# Norman presentation

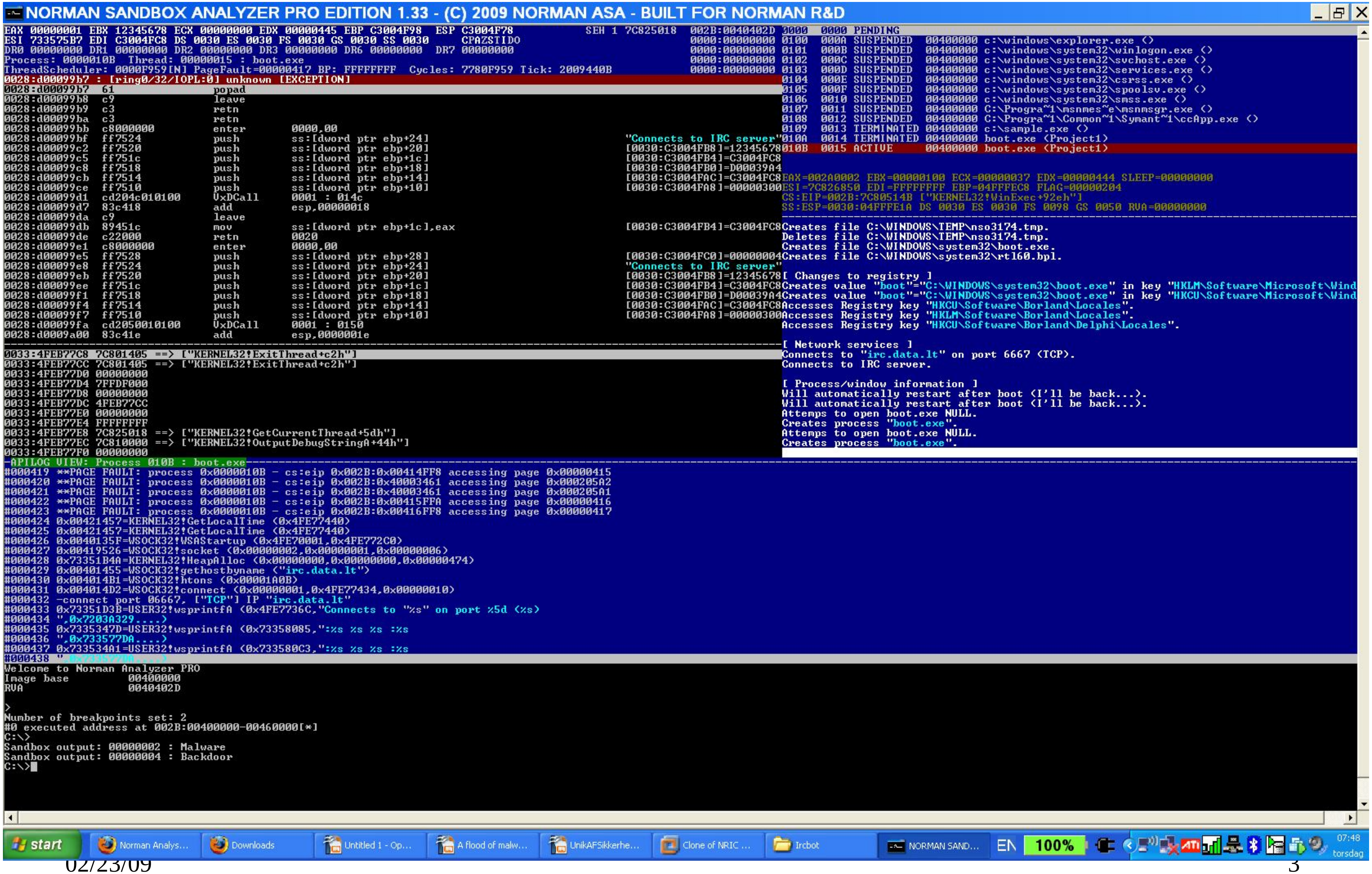
# From Storm to Waledac

By
Hans Christoffer Gaardløs Hansen
virus analyst, Norman ASA

# Storm – first peer-to-peer botnet

**Old method**

- IRC-server
- Specific chat-channels and run commandoes via these.
- Spread via exploits in webservers and networksprotokolls.



