Making Life Difficult for Malware

Jarno Niemelä

Senior Security Researcher, F-Secure jarno.niemela@f-secure.com

Assumptions

To avoid wasting time we are going to make some assumptions

- We focus on preventing Windows malware
- Yes switching to OSX or Linux makes things relatively safe
- For the time being that is
- But people have various reasons why that is not feasible

Methods presented here are focused on securing Windows 7

- Because Windows XP needs to die
- However if you are stuck with XP, most tricks work on XP

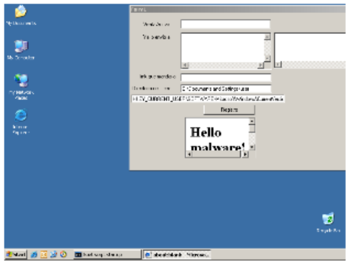
Scope

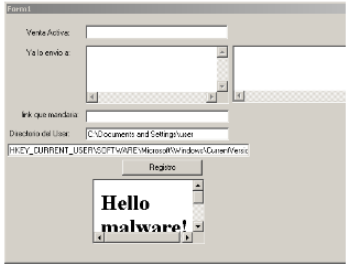
- There is no perfect safety
- And there is no way to cover all security measures
- Thus this presentation focuses on how to break as much malware as possible without breaking clean applications

Groundwork

For this research I gathered behavior data of ~750000 known malware

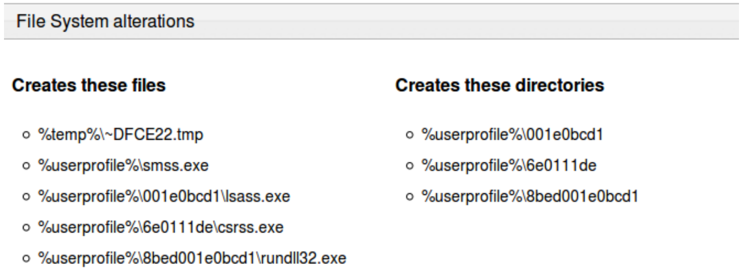
- We used dynamic analysis that tracks operations done in the system
- With this information we can mine for common operations malware does
- And come up with defense mechanisms that will kill most of infections





Directorio del User: C:\Documents and Settings\user

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersic



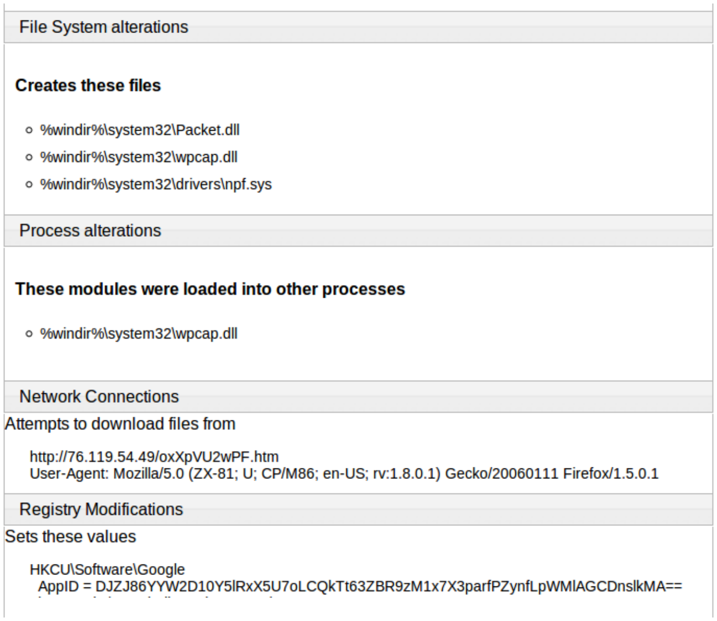
File System alterations

Creates these files

- %temp%\~DFCE22.tmp
- %userprofile%\smss.exe
- %userprofile%\001e0bcd1\lsass.exe
- %userprofile%\6e0111de\csrss.exe
- %userprofile%\8bed001e0bcd1\rundll32.exe

Creates these directories

- %userprofile%\001e0bcd1
- %userprofile%\6e0111de
- %userprofile%\8bed001e0bcd1



File System alterations

Creates these files

- %windir%\system32\Packet.dll
- %windir%\system32\wpcap.dll
- %windir%\system32\drivers\npf.sys

Process alterations

These modules were loaded into other processes

- %windir%\system32\wpcap.dll

Network Connections

Attempts to download files from

```
http://76.119.54.49/oxXpVU2wPF.htm
User-Agent: Mozilla/5.0 (ZX-81; U; CP/M86; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1
```

Registry Modifications

Sets these values

```
HKCU\Software\Google
  AppID = DJZJ86YYW2D10Y5lRxX5U7oLCQkTt63ZBR9zM1x7X3parfPZynfLpWMlAGCDnslkMA==
```

Story Of A Typical Malware Infection

Infections typically start by exploiting some client/reader software

- Web browser, PDF reader, flash player, Java runtime, video player..

The initial exploit is limited in scope what it can do

- Mostly what they do is to drop a payload for actual work and die

The payload is what does the actual work in infection

- Downloads or drops additional components
- Hides as well as the author knows how
- Sets itself to start when system boots
- Executes the monetizing payload

What Malware Needs To Live In the System

From technical point of view a typical malware needs

- User client to load the content that contains exploit code
- Vulnerability that it can exploit to get code running
- Write access to system in order to create files
- File execution capabilities to place where it wrote files
- Capability to start automatically on boot
- Ability to communicate with C&C or drop point

System Infection Is Very Fragile

Malware is very bad at dealing with surprises

- Anything of out of spec is not a target

Thus if there is even slight modification in system

- The infection will likely break as a pieces are missing

Thorough hardening will make system hostile for malware

- Lets make system incompatible for malware

Defence 1

Prevent Hostile Content From Reaching User

Prevent Clients From Accessing Hostile Content

The best way to protect users is to keep them away from malware ☺

Which means keeping them away from hostile web sites

Web filters won’t protect against totally new attack sites

- But, it’s very unlikely that your user would be the first one to be hit

However even totally new attacks can be blocked

- Prevent DNS resolving for kinds of sites that host attack sites
- Limit access to only the kinds of sites your people use and need
- Why would your user need to browse to a dynamic DNS hosted site?

Block Traffic To Sites Your Users Don't Go To

Block subdomain hosting TLDs

- co.cc, co.tv, ce.ms, rr.nu, cu.cc, cz.cc, vv.cc, cw.cm, cx.cc, etc

Block domains that provide dynamic DNS

- *dyndns*, *no-ip*, 8866.org, thescx.info, 3322.org, sock8.com

Block file sharing sites, some malware use them

- fileleave.com, dropbox.com, rapidshare.com, megafiles.com

For strict policy, allow DNS resolving only to Alexa top 1M[1]

- Tip: Instead of null routing domains set up landing page
- Either with a link that allows domain or IT ticket

Stay In Well Lit Guarded Areas

Comparison between common and malware domains

- 1 Million most common domains rated by Alexa[1]
- 369K malicious domains
- Cross section gives 1432 hits

So by limiting web to 1 million most popular domains

- You would avoid 99,61% of web attacks
- At least according to our test data

Filter Content With Known Exploits

There is no point in letting exploit content to reach it’s target

Thus use web content scanning to kill known exploits

- Flash, PDF, Java, Office documents

Defence 2

Prevent Software From Being Exploited

Harden Web Browsers And Other Client Software

Disable types of content that users don’t need

- Disable Java and ActiveX unless you need them for something
- Disable or remove any plugin that you don’t know for what it is

Block Flash, Javascript and videos from all unknown sites

- Install no-script, flashblock or similar blocking modules

Harden office applications

- Install office file validation [2]
- Block ActiveX and Flash components in office documents [3]

Harden Client Application Memory Handling

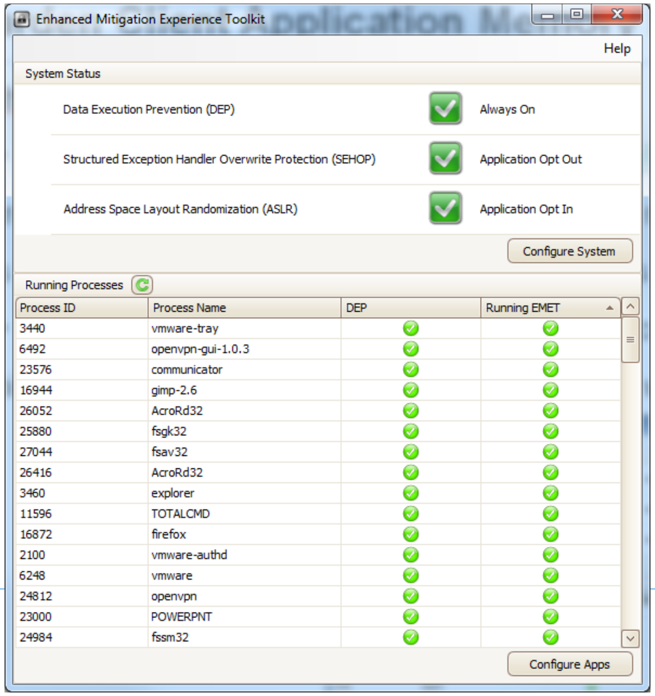
Enhanced Mitigation Experience Toolkit [4]

Harden any application that does use advanced memory protections

It is possible to write exploits so that they bypass EMET

- But then attacker has to knowingly try to circumvent EMET

Which means that anything but targeted attacks will almost certainly fail



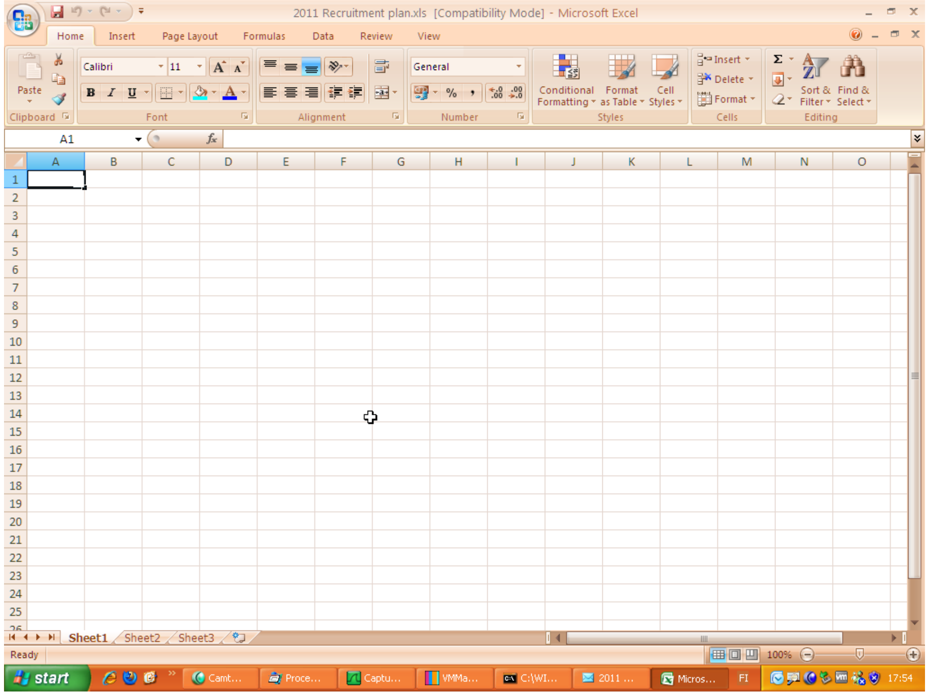
System Status

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

Process ID	Process Name	DEP	Running EMET
3440	vmware-tray	✓	✓
6492	openvpn-gui-1.0.3	✓	✓
23576	communicator	✓	✓
16944	gimp-2.6	✓	✓
26052	AcroRd32	✓	✓
25880	fsgk32	✓	✓
27044	fsav32	✓	✓
26416	AcroRd32	✓	✓
3460	explorer	✓	✓
11596	TOTALCMD	✓	✓
16872	firefox	✓	✓
2100	vmware-authd	✓	✓
6248	vmware	✓	✓
24812	openvpn	✓	✓
23000	POWERPNT	✓	✓
24984	fssm32	✓	✓

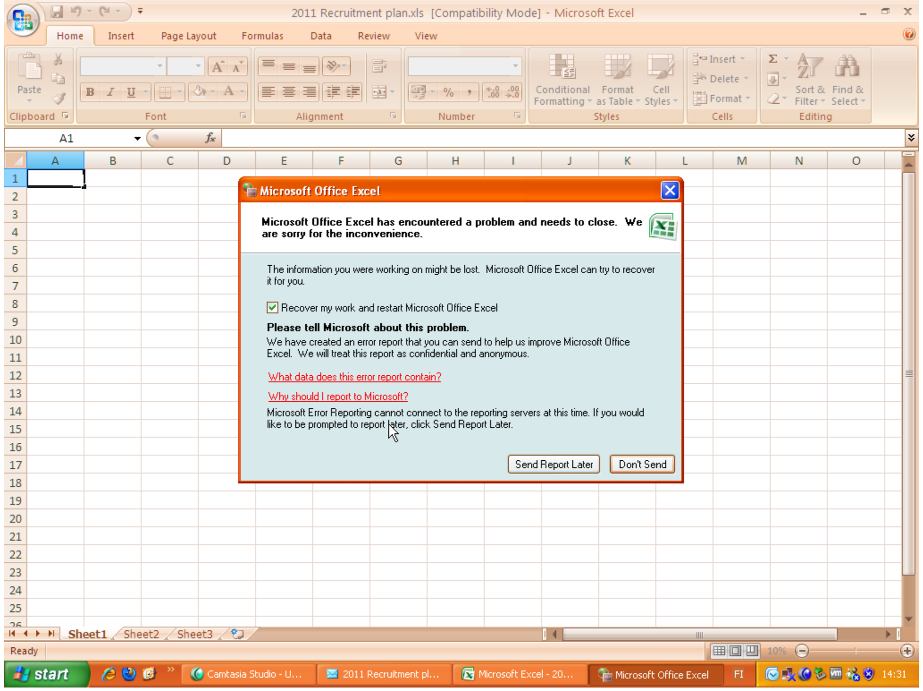
Trying Office Exploit Under Emet

- Without Emet


2011 Recruitment plan.xls [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Ready
start

Excel crashes and payload executes

With Emet


2011 Recruitment plan.xls [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Ready
start

Microsoft Office Excel

Microsoft Office Excel has encountered a problem and needs to close. We are sorry for the inconvenience.

The information you were working on might be lost. Microsoft Office Excel can try to recover it for you.

☑ Recover my work and restart Microsoft Office Excel

Please tell Microsoft about this problem.

We have created an error report that you can send to help us improve Microsoft Office Excel. We will treat this report as confidential and anonymous.

What data does this error report contain?

Why should I report to Microsoft?

Microsoft Error Reporting cannot connect to the reporting servers at this time. If you would like to be prompted to report later, click Send Report Later.

Send Report Later | Don't Send

Excel crashes with error message and payload is not executed

Defence 3

Prevent Exploit From Dropping Payload

Sandbox Applications That Deal With External Data

Clients that read external data should not write local files

Thus it makes sense to sandbox them with app sandbox

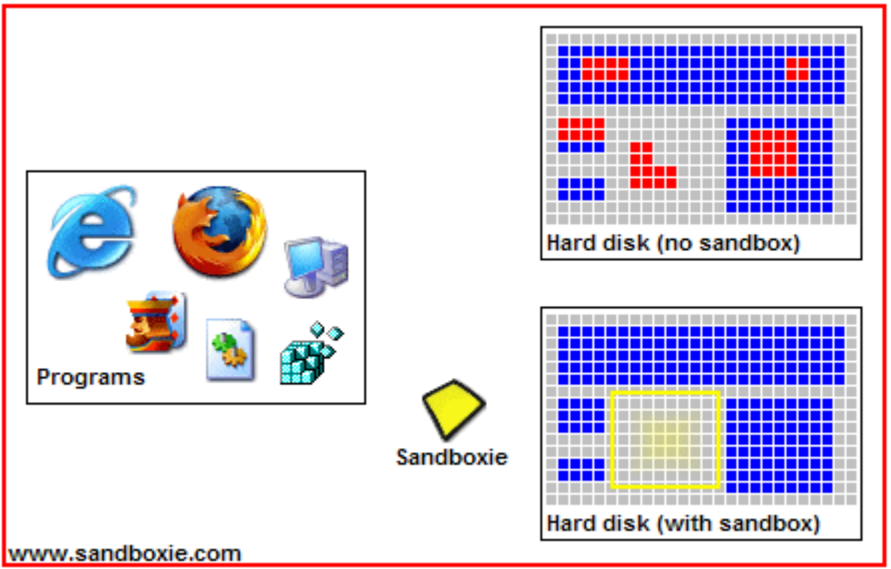
- Exploited application should not be able to break free

In reality sandboxes are not 100% reliable

- But it is unlikely that malware writer would bother

Third party sandboxes

- Sandboxie.com,Winjail.com



Prevent File Creation To Locations Preferred By Malware

Most malware authors use exploit only as a dropper

- Actual infection is done by traditional bot client or other malware

If exploit can be prevented from creating files the attack will fail

In Windows 7 effective hiding requires more permissions than user has

- Thus malware authors prefer drop locations where user can write

Blocking creation of files to locations preferred by malware authors

- Will kill a lot of exploit code

Locations Where File Creation Should Prevented

Change ACL to prevent users from writing and executing files to

- C:\users\USER (%userprofile%)
- C:\users\USER\AppData\Roaming (%appdata%)
- C:\users\USER\AppData\LocalLow
- C:\ProgramData\
- C:\Program Files\
- C:\, D:\, E:\, F:\, etc root of any drive
  this will stop autorun worms
- c:\Users\USER\AppData\Roaming\
  Microsoft\Windows\Start Menu\Startup\

Remember to allow directories, but these roots should not have files

Defence 4

Prevent Payload From Being Executed

Prevent Execution From Where There Are no Exes

Use Applocker[6] to prevent execution from

- %HOT%,%REMOVABLE% (USB and other removable)
- c:\Users\USER\Documents\
- c:\$Recycle.Bin\
- C:\recovery
- C:\system volume information\
- %APPDATA%, make exceptions for Google, Eclipse, etc

Alternative approach is to allow only program files and windows dir.

- Or even allow only signed files and make exceptions for others
- But this can be rather high maintenance as all programs are not signed and run exes from stupid locations (I am looking at you Google ☺

Defence 5

Prevent Communication To C&C

Prevent Malware From Communicating

Without communication malware infections are crippled

Limiting DNS resolving to well known domains works here

Application control firewall at clients also blocks helps

But above all harden your network also for outbound traffic

- No host in your network should have direct channel outside
- Or to anything else than servers it is supposed to access
- Be at least as strict controlling outbound as you are for inbound

Malware Hostile Networking

Workstations are supposed to be clients not servers

- Block all inbound traffic to workstations
- Allow outbound traffic only to servers and proxies
- Don’t allow servers to make outbound requests

Route all outgoing traffic over proxies

- Use content scanning and type inspection where possible

Block DNS resolving for little used domains

This will break Skype, when done right

- If users have valid use for IM clients
- Give them smartphones or tablets for that

Defence 7

Turn Malware Against Itself

Pretend To Be Malware Analyst

Malware tends to act nice when analysts or sysadmins are around

- A lot of malware check for signs of analysis environment
- If malware thinks it is being investigated it does not do anything

This makes analysts more difficult, but it can be turned against malware

- Add telltale signs of analysis environment to your system
- And a lot of malware will fail to run

However some rare malware cases are known to retaliate

- So make sure you have proper backups
- Although I prefer “Format C:” to malware hiding on my system

Faking Malware Analysis Environment

Copy registry keys from VMWare tools installation

”HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Disk\Enum” field ”0” Value ”VMWare”

”HKEY_LOCAL_MACHINE\SOFTWARE\VMWare, inc.\VMWare Tools ” field ”InstallPath” Value ”c:\prog…”

Create dummy processes

- Vbox.exe
- Vmware.exe
- wireshark.exe
- regshot.exe
- procmon.exe
- filemon.exe
- regmon.exe
- procdump.exe
- cports.exe
- procexp.exe
- squid.exe
- dumpcap.exe
- sbiectrl.exe

Create dummy files

- C:\Program Files\WinPcap\rpcapd.exe
- C:\Program Files\WireShark\rawshark.exe
- C:\Program Files\Ethereal\ethereal.html
- C:\Program Files\wireshark\wireshark.exe
- C:\Program Files\Microsoft Network Monitor 3\netmon.exe
- C:\program files\ollydbg\Ollydbg.exe
- C:\program files\sysinternals\Procmon.exe
- C:\program files\sysinternals\Procexp.exe
- C:\program files\sysinternals\Diskmon.exe
- C:\program files\sysinternals\Autoruns.exe
- C:\program files\debugging tools for windows \Windbg.exe

Conclusions

- Proper defense is based on layers
- The more defenses you have the
- The less likely it will be that malware survives
- Good luck in ruining attackers day

References

- [1] http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
- [2] http://support.microsoft.com/kb/2501584
- [3] http://blogs.technet.com/b/srd/archive/2011/03/16/blocking-exploit-attempts-of-the-recent-flash-0-day.aspx
- [4] http://www.microsoft.com/download/en/details.aspx?id=1677
- [5] http://www.victorc.org/2008/03/internet-explorer-7-protected-mode-vs.html
- [6] http://www.howtogeek.com/howto/6317/block-users-from-using-certain-applications-with-applocker/
- [7] http://technet.microsoft.com/en-us/library/cc749022%28WS.10%29.aspx
- [8] http://theinvisiblethings.blogspot.com/2009/01/why-do-i-miss-microsoft-bitlocker.html
- http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Thanks to

- Timo Hirvonen
- Christine Bejerasco
- Marko Thure
- Mikko Suominen
- Mikko Hyykoski
- Chin Yick Low

Protecting
the
irreplaceable

F-Secure.