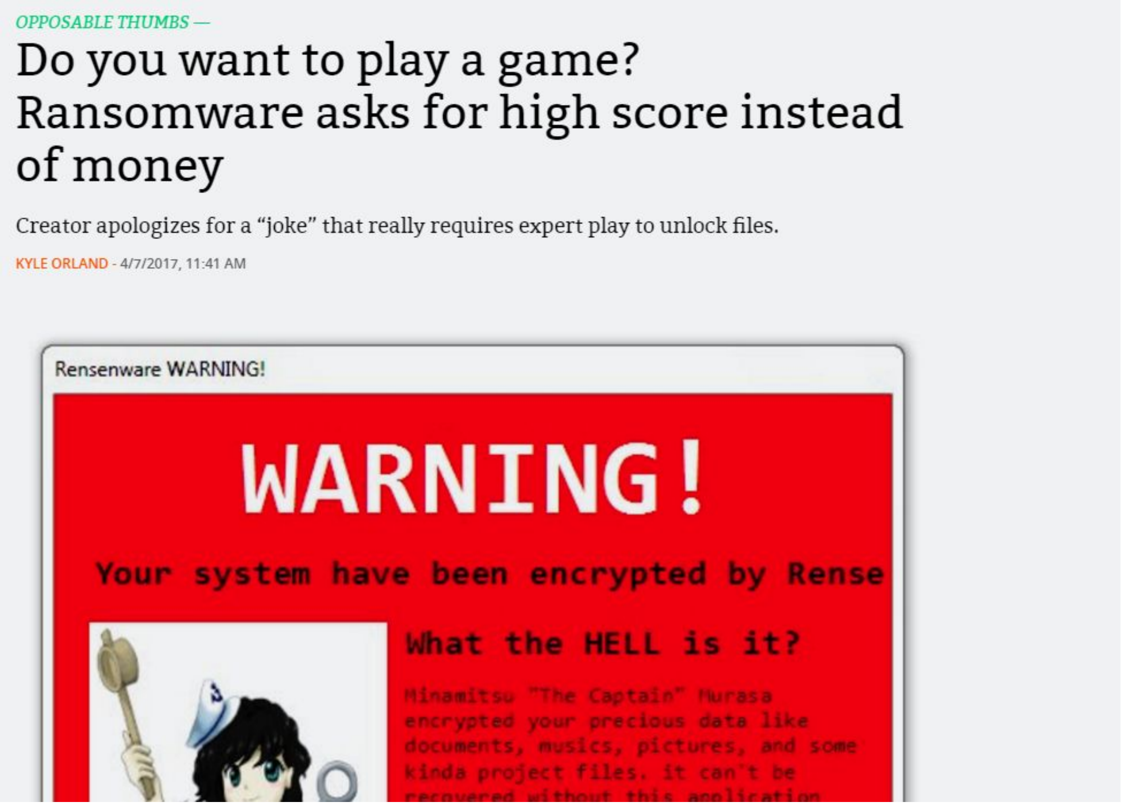
Windows Security

Ransomware in the news



OPPOSABLE THUMBS —

Do you want to play a game? Ransomware asks for high score instead of money

Creator apologizes for a “joke” that really requires expert play to unlock files.

KYLE ORLAND - 4/7/2017, 11:41 AM

Rensenware WARNING!

WARNING!

Your system have been encrypted by Rense

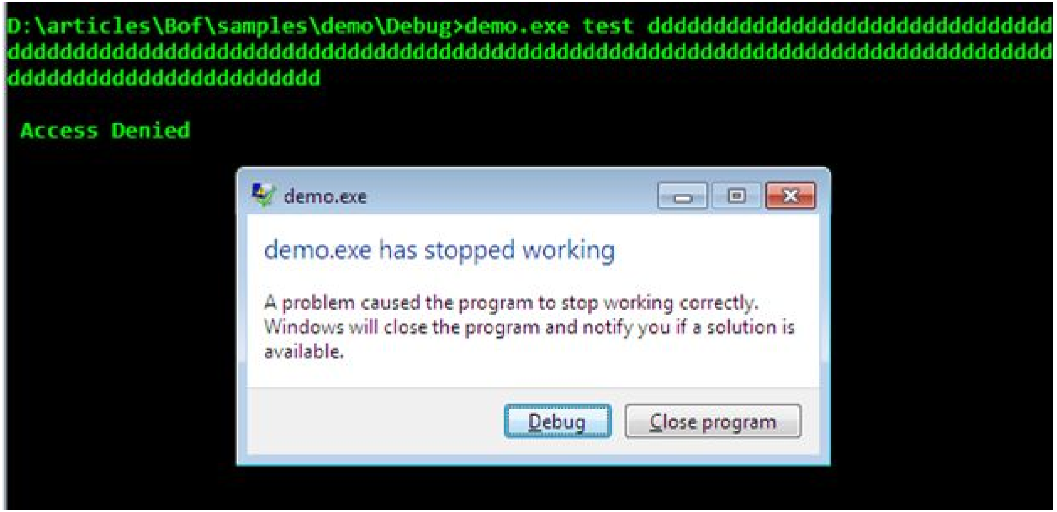
What the HELL is it?

