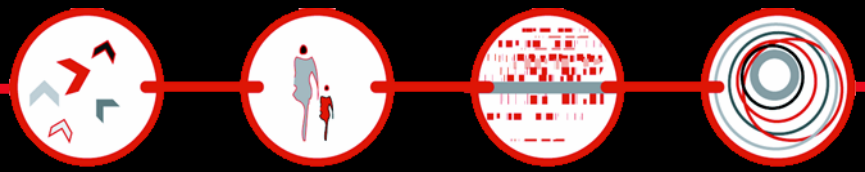
Sitic Honeynet

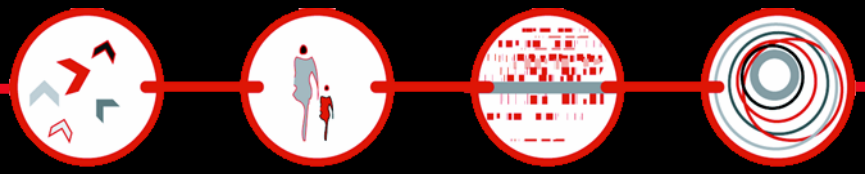
jonas.thambert@sitic.se

Sveriges IT-incidentcentrum
GovCERT-SE



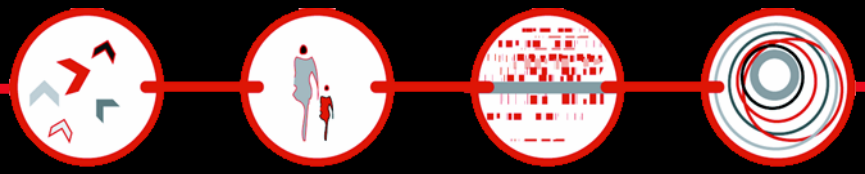
Innehåll

- Beskrivning av varför vi gör det här
- Genomgång av teknisk plattform och design
- Live-demo av testsystem
- Malware-analys



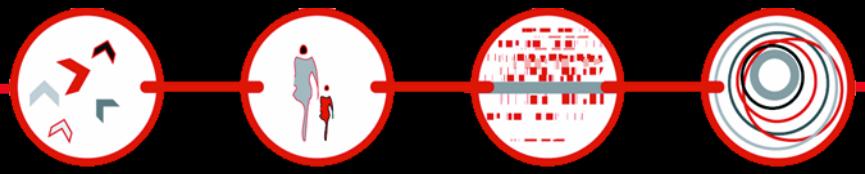
Varför gör vi det här?

- Se trender och beteendemönster
- Ta “tempen” på Internet i Sverige
- Fånga skadlig kod för vidare analys
  - Input till vår labb-verksamhet
- Samla statistik över attacker/binärer
- Öka vår och andras förståelse för attacker
- Sammanställa informationen på http://www.sitic.se



Mål och visioner

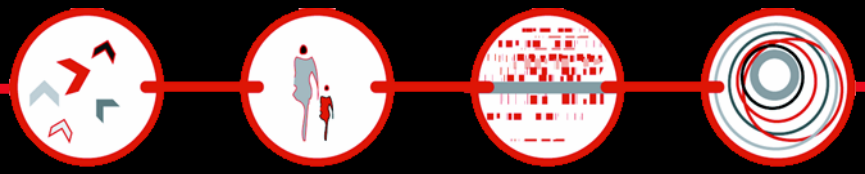
- Minimera “False positives”
- Skapa ett svenskt honeypot-nät med våra intressenter
- Totalt ca 25-50 sensorer
- Addera funktionalitet till lösningen
- Jämföra resultat med liknande projekt i andra länder
- Gruppera sensorerna branschvis. Hitta anomalier och riktade attacker.



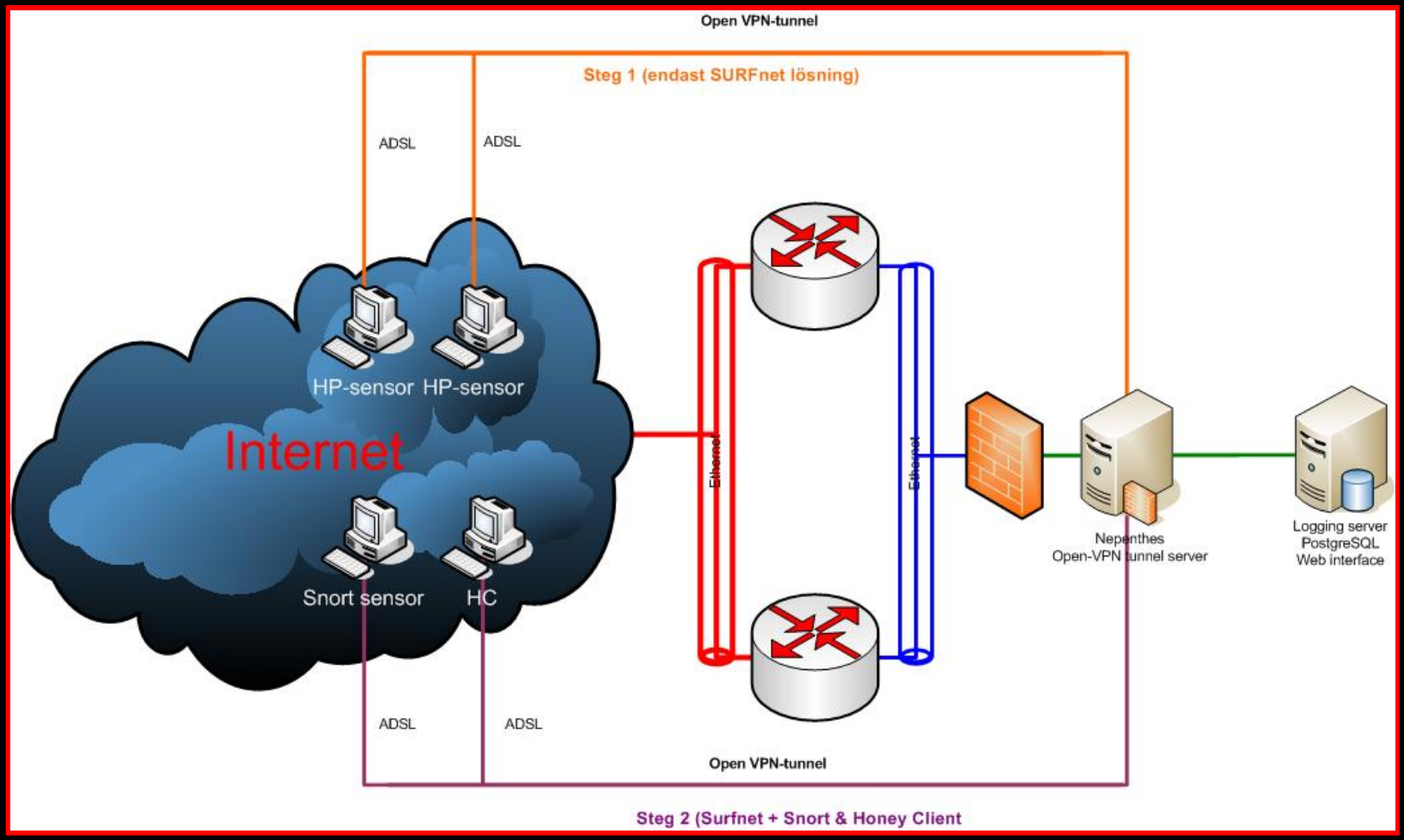
Teknisk lösning

"Open source"-produkt utvecklad av SURFnet och GovCERT-NL. Sitic som deltagare/beta-testare.