NORMAN SANDBOX ANALYZER PRO EDITION 1.33 - (C) 2009 NORMAN ASA - BUILT FOR NORMAN R&D

```
EAX 00000001 EBX 12345678 ECX 00000000 EDX 00000445 EBP C3004F98  ESP C3004F78             SEH 1 7C825018  002B:0040402D
ESI 733575B7 EDI C3004FC8 DS 0030 ES 0030 FS 0030 GS 0030 SS 0030      CPAZSTIDO                            0000:00000000
DR0 00000000 DR1 00000000 DR2 00000000 DR3 00000000 DR6 00000000  DR7 00000000                             0000:00000000
Process: 0000010B  Thread: 00000015 : boot.exe                                                               0000:00000000
ThreadScheduler: 0000F959[N] PageFault=00000417 BP: FFFFFFFF  Cycles: 7780F959 Tick: 2009440B               0000:00000000
0028:d00099b7 : [ring0/32/IOPL:0] unknown [EXCEPTION]
0028:d00099b7  61                  popad
0028:d00099b8  c9                  leave
0028:d00099b9  c3                  retn
0028:d00099ba  c3                  retn
0028:d00099bb  c8000000            enter      0000,00
0028:d00099bf  ff7524              push       ss:[dword ptr ebp+24]                  "Connects to IRC server"
0028:d00099c2  ff7520              push       ss:[dword ptr ebp+20]                  [0030:C3004FB8]=12345678
0028:d00099c5  ff751c              push       ss:[dword ptr ebp+1c]                  [0030:C3004FB4]=C3004FC8
0028:d00099c8  ff7518              push       ss:[dword ptr ebp+18]                  [0030:C3004FB0]=D00039A4
0028:d00099cb  ff7514              push       ss:[dword ptr ebp+14]                  [0030:C3004FAC]=C3004FC8
0028:d00099ce  ff7510              push       ss:[dword ptr ebp+10]                  [0030:C3004FA8]=00000300
0028:d00099d1  cd204c010100        VxDCall    0001 : 014c
0028:d00099d7  83c418              add        esp,00000018
0028:d00099da  c9                  leave
0028:d00099db  89451c              mov        ss:[dword ptr ebp+1c],eax             [0030:C3004FB4]=C3004FC8
0028:d00099de  c22000              retn       0020
0028:d00099e1  c8000000            enter      0000,00
0028:d00099e5  ff7528              push       ss:[dword ptr ebp+28]                  [0030:C3004FC0]=00000004
0028:d00099e8  ff7524              push       ss:[dword ptr ebp+24]                  "Connects to IRC server"
0028:d00099eb  ff7520              push       ss:[dword ptr ebp+20]                  [0030:C3004FB8]=12345678
0028:d00099ee  ff751c              push       ss:[dword ptr ebp+1c]                  [0030:C3004FB4]=C3004FC8
0028:d00099f1  ff7518              push       ss:[dword ptr ebp+18]                  [0030:C3004FB0]=D00039A4
0028:d00099f4  ff7514              push       ss:[dword ptr ebp+14]                  [0030:C3004FAC]=C3004FC8
0028:d00099f7  ff7510              push       ss:[dword ptr ebp+10]                  [0030:C3004FA8]=00000300
0028:d00099fa  cd2050010100        VxDCall    0001 : 0150
0028:d0009a00  83c41e              add        esp,0000001e
-------------------------------------------------------------------------------------------------------
0033:4FEB77C8  7C801405 ==> ["KERNEL32!ExitThread+c2h"]
0033:4FEB77CC  7C801405 ==> ["KERNEL32!ExitThread+c2h"]
0033:4FEB77D0  00000000
0033:4FEB77D4  7FFDF000
0033:4FEB77D8  00000000
0033:4FEB77DC  4FEB77CC
0033:4FEB77E0  00000000
0033:4FEB77E4  FFFFFFFF
0033:4FEB77E8  7C825018 ==> ["KERNEL32!GetCurrentThread+5dh"]
0033:4FEB77EC  7C810000 ==> ["KERNEL32!OutputDebugStringA+44h"]
0033:4FEB77F0  00000000
```

```
0000  0000 PENDING
0100  000A SUSPENDED  00400000 c:\windows\explorer.exe ()
0101  000B SUSPENDED  00400000 c:\windows\system32\winlogon.exe ()
0102  000C SUSPENDED  00400000 c:\windows\system32\svchost.exe ()
0103  000D SUSPENDED  00400000 c:\windows\system32\services.exe ()
0104  000E SUSPENDED  00400000 c:\windows\system32\csrss.exe ()
0105  000F SUSPENDED  00400000 c:\windows\system32\spoolsv.exe ()
0106  0010 SUSPENDED  00400000 c:\windows\system32\smss.exe ()
0107  0011 SUSPENDED  00400000 C:\Progra~1\msnmes~e\msnmsgr.exe ()
0108  0012 SUSPENDED  00400000 C:\Progra~1\Common~1\Symant~1\ccApp.exe ()
0109  0013 TERMINATED 00400000 c:\sample.exe ()
010A  0014 TERMINATED 00400000 boot.exe (Project1)
010B  0015 ACTIVE     00400000 boot.exe (Project1)


EAX=002A0002 EBX=00000100 ECX=00000037 EDX=00000444 SLEEP=00000000
ESI=7C826850 EDI=FFFFFFFF EBP=04FFFEC8 FLAG=00000204
CS:EIP=002B:7C80514B ["KERNEL32!WinExec+92eh"]
SS:ESP=0030:04FFFE1A DS 0030 ES 0030 FS 0098 GS 0050 RVA=00000000
-----------------------------------------------------------------------------------------
Creates file C:\WINDOWS\TEMP\nso3174.tmp.
Deletes file C:\WINDOWS\TEMP\nso3174.tmp.
Creates file C:\WINDOWS\system32\boot.exe.
Creates file C:\WINDOWS\system32\rtl60.bpl.

[ Changes to registry ]
Creates value "boot"="C:\WINDOWS\system32\boot.exe" in key "HKLM\Software\Microsoft\Wind
Creates value "boot"="C:\WINDOWS\system32\boot.exe" in key "HKCU\Software\Microsoft\Wind
Accesses Registry key "HKCU\Software\Borland\Locales".
Accesses Registry key "HKLM\Software\Borland\Locales".
Accesses Registry key "HKCU\Software\Borland\Delphi\Locales".

[ Network services ]
Connects to "irc.data.lt" on port 6667 (TCP).
Connects to IRC server.

[ Process/window information ]
Will automatically restart after boot (I'll be back...).
Will automatically restart after boot (I'll be back...).
Attemps to open boot.exe NULL.
Creates process "boot.exe".
Attemps to open boot.exe NULL.
Creates process "boot.exe".
```

```
-APILOG VIEW: Process 010B : boot.exe----------------------------------------------------------------------------------
#000419 **PAGE FAULT: process 0x0000010B - cs:eip 0x002B:0x00414FF8 accessing page 0x00000415
#000420 **PAGE FAULT: process 0x0000010B - cs:eip 0x002B:0x40003461 accessing page 0x000205A2
#000421 **PAGE FAULT: process 0x0000010B - cs:eip 0x002B:0x40003461 accessing page 0x000205A1
#000422 **PAGE FAULT: process 0x0000010B - cs:eip 0x002B:0x00415FFA accessing page 0x00000416
#000423 **PAGE FAULT: process 0x0000010B - cs:eip 0x002B:0x00416FF8 accessing page 0x00000417
#000424 0x00421457=KERNEL32!GetLocalTime (0x4FE77440)
#000425 0x00421457=KERNEL32!GetLocalTime (0x4FE77440)
#000426 0x0040135F=WSOCK32!WSAStartup (0x4FE70001,0x4FE772C0)
#000427 0x00419526=WSOCK32!socket (0x00000002,0x00000001,0x00000006)
#000428 0x73351B4A=KERNEL32!HeapAlloc (0x00000000,0x00000000,0x00000474)
#000429 0x00401455=WSOCK32!gethostbyname ("irc.data.lt")
#000430 0x004014B1=WSOCK32!htons (0x00001A0B)
#000431 0x004014D2=WSOCK32!connect (0x00000001,0x4FE77434,0x00000010)
#000432 -connect port 06667, ["TCP"] IP "irc.data.lt"
#000433 0x73351D3B=USER32!wsprintfA (0x4FE7736C,"Connects to "%s" on port %5d (%s)
#000434 ",0x7203A329....)
#000435 0x7335347D=USER32!wsprintfA (0x73358085,":%s %s %s :%s
#000436 ",0x733577DA....)
#000437 0x733534A1=USER32!wsprintfA (0x733580C3,":%s %s %s :%s
#000438 ",0x733577DA....)
Welcome to Norman Analyzer PRO
Image base          00400000
RVA                 0040402D

>
Number of breakpoints set: 2
#0 executed address at 002B:00400000-00460000[*]
C:\>
Sandbox output: 00000002 : Malware
Sandbox output: 00000004 : Backdoor
C:\>
```

# Peer-to-Peer - continued

- No central command-server
- Harder to track
- Client and server in one
- Information between nodes/bots not sent directly but published by a bot based on a derivate common to the bots
- Filtered/subscribed to by the other bots again based on that common derivate
- Common identificator = same information received

# Peer-to-peer - cont.

- The peer-to-peer system matches published information objects to subscribers and delievers the requested information to the customer

  *The weakness or rather what proved to be the Akkillevs heel for Storm was the unauthenticated communication sent between the bots.*

- *Authentication was implicit, meaning the information a subscriber received was assumed to be correct*

# Expantion

- New bots created needed built-in information on how to connect to and receive info from the other nodes
- IP-addresses for excisting nodes, service ports and application specific connectivity info.

# Vectors for spreading

- ecard.exe
- First phase: binary sent by email
- Second phase: link sent by email, link to site containing packs of exploits, i.ex. Mpack
- If vulnerable browser version -> run specific exploits -> binary dropped on computer
- Binary dropped changed MD5 every minute on server
- Rootkits for all binaries

# Communication protocols

- First version of Storm: OVERNET

  P2P distributed hash table routing protocol used by Edonkey

- Second version of Storm: Stormnet

  OVERNET + 40 byte XOR encryption on all messages

  *But still used unauthenticated communication*

# Storm

- Sensational and tragic news:

  *“230 people killed by the storm Kyrill in Europe in January 2007”*

- Creative and good timing:

  “Valentine”-cards sent right before Valentine's Day

  “Christmas”-cards sent right before Christmas

  etc.

# Storm dies out...

MSRT

Microsoft's Malicious Software Removal Tool

→ Wiped out Storm

- July 2007: 20% of all spam sent around the world came from the Storm-botnet
- September 2008: No more spam

Reasons: Partly MSRT partly other plans

# But

- Storm not only used for spamming you and me
- Estonia under virtual siege in April 2007
- Background: removal of russian 2nd World War monument in Tallinn
- First DdoS (Distributed denial of Service) on estonian news sites and spamming to fill their storage servers
- Storm-botnet used to carpet-bomb estonian infrastructural sites with several different network-traffic inhibiting data

# No bandwidth for you

- The force of the attack was doubled at least 200 percent on the third day peaking with four million bytepacks per second with the result of hogging the entire estonian bandwidth.

# Waledac

- Storm new and improved:

  How many americans were at the presidential acceptance to see Obama?

  How many americans wanted to buy something with Obama's face on it?

  How many americans wanted to hear his speech one more time?

# Obama netshop

_store.greatobamaguide .com_

_store.superobamadirect .com_

_www.greatobamaguide .com_

_www.greatobamaonline .com_

_www.superobamaonline .com_

Free to the american public:

*speech.exe, obama.exe*

# A few tech details

Speech.exe ~ W32/Waledac.A

Obama.exe ~ W32/Waledac.A

- New tricks adopted:

Built-in algorithm to generate not yet bought and not yet excisting domains

*Why?*

# Takedown and costs

- Malicious links → send it to a friend who talks to other friends in the hosting country → takes time and cost money
- Many different possible sites to take down → takes more time and cost money for researching companies to buy the possible domains before the bad guys do it
- Only one domain needed to issue commands to entire botnet

# Waledac evolves

- Authenticated communication
- Steals information, encrypts it and sends it here

# 116.122.25.144

# 116.16.203.123

# 116.254.87.118

# 116.73.41.45

# 116.74.181.12

randomly of course

# More functionality

- End processes

  (AV- and monitoring- related ones)
- Update the worm
- Download files
- Send spam

# Why change a winning receipe?

Which day is the upcoming Saturday, 14th of February?

# Valentine's Day

This week:

***This is you Valentine card ~ Valentine.exe***

***Valentine lovely love ~ ValentineLove.exe***

***Even more love***

etc

ILOVEYOU = W32/Loveletter, May 4th 2000

# Fool me once...

Waledac will have some success for three reasons:

1. People are suckers for love and greeting-cards

2. They will update the domain-calculation algorithm on a regular basis

3. They use fast-flux

# Fast flux

- Fast flux service networks are networks of compromised computer systems with public DNS (Domain Name Servers) records, shifting constantly as rapidly as every 30 seconds
- This rapidly changing architecture makes it harder to track criminal activity and take down domains
- Like tracing a butterfly with chameleon abilities and the power to teleport

# Questions?

**Sources:**

http://en.wikipedia.org/wiki/Storm_botnet

http://www.icann.org/en/committees/security/sac025.pdf

http://www.honeynet.org/papers/ff/

http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1

http://www.honeyblog.org/junkyard/paper/storm-leet08.pdf

http://www.hardware.no/artikler/storm-botnettet_forsvinner/57032

http://blog.threatfire.com/2009/01/ongoing-waledac-botnet-and-spam.html

**http://www.honeynet.org/papers/ff/**

**Keywords:**

Storm

Waledac

Conficker/Downadup

Fast-flux

Exploits