Minamitsu "The Captain" Murasa encrypted your precious data like documents, musics, pictures, and some kinda project files. it can't be recovered without this application

Windows vs. Linux

We’ve discussed security and exploitation on Linux platforms, but what about Windows?

How do the exploits we’ve seen (buffer overflows, ROP, etc) differ on Windows?



```
D:\articles\Bof\samples\demo\Debug>demo.exe test ddddddddddddddddddddddddddddddd
dddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
dddddddddddddddddddddddd

 Access Denied
```

demo.exe

demo.exe has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Pretty much the same?

Almost everything you have learned about Linux exploitation applies directly to Windows

Memory corruption bugs are exploited in exactly the same way

```
int main() {
    char buf[100]; // Long enough!
    printf("Your name: ");
    gets(buf);
    printf("Hello, %s\n", buf);
    return 0;
}
```

Pretty much the same?

Linux shellcode relies heavily on syscalls directly to the Linux kernel

```
xor     eax,eax
push    eax
push    “hs//”
push    “nib/”
mov     ebx, esp
push    eax
push    ebx
mov     ecx, esp
mov     al, 0xb ; exec
int     0x80
```

Pretty much the same?

Windows shellcode doesn’t usually use syscalls. Instead, we call functions in **DLLs**

ntdll.dll is the low-level interface to Windows kernel functions

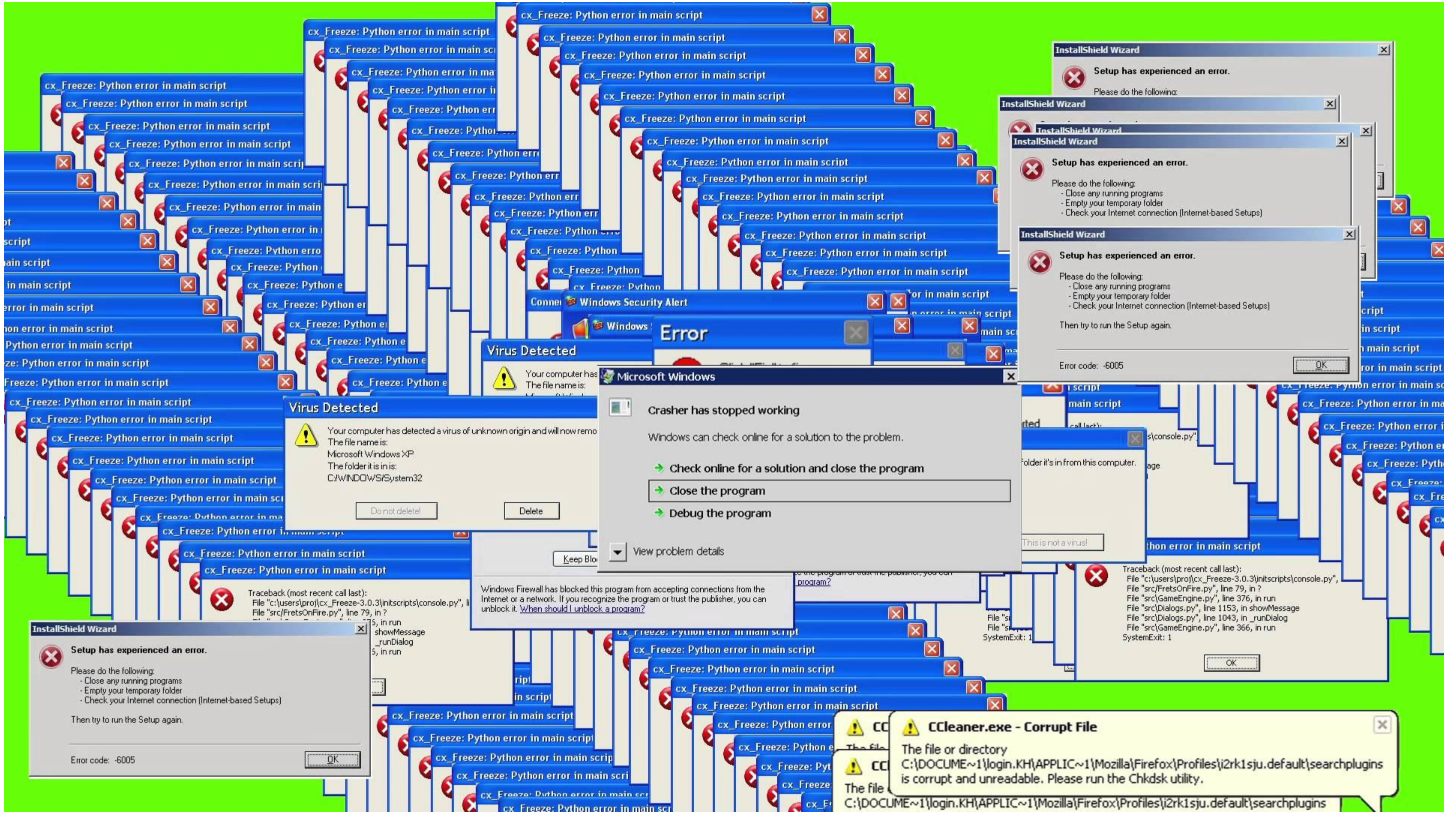
kernel32.dll is a higher level interface with common functions (OpenFile, ReadFile, CreateProcess, etc)

Pretty much the same?

Windows shellcode doesn’t use syscalls. Instead, we rely on calling functions in **DLLs** that the application uses

```
xor ecx, ecx
push ecx
push 0x636c6163 ; “clac”
push esp
mov eax,0x77c293c7 ; System
call eax
```

Windows XP (2001)



cx_Freeze: Python error in main script

InstallShield Wizard

Setup has experienced an error.

Please do the following:
- Close any running programs
- Empty your temporary folder
- Check your Internet connection (Internet-based Setups)

Then try to run the Setup again.

Error code: -6005

OK

Virus Detected

Your computer has detected a virus of unknown origin and will now remo
The file name is:
Microsoft Windows XP
The folder it is in is:
C:/WINDOWS/System32

Do not delete! | Delete

Windows Security Alert

Error

Microsoft Windows

Crasher has stopped working

Windows can check online for a solution to the problem.

→ Check online for a solution and close the program

→ Close the program

→ Debug the program

View problem details

Keep Blo

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

folder it's in from this computer.

This is not a virus!

```
Traceback (most recent call last):
  File "c:\users\proj\cx_Freeze-3.0.3\initscripts\console.py",
  File "src/FretsOnFire.py", line 79, in ?
  File "src\GameEngine.py", line 376, in run
  File "src\Dialogs.py", line 1153, in showMessage
  File "src\Dialogs.py", line 1043, in _runDialog
  File "src\GameEngine.py", line 366, in run
SystemExit: 1
```

OK

CCleaner.exe - Corrupt File

The file or directory C:\DOCUME~1\login.KH\APPLIC~1\Mozilla\Firefox\Profiles\i2rk1sju.default\searchplugins is corrupt and unreadable. Please run the Chkdsk utility.

Windows XP SP2 (2004)

DEP support in XP emerges and changes the exploit/malware landscape

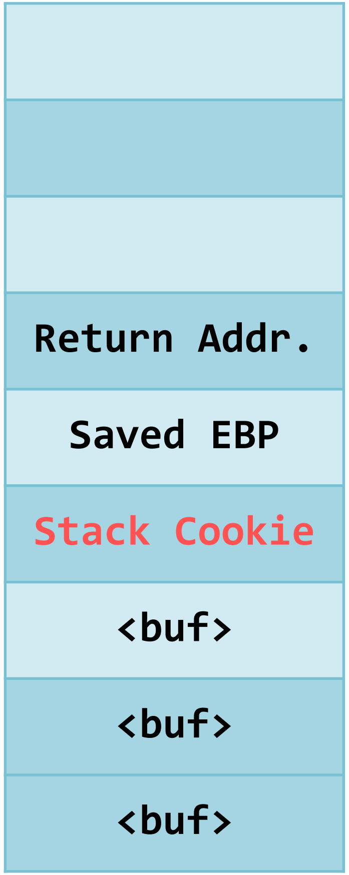
Stack cookies emerge in default applications which protect against trivial buffer overflows

Problem: No defense against ROP or other non-trivial exploits

Malware authors aren’t scared yet

Stack Cookies

```
int main() {
    char buf[12];
    printf("Your name: ");
    gets(buf);
    printf("%s\n", buf);
    return 0;
}
```



Windows Vista (2006)

ASLR is now supported by the OS and prevent ROP attacks

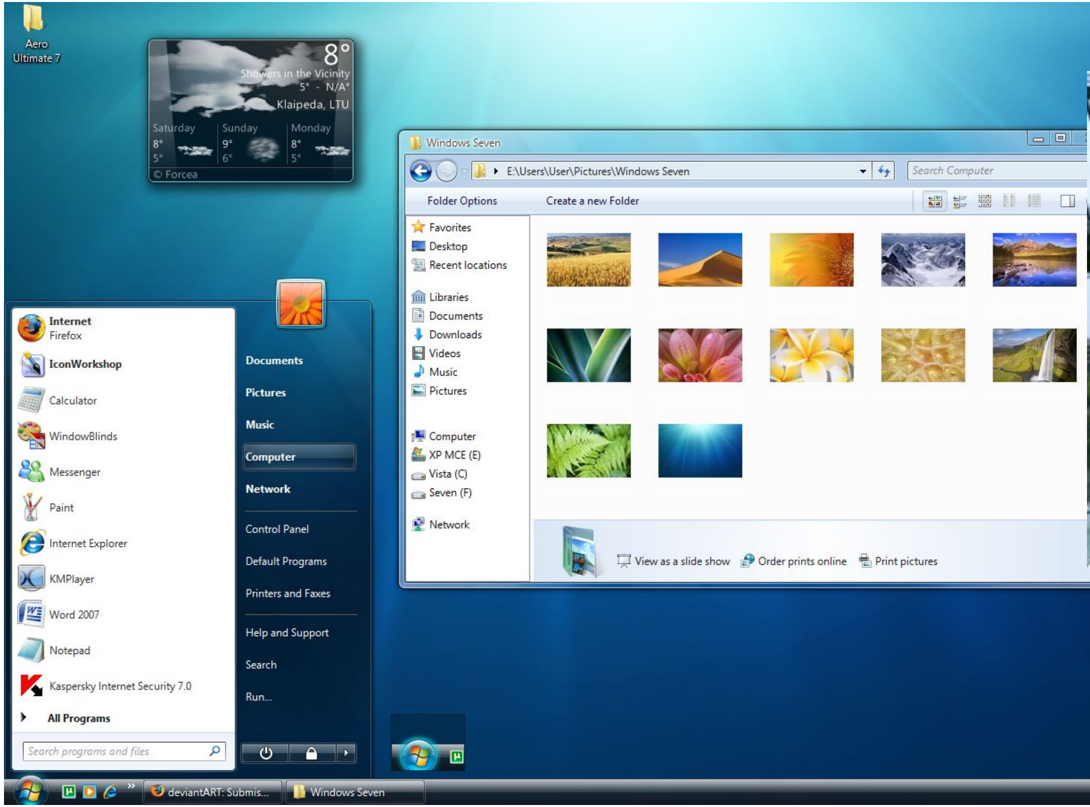
Practical bar on exploits is now much higher -- we can't write non-interactive exploits (but address leaks still help)

Introduction of **UAC** actually helps people who don't disable it

Many applications still **don't enable ASLR**

(Also, Vista sucks)

Windows 7 (2009)



(Mostly just iterations on existing security features)

Windows 8 (2012)

More powerful ASLR works to reduce surface area of applications (more entropy with 64-bit address space, all memory allocations randomized, etc)

DEP is broadly deployed throughout the kernel and first-party programs

SecureBoot ensures the Windows boot path is signed by Microsoft

SMEP/SMAP protect against kernel exploits

Cost of exploits is now very high

Windows 10 (2015)

Better support for **Control-Flow Guard** protections make ASLR even harder

Virtualization-based Security keeps privileged Windows services running in a separate VM -- completely isolated from the main Windows kernel

SecureBoot expanded and tightened with heavy use of hardware support

Early-launch antimalware support allows AV/AM to run before any non-Microsoft processes

Cost of exploits is now astronomically high

Windows 10 (2015)

Better suppor arder

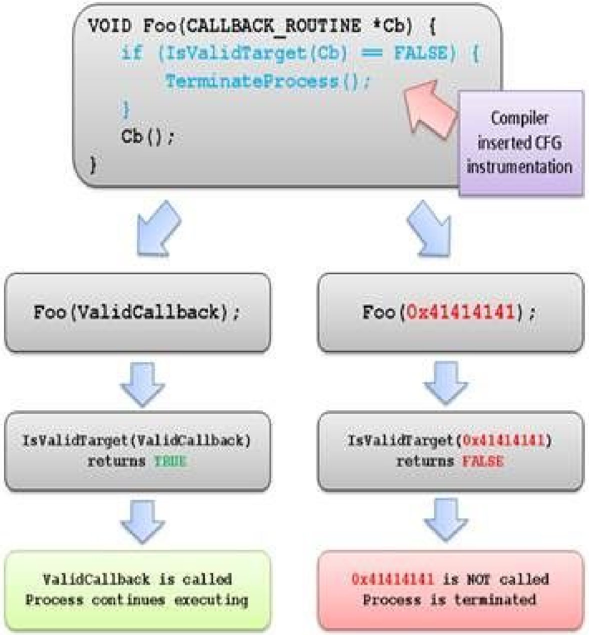
Virtualization ning in a separate VM -

SecureBoot e

Early-launch a soft processes

Cost of exploi

Control-Flow Guard



```
VOID Foo(CALLBACK_ROUTINE *Cb) {
    if (IsValidTarget(Cb) == FALSE) {
        TerminateProcess();
    }
    Cb();
}
```

Compiler inserted CFG instrumentation

`Foo(ValidCallback);`

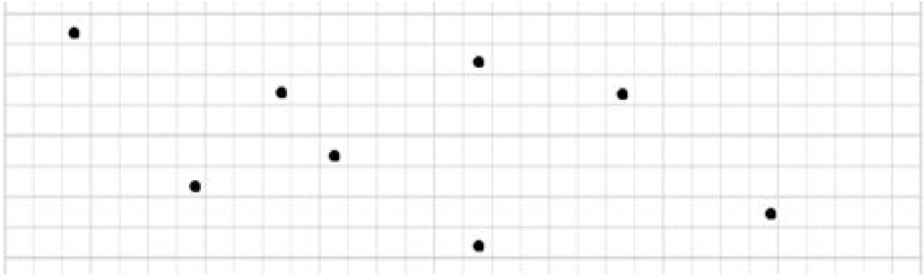
`IsValidTarget(ValidCallback)` returns `TRUE`

ValidCallback is called
Process continues executing

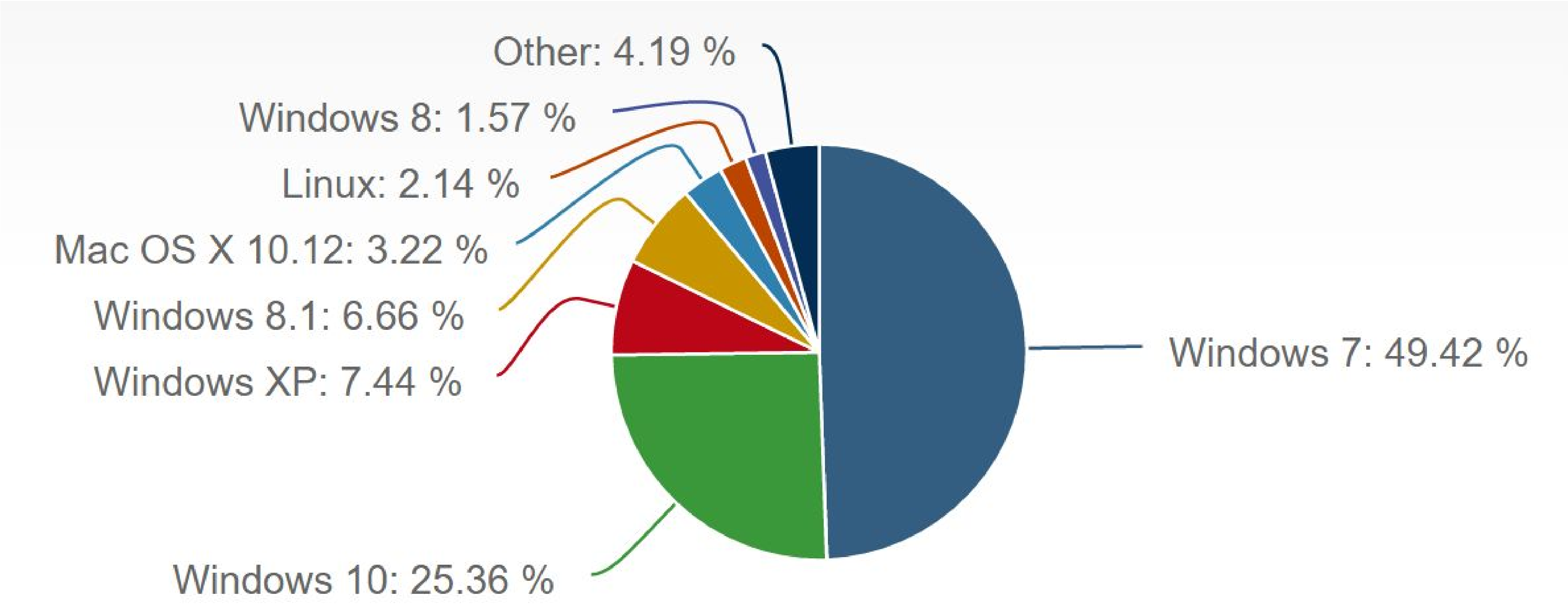
`Foo(0x41414141);`

`IsValidTarget(0x41414141)` returns `FALSE`

0x41414141 is NOT called
Process is terminated



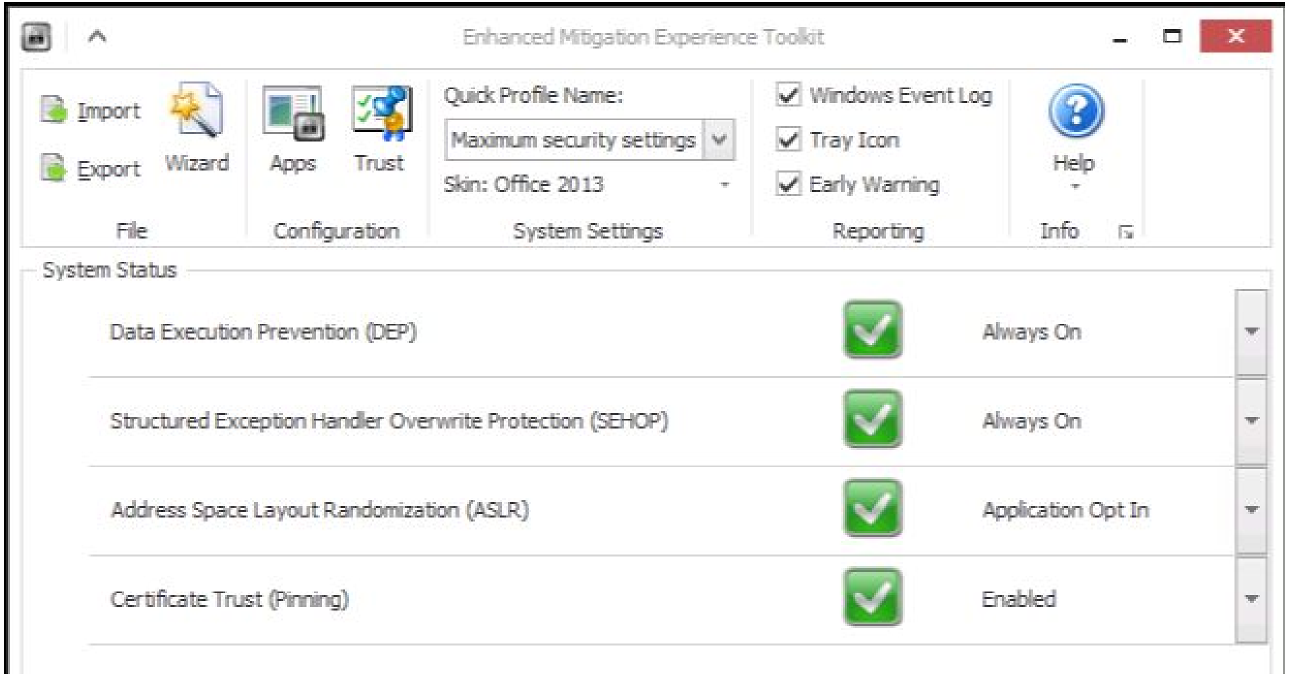
OS Usage


Other: 4.19 %
Windows 8: 1.57 %
Linux: 2.14 %
Mac OS X 10.12: 3.22 %
Windows 8.1: 6.66 %
Windows XP: 7.44 %
Windows 10: 25.36 %
Windows 7: 49.42 %

EMET

Enhanced Mitigation Experience Toolkit

All software is vulnerable. How can we make it harder for hackers to exploit bugs?



Quick Profile Name: Maximum security settings

Skin: Office 2013

☑ Windows Event Log

☑ Tray Icon

☑ Early Warning

System Status

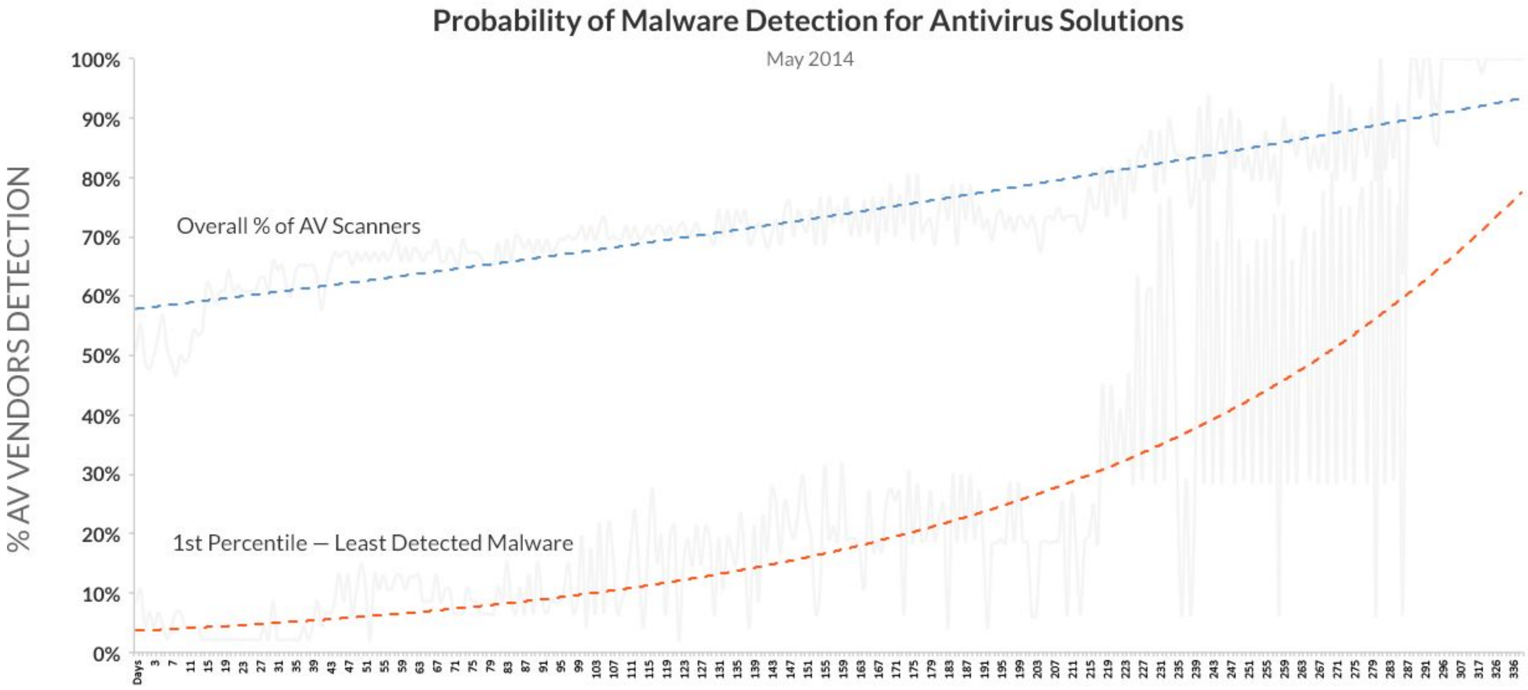
Data Execution Prevention (DEP)	✓	Always On
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Always On
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

ROP mitigations in EMET

- ASLR
- Bottom-up ASLR
- Disallow making the stack executable
- Ensure functions are reached by CALL, not RET
- Detect out-of-bounds stack pivots

Windows Defender and AV

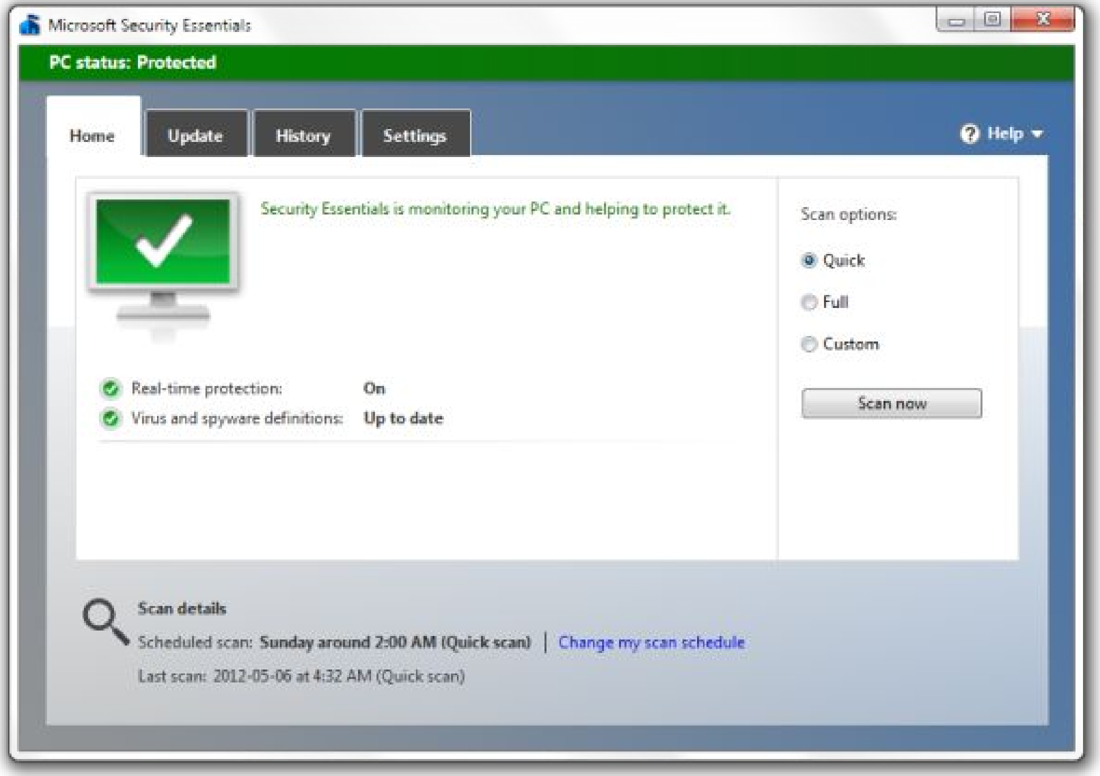
Remember: AV sucks



lastline labs

Data collected and research performed by Lastline Labs.
For more information, please visit www.lastline.com/labs.

Windows Security Essentials



PC status: Protected

Security Essentials is monitoring your PC and helping to protect it.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

Scan details

Scheduled scan: **Sunday around 2:00 AM (Quick scan)** | Change my scan schedule

Last scan: 2012-05-06 at 4:32 AM (Quick scan)

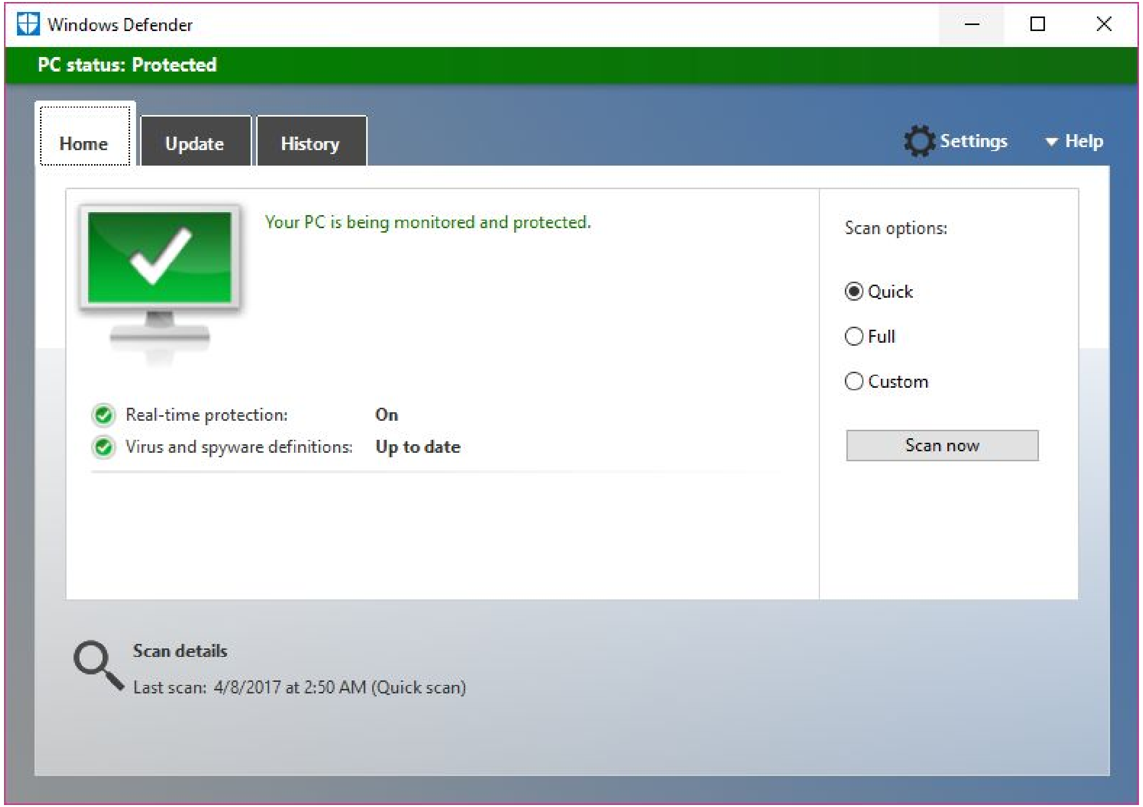
Windows Security Essentials

Free antivirus distributed by Microsoft for Windows XP/Vista/7

When launched, combined best performance with excellent detection rates

Quickly fell to **worst** in 2013 -- why?

Windows Defender



PC status: Protected

Your PC is being monitored and protected.

✓ Real-time protection: On

✓ Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

Scan details

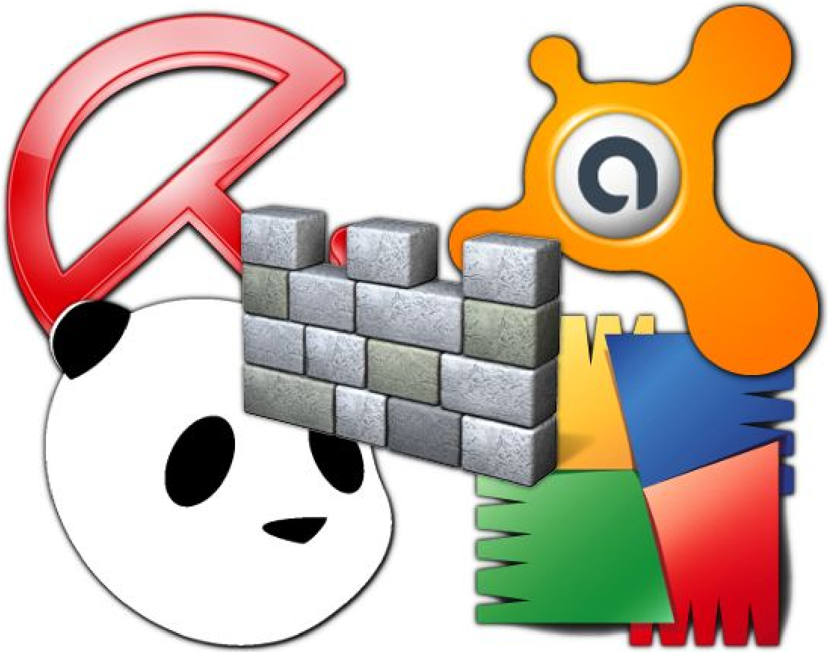
Last scan: 4/8/2017 at 2:50 AM (Quick scan)

Windows Defender

If we have to use antivirus, better to trust ~~the devil we already know~~ Microsoft

Any antivirus software bundled with Microsoft becomes the **baseline** for security defense

Malware MUST bypass Windows Defender to even spread



Security Takeaways

Fully-patched Windows 10 has many powerful security features that elevate it above most Linux distributions in exploit defence, **BUT**

- Few people run Windows 10
- Few people always apply the latest patches to their systems
- There are many avenues of attack (eg: ransomware) that don’t rely on exploitation
- Windows user share means many more people are trying to attack it

Homework

- Send a brief (1-paragraph) email on any thoughts you have on Windows vs. Linux security to cm7bv@virginia.edu with the subject “MST Assignment 10 - <YOUR_UVA_ID>”
- **Don’t hesitate to ask questions**

Additional Resources

- Windows Security Bulletins (“Patch Tuesdays”)
  https://technet.microsoft.com/en-us/security/bulletins.aspx
- Compilation of Windows exploitation resources
  https://github.com/enddo/awesome-windows-exploitation