- http://ids.surfnet.nl
- Maskiner:
  - Sensorer
  - Honeypot / tunnelserver
  - Loggserver



Översiktsbild



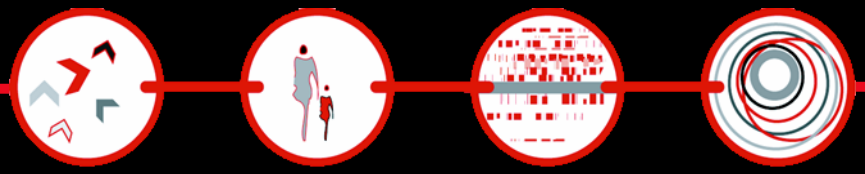
Sensor

- Ombyggd Knoppix-distribution
- “Bootar” från USB-sticka
- OpenVPN Client – SSL-tunnel till server - layer 2
  http://www.openvpn.net
- USB-stickan kan uppgraderas centralt från tunnelservern
- VLAN-stöd

Minimikrav:

PC som kan “boota” från USB

TCP port 1194 öppen mellan sensor och HP

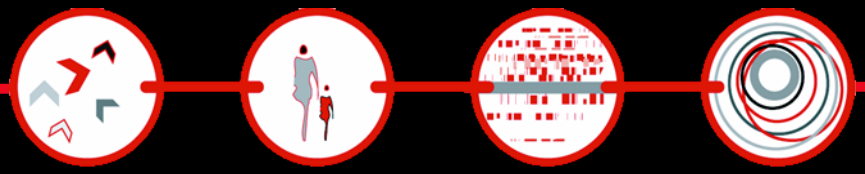


Sensor

- Billiga, saknar rörliga delar, låg energi-förbrukning, bootar från USB.

Honeypot/tunnel-server

- Debian Linux
- OpenVPN Server
- Bryggade nätverksinterface mot sensorerna över vpn
- Nepenthes Honeypot http//nepenthes.sourceforge.net
- POF – Passive Os Fingerprinting
  - http://lcamtuf.coredump.cx/p0f.shtml
- Source routing – IP route
- Antivirus för identifiering av nedladdade binärer
  - ClamAV
  - Antivir
  - Kaspersky m.fl

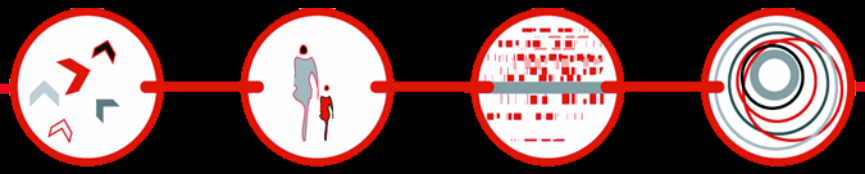


Honeypot/tunnel-server

- Nepenthes lyssnar på en rad portar och emulerar svar för de vanligaste protokollen.
- Tolkar exploit-payload vilket allt som oftast säger ladda hem binär och exekvera.
- Sparar payloads den inte kan tolka. 0day?

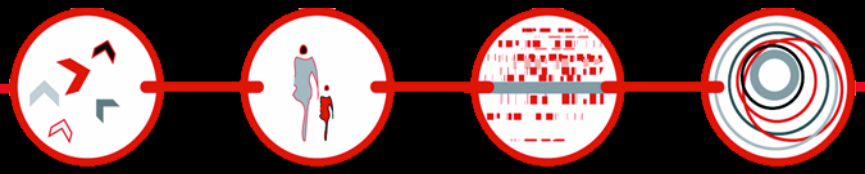
```
IPv4 1583462       UDP *:32811
IPv4 1583469       TCP 192.168.2.200:smtp (LISTEN)
IPv4 1583470       TCP 192.168.2.200:pop3 (LISTEN)
IPv4 1583471       TCP 192.168.2.200:imap (LISTEN)
IPv4 1583472       TCP 192.168.2.200:imap3 (LISTEN)
IPv4 1583473       TCP 192.168.2.200:smtps (LISTEN)
IPv4 1583474       TCP 192.168.2.200:imaps (LISTEN)
IPv4 1583475       TCP 192.168.2.200:pop3s (LISTEN)
IPv4 1583476       TCP 192.168.2.200:2745 (LISTEN)
IPv4 1583477       TCP 192.168.2.200:6129 (LISTEN)
IPv4 1583478       TCP 192.168.2.200:135 (LISTEN)
IPv4 1583479       TCP 192.168.2.200:microsoft-ds (LISTEN)
IPv4 1583480       TCP 192.168.2.200:1025 (LISTEN)
IPv4 1583481       TCP 192.168.2.200:ftp (LISTEN)
IPv4 1583482       TCP 192.168.2.200:https (LISTEN)
IPv4 1583483       TCP 192.168.2.200:17300 (LISTEN)
IPv4 1583484       TCP 192.168.2.200:zephyr-clt (LISTEN)
IPv4 1583485       TCP 192.168.2.200:eklogin (LISTEN)
IPv4 1583486       TCP 192.168.2.200:2107 (LISTEN)
IPv4 1583487       TCP 192.168.2.200:3372 (LISTEN)
IPv4 1583488       UDP 192.168.2.200:ms-sql-m
IPv4 1583489       TCP 192.168.2.200:3127 (LISTEN)
IPv4 1583490       TCP 192.168.2.200:netbios-ssn (LISTEN)
```

```
[ warn module ] Unknown SMBName exploit 4 bytes State 1
[ info down handler dia ] Found unused bind socket on port 62001
[ info mgr submit ] File 83edcf7decffd305504103510b56c4ef has type PE executable for MS
Windows (GUI) Intel 80386 32-bit
[ warn dia ] Unknown ASN1_SMB Shellcode (Buffer 0 bytes) (State 0)
[ dia  ] Ignoring zero-length hexdump.
[ warn module ] Unknown PNP Shellcode (Buffer 0 bytes) (State 0)
[ module ] Ignoring zero-length hexdump.
[ warn module ] Unknown LSASS Shellcode (Buffer 0 bytes) (State 0)
[ module ] Ignoring zero-length hexdump.
[ warn handler dia ] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[ handler dia ] Ignoring zero-length hexdump.
[ info handler dia ] Unknown DCOM request, dropping
[ info down mgr ] Handler ftp download handler will download ftp://[illegible]/
SDMSiTou.exe
[ info down handler ] url [illegible] resolved
[ info down handler ] url has ftp://[illegible]/SDMSiTou.exe ip, we will downlo
ad it now
[ info down handler dia ] Found unused bind socket on port 62001
[ info mgr submit ] File 83edcf7decffd305504103510b56c4ef has type PE executable for MS
```



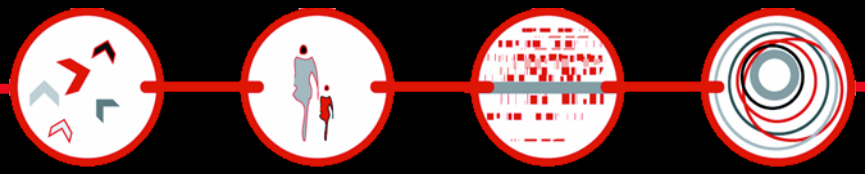
Logging-server

- Debian Linux
- PostgreSQL Databas
- Web interface / portal för statistik
- PHP
- Norman sandbox & CW Sandbox



Demo

- Demo av nya ver. 2.0rc1
- 3 test-sensorer på vanliga DSL anslutningar
- Sista oktetten i alla IP-adresser ändrad till 1.

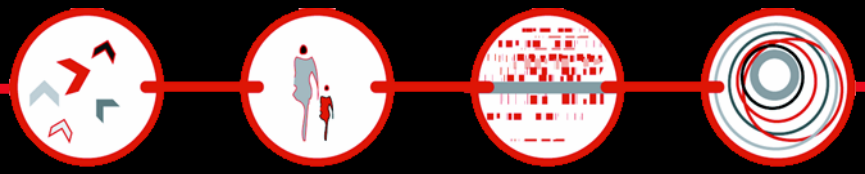


Demo

May the force be with me...

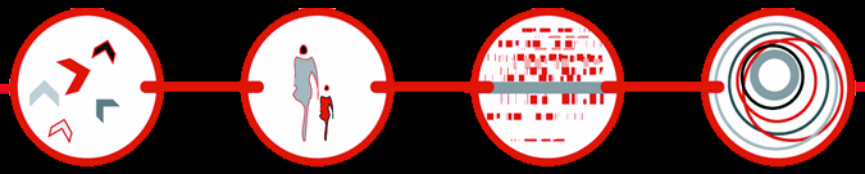
Under utveckling

- OpenBSD-sensorer
- Lokal språkanpassning i webbgränssnittet
- Honeytrap, Honeyclient etc.
- Bransch/sektors-indelning av sensorer



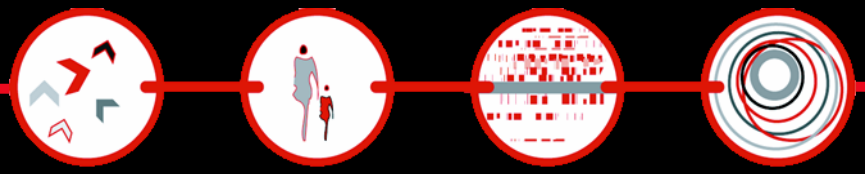
Analys av malware

- Surface Analys
- Runtime Analys
- Statisk Analys
- Sandboxing



Surface Analys

- Snabbt ta reda på enkel karaktäristik av binären
- Ge en bild av hur man ska gå vidare i sin analys
- Vanliga verktyg
  - Unix: file, strings, AV-motorer m.fl.
  - Win32: PEid, SIGbuster, PE Explorer m.fl.

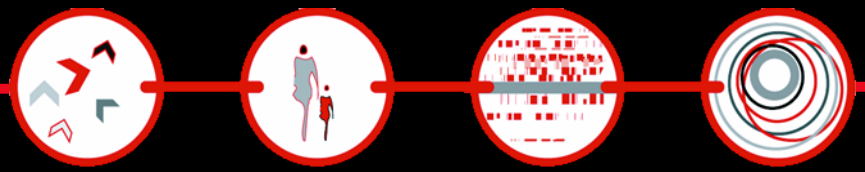


Surface Analys

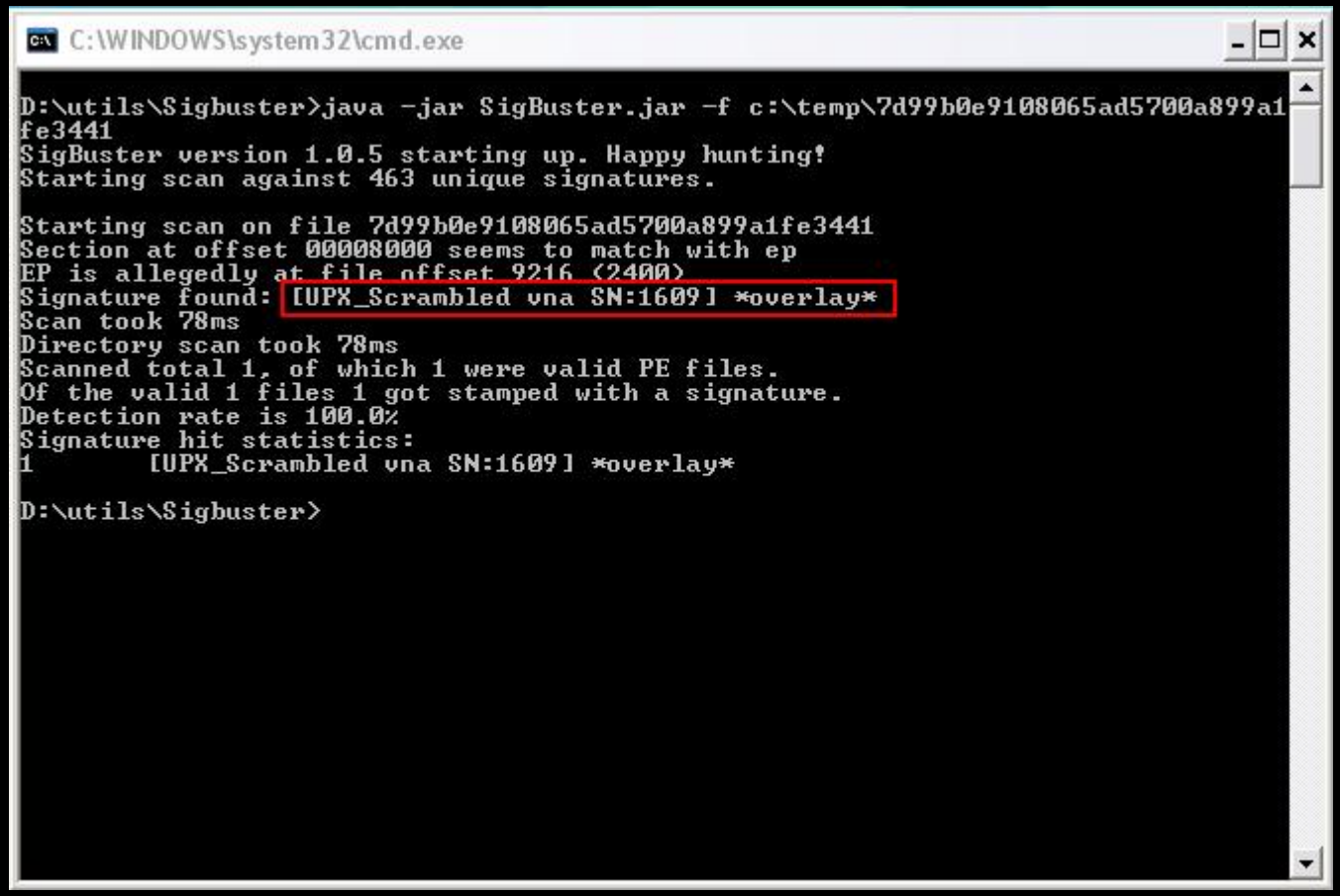
```
jonas@sysctl:/tmp$ file 7d99b0e9108065ad5700a899a1fe3441
7d99b0e9108065ad5700a899a1fe3441: MS-DOS executable PE  for MS Windows (GUI) Intel 80386 32-bit, UPX compressed
jonas@sysctl:/tmp$
jonas@sysctl:/tmp$ strings 7d99b0e9108065ad5700a899a1fe3441 | tail -13
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
USER32.dll
WININET.dll
WS2_32.dll
LoadLibraryA
GetProcAddress
ExitProcess
RegCloseKey
rand
wsprintfA
InternetOpenA
jonas@sysctl:/tmp$
```

OpenBSD

...oh yeah, 10\/\/njoo!
...and i dare you to try.
Requires: 1WH and 1AP
Hack Factor: 2
Point Value: 5
Kill Value: 22
(like www.Com4Dev.org: ues



Surface Analys

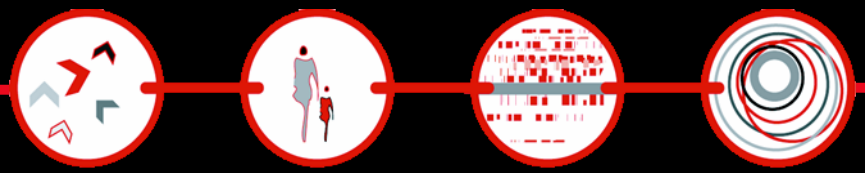


Surface Analys

```
AntiVir / Linux Version 2.1.11-32
Copyright (c) 2007 by Avira GmbH.
All rights reserved.

VDF version: 7.0.0.143 created 28 Oct 2007

For private, non-commercial use only.
AntiVir license: 149996 for Avira AntiVir PersonalEdition Classic

auto excluding /sys/ from scans (is a special fs)
auto excluding /proc from scans (is a special fs)
7d99b0e9108065ad5700a899a1fe3441
 Date: 22.10.2007  Time: 14:44:43  Size: 9353
ALERT: [WORM/Korgo.U] 7d99b0e9108065ad5700a899a1fe3441 <<< Contains detection pattern of the worm WORM/Korgo.U


------ scan results ------
   directories:       0
 scanned files:       1
        alerts:       1
    suspicious:       0
      repaired:       0
       deleted:       0
       renamed:       0
   quarantined:       0
     scan time: 00:00:01
--------------------------
Thank you for using AntiVir.
```

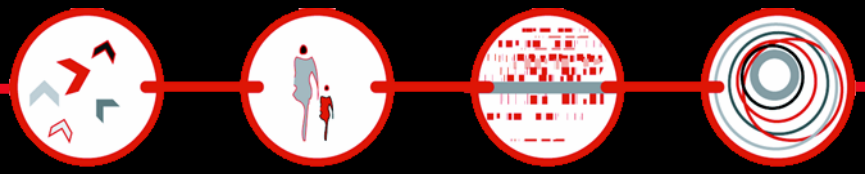
OpenBSD

...oh yeah, 10\/\/njoo!
...and i dare you to try.
Requires: 1WH and 1AP
Hack Factor: 2
Point Value: 5

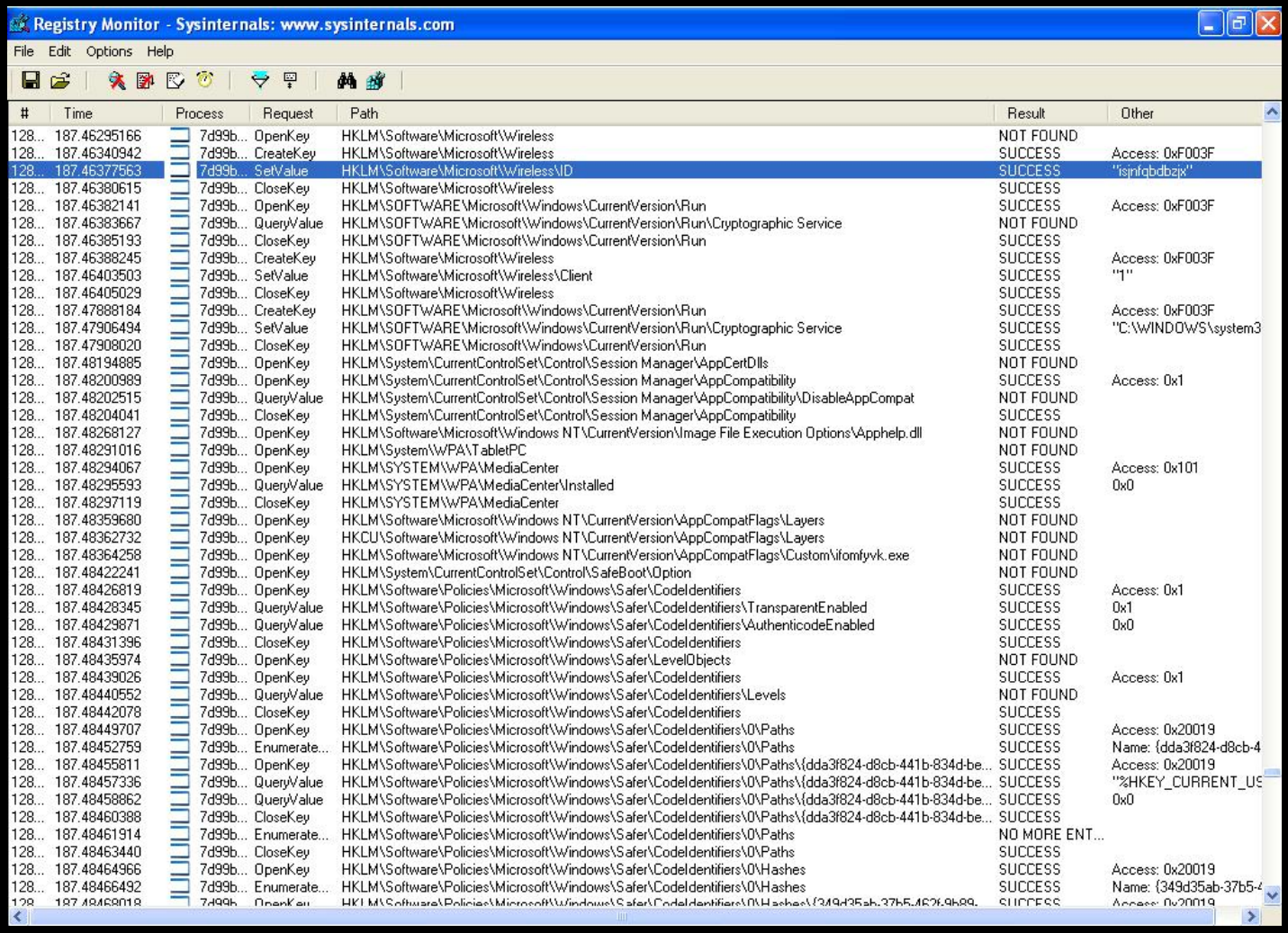


Runtime Analys

- Testköra binären i en isolerad miljö.
- Virtualisering gör det enkelt, men fungerar sällan.
  - Moderna packers/malware har skydd mot detta.
- Isolerad labbmiljö med routrar, dns, irc och webbservrar fungerar bäst.
- Svårt att ta reda på alla scenarion och funktioner som finns inbyggt i koden.
- Största fördel – Går snabbt och många kan utföra denna analys.

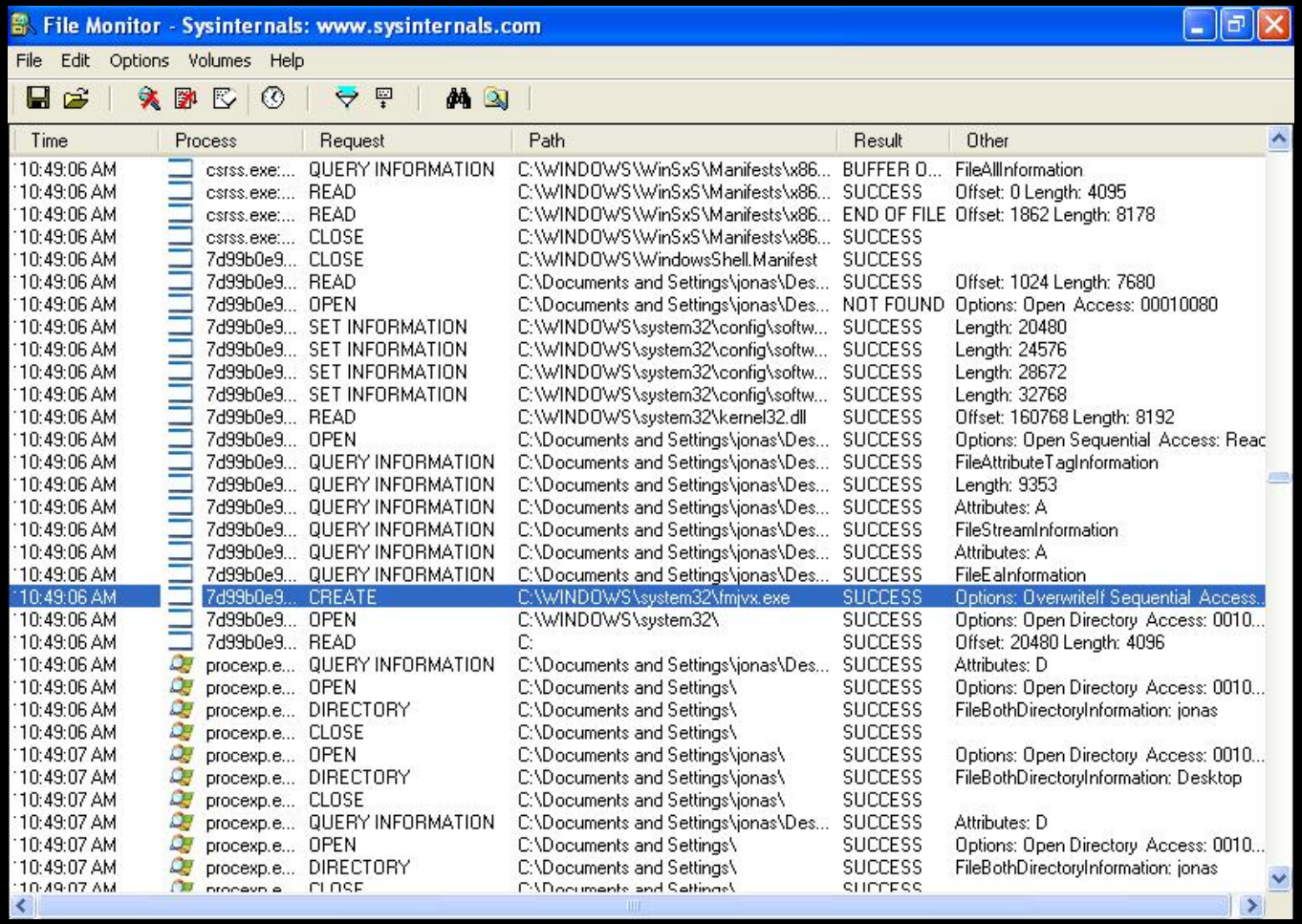


Runtime Analys

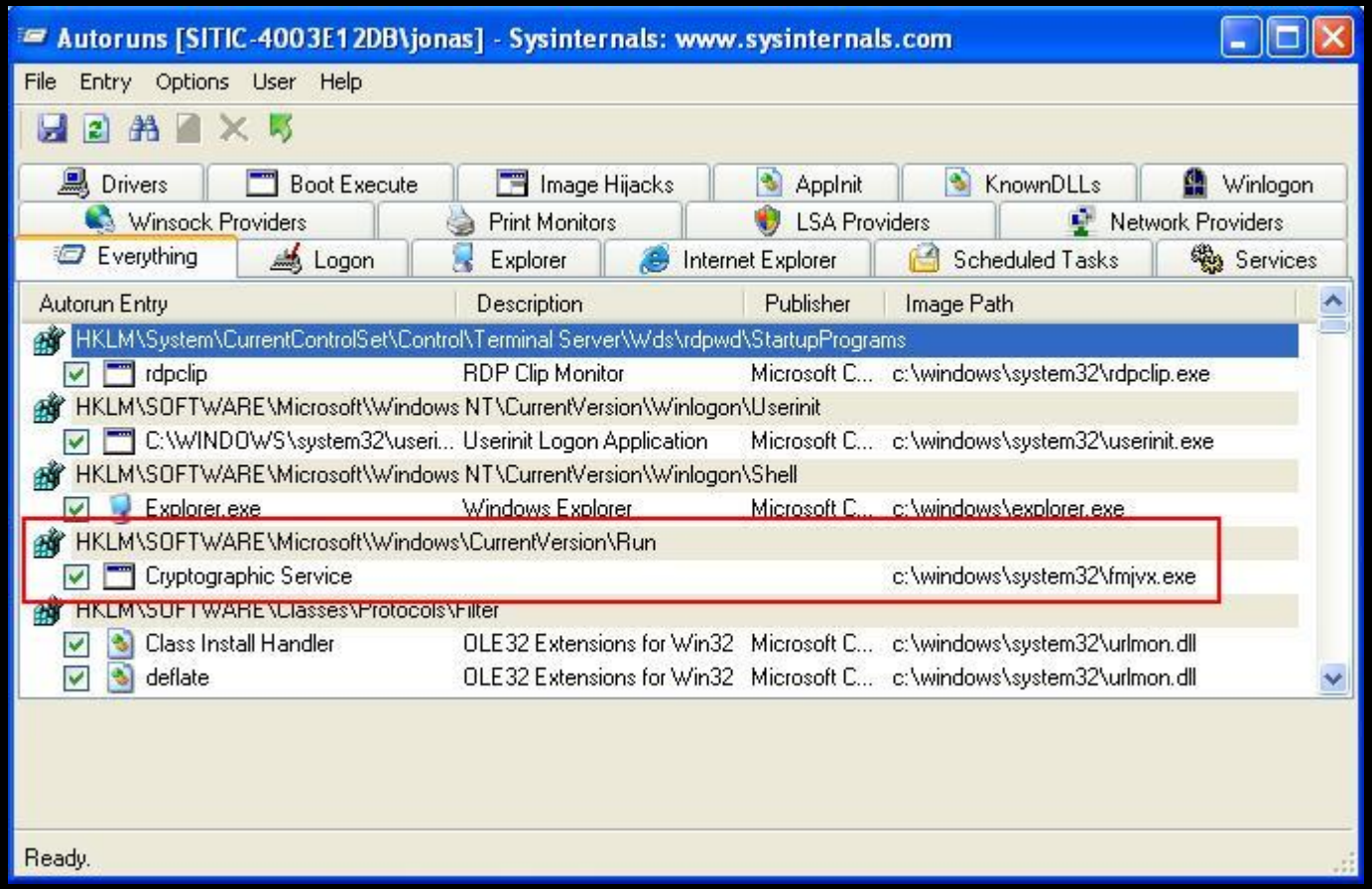


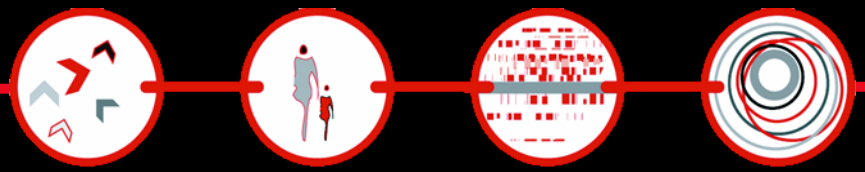
#	Time	Process	Request	Path	Result	Other
128...	187.46295166	7d99b...	OpenKey	HKLM\Software\Microsoft\Wireless	NOT FOUND	
128...	187.46340942	7d99b...	CreateKey	HKLM\Software\Microsoft\Wireless	SUCCESS	Access: 0xF003F
128...	187.46377563	7d99b...	SetValue	HKLM\Software\Microsoft\Wireless\ID	SUCCESS	"isjnfqbdbzjx"
128...	187.46380615	7d99b...	CloseKey	HKLM\Software\Microsoft\Wireless	SUCCESS	
128...	187.46382141	7d99b...	OpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Access: 0xF003F
128...	187.46383667	7d99b...	QueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Cryptographic Service	NOT FOUND	
128...	187.46385193	7d99b...	CloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	
128...	187.46388245	7d99b...	CreateKey	HKLM\Software\Microsoft\Wireless	SUCCESS	Access: 0xF003F
128...	187.46403503	7d99b...	SetValue	HKLM\Software\Microsoft\Wireless\Client	SUCCESS	"1"
128...	187.46405029	7d99b...	CloseKey	HKLM\Software\Microsoft\Wireless	SUCCESS	
128...	187.47888184	7d99b...	CreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Access: 0xF003F
128...	187.47906494	7d99b...	SetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Cryptographic Service	SUCCESS	"C:\WINDOWS\system3
128...	187.47908020	7d99b...	CloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	
128...	187.48194885	7d99b...	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	NOT FOUND	
128...	187.48200989	7d99b...	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS	Access: 0x1
128...	187.48202515	7d99b...	QueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\DisableAppCompat	NOT FOUND	
128...	187.48204041	7d99b...	CloseKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS	
128...	187.48268127	7d99b...	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Apphelp.dll	NOT FOUND	
128...	187.48291016	7d99b...	OpenKey	HKLM\System\WPA\TabletPC	NOT FOUND	
128...	187.48294067	7d99b...	OpenKey	HKLM\SYSTEM\WPA\MediaCenter	SUCCESS	Access: 0x101
128...	187.48295593	7d99b...	QueryValue	HKLM\SYSTEM\WPA\MediaCenter\Installed	SUCCESS	0x0
128...	187.48297119	7d99b...	CloseKey	HKLM\SYSTEM\WPA\MediaCenter	SUCCESS	
128...	187.48359680	7d99b...	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	NOT FOUND	
128...	187.48362732	7d99b...	OpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	NOT FOUND	
128...	187.48364258	7d99b...	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\ifomfyvk.exe	NOT FOUND	
128...	187.48422241	7d99b...	OpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NOT FOUND	
128...	187.48426819	7d99b...	OpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Access: 0x1
128...	187.48428345	7d99b...	QueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	SUCCESS	0x1
128...	187.48429871	7d99b...	QueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\AuthenticodeEnabled	SUCCESS	0x0
128...	187.48431396	7d99b...	CloseKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
128...	187.48435974	7d99b...	OpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\LevelObjects	NOT FOUND	
128...	187.48439026	7d99b...	OpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Access: 0x1
128...	187.48440552	7d99b...	QueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\Levels	NOT FOUND	
128...	187.48442078	7d99b...	CloseKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
128...	187.48449707	7d99b...	OpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths	SUCCESS	Access: 0x20019
128...	187.48452759	7d99b...	Enumerate...	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths	SUCCESS	Name: {dda3f824-d8cb-4
128...	187.48455811	7d99b...	OpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be...	SUCCESS	Access: 0x20019
128...	187.48457336	7d99b...	QueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be...	SUCCESS	"%HKEY_CURRENT_US
128...	187.48458862	7d99b...	QueryValue	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be...	SUCCESS	0x0
128...	187.48460388	7d99b...	CloseKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths\{dda3f824-d8cb-441b-834d-be...	SUCCESS	
128...	187.48461914	7d99b...	Enumerate...	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths	NO MORE ENT...	
128...	187.48463440	7d99b...	CloseKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths	SUCCESS	
128...	187.48464966	7d99b...	OpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes	SUCCESS	Access: 0x20019
128...	187.48466492	7d99b...	Enumerate...	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes	SUCCESS	Name: {349d35ab-37b5-4

Runtime Analys



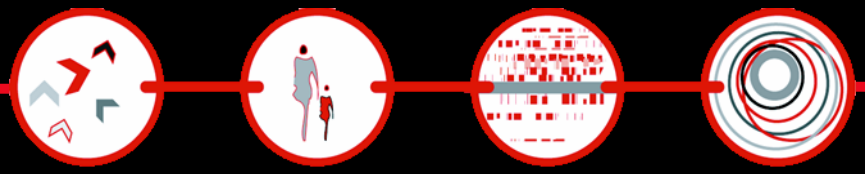
Runtime Analys





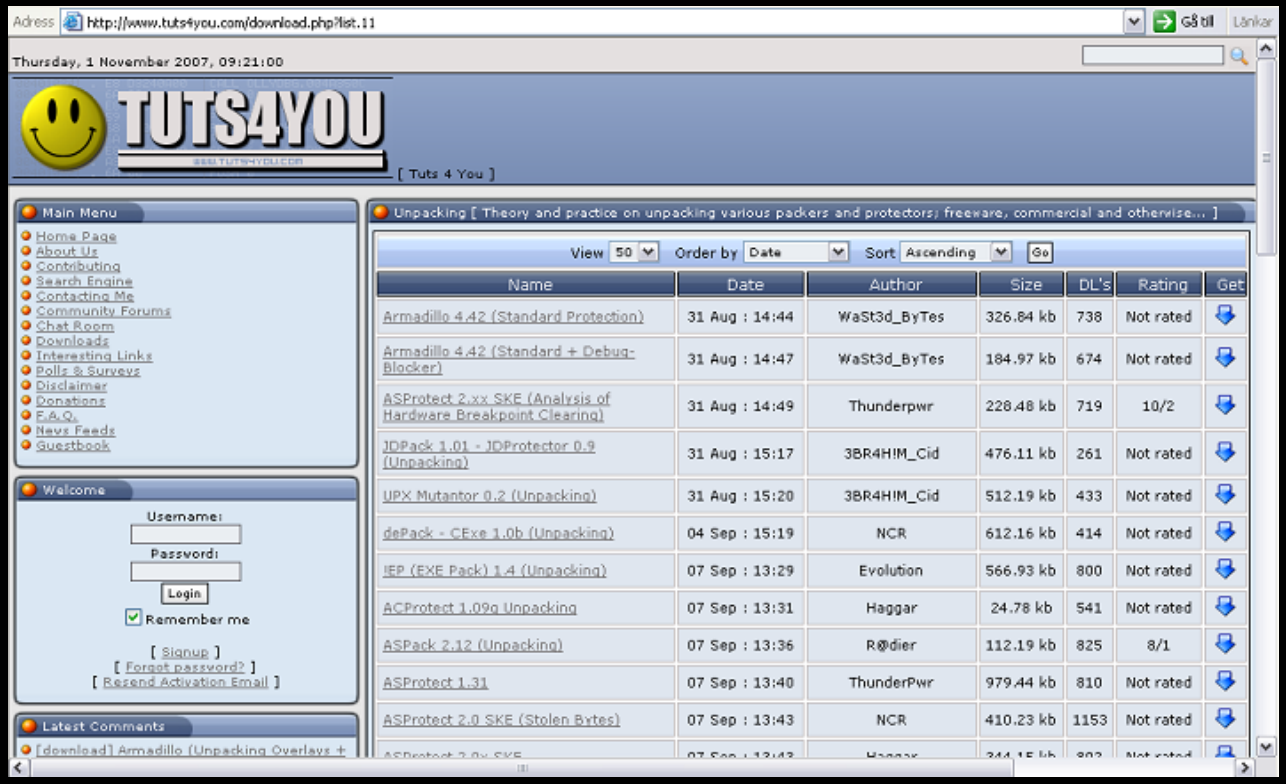
Statisk Analys

- Kräver hög kompetens inom Reverse Engineering.
  - Assembler, Win32 API, Packers & Cryptors
- Väldigt tidskrävande
- Enda sättet att verkligen ta reda på exakt vad koden gör.

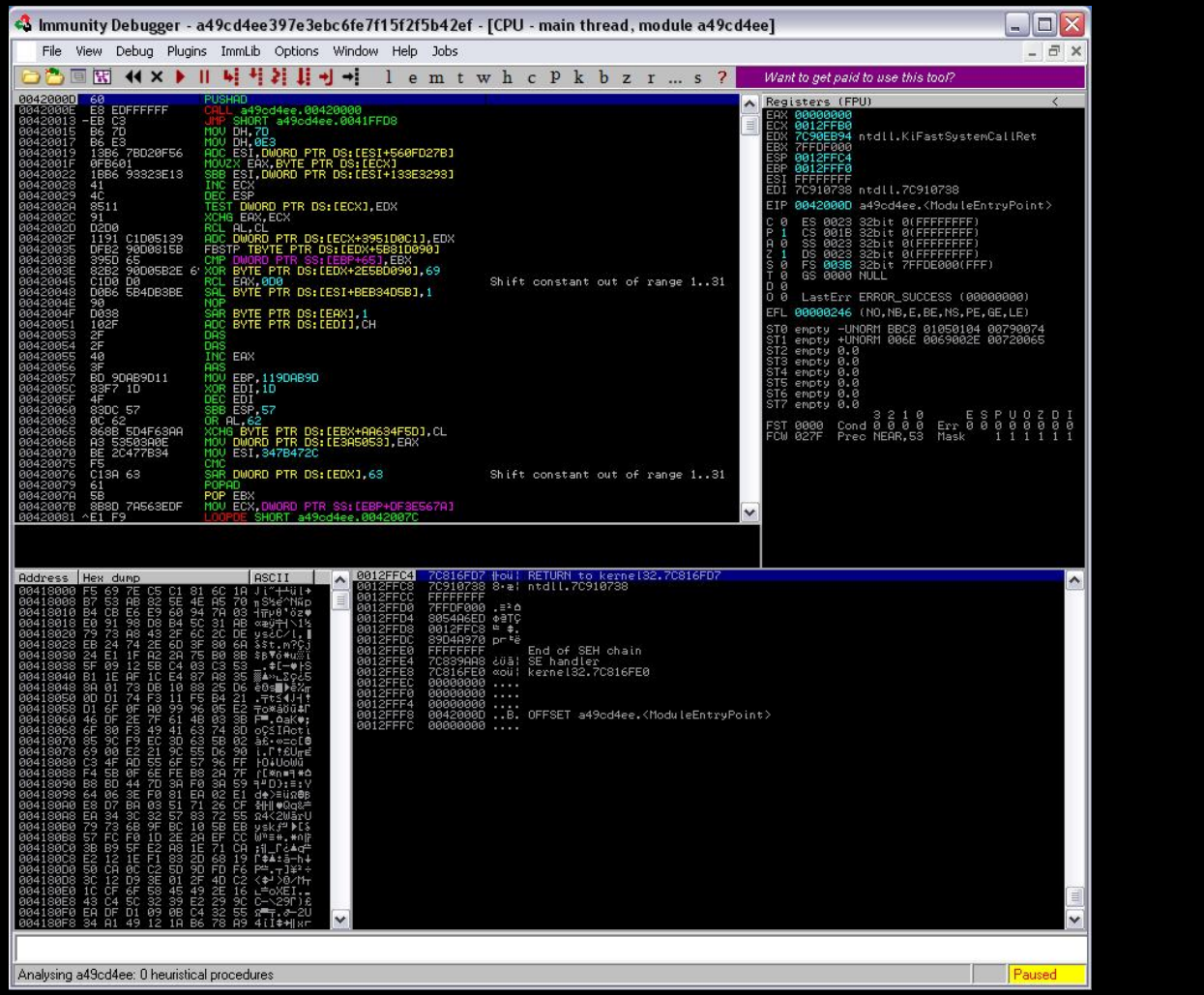


Statisk Analys

- Steg 1: Packa upp binären. Hitta OEP (Original Entry point), dumpa binär från minnet, återskapa importtable med ImpRec.

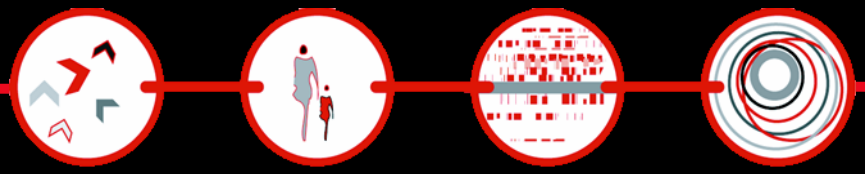


Statisk Analys



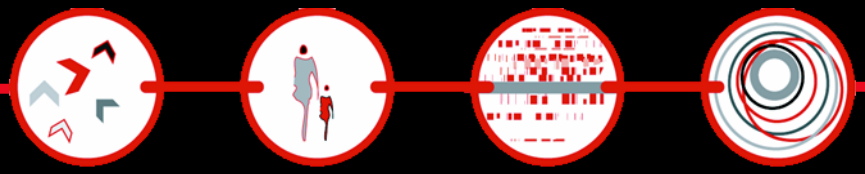
Sandbox Analys

- Ultra-snabb testkörning av koden.
- Klarar inte av att köra/analysera alla typer av binärer.
- Endast en del av binärens funktionalitet redovisas.
- Kostar mycket pengar men kan spara en hel del tid.



Norman Sandbox

```
[00000]  c:\temp\7d99b0e9108065ad5700a899a1fe3441 : W32/Malware
====> Sandbox output:

 [ DetectionInfo ]
    * Sandbox name: W32/Malware
    * Signature name: NOT_SCANNED
    * Compressed: YES

 [ General information ]
    * **IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.NO - REMEMBE
R TO ENCRYPT IT (E.G. ZIP WITH PASSWORD)**.
    * Drops files in %WINSYS% folder.
    * **Locates window "NULL [class Shell_TrayWnd]" on desktop.
    * File length:          9353 bytes.
    * MD5 hash: 7d99b0e9108065ad5700a899a1fe3441.

 [ Changes to filesystem ]
    * Deletes file ftpupd.exe.
    * Creates file C:\WINDOWS\SYSTEM32\kmuwy.exe.

 [ Changes to registry ]
    * Creates key "HKLM\Software\Microsoft\Wireless".
    * Sets value "ID"="zbjjlrqvllorvb" in key "HKLM\Software\Microsoft\Wireless"
.
    * Sets value "Client"="1" in key "HKLM\Software\Microsoft\Wireless".
    * Creates value "Cryptographic Service"="C:\WINDOWS\SYSTEM32\kmuwy.exe" in k
ey "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
    * Deletes value "Client" in key "HKLM\Software\Microsoft\Wireless".

 [ Process/window information ]
    * Creates a mutex uterm19.
    * Checks if privilege "SeDebugPrivilege" is available.
    * Will automatically restart after boot (I'll be back...).
    * Modifies other process memory.
    * Creates a remote thread.

 [ Signature Scanning ]
    * C:\WINDOWS\SYSTEM32\kmuwy.exe (9353 bytes) : W32/Korgo.AL.

Files checked : 1
Files infected: 1

D:\utils\norman>
```



Antivirus Information

Detailed Description

The worm's file is a PE executable 9353 bytes long packed with PE-Patch and UPX file compressor. The unpacked file's size is about 19.6 kilobytes in size.

When the worm's file is run, it first deletes the FTPUPD.EXE file. Then the worm creates a mutex with the "uterm19" name. This is done to avoid loading multiple copies of the worm into memory.

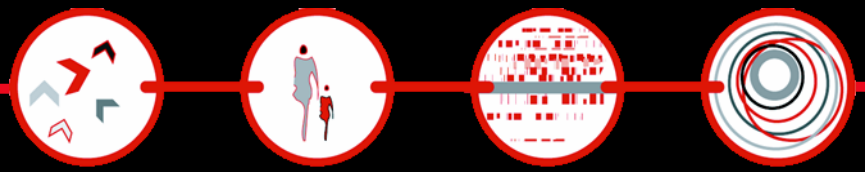
Next, the worm deletes Registry key values and terminates processes with any of the following names:

Windows Security Manager
Disk Defragmenter
System Restore Service
Bot Loader
SysTray
WinUpdate
Windows Update Service
avserve.exe
avserve2.exeUpdate Service
MS Config v13
Windows Update

The key values are deleted from the following Registry key:

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

After that the worm installs itself to system and creates a startup key for its file in the Registry.



Frågor